IMPLEMENTING ADDITIONAL SECURITY MEASURE ON ATM THROUGH BIOMETRIC

HAYDER HUSSEIN AZEEZ

UNIVERSITI UTARA MALAYSIA
FEBRUARY 2011

IMPLEMENTING ADDITIONAL SECURITY MEASURE ON ATM THROUGH BIOMETRIC

A project submitted Dean Awang Had Salleh Graduate School Office in partial

Fulfillment of the requirement for the degree

Master of Science (Information Technology)

Universiti Utara Malaysia

By

HAYDER HUSSEIN AZEEZ

PERMISSION TO USE

In presenting this project in partial fulfillment of the requirements for a postgraduate degree from Universiti Utara Malaysia, I agree that the University Library may make it freely available for inspection. I further agree that permission for copying of this project in any manner, in whole or in part, for scholarly purpose may be granted by my supervisor(s) or, in their absence by the Dean wang Had Salleh Graduate School. It is understood that any copying or publication or use of this project or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from my project.

Requests for permission to copy or to make other use of materials in this project, in whole or in part, should be addressed to

Dean Awang Had Salleh Graduate School
Collage Of Art and Sciences
Universiti Utara Malaysia
06010 UUM Sintok
Kedah Darul Aman
Malaysia

KOLEJ SASTERA DAN SAINS
(College of Arts and Sciences)
Universiti Utara Malaysia

PERAKUAN KERJA KERTAS PROJEK
(Certificate of Project Paper)

Saya, yang bertandatangan, memperakukan bahawa
(I, the undersigned, certifies that)

HYDER HUSSEIN AZEEZ
(802829)

calon untuk Ijazah
(candidate for the degree of) **MSc. (Information Technology)**

telah mengemukakan kertas projek yang bertajuk
(has presented his/her project of the following title)

IMPLEMENTING ADDITIONAL SECURITY MEASURE
ON ATM THROUGH BIOMETRIC

seperti yang tercatat di muka surat tajuk dan kulit kertas projek
(as it appears on the title page and front cover of project)

bahawa kertas projek tersebut boleh diterima dari segi bentuk serta kandungan dan meliputi bidang ilmu dengan memuaskan.
(that this project is in acceptable form and content, and that a satisfactory knowledge of the field is covered by the project).

Nama Penyelia
(Name of Supervisor) : **DR. ABDUL JALEEL K.SHITTU**

DR. ABDUL JALEEL K. SHITTU
Senior Lecturer
Information Technology
UUM College of Arts and Sciences
Universiti Utara Malaysia

Tandatangan
(Signature) : ______ Tarikh (Date) : 03/03/2011

Nama Penilai
(Name of Evaluator) : **DR.AZMAN YASIN**

Tandatangan
(Signature) : ______ Tarikh (Date) : 7/3/2011

ABSTRACT

With the development of computer network technology and e-commerce, the self-service banking system has got extensive generalization with the characteristic offering high-quality 24 hours service for customer. Nowadays, using the ATM (Automatic Teller Machine) which provides customers with the convenient banknote trading is very common. However, the financial crime case rises repeatedly in recent years. A lot of criminals tamper with the ATM and steal user's credit card and password by illegal means. Once user's bank card is lost and the password is stolen, the criminal will draw all cash in the shortest time, which will bring enormous financial losses to customer. How to carry on the valid identity to the customer becomes the focus in current financial circle.

Traditional ATM systems authenticate generally by using the credit card and the password, the method has some defects. Using credit card and password cannot verify the client's identity exactly. In recent years, Biometric systems, fingerprint technology in particular, can give the possibility to develop a system of protection in ATM machines.

ACKNOWLEDGMENT

Praise belongs to God

The first, without a first before him, the last, without a last him

Beholder's eyes fall short seeing him.

Describer's imaginations are unable to depict him.

I would like to thank my supervisor DR.ABDUL JALEEL K.SHITTU, for giving me his support, motivation, time and guidance throughout this dissertation.

Special thanks to my evaluator Dr. AZMAN YASIN for spending time reviewing this work and giving valuable suggestions and comments on my work.

Last but not least, thinks a lot to my family to their giving unlimited, taking care and supporting me to whole of my study.

Hayder Hussein Azeez

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION

CHAPTER 2: LITERATURE REVIEW

LIST OF TABLE

LIST OF FIGURE

CHAPTER 1

INTRODUCTION

1.1 BACKGROUND

A reliable identity validation management system is urgently needed to combat the endemic growth in identity thefts and to meet the increased security requirements, in a variety of applications, ranging from international border crossings to securing information through databases. Establishing the identity of a person is critical in any identity management system. Surrogate representations of identity such as passwords and ID cards are not sufficient for reliable identity determinations because they can be easily misplaced, shared, or stolen.

Automated teller machines (ATMs) are embedded systems for financial-related services. An automated teller machine (ATM), also known as an automated banking machine (ABM) is a computerized telecommunications device that provides the clients of a financial institution with access to financial transactions in public spaces without the need for cashiers, human clerks or bank tellers.

ATM services are highly profitable for banks and banks aggressively market the use of ATM cards. ATMs that are off bank premises are usually very profitable because they attract high volumes of non-bank customers, who must pay service fees. Unfortunately, customers using off-premise ATMs are very vulnerable to robberies (Guerette & Clarke, 2003).

With the development of computer network technology and e-commerce, the self-service banking system is highly popular with the characteristic offerings of high-quality 24 hour services, for customers. Nowadays, using the ATMs (Automatic Teller Machines) which provide customers with the convenient banknote trading is very common. However, financial crime cases have risen repeatedly in recent years; a lot of criminals tampering with the ATM terminals and stealing credit cards and passwords by illegal means. Once a user's bank card is lost and the password is stolen, the criminal can draw out the user's cash in a very short time and this can bring enormous financial loss to the user. Traditional ATM systems authenticate users generally through the credit cards and the passwords used. However, this method has some defects. Using the credit card and the password cannot verify the client's identity, exactly (Yang & Mi, 2010).

Biometric recognition is the science of establishing the identity of a person using his/her anatomical and behavioral traits. Commonly used biometric traits include fingerprints, faces, irises, hand geometries, voices, palm-prints, handwritten signatures, and gaits as shown in figure 1.1 (Prabhakar, Pankanti & Jain, 2003). Biometric traits have a number of desirable properties, with respect to their uses, as authentication tokens, namely, reliability, convenience, universality, and so forth. These characteristics have led to the widespread deployment of biometric authentication systems.

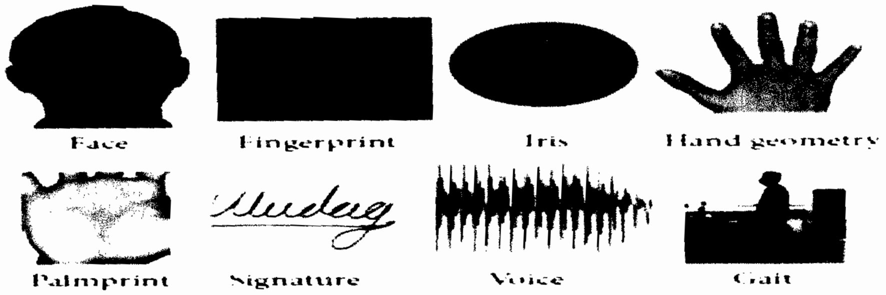


Figure 1. 1 Body traits used for biometric recognition

Among all the biometric techniques, fingerprint-based identification is the oldest method successfully used in numerous applications. Everyone is known to have a unique, immutable fingerprint (Zhou, Su, Jiang, Deng & Li, 2007). A fingerprint is a series of ridges and furrows on the surface of the finger. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as other minutiae points. Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending (Darwish, Zaki, Saad, Nassar & Schaefer, 2010).

The importance of biometrics has grown tremendously, lately, with an increasing demand for security in accordance with the unique identifications of individuals. Apart from banking, biometrics has found its way to the retail payment arena. Since biometric technology can be used in place of PIN codes in ATMs biometric, it offers a promising approach, for security applications, over the classical methods. In other words, using biometrics makes it possible to establish an identity-based method, which can provide sufficient security in many applications (Ross, & Jain, 2003).

Customers are always driven to best services. ATM services are good but with the fear of theft of ATM cards by customers (Abdulahi & Demisse, 2009), there is a need to use biometric systems in ATMs to provide greater protections and provide confidence, to customers, when withdrawing huge amounts of money from ATMs.

The purpose of this study is to design an ATM system based on fingerprint recognition, for the stability and reliability of the banking system. Besides containing the original verifying methods of inputting owners' passwords, the security features will be enhanced largely for the stability and reliability of the ATM system. The design will make the system safer, more reliable and easier to use.

1.2 PROBLEM STATEMENT

Automatic Teller Machines (ATMs) are electronic banking outlets which allow customers to complete their basic transactions without the aid of branch representatives or tellers (Qadrei & Habib, 2009). Nowadays, using the ATMs, which provide customers with the convenient banknote trading, is very common. However, financial crime cases have risen repeatedly in recent years with a lot of criminals tampering ATM terminals and stealing credit cards and passwords. Once a user's bank card is lost and the password stolen, the criminal will draw all his or her cash in a very short time and bring enormous financial loss to the said customer. Being able to validate the identity of customers has now become the focus of the current financial circle (Yang & Mi, 2010)?

Traditional ATM systems, in authenticating credit cards and the passwords, have some defects. The use of credit cards and passwords cannot verify the clients' identities accurately. With the rapid increase in the number of break-in reports involving traditional PIN and password, there is a high demand for greater security in accessing sensitive personal data. These days, biometric technologies are typically used to analyze human characteristics for security purposes (Cavoukian & Stoianov, 2007). Biometrics based authentication is a potential candidate to replace password-based authentication (Uludag, Pankanti, Prabhakar & Jain, 2004). The technique of fingerprint recognition is being continuously updated offering new verification methods; the original password authentication method is being combined with the biometric identification technology to verify the clients' identity and to improve effectively the safe use of the ATM machines.

1.3 RESEARCH QUESTIONS

The objective of this study is come out with a security system, for ATM machines, using fingerprint techniques. Among the questions to be asked are:

1. What are the requirements for a security system for ATM machines using fingerprint techniques?
2. How to evaluate functionality the security system for ATM machines using fingerprint techniques?

1.4 RESEARCH OBJECTIVE

The objective of this study is to design a prototype security system for ATM machines using fingerprint techniques. Among the procedures to be carried out include:

1. Determining the requirements of the security system for ATM machines using fingerprint techniques.
2. Building a prototype security system for ATM machines using fingerprint techniques.
3. Qualifying the functionality of the security system for ATM machines using fingerprint techniques.

1.5 SCOPE OF THE STUDY

The scope of study is to focus on the customers and the services provided to them by the ATM bank machines in terms of customer confidence in dealing with ATM transactions and the safe-guarding of the security through the use of fingerprint techniques.

1.6 SIGNIFICANCE OF THE STUDY

Since biometric features are unique identifications of individuals and hence difficult to steal or copy they can,

- Provide strong authentications and triple securities to the bank customers.
- Be used in place of PINs; customers need not remember the PIN numbers.

- Overcome hidden costs of ATM card management like card personalization, delivery, management, re-issuance, PIN generation and help-desk.
- Provide good and accurate services.
- Allow clients to access their accounts at their own conveniences.

1.7 ORGANIZATION OF THE REPORT

This research is divided into six chapters. This first chapter gives a brief background of the study whereby the problem of the research is put into light and the objectives and research questions are set. Moreover, the research scope and significance are also pointed out.

Chapter Two provides a review of literature related to the design and development of a security system for ATM machines using fingerprint techniques.

Chapter Three emphasizes the research methodology developed by Beck (2000), with the elaboration of its six stages (Selection & Planning, Requirements Analysis, Design of the UML Diagram, Design of the Interfaces and the Written Codes, Usability Testing and Documentation) in line with the development of the assessment system for knowledge sharing among teachers in secondary schools.

Chapter Four presents the analysis and design of the research comprising the system users' requirements, system design and the prototype development.

Chapter Five provides the evaluation of the system, its usability as well as the ease of use and a full assessment of the system.

Finally, chapter six provides the concluding remarks of the system, its limitations as well as suggestions and recommendations for future research.

1.8 SUMMARY

In this chapter a brief background of the study, the problem statement, research objectives, the scope of the research and research significance were provided. The objective of this research is to develop a security system for ATM machines using fingerprint techniques.

CHAPTER 2

LITERATURE REVIEW

2.1 INTRODUCTION

The chapter begins with a review of literature related to automatic teller machines (ATMs) and biometric technology. Section 2.2 starts with overview about automatic teller machines. Challenge of automatic teller machines was discussed in section 2.3. In the section 2.4 was shows definition and describe about biometric technology. An overview of fingerprint technique was shown in section 2.5. Some related works for this study are appeared in section 2.6. Finally, in section 2.7 summary of this chapter.

2.2 AUTOMATIC TELLER MACHINES

Automatic Teller Machines (ATM) is an electronic banking outlet, which allows customers to complete basic transactions without the aid of a branch representative or teller (Qadrei & Habib, 2009). ATM has been adopted and is still being adopted by banks. They offer considerable benefit to both banks and their depositors. The machines can enable depositors to withdraw cash at more convenient times and places than during banking hours at branches. In addition, by automating services that were previously completed manually, ATMs reduce the costs of service some depositor demands. These potential benefits are multiplied when banks share their ATMs, allowing depositors of other banks to access their accounts through a bank's ATM (McAndrews, 2003).

ATM innovation paralleled the growth of the PC and telecommunications industries. Each machine operated in a local mode without any connection to the banking systems, and transaction authorization took place based on the information recorded in the magnetic bands of the cards. The next step in the evolution of this industry was to connect these devices to the bank's centralized systems; by then, mid -1980's, banks would work in a dual modality (Yanez & Gomez, 2004), in other words, the ATM would work on-line but in the event of communication loss it had the ability to authorize the transaction with the information recorded on the magnetic band (Stavins, 2000).

In the early 90's, taking advantage of the technological boom in microcomputers and communications, ATMs started to work exclusively on-line implying that, if the ATM loss communication with its central system, there would not be service. Once ATMs were connected directly, the need arose to protect the information in the card and the client's PIN (Personal Identification Number) found in messages that had to travel across public telecommunication lines. For this purpose, from the beginning, algorithms that allowed for the encryption of the information were utilized; the most commonly utilized algorithm is DES (Delta Encryption Standard) (Han, et al., 2005).

It is important to mention that in parallel to the development of the industry different modes of fraud have made it necessary to reinforce the levels of security utilized in ATMs; this leads to the theme of this study to adapt biometric technology to the ATM networks.

2.2.1 Cards with Magnetic Bands

Cards with Magnetic Bands The plastic cards with magnetic bands date back to more than 30 years. The financial sector has used them as a means to making payments and to offer access to the financial services for clients. The magnetic band contains unique information for every card allowing for user identification and providing access to its products through the various electronic channels (Matutes & Padilla, 1994). In order to provide access to these products, cards with magnetic bands are normally associated to a personal identification number (PIN) which is initially assigned by the entity issuing the card and, in some cases, the client can then change it at his/her convenience. The card and the PIN are directly related to the user identification and allow for the utilization of electronic channels just like as is the case with the ATMs (Stavins, 2000).

2.2.2 ATM Hardware and Software Characteristics

ATM Hardware and Software Characteristics We may classify the hardware for an ATM in two major categories: the first one, corresponding to its PC architecture (a microprocessor, memory, drives, monitor, keyboard, etc.), the second one related to ATM specific functions such as card reading, cash dispensing, cash storage, user and operator's video and keyboard interaction, etc. (Hayashi, Sullivan &

conducted (Hannan, 2007). This information is combining d with control data (ATM number, date, time, transaction sequence, etc.) to create a requirements message to the authorizing system; this message, a Transaction Request or TREQ, is sent over a public or private data communications network (Coventry, Angeli & Johnson, 2003).

The authorizing system receives the TREQ and proceeds to decode and process the information as follows: card identification, PIN validation, financial transaction execution (or denial), application file updates, and reply preparation. The Transaction Reply, or TREPLY, is then sent via the communications network to the ATM originating the transaction (Yanez & Gomez, 2004).

Upon TREPLY reception, the ATM decodes and processes the information and presents the transaction results to the user. If it is a cash request, the cash is presented; if it is an information request, it is shown on the screen or printed on a receipt. Finally, the ATM's application puts together and transmits a Transaction Confirmation or, TCONFIRM, to the authorizing system including feedback on the success or failure of the transaction (Hannan, 2007).

In general, a centralized system has the ability to connect with each and every ATM, and at the same time communicate with each and every centralized system that is required to complete a transaction.

2.3 CHALLENGE OF AUTOMATIC TELLER MACHINES

A widely held concept among security professionals is that security for its own sake is not a wise business investment. Before investing in security measures, an organization should undertake a risk assessment to identify possible threats, their likelihood and their possible impact. When reviewing ATM security, a pragmatic approach is a risk-based one. Especially in today's economic climate, it makes little sense to spend money on ATM security measures that don't address real business risks. There are many ways for theft ATM such as skimming and card theft will be illustrated.

2.3.1 Skimming

Skimming occurs when a consumer swipes their card through a reader that has been compromised by criminals that will later retrieve the card data. Criminals also usually obtain the card's matching PIN through concealed cameras or "over the shoulder" and either sell this information or withdraw the cash directly from the consumer's account with cloned cards. A skimming attack is relatively easy to perform and the equipment for skimming (card readers, miniature cameras) can be easily obtained online.

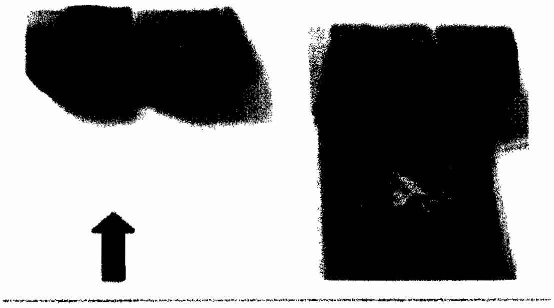


Figure 2. 2 The slot on the left is the real one

Skimming is by far the most popular form of ATM attack, accounting for over 80% of ATM fraud, or around $800 million per year in 2008 (Sullivan, 2008). It is also gaining popularity among criminals as it is a “much more profitable crime to commit (compared to other crimes)” (Peretti, 2009) because large amounts of money can be collected quickly and with a relatively low risk of detection.

For example, In January 2010, two criminals in Houston, Texas ran a skimming operation at a single ATM that resulted in more than $200,000 in bank losses. Their operation was fairly low-tech compared to other skimming operations, illustrating how easy it is to perform these attacks. They installed a skimmer at an ATM and parked across the street, observing the ATM through binoculars. When a victim approached the ATM, they would move in with a camera and capture the PIN number being entered (Peretti, 2009).

2.3.2 Card Theft

There are many ways to theft ATM card, one of them is the thief puts wire, VHS tape or other mechanism in the ATM card slot to “catch” the card and prevent it from being ejected. They then often observe the cardholder entering their PIN or “help” the cardholder by recommending they enter their PIN to retrieve the card (Lee, 2006). The thieves later use tweezers to remove the card.

On other hand a scam involves the thieves putting a thin, clear, rigid plastic 'sleeve' into the ATM card slot. When the victim inserts his card, the ATM cannot read the strip, so it repeatedly asks him to enter his PIN number. Meanwhile, someone behind him watches as he taps in his PIN. Eventually the victim leaves, thinking the ATM has swallowed his card.

The thieves then remove both the plastic sleeve and the card, and withdraw from the victim's account. (Walsh, 2005)

2.4 BIOMETRIC TECHNOLOGY

Biometric technology utilizes a human's unique physical or behavioral characteristics to authenticate individuals (Rhodes, 2003). The main motivation for employing biometric technology is to efficiently and effectively control access by authenticating users via their unique biometric characteristics. Due to the potential usefulness of this new technology, its applications are becoming pervasive throughout government programs and the private sector (Coventry, Angeli, & Johnson, 2003).

Market experts forecast that biometrics will be at the main stream of information technology within a decade (Halal, 2006). The International Biometric Group (IBG) predicts that biometrics market size will reach $4.6 billion in 2008 (Das, 2005). The leading biometric modalities include fingerprint recognition, iris recognition, facial recognition, hand or two-finger geometry, voice recognition, and signature recognition. It is clear that there are significant differences in these modalities in terms of performances, complexities, vulnerabilities, and acceptance by consumers (Rhodes, 2003).

As mentioned previously, fingerprint recognition technology is the most commonly used biometric technology making up about 67% of the present day biometrics market (IBG, 2005). This type of biometric analyzes the forms and patterns of the ridges and valleys on the surface tips of human fingers (Yun, 2002). The popularity of fingerprint recognition technology is due to its high reliability, ease-of-use, and low system cost, as well as the long lifespan of fingerprints (Halal, 2006). Similarly, iris recognition technology analyzes the rich patterns of the eye's iris to uniquely identify individuals. This modality is more reliable than fingerprints, however, businesses have been slow to embrace this biometric due to its expensive costs and because of consumer concerns (Cavoukian, 1999).

Several less reliable biometric forms are also available. For instance, a more widely accepted option by consumers is that of the hand or finger geometry technology. This form captures a three-dimensional image of a person's hand or of specific fingers (Das, 2005). Although it is not as reliable as using fingerprints or irises, it is reliable enough to be used for a specific population. Additionally, given its general acceptance by consumers, this modality has been applied in school settings, such as for meal plans. A less desirable alternative is voice recognition technology, which analyzes various characteristics of the human voice including cadence, pitch, and tone (Levine, 2000). Unfortunately, its reliability is significantly influenced by multiple factors such as background noise, the person's health and emotional condition at the time, and the quality of the input devices (Cavoukian, 1999). Signature recognition can also be a useful biometric in certain situations. Individuals are identified by analyzing behavioral features that include pen pressure and speed of writing, as well as the shape of the signature (Das, 2005). A final biometric option is that of facial recognition, which analyzes the unique shape and patterns of an individual's facial features. This type of technology has the distinction of being the only biometric that can be used covertly (Cavoukian, 1999). In other words, it can be used to identify criminals on watch lists by capturing the facial images of someone in a public area, without that person's knowledge.

Biometric identification systems typically follow three high-level processing steps as showing in figure 2.3. First, the system must **acquire** an image of the attribute through an appropriate scanning technique. Once the scanned content is acquired, it must be **localized** for processing purposes. During this step, extraneous informational content is discarded and **minutiae** are isolated and turned into a **template**, a sort of internal canonical form for matching attributes stored in a database. Minutiae are the uniquely differentiating characteristics of the biometric attribute. Whorls and loops and their relationship to one another on a fingerprint are an example of the minutiae that might be extracted. Finally, templates stored in the database are searched for a match with the one just presented. If a match is found, the identification is a success and the succeeding steps of the security process can begin (Coventry et al., 2003).

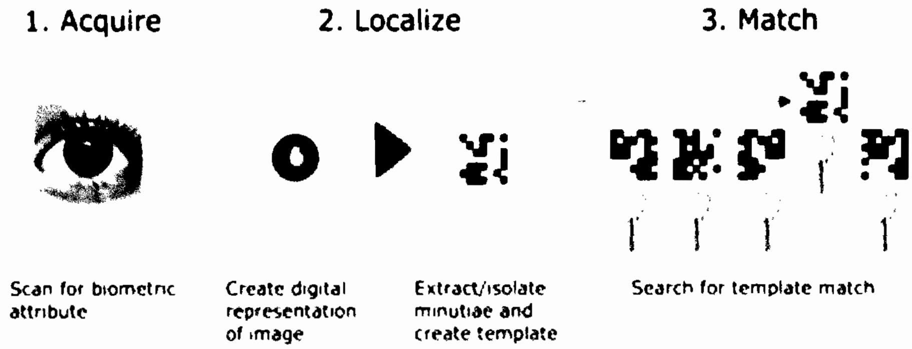

1. Acquire
2. Localize
3. Match
Scan for biometric attribute
Create digital representation of image
Extract/isolate minutiae and create template
Search for template match

Figure 2. 3 Biometric Identification Process (Coventry et al., 2003)

2.5 FINGERPRINT TECHNIQUE

There have been many developments in the world have focused our attention on the reliability and security. In particular, the tragic events of September 11, 2001 have increased attention to security at airports and on airplanes. Use many biometric method introduced from fingerprints to facial recognition, etc. Authentication Onboard the Aircraft (Single Biometric Device) (Caparroz, et al., 2006). As shown in Figure 2.4.

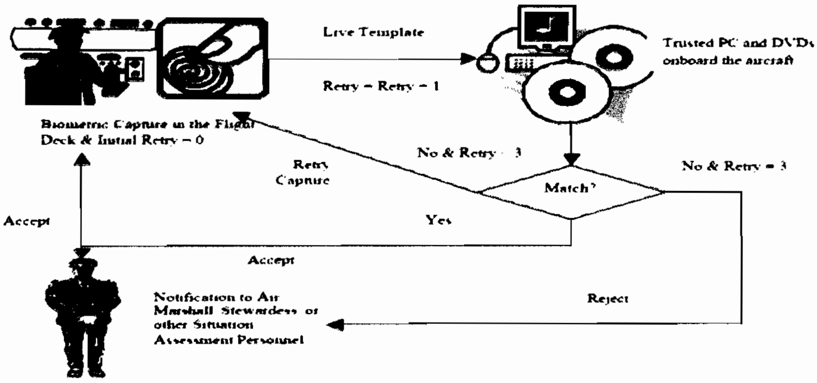

Live Template
Trusted PC and DVDs onboard the aircraft
Retry = Retry + 1
Biometric Capture in the Flight Deck & Initial Retry = 0
No & Retry < 3
Retry Capture
No & Retry = 3
Match?
Accept
Yes
Accept
Notification to Air Marshall Stewardess or other Situation Assessment Personnel
Reject

Figure 2.4 Process of Single Biometric Device (Caparroz, et al., 2006)

How to get the right one-to-one correspondence of pairs has a great impact on the results of the comparison of fingerprints algorithm. Use algorithm for fingerprint matching worldwide. The main contribution is a novel and efficient algorithm for one-to-one matching pairs based on the coherence of the movement. Coherence of motion is a useful function for the fingerprint matching to the improvement of traditional minutiae based fingerprint matching method. The experimental results show that the proposed method with a good strategy to strengthen the principle of movement and makes consistency works well EER (error results of the experiment) is lower (Wen & Wang, 2009).

Fingerprint image quality testing is one of the most important issues in fingerprint recognition, because recognition is highly dependent on the quality of fingerprint images. Use new quality control algorithm that considers of the input fingerprints and errors in orientation estimates. The experimental results showed that the proposed method gave a reasonable indicator of quality in terms of quality of the environment. Moreover, the proposed method proved superior to existing methods in terms of separation and performance verification (Lee, Choi, Choi, & Kim, 2008).

It is poor quality of the image as a result of false and lack of opportunities that degrades the performance of the identification system. The based on tree theory for classification of fingerprint image quality is proposed. This new classification has many advantages in solving the problem of the quality of fingerprint classification. Classification of the quality of fingerprint images is proposed and it techniques in user interfaces of various systems (Sugiura, & Koseki, 1998).

The impersonation is one of most dangerous security threats, in which, somebody claims to be somebody else. Anyone can be stolen identities, and also the password can be forgotten or cracked. The fingerprint recognition in wavelet to instance has been implemented. All input fingerprints are in the format of 256 × 256 resolution. Images of the entrance exams into two groups, which is enhanced fingerprint images (E-input), and unprocessed (raw) fingerprint images (U-input).

They focused on data leakage in connection with the biometric equipment and offers countermeasures. The method is applied to a system for comparing fingerprints and determined that the secret data can be restored to a high probability if it is an authorized person, setting the number of elements of A and the number of code elements parity with the corresponding values of r. Submitted biometric data, appear to provide very good privacy, not only employees, but also sensitive data (Hidano, Ohki, Komatsu & Kasahara, 2009).

The problem it is easy for attackers to guess passwords because as users select a user name and password, and information that is easy to remember. Use method of one time password key generation of OTP (One Time Password) using fingerprint features. As shown in figure 2.5.

2.6.3 Bank saving network systems

Compared with formerly network system logged on with password, fingerprint identification technology based bank saving network system is much safer (Xiaohua & Yansheng, 1998). Figure 2.7 shows the systemic frame, under the network environment; both fingerprint templates and corresponding registration information are saved in a security database in the remote server. If one user locating in one sub branch of a bank wants to access those resource managed by remote server, (he/she) needs identity verification through fingerprints identification system, otherwise, he can't finish such operations as depositing and fetching. In addition, in order to enhance system security, data and fingerprint features transmitting between the customer and the server must be encrypted.

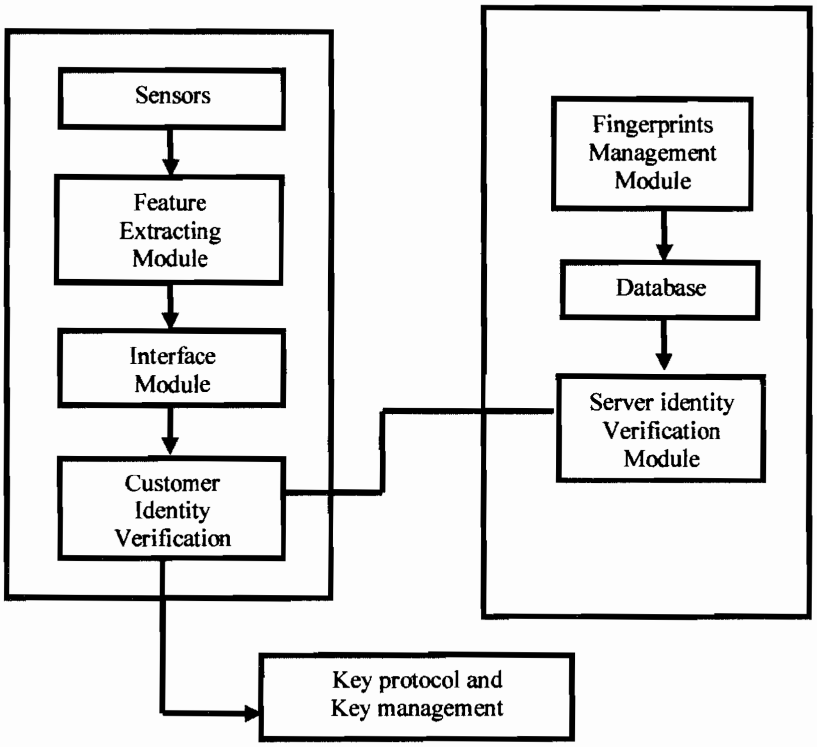

Sensors
Feature Extracting Module
Interface Module
Customer Identity Verification
Fingerprints Management Module
Database
Server identity Verification Module
Key protocol and Key management

Figure 2.7 Bank saving network system frame based on fingerprints

2.6.4 All kinds of network exchange.

Electronic commerce is a developing field. Generally, traditional security mechanism uses password verification during identification and authorization of person/machine systems, which makes well-connected information storing and transmitting security systems become insignificant due to some weaknesses resulting from the users themselves, such as the password being too simple and easily decoded. Fingerprint identification technology and its applications make it possible to eliminate such limitations in the information fields (Ke, 2002).

2.7 SUMMARY

After presenting this chapter, it would be clear to analysis ATMs system which means an electronic banking outlet, which allows customers to complete basic transactions without the aid of a branch representative or teller. On other hand, Biometric technology refers to utilize a human's unique physical or behavioral characteristics to authenticate individuals the provision. Therefore, as an effective biology identification method, fingerprint identification has been concerned widely and developed remarkably. It has extensive applications in the field of information security as well as police system and worker attendance system.

CHAPTER 3

METHODOLOGY

This section describes the research methodology that used in this project. Section 3.2 provides important information about agile software development methodology Extreme Programming (XP) approach that used in this study. Then, the stage of methodology was discussed in section 3.3. Finally, summery placed at end of the chapter.

3.1 RESEARCH METHODOLOGY

There are numerous methodologies available today that can be used as tools to develop a system. This research adopted the agile methodology (XP) proposed by Beck (2000). Extreme Programming (XP) is a lightweight software development methodology. The fundamental concept of XP is to start simply, divide a project into a series of iterations each ending with a rigorously tested release that works in its limited way, and then fit it into a specific structure designed to simplify and expedite the process of software development rather than an exhaustive structure based on the thorough and time-consuming analysis.

Extreme Programming is actually a deliberate and disciplined approach created in response to software development in the environment of rapidly changing requirements. High-risk projects and those with vague or dynamical requirements are perfect for XP and they will experience greater success and developer productivity in comparison with other software development methodologies.

So, if you do not have a firm idea of the new system functionality or the software functionality is expected to change frequently, this is when XP will succeed and rapidly produce extremely reliable, efficient, well-factored software.

3.2 METHODOLOGY STAGE

Agile software development methodology (Extreme Programming (XP) Approach) has six stages to design and develop the prototype model of the system. The methodology adopted from Beck (2000) that followed in this study is as shown in Figure 3.1.

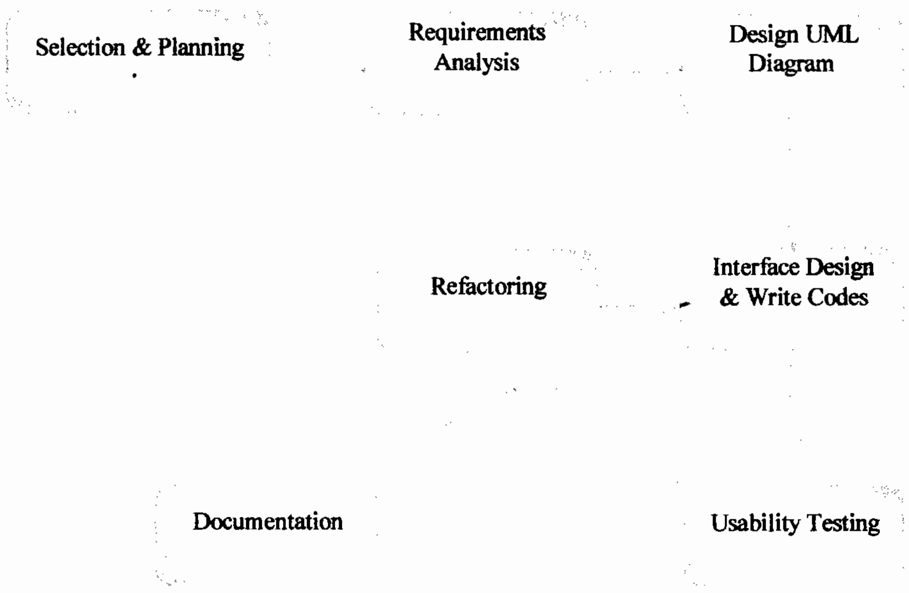


Figure 3.1 Agile Software Development Methodology XP Approach (Beck, 2000)

3.2.1 Selection & Planning

During first stage, a comprehensive study has been done to identifying the activities, milestones and deliverables produced by the project. According to Sommerville (2007), well plan drawn up to guide the development towards the research goals. At the beginning of this stage project scheduling, cost estimation, risk analysis, and work break down structure has been carried out. This stage enables most of the other practices by reducing by the bulk of what needs to be considered by the programmers at any time to the user's immediate needs.

3.2.2 Requirements Analysis

The second stage has identified the end user's requirements towards the ATM system by using biometric security (fingerprint). The process starts by getting information about exiting process, manual system, features & functions provided and identifying the problems. This stage defined how the current system works, determine & analyze facts and documents how system should work better to support, develop a logical prototype of the proposed ATM system by using biometric security (fingerprint).

3.2.3 Design UML Diagram

Design is essential part of the overall software design process. A poorly designed that user probably unable to access some of the features; based on the analysis requirements in the form of user stories card which has been followed to construct use case diagram and drowning using Rational Rose 2003. Also during this phase several designs have been produced using unified modeling language (UML) such as sequence diagram and class diagram.

3.2.4 Design Interfaces and Write Codes

Active Server Pages (ASP .NET Programming) and SQL has been followed go through the project. ASP .NET used as programming language. In the code, all of the class name, variables name has in the same style for long term benefit to coding standards. Coding standards that are chosen for communication help new people learn the system and improve productivity.

3.2.5 Usability Testing

All scripts and classes configured to test packages in order to meet external requirements and achieved the goals set for the study. The evaluation will performed to determine the level of usefulness and operability of the system after the system has been developed; it is tested through a questionnaire technique based on usability testing by using System Usability Scale (SUS) proposed by Brooke (Bangor, Kortum & Miller, 2008)..

3.2.6 Documentation

A well documentation has been written at the end of the study for future enhancement and development.

3.3 SUMMARY

Methodology is essential in every project to proper guide for attaining a study's aims. The methodology for this study is adapted from Beck (2000). A prototyping approach has been used in the third phase of the adapted methodology in order to design requirements model. The next chapter will present the details design of the proposed requirement model using UML diagram and interface design.

CHAPTER 4

SYSTEM ANALYSIS & DESIGN

The present chapter discusses succinctly proposal ATM system using fingerprint technique (ATM_UFP). The outcome of this chapter are determined the requirements of ATM system using fingerprint technique (ATM_UFP) and analysis the system using UML language to understood how the system works through designing use case diagram, class diagram, sequence and collaboration diagram. Finally, build the interface for assessment system.

4.1 SYSTEM REQUIREMENTS

4.1.1 Functional Requirements

Functional requirements are associated with specific functions, tasks or behaviors the system must support (Chung & do Prado Leite, 2009). ATM system is treating private with customers' bank. The customer will interact with the system through interfaces in addition to the requirements appear when it is base on the users interface. Table (4.1) summarizes the functional requirements for the system and gives a brief description of the different requirements.

- M – mandatory requirements (something the system must do)
- D – desirable requirements (something the system preferably should do)
- O– optional requirements (something the system may do)

Table 4. 1 List of Functional Requirements

No.	Requirement ID	Requirement Description	Priority
	ATM_UFP _01	**Login**	
1.	ATM_UFP_ 01_01	User of the system (customers) can key in the credit card and PIN code.	D
2.	ATM_UFP _01_02	If user key in wrong user name or password the system will display error Message and ask to re-enter the user name and the password again	D
3.	ATM_UFP _01_03	Customer can using fingerprint to enter the system, if he/she have problem with credit card or PIN code.	M
	ATM_UFP _02	**Account Manage**	
4.	ATM_UFP _02_01	Customer can click on view services pages	D
5.	ATM_UFP _02_02	System will display for the customer all the available services	M
6.	ATM_UFP _02_03	Customer could be requesting any available services by click on services button.	M
	ATM_UFP _03	**Withdraw**	
7.	ATM_UFP _03_01	Customer can click on withdraw services pages.	M
8.	ATM_UFP _03_02	System will display for the customer withdraw services pages.	D
9.	ATM_UFP _03_03	Customer could be requesting any available amount or click on other	

		amount if he/she need anther amount not available.	M
10.	ATM_UFP _03_04	Customer can enter any amount (maximum 1500 RM) he/she need to withdraw.	M
	ATM_UFP _04	**Login use Fingerprint**	
11.	ATM_UFP _04_01	User of the system (customers) can key via using fingerprint, if he/she forget PIN code.	D
12.	ATM_UFP _04_02	If user key in wrong fingerprint the system will display error Message and ask to re-scan the fingerprint again	D
	ATM_UFP _05	**Withdraw Extra**	
13.	ATM_UFP _05_01	Customer can click on withdraw services pages.	M
14.	ATM_UFP _05_02	System will display for the customer withdraw services pages.	M
15.	ATM_UFP _05_03	Customer could be requesting any available amount or click on extra amount if he/she need anther amount not available.	M
16.	ATM_UFP _05_04	Customer can enter any amount (maximum 15,000 RM) he/she need to withdraw, then click Yes button.	M

4.1.2 Non Functional Requirements

Non-functional requirements are constraints on various attributes of these functions or tasks (Chung & do Prado Leite, 2009). It will capture properties that are not primary for the system to work or features of the system that has to do with performance and quality. However, it's very important because, its can help the system gain competitive advantage over other systems and they are often features that highly desired by the user. Table (4.2) summarizes the non-functional requirements for the system.

Table 4. 2 List of Non-Functional Requirements

No.	Requirement ID	Requirement Description	Priority
	ATM_UFP _6	**Usability issues**	
17.	ATM_UFP _6_01	The system must provide the easy access.	M
18.	ATM_UFP _6_02	The system must be easy to deal with.	M
19.	ATM_UFP _6_03	The admin should be able to view assessment result in 4 second after click	M
20.	ATM_UFP_6_04	The system should be easy to understand	D
21.	ATM_UFP _6_05	The system should be easy to understand	M
22.	ATM_UFP _6_06	The teacher will wait few mounts to process confinement teacher's assessment.	M
	ATM_UFP _7	**Maintainability requirements**	
23.	ATM_UFP _7_01	In case of change or addition demand, the maintainability shall be easily done by integrating new modules and offering new software solutions.	D
	ATM_UFP _8	**Operational requirements**	
24.	ATM_UFP _8_01	The system will have server for the database and connection to the main database.	M

	ATM_UFP _9	**Performance requirement**	
25.	ATM_UFP _9_01	The system database must be updated in real time.	M
26.	ATM_UFP _9_02	The system must have reasonable speed according to technology use to access many of users at the same time.	M
27.	ATM_UFP _9_03	The system should be available 24x7.	M
	ATM_UFP _10	**Security requirements**	
28.	ATM_UFP _10_01	Only who has credit card and PIN code or using fingerprint can access the system.	M
29.	ATM_UFP _10_02	Unauthorized person should not use the system.	M
30.	ATM_UFP _10_03	No one can change the password without login to the system.	M
	ATM_UFP _11	**Availability requirements**	
31.	ATM_UFP _11_01	The availability of this system is up to the internet connection of the client (teacher & admin).	M

4.2 USE CASE

Use case approaches are increasingly attracting attention in requirements engineering because the user-centered concept is valuable in eliciting, analyzing, and documenting requirements (Duan, 2009). One of the main goals of the requirements engineering process is to get agreement on the views of the involved users (Knapp, e al., 2004), and use cases are a good way to elicit requirements from a user's point of view (Dedeke & Lieberman, 2006).

Adopting a met model for use-case-based requirements generation helps avoid confusion. The Meta model describes the elements comprising the collection of artifacts developed as part of the solution statement, which in turn resolves a particular problem statement or business need. The solution statement includes the use case narrative, the use case diagram, and the domain model (Dedeke & Lieberman, 2006).

Use cases are not only a requirements description tool; they are also useful in recommended means of aiding the transition from a problem domain-oriented view to a solution-oriented view of the system (Overmyer, Lavoie & Rambow, 2001).

Generally, use case steps are written in an easy-to-understand structured narrative using the vocabulary of the domain. This is engaging for users who can easily follow and validate the use cases, and the accessibility encourages users to be actively involved in defining the requirements.

4.2.1 Use Case Diagram

The Use case diagram is used to identify the primary elements and processes that form the system. The primary elements are termed as "actors" and the processes are called "use cases." The Use case diagram shows which actors interact with each use case. The above statement pretty much sums up what a use case diagram is primarily made up of actors and use cases.

A use case diagram captures the functional aspects of a system. More specifically, it captures the business processes carried out in the system.

As you discuss the functionality and processes of the system, you discover significant characteristics of the system that you model in the use case diagram. Due to the simplicity of use case diagrams, and more importantly, because they are shorn of all technical jargon, use case diagrams are a great storyboard tool for user meetings. Use case diagrams have another important use. Use case diagrams define the requirements of the system being modeled and hence are used to write test scripts for the modeled system.

A generalization relationship between use cases "implies that the child use case contains all the attributes, sequences of behavior, and extension points defined in the parent use case, and participates in all relationships of the parent use case." The child use case may define new behavior sequences, as well as add behavior into and specialized existing behavior of the parent (Alhir, 2003).

According to the use case diagram the system has two main components (actor/use case). In this study actor represent by customer. The customer has two ways to login (credit card and fingerprint) to the system. The customer can withdraw limited amount when he/she login via credit card and PIN code. On other hand, customer can withdraw huge amount when he/she login by using fingerprint technique. The use case it represented in the following Figure (4.1):

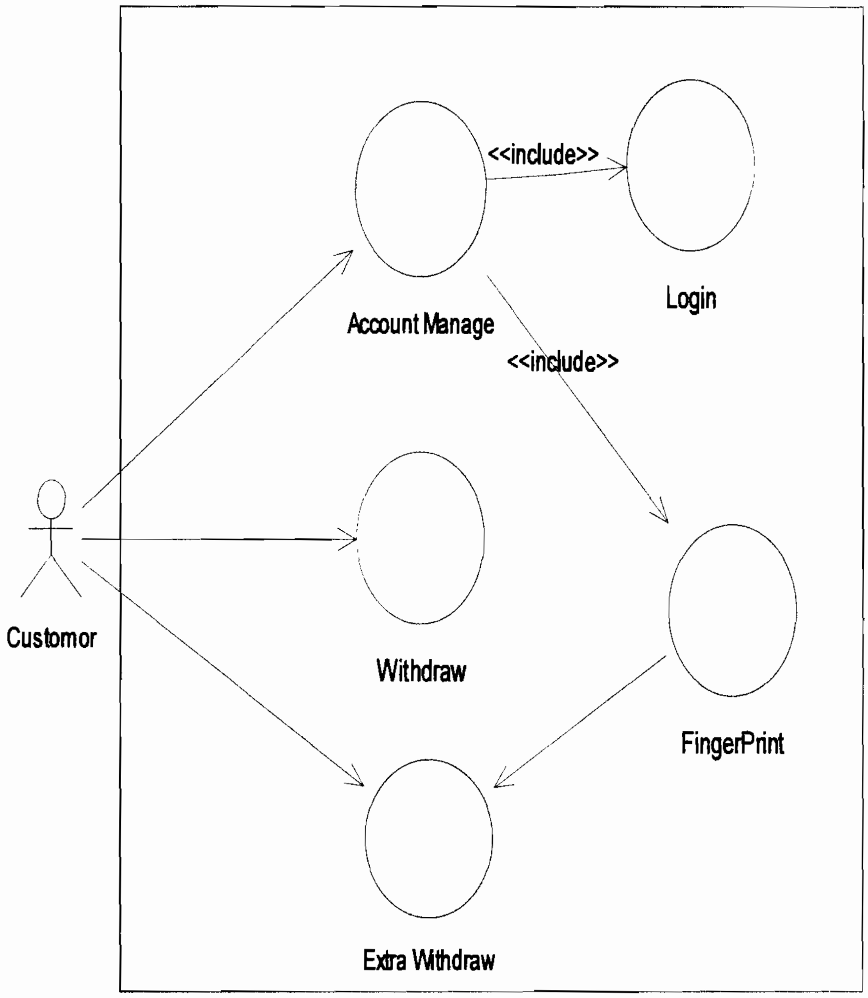


Figure 4. 1 ATM_UFP Use Case Diagram

4.3 USE CASE SPECIFICATION

According to Dutoit & Paech (2002), a use case specification is a document used to capture the specific details of a use case. Use case specifications provide a way to capture the functional requirements of a system. Use case specifications provide a means of organizing all of the different scenarios that exist. They add detail beyond what is shown in a use case diagram. They are a useful tool in communicating with project stakeholders, system users, business analysts, and developers. These specifications define requirements in a way that all consumers of the project can understand, creating a common vocabulary for the impacted parties (Anton, Carter, Dagnino, Dempster & Siege, 2001). All the detail about EMS system has been placed in the appendix B

4.4 SEQUENCE AND COLLABORATION DIAGRAM

A sequence diagram describes how groups of objects collaborate in accomplishing some system behavior. This collaboration is implemented as a series of messages between objects. Typically, a sequence diagram describes the detailed implementation of a single use case (or one variation of a single use case). Sequence diagrams are not useful for showing the behavior within an object. Consider using state-transition diagrams for that purpose (Li, Liu & Jifeng, 2004).

Login

As shown in figure 4.2 it does describe the sequence diagram for system login. Customer can access to system by login his/her account through the credit card and the PIN code.

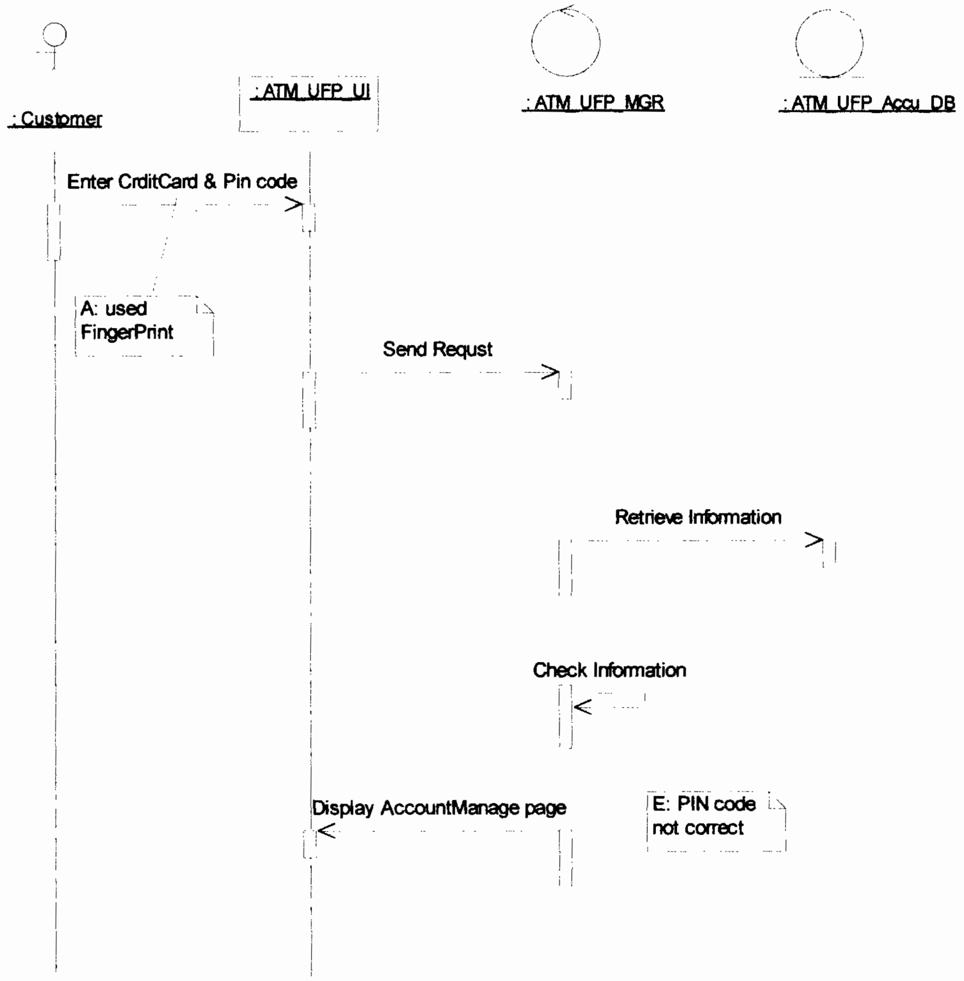


Figure 4. 2 Login Sequence Diagram

As shown in figure 4.3 it does illustrate collaboration diagram for system login. It was explain all the details of movement for system in use case login.

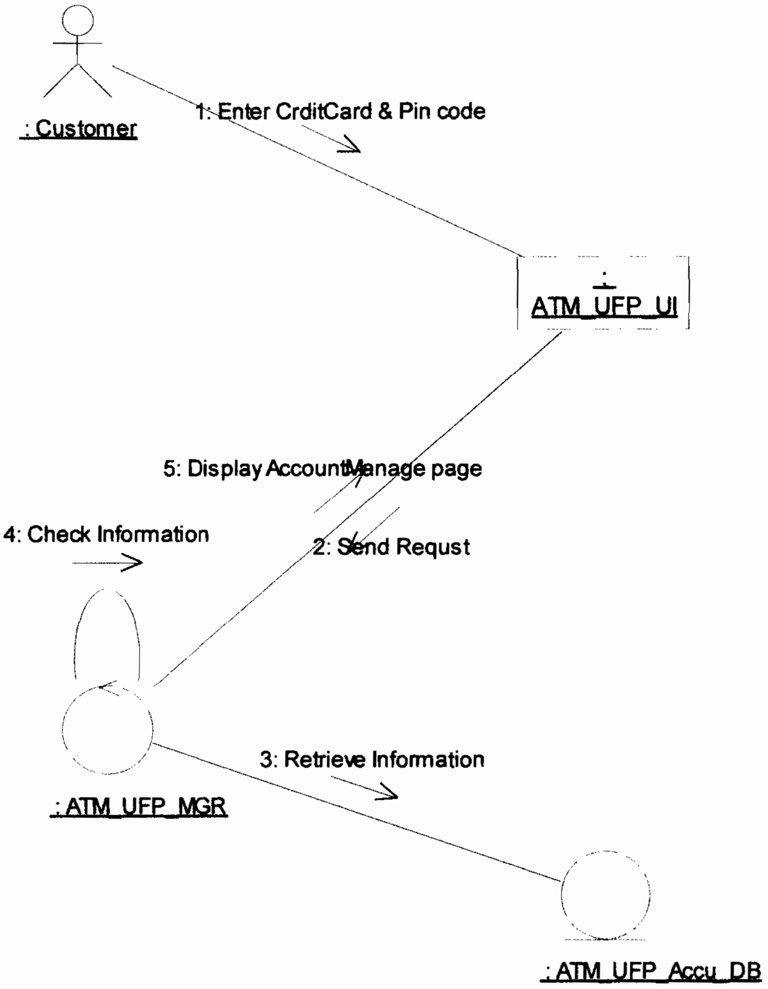


Figure 4. 3 Login Collaboration Diagram

Account manage

As shown in figure 4.4 it dose explain the sequence diagram for account manage. Customer can manage his/she account through this main page. Customer will view the service and select any service he/she needs.

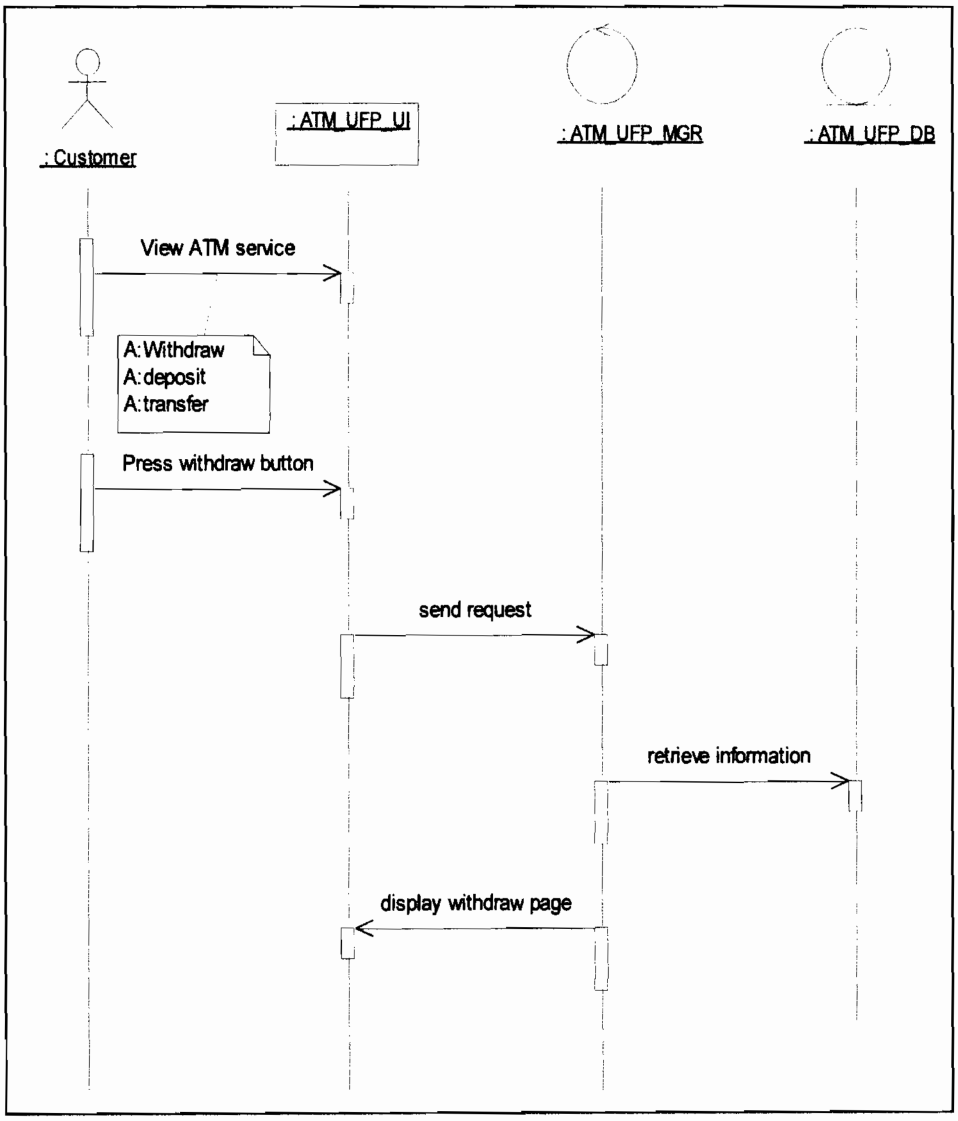


Figure 4. 4 Account Manage Sequence Diagram

As shown in figure 4.5 it does illustrate collaboration diagram for system account manage. It was explain all the details of movement for system in use case account manage.

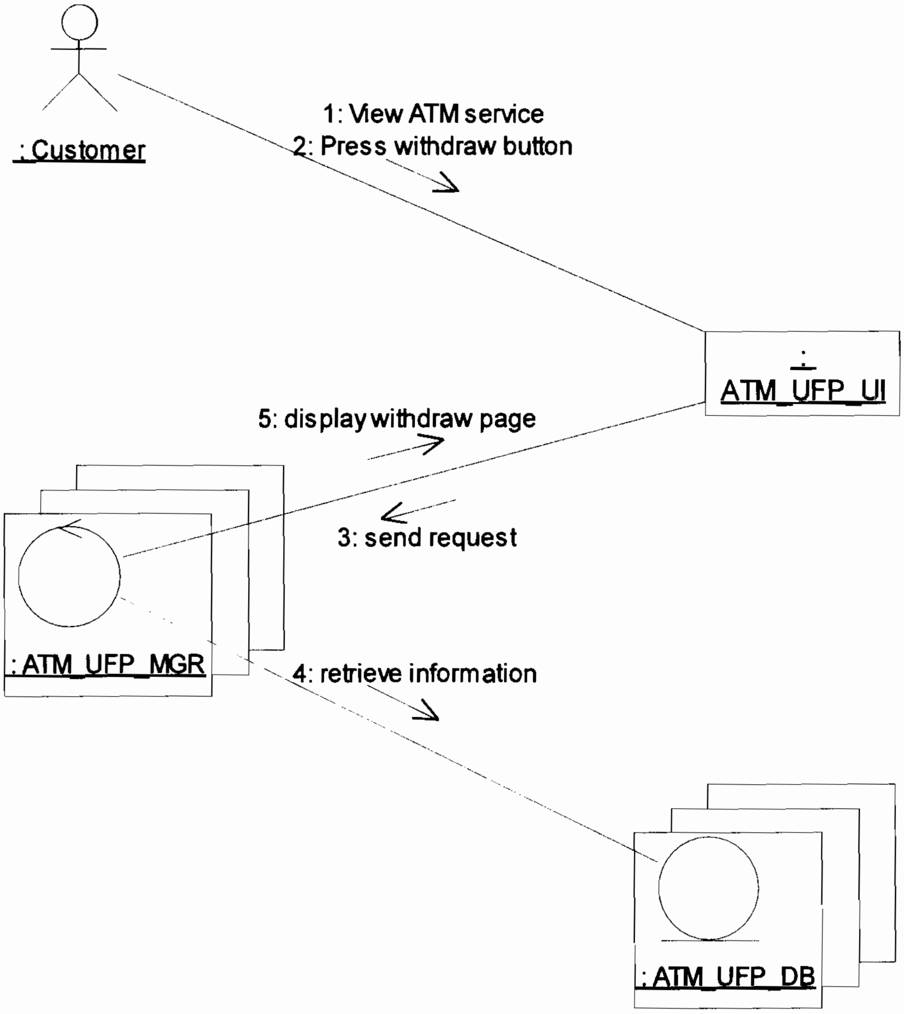


Figure 4. 5 Account Manage Collaboration Diagram

Withdraw

As illustrated in figure 4.6 it does describe the sequence diagram for withdraw. A customer can enter withdraw page after selected from account manage page. When the customer access withdraw page he/she can select the amount to withdraw or enter the number he/she needs to withdraw (MIX 1500 RM).

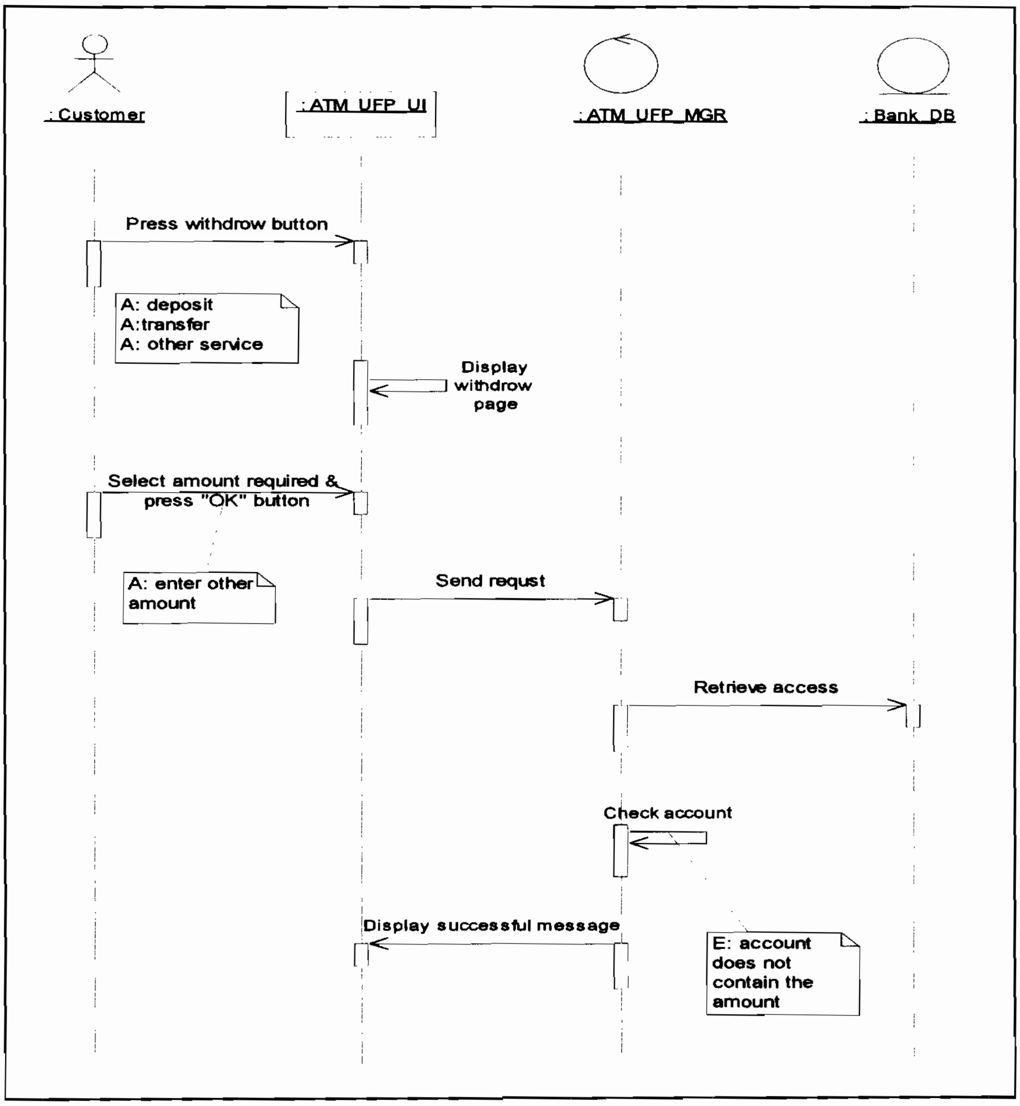


Figure 4. 6 Withdraw Sequence Diagram

As shown in figure 4.7 it does explain collaboration diagram for use case withdraw. It was explain all the details of movement for system in use case withdraw.

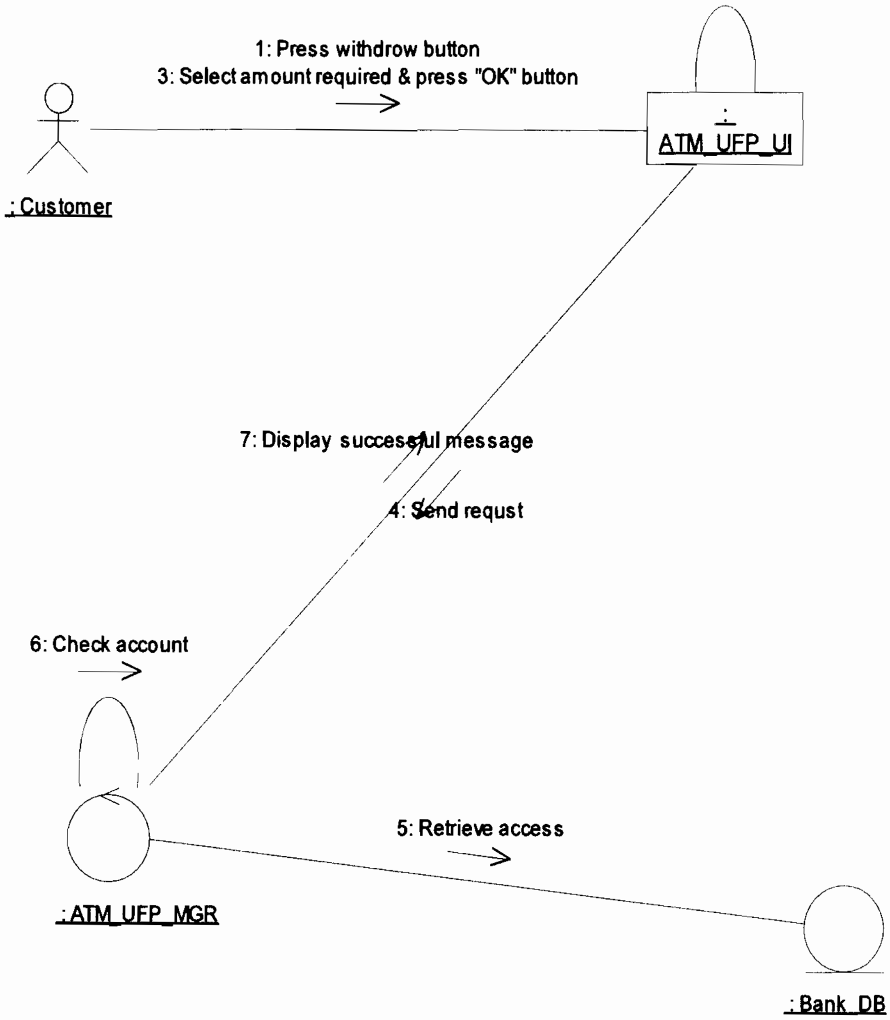


Figure 4. 7 withdraw collaboration diagram

Login by Fingerprint

As shown in figure 4.8 it does explain the sequence diagram for system login by use fingerprint technique. The other way to login to system is use fingerprint technique. Customer can use this technique when he/she forgets PIN code.

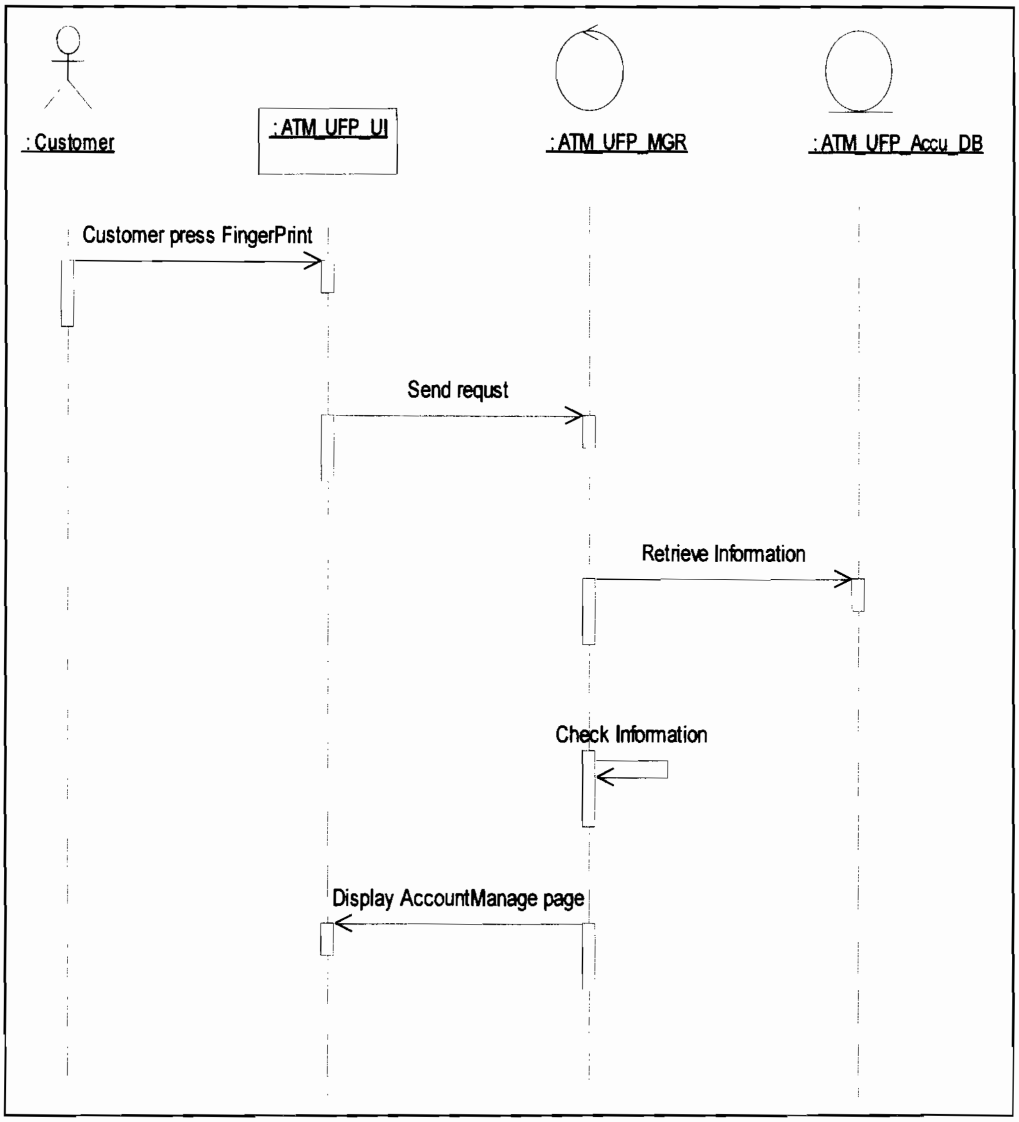


Figure 4. 8 Login by use fingerprint Sequence Diagram

As shown in figure 4.9 it does illustrate collaboration diagram for system login by use fingerprint technique. It was explain all the details of movement for system in use case login by use fingerprint technique.

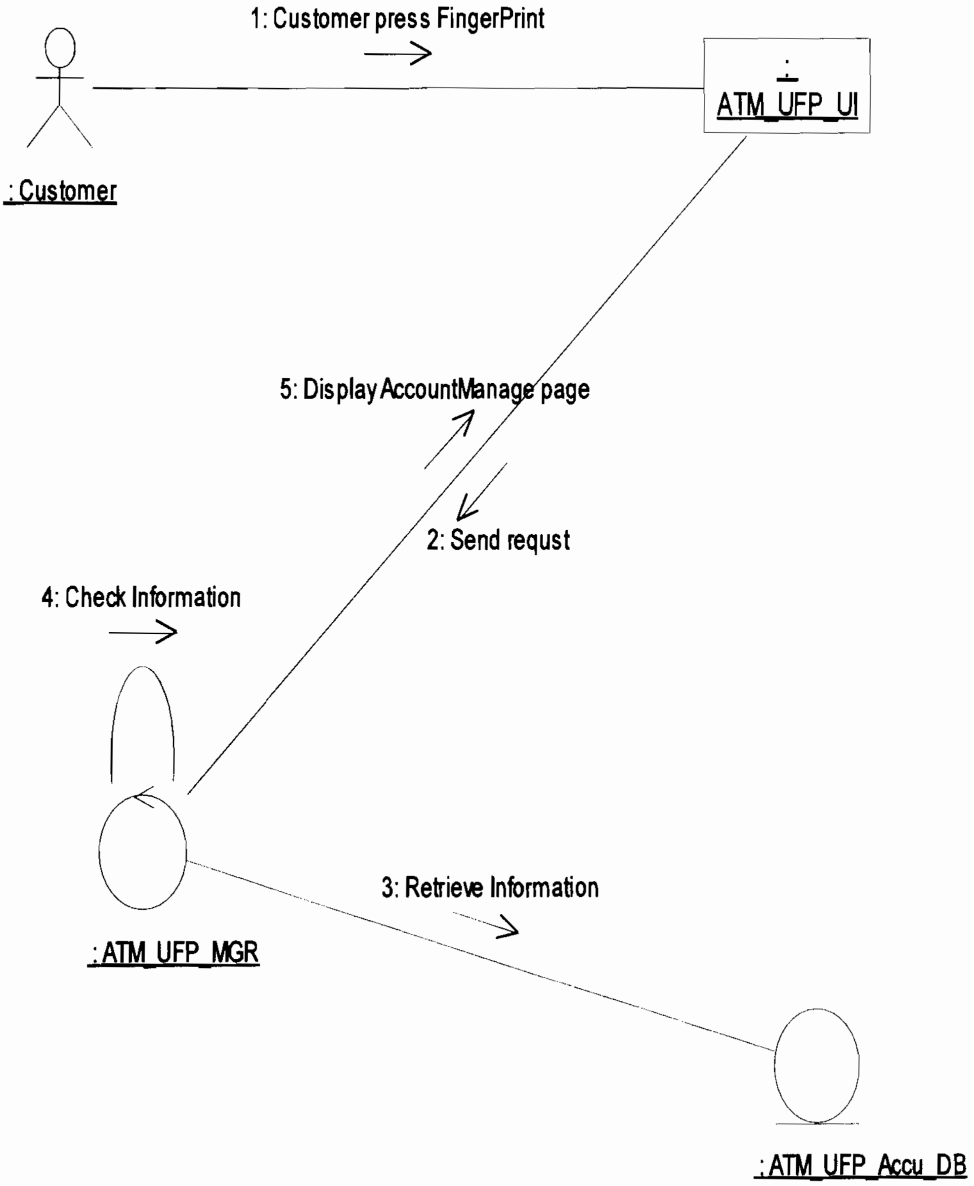


Figure 4. 9 Login by use fingerprint Collaboration Diagram

Extra Withdraw

As shown in figure 4.10 it dose describe the sequence diagram for extra withdraw. When the customer access extra withdraw page he/she can select the amount to withdraw or enter the number he/she needs to withdraw (MIX 15000 RM).

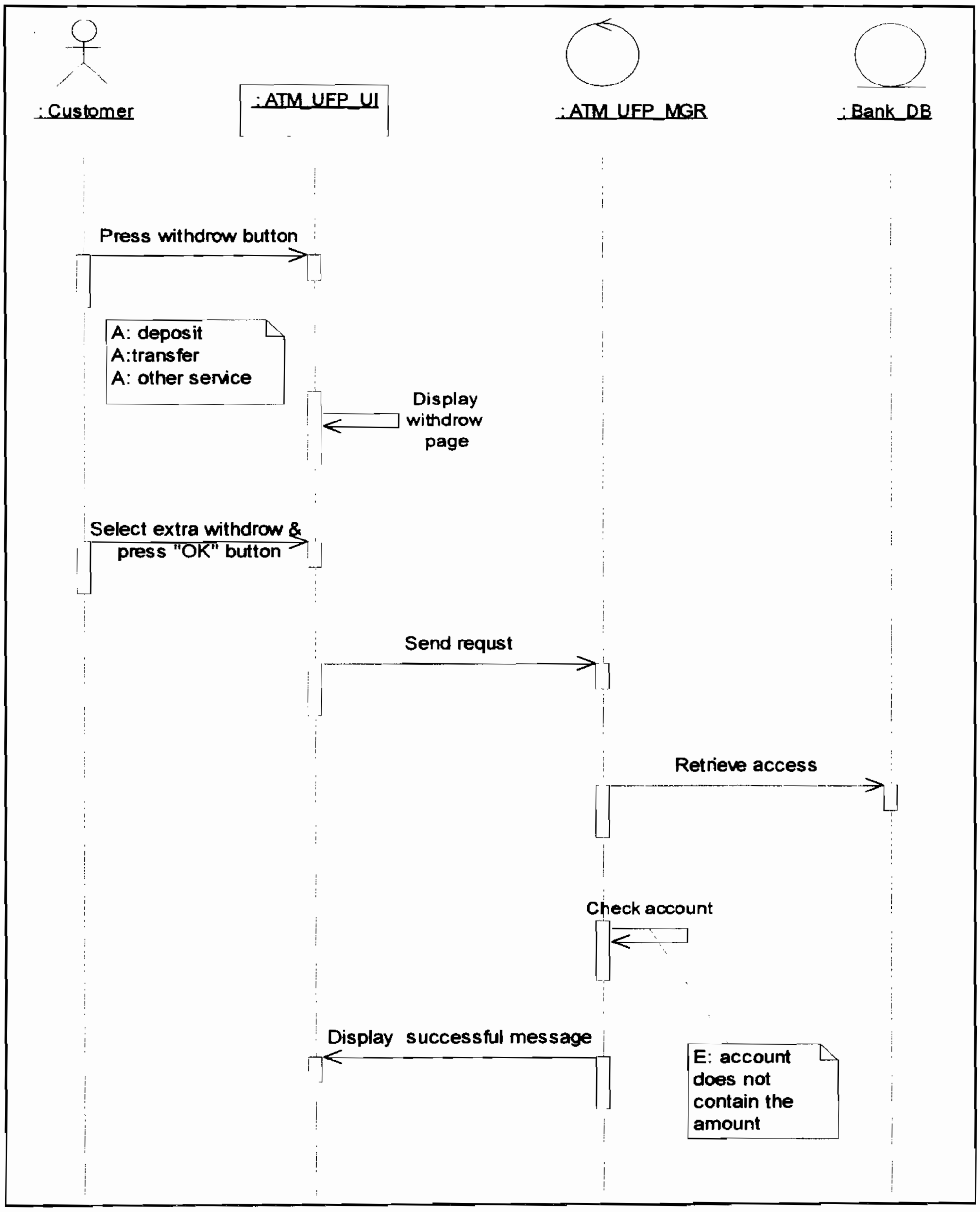


Figure 4. 10 Extra Withdraw Sequence Diagram

As shown in figure 4.9 it does explain collaboration diagram for use case extra withdraw. It was explain all the details of movement for system in use case extra withdraw.

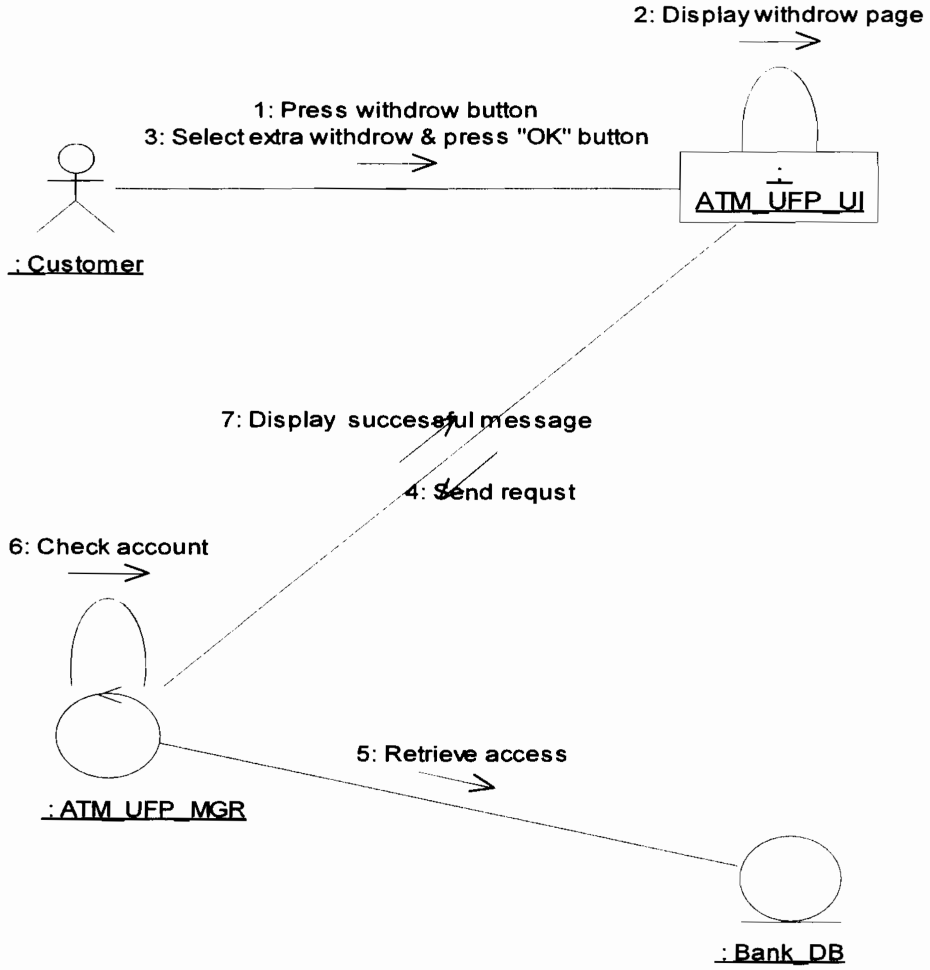


Figure 4. 11 Extra Withdraw Collaboration Diagram

4.5 CLASS DIAGRAM

According Berardi, Calvanese, & Giacomo (2005) class diagrams are the mainstay of object-oriented analysis and design. Class diagrams show the classes of the system, their interrelationships (including inheritance, aggregation, and association), and the operations and attributes of the classes.

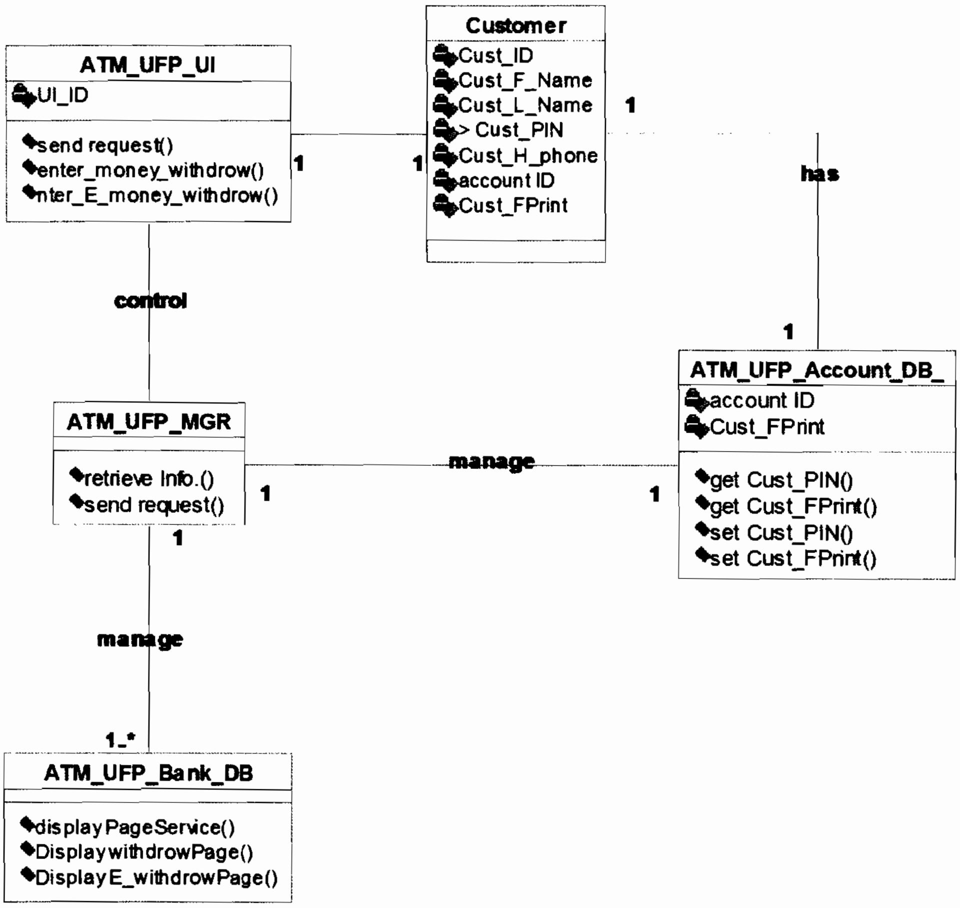


Figure 4. 12 Class Diagram for ATM_UFP

The class diagram of the system was illustrated in figure 4.12. The class diagram content six classes that represented are customer; and two entities for account information and bank data base.

4.6 SYSTEM INTERFACE

Login Interface

The bank gives customers credit card and PIN code for use it with ATMs of the Bank, or even of the other banks, In ATM_UFP customer has two ways to enter the system, credit card or fingerprint as illustrated in figure 4.13.

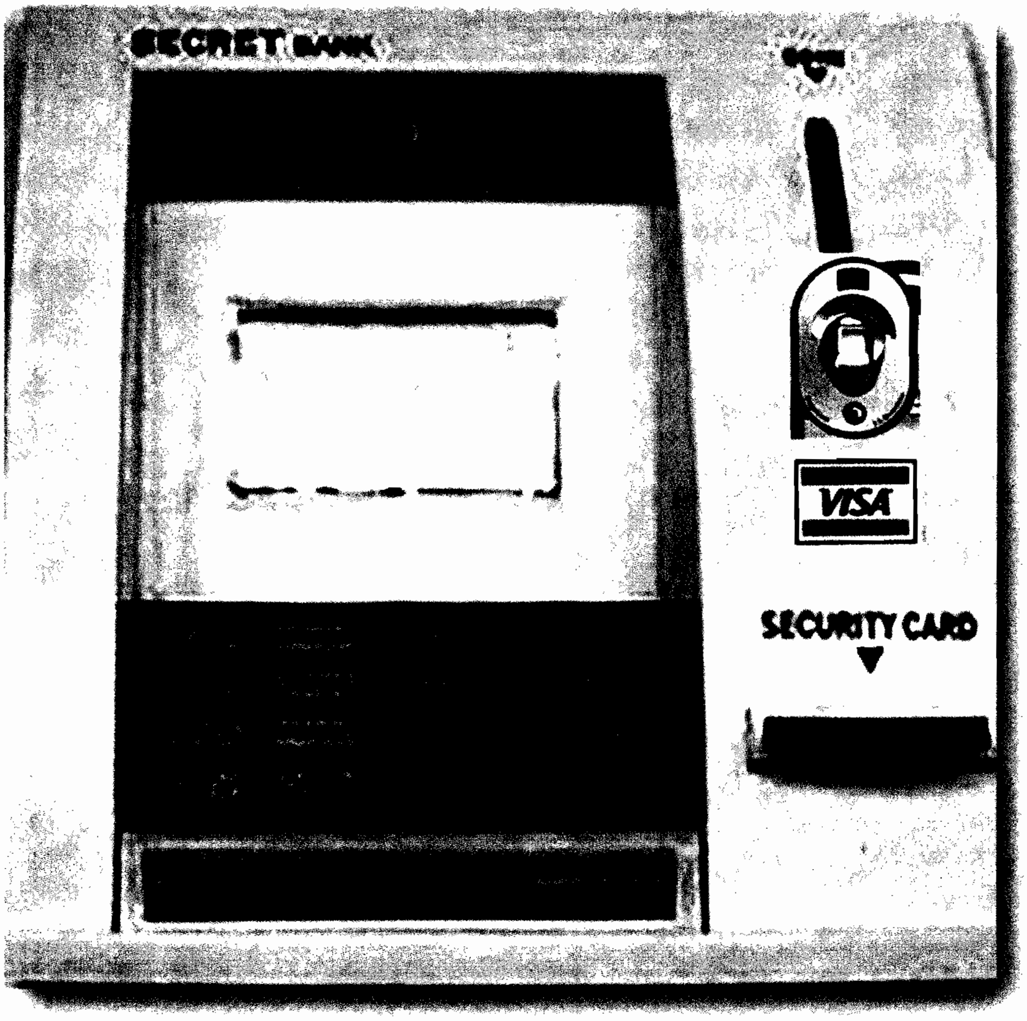


Figure 4. 13 Login Interface

Account Manage Interface

Through this interface the customer can mange his/her an account; he/she can withdraw, deposit, and transfer or any service provided by the Bank as illustrate in figure 4.14. This interface will display when customer enter in both way (credit card or fingerprint).

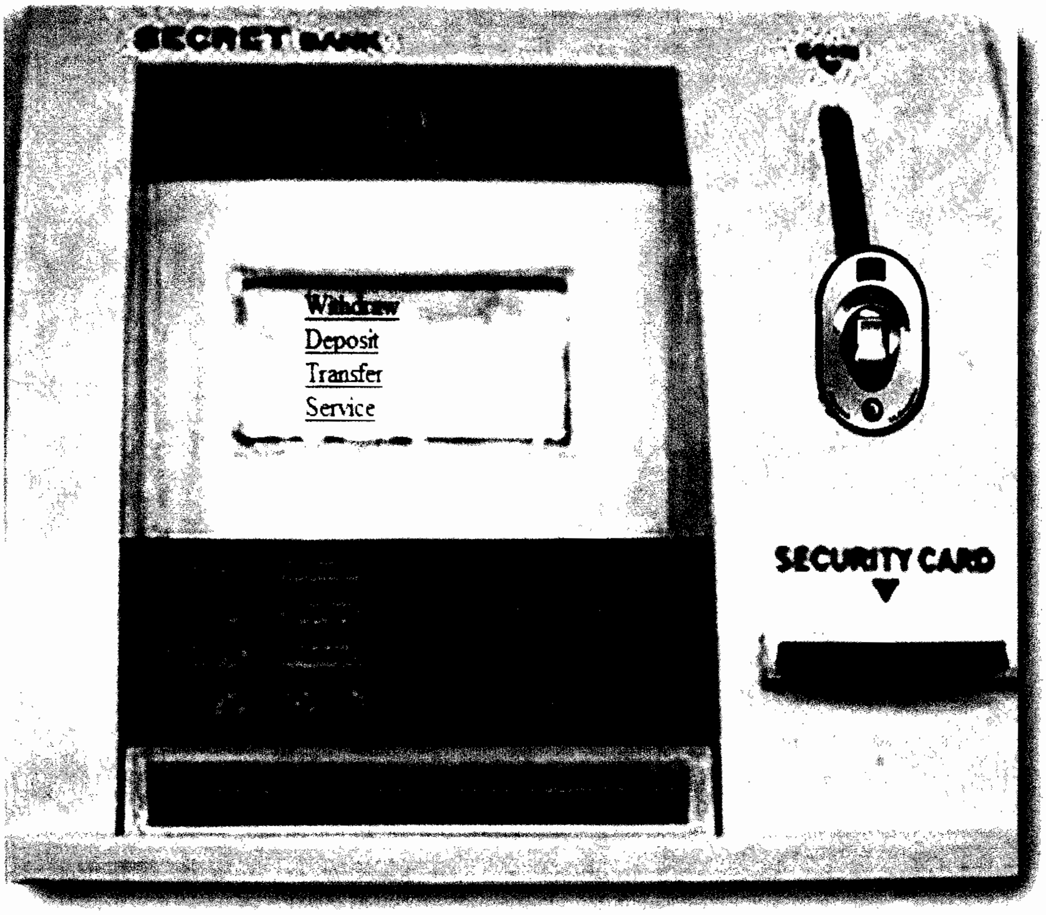


Figure 4. 14 Account Manage Interface

Withdraw Interface

This interface will display when the customer enter via using credit card only. The customer can select any number he/she need to withdraw, or he/she can choose the optional about other number to enter the amount he/she need to withdraw as shown in figure 4.15.

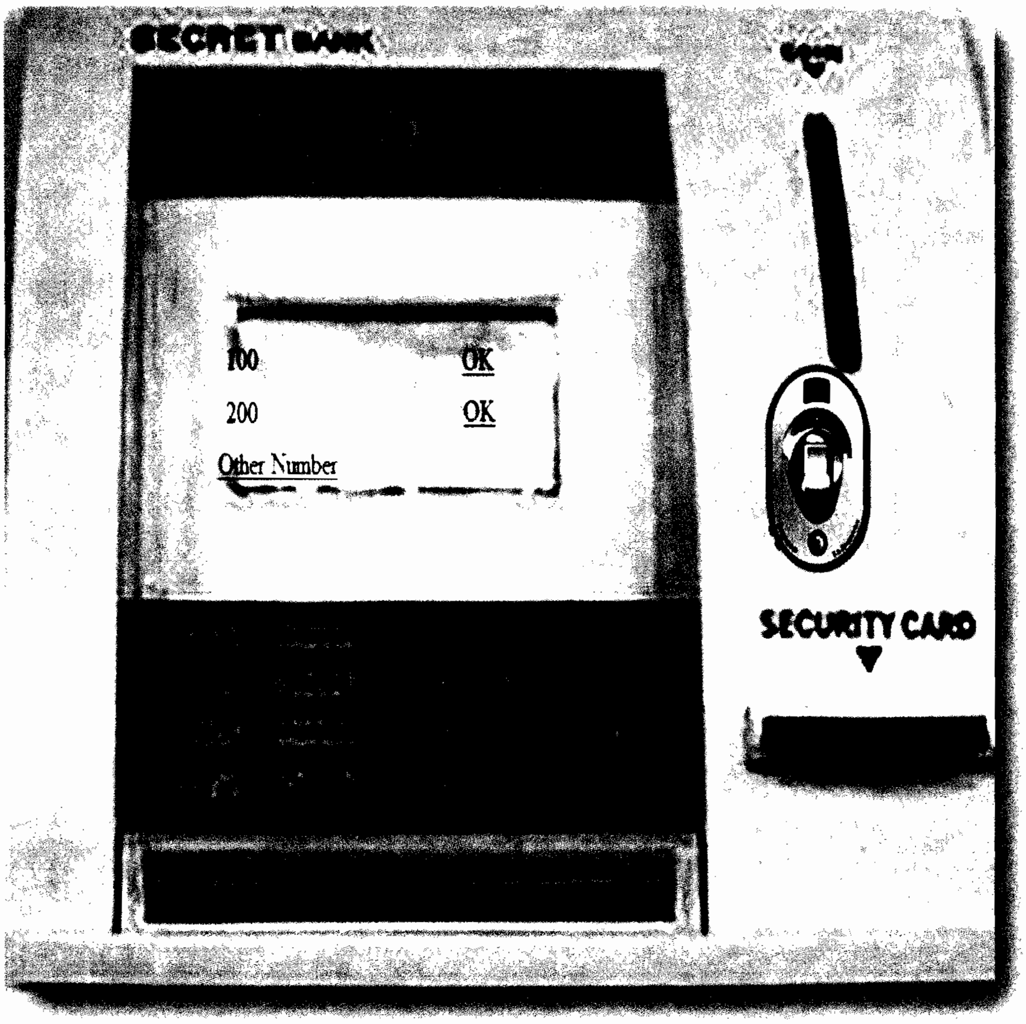


Figure 4. 15 Withdraw Interface

Withdraw Other Amount Interface

In normal way the customer can enter any amount he/she needs to withdraw (not more than 1500 RM) as shown in figure 4.16.

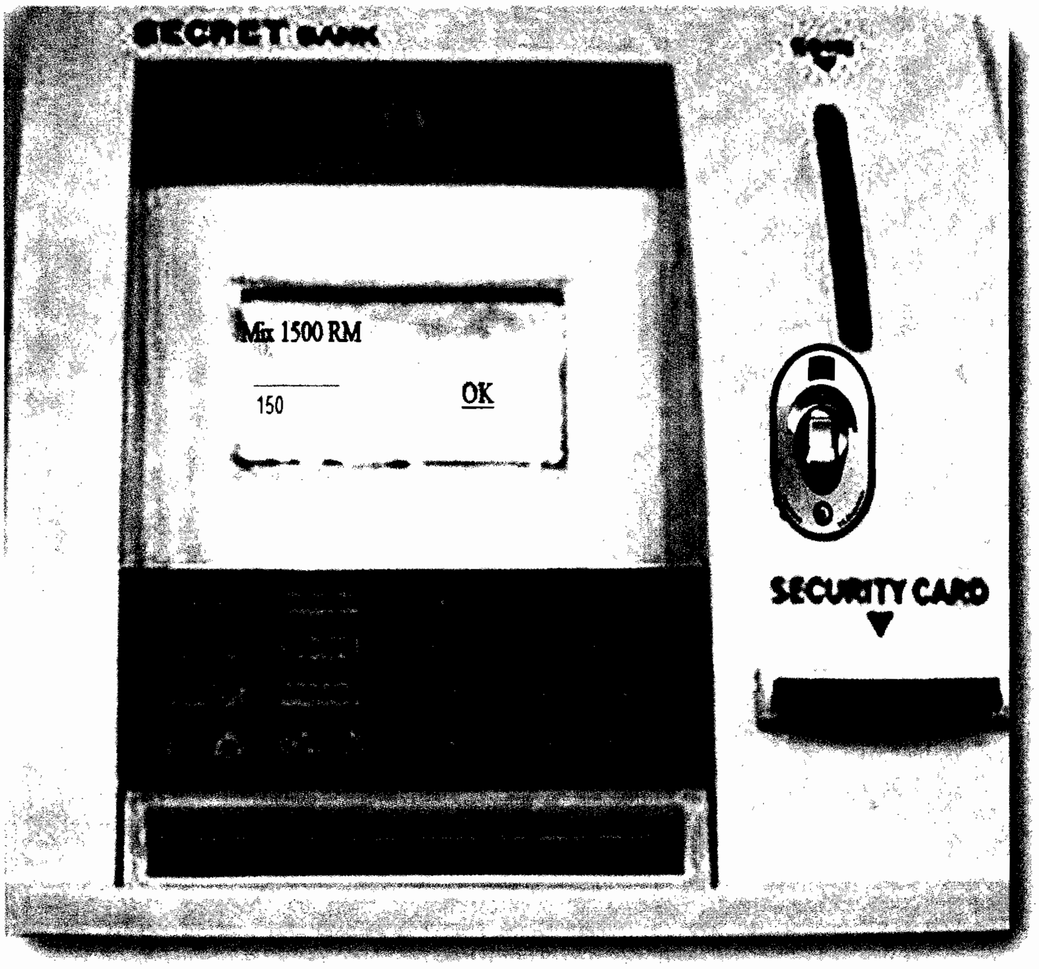


Figure 4. 16 Withdraw Other Amount Interface

Login with Fingerprint Interface

The customer can use fingerprint technique to enter the ATM system, if he/she forgets the private PIN code as shown in figure 4.17.

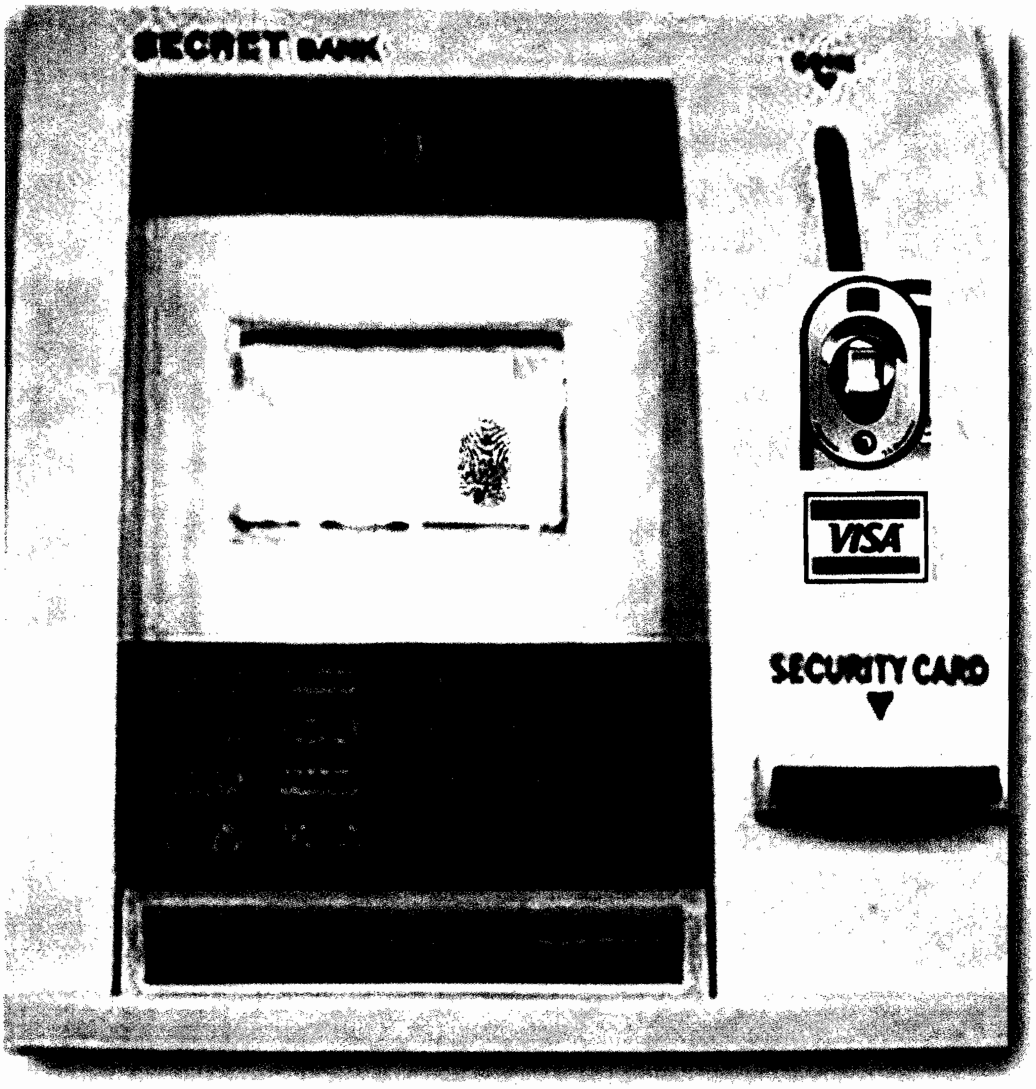


Figure 4. 17 Login with Fingerprint Interface

Withdraw with Extra Amount Interface

The withdraw interface, after customer enter through use his/her fingerprint, have extra optional given to customer to withdraw huge amount as illustrate in figure 4.18.

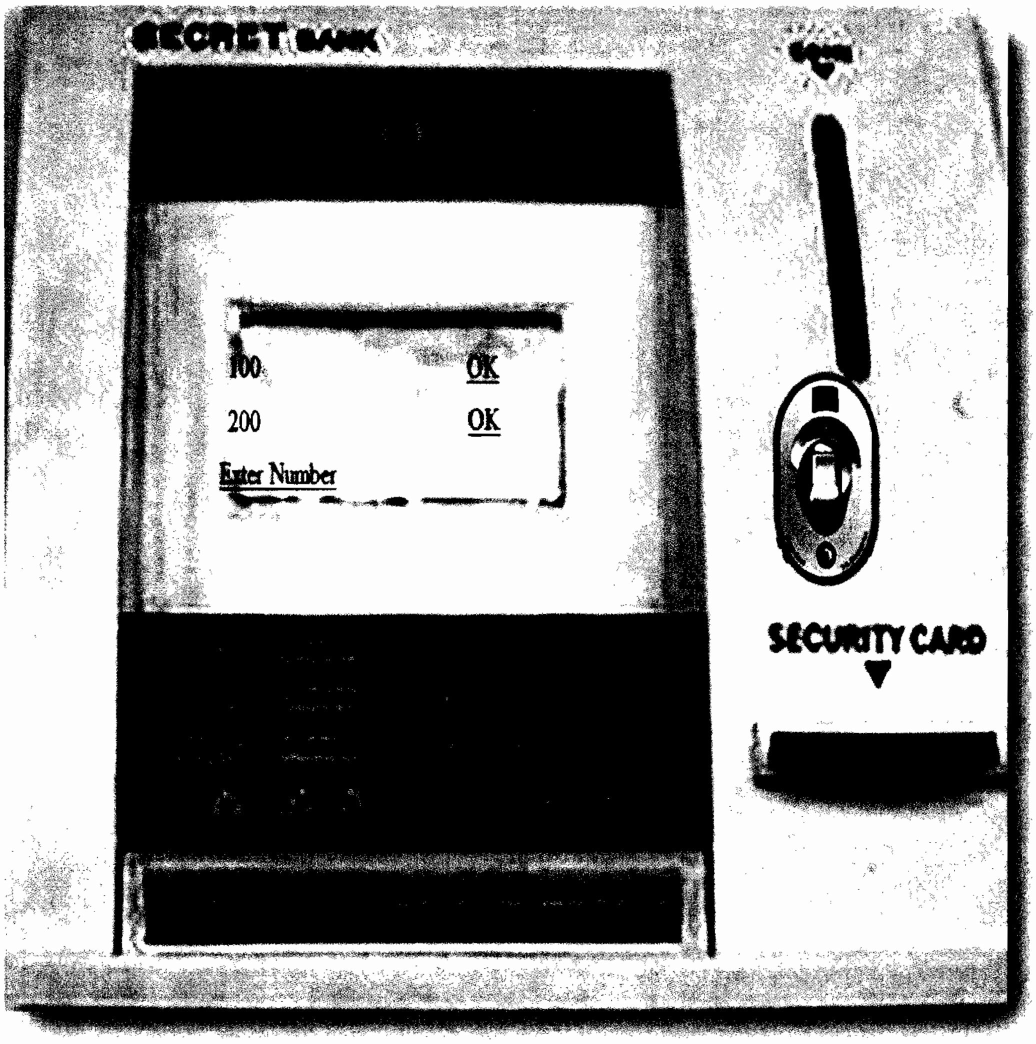
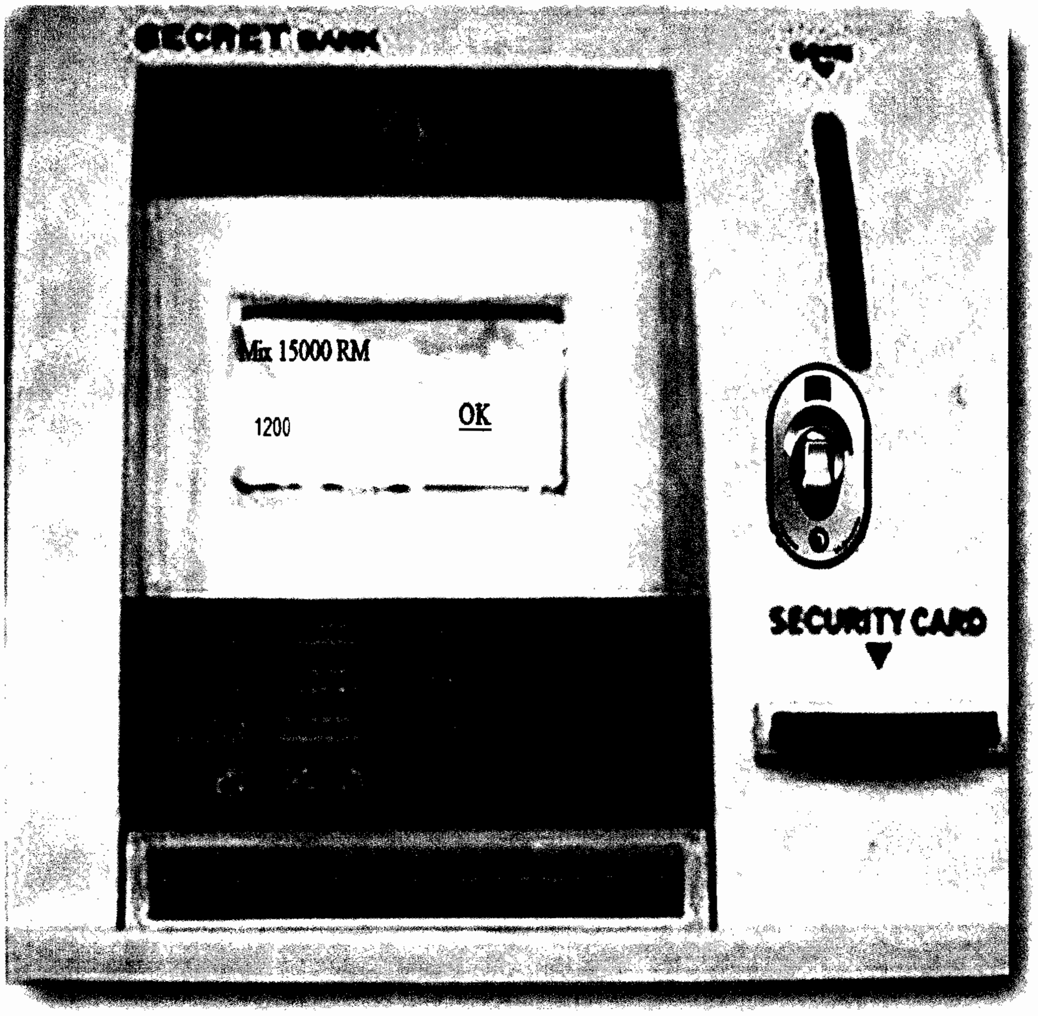


Figure 4. 18 Withdraw with Extra Amount Interface

Extra Withdraw Interface

The customer can enter any amount he/she needs to withdraw (not more than 15000 RM) as shown in figure 4.19.



Max 15000 RM

1200

Figure 4. 19 Extra Withdraw Interface

Successful Operation Interface

After finishing the withdraw operation, the system will display message for he/she to inform that the operation is successful as shown in figure 4.20.

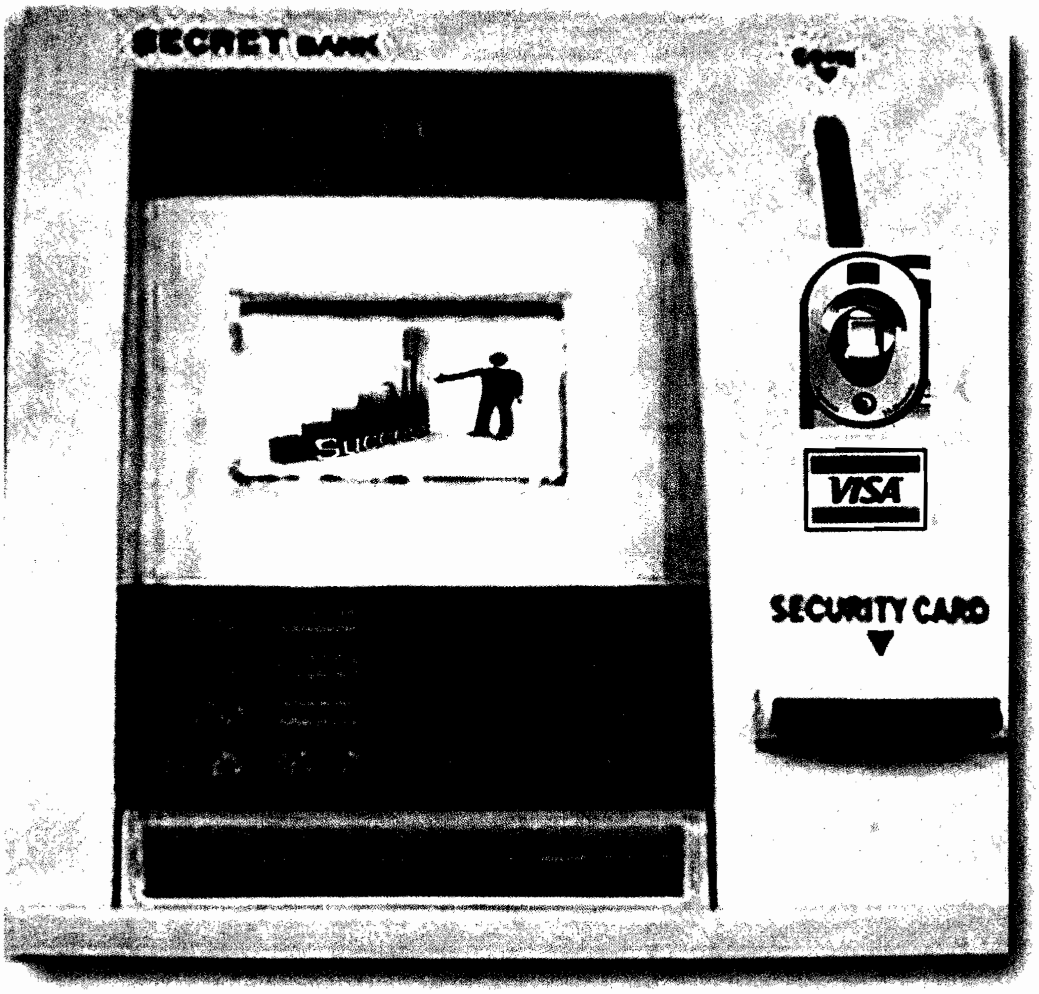


Figure 4. 20 Successful Operation Interface

4.7 SUMMARY

This chapter are content the analysis about the system, the requirement, use cases and the entire diagram which describe the function of ATM_UFP system. The result of running the system illustrated that target of the study is done successfully. The output of chapter four is the developed prototype and the design of interface for the prototype.

CHAPTER 5

EVALUATION & RESULTS

The main aim of this chapter is to discuss the evaluation of the Automatic Teller Machines Using Fingerprint (ATM_UFP). A usability test is one of the most fundamental methods in usability evaluation, because real test users are asked to use the product. The moderator of the test gives predetermined test tasks one at a time to the test user, who in turn performs the tasks with the user interface (Nielson, 2002). The users are usually asked to think while doing the test tasks. Interviews are also often used in order to gain more insight into the user's actions with the interface.

The evaluation is based on usability testing by using System Usability Scale (SUS) proposed by Brooke (Bangor, Kortum & Miller, 2008). The questioners have two part the first one talk about General information and the second one system aspects have some of categories are perceived usefulness, perceived ease of use, Attribute of usability and user Satisfaction.

5.1 EVALUATION TECHNIQUES

The system evaluation measures the system usability that achieved the proposed objective which to improve the interaction between the customers and Automatic Teller Machines Using Fingerprint (ATM_UFP). The questionnaire consists of two section, general information and evaluation of user, the prototype was assessed through a sample consists of forty customers. The Statistical Package for Social Sciences version 13 has been used to perform descriptive statistics analysis for the collected data. Also the (SPSS) used to determine the frequencies of each question; however, the histogram has been provided in this evaluation.

Table 5. 1 Summary of Demographics Data

Gender	**Frequency**	**Percentage (%)**
Male	25	62.5%
Female	15	37.5%
Age		
20-30	22	55%
30-40	8	20%
Above 40	10	25%
Education		
PhD	2	5%
Master	9	22.5%
Degree	22	55%
Diploma	5	12.5%
High School	2	5%

As illustrate in Table 5.1, 25 (62.50%) of the respondents were male and 15 (37.50%) were female. Most of the respondents 22 (55%) have degree certificate and the minority of them are have PhD and high school certificate 2 (5%). The remaining 9 (22.5%) are Master certificate and 5 (12.5) have diploma certificate. Finally, the majority of simple age is 20-30 years with 22 (55%).

5.2 EVALUATION OF USER

Measure the performance of the system depends mainly on the assessment of users and as described earlier that the system is interested to ATM using fingerprint. Each questions in the measurement has a rate from 1 - 5 (1 mean Strongly Disagree, 2 mean Disagree, 3 mean Neutral, 4 mean Agree, and 5 mean Strongly Agree).

As describe in Table 5.2 the survey focus on two dimension the usefulness and ease of use; the result illustrates that the mean for every dimension is around 3.9.

Table 5. 2 attributive statistics for dimensions

Dimension	Number	Mean
Perceived Usefulness	40	3.8888
Perceived Ease of Use	40	3.8500

As shown in tables 5.3 there is an indicate details about the mean for each questions. All the details for the questionnaire are existed in appendix C.

Table 5. 3 Illustrate Statistics for All Elements

PERCEIVED USEFULNESS		Mean
Q1	Using ATM_UFP helps me to be more effective	3.8000
Q2	Using ATM_UFP helps me to be more productive.	3.7667
Q3	Using ATM_UFP saves my time when I use it	3.8333
Q4	Using ATM_UFP would enhance my effectiveness	3.7333
Q5	Using ATM_UFP would make it easier to do my tasks	4.1333
Q6	ATM_UFP was competency increased security of ATM system	4.0667
PERCEIVED EASE OF USE		**Mean**
Q7	ATM_UFP is simple to use.	3.8000
Q8	ATM_UFP is very friendly to use	4.0667
Q9	It requires the fewest steps possible to accomplish what I want to do with it	3.8000
Q10	I can use it without written instructions	4.1333
Q11	I don't notice any inconsistencies as I use ATM_UFP	3.4333
Q12	I can use ATM_UFP successfully every time.	3.8667

The analysis for question one as illustrate in table 5.4 describes four level of response the high degree focus on level agree with (55%).

Table 5. 4 **Q1** Using ATM_UFP helps me to be more effective

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	disagree	2	5.0	5.0	5.0
	natural	9	22.5	22.5	27.5
	agree	22	55.0	55.0	82.5
	strongly agree	7	17.5	17.5	100.0
	Total	40	100.0	100.0	

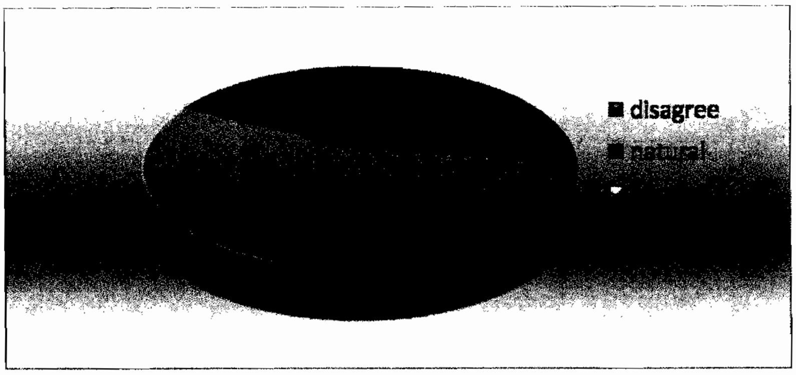


Figure 5. 1 Statistics for question one

The analysis for question two as shown in table 5.5 describes four level of response, agree level is the first with (37.5%) meant (15) users gave (4), and then the second level is natural with (35%) meant (14) users give (3). Three of users disagree oppose with (8) users give strongly agree.

Table 5. 5 **Q2** Using ATM_UFP helps me to be more productive.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	disagree	3	7.5	7.5	7.5
	natural	14	35.0	35.0	42.5
	agree	15	37.5	37.5	80.0
	strongly agree	8	20.0	20.0	100.0
	Total	40	100.0	100.0	

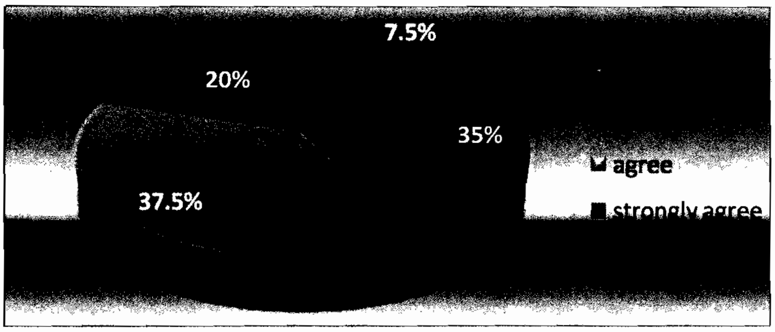


Figure 5. 2 Statistics for question two

The analysis for question three as shown in table 5.6 and figure 5.3 describe four level of response, agree level is the first with (35%) meant (14) users gave (4) degree to save time, also, (12) users (30%) strongly agree give to the system for save time; five of users disagree with that in (12.5%) but (9) of users are natural with that in (22.5%).

Table 5. 6 **Q3** Using ATM_UFP saves my time when I use it

		Frequency	**Percent**	**Valid Percent**	**Cumulative Percent**
Valid	disagree	5	12.5	12.5	12.5
	natural	9	22.5	22.5	35.0
	agree	14	35.0	35.0	70.0
	strongly agree	12	30.0	30.0	100.0
	Total	40	100.0	100.0	

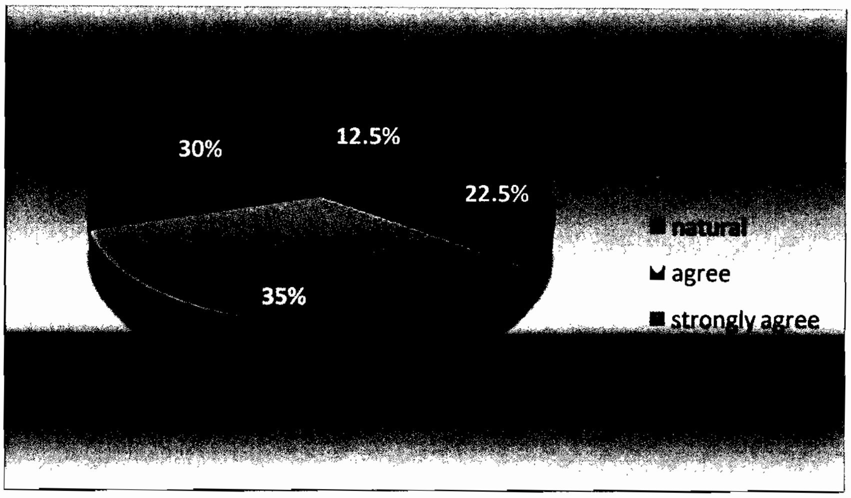


Figure 5. 3 Statistics for question three

The analysis for question four as shown in table 5.7 and figure 5.4 describes four level of response, agree level is the first with (60%) meant (24) users gave (4), then the second level is natural with (20%) meant (8) users give (3). Tows of users disagree and others strongly agree with same percent (10%).

Table 5.7 **Q4** Using ATM_UFP would enhance my effectiveness

		Frequency	**Percent**	**Valid Percent**	**Cumulative Percent**
Valid	disagree	4	10.0	10.0	10.0
	natural	8	20.0	20.0	30.0
	agree	24	60.0	60.0	90.0
	strongly agree	4	10.0	10.0	100.0
	Total	40	100.0	100.0	

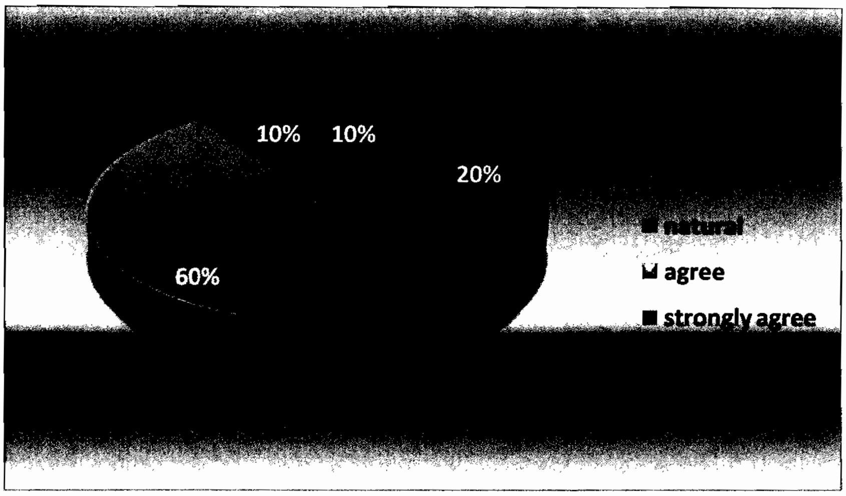


Figure 5. 4 Statistics for question four

The analysis for question five as shown in table 5.8 and figure 5.5 illustrate three level of response, the agree level is the first with (45%) meant (18) users gave (4), then the second level is strongly agree with (30%) meant (12) users give (5). Ten of users natural with (25%) that mean the system are easier to do tasks.

Table 5. 8 **Q5** Using ATM_UFP would make it easier to do my tasks

		Frequency	**Percent**	**Valid Percent**	**Cumulative Percent**
Valid	natural	10	25.0	25.0	25.0
	agree	18	45.0	45.0	70.0
	strongly agree	12	30.0	30.0	100.0
	Total	40	100.0	100.0	

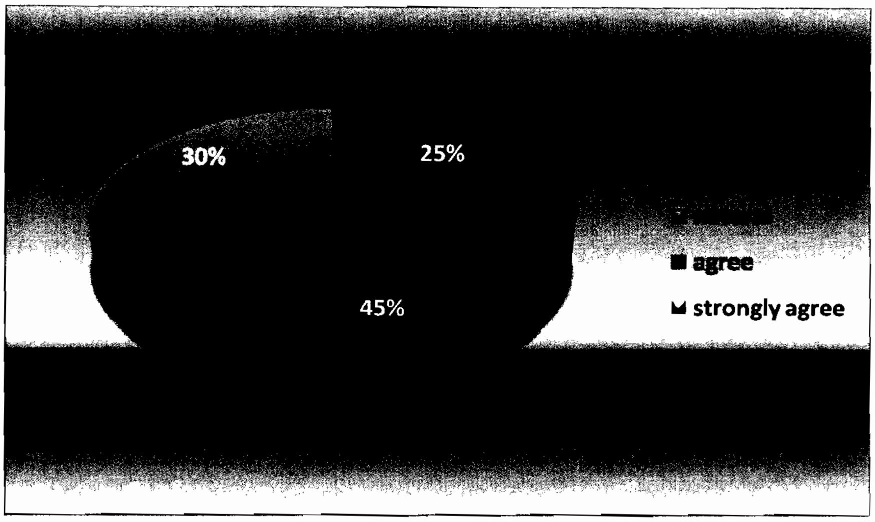


Figure 5. 5 Statistics for question five

The analysis for question six as shown in table 5.9 and figure 5.6 illustrate three level of response, the agree level is the first with (50%) meant (20) users gave (4), then the second level is strongly agree with (27.5%) meant (11) users give (5). Nine of users give natural with (22.5%). That mean the system was secured for ATM more than before.

Table 5. 9 **Q6** ATM_UFP was competency increased security of ATM system

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	natural	9	22.5	22.5	22.5
	agree	20	50.0	50.0	72.5
	strongly agree	11	27.5	27.5	100.0
	Total	40	100.0	100.0	

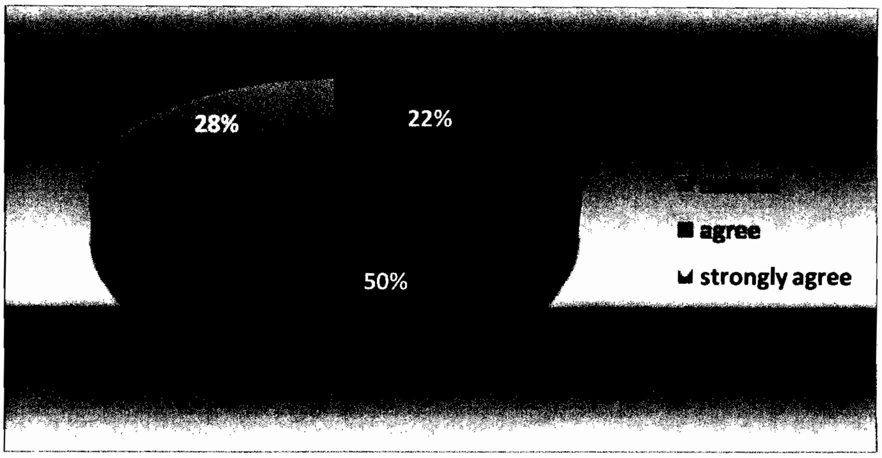


Figure 5. 6 Statistics for question six

The analysis for question seven as shown in table 5.10 and figure 5.7 describes four level of response, the agree level is the first with (37.5%) meant (15) users gave (4), then the second level is natural with (30%) meant (12) users give (3). Four of users disagree in (10%) and (9) users give strongly agree in (22.5%), that mean the system are simple to use.

Table 5. 10 **Q**7 ATM_UFP is simple to use

		Frequency	**Percent**	**Valid Percent**	**Cumulative Percent**
Valid	disagree	4	10.0	10.0	10.0
	natural	12	30.0	30.0	40.0
	agree	15	37.5	37.5	77.5
	strongly agree	9	22.5	22.5	100.0
	Total	40	100.0	100.0	

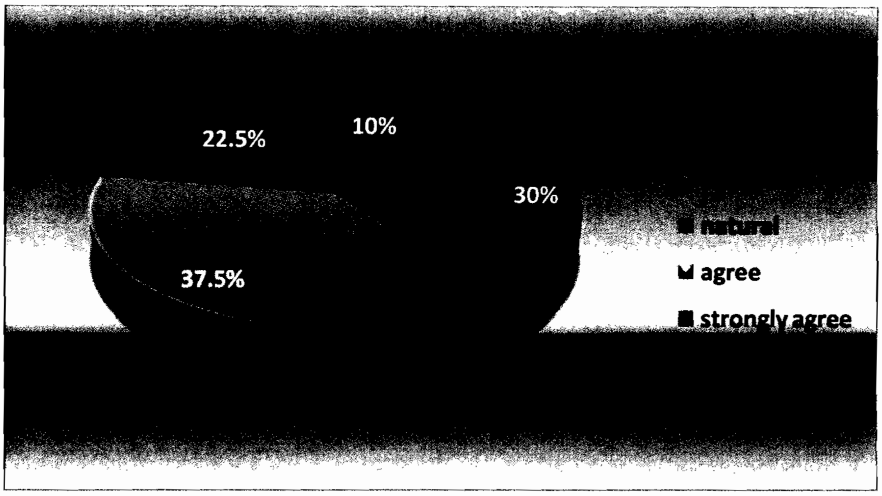


Figure 5. 7 Statistics for question seven

The analysis for question eight as shown in table 5.11 and figure 5.8 describes four level of response, the natural level is the first with (45%) meant (18) users gave (3), then the second level is agree with (35%) meant (14) users give (4). Four of users disagree and others strongly agree with same percent (10%) that mean the system is friendly.

Table 5. 11 **Q8** ATM_UFP is very friendly to use

		Frequency	**Percent**	**Valid Percent**	**Cumulative Percent**
Valid	disagree	4	10.0	10.0	10.0
	natural	18	45.0	45.0	55.0
	agree	14	35.0	35.0	90.0
	strongly agree	4	10.0	10.0	100.0
	Total	40	100.0	100.0	

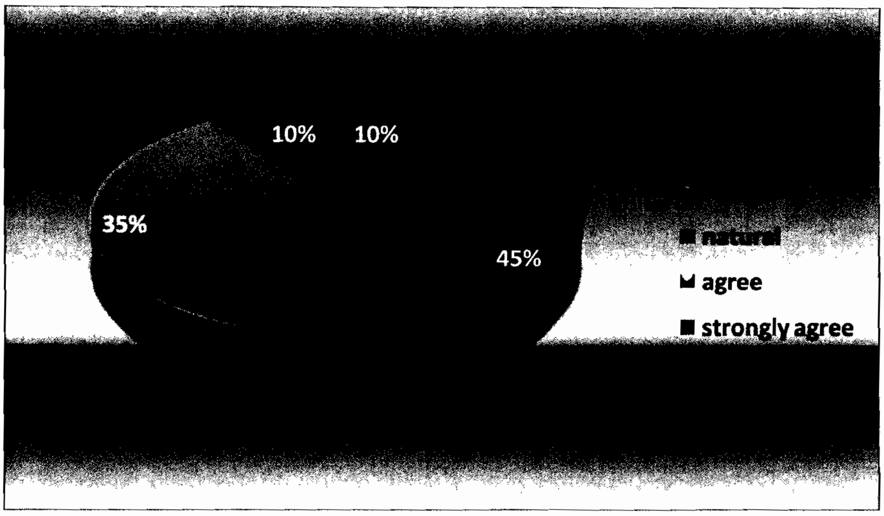


Figure 5. 8 Statistics for question eight

The analysis for question nine as shown in table 5.12 and figure 5.9 illustrate three level of response, the strongly agree level is the first with (37.5%) meant (15) users gave (5), then the second level is agree with (32.5%) meant (13) users give (4). Twelve of users give natural with (30%), that mean the system are very shortly to accomplish any task.

Table 5. 12 **Q9** requires the fewest steps possible to accomplish what I want to do with it

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	natural	12	30.0	30.0	30.0
	agree	13	32.5	32.5	62.5
	strongly agree	15	37.5	37.5	100.0
	Total	40	100.0	100.0	

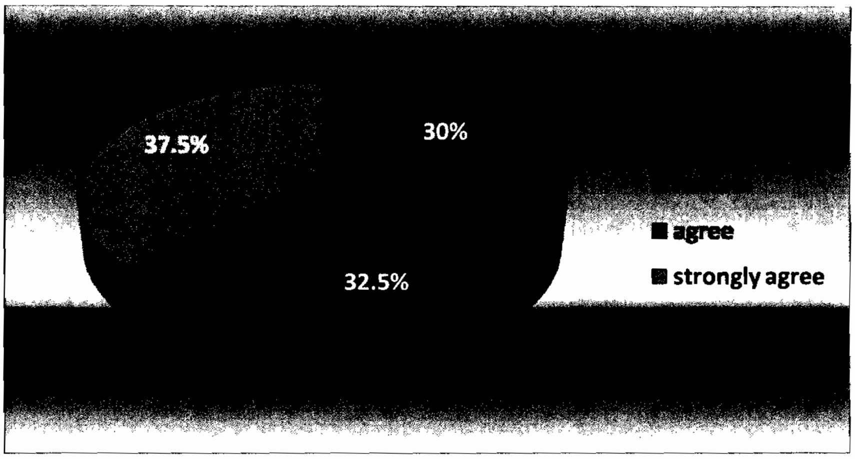


Figure 5. 9 Statistics for question nine

The analysis for question ten as shown in table 5.13 and figure 5.10 describes four level of response, the strongly agree level is the first with (35%) meant (14) users gives (5), then the second level is natural with (25%) meant (10) users gives (3). Six of users disagree in (15%) and (10) users give agree in (25%), that mean the system can use without written instructions.

Table 5. 13 **Q10** I can use it without written instructions

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	disagree	6	15.0	15.0	15.0
	natural	10	25.0	25.0	40.0
	agree	10	25.0	25.0	65.0
	strongly agree	14	35.0	35.0	100.0
	Total	40	100.0	100.0	

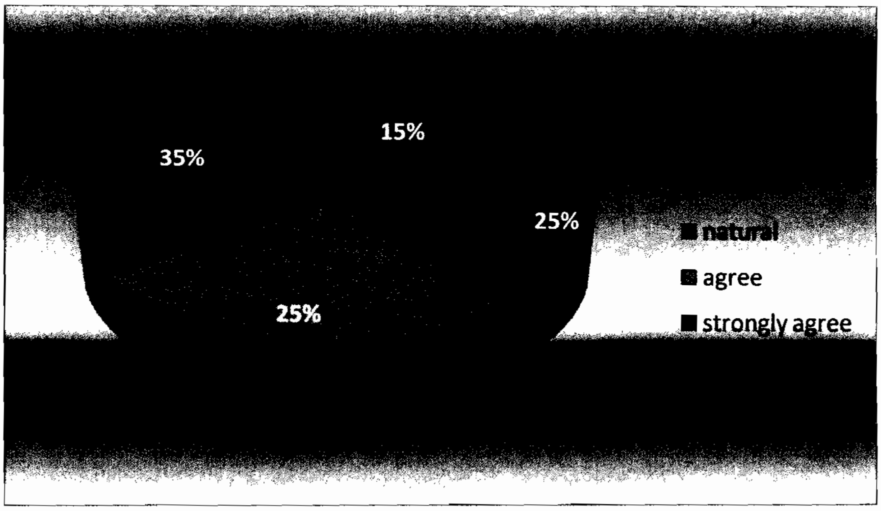


Figure 5. 10 Statistics for question ten

The analysis for question eleven as shown in table 5.14 and figure 5.11 describes four level of response, the strongly agree level is the first with (37.5%) meant (15) users gave (5), at the same time, the second level is natural with (37.5%) meant (15) users give (3). Twos of users disagree in (5%) and (8) users give agree in (20%), that mean there aren't inconsistencies in the system.

Table 5. 14 **Q11** I don't notice any inconsistencies as I use ATM_UFP

		Frequency	**Percent**	**Valid Percent**	**Cumulative Percent**
Valid	disagree	2	5.0	5.0	5.0
	natural	15	37.5	37.5	42.5
	agree	8	20.0	20.0	62.5
	strongly agree	15	37.5	37.5	100.0
	Total	40	100.0	100.0	

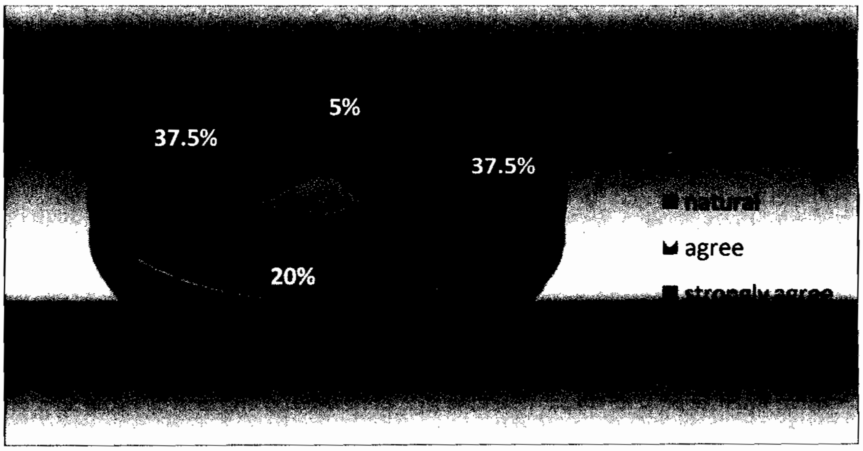


Figure 5. 11 Statistics for question eleven

The analysis for last questions as shown in table 5.15 and figure 5.12 describes three level of response, the agree level is the first with (47.5%) meant (19) users gave (4), then the second level is strongly agree with (32.5%) meant (13) users give (5). Eight of users give natural with (20%), that mean the system are successfully to use every time.

Table 5. 15 **Q12** I can use ATM_UFP successfully every time.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	natural	8	20.0	20.0	20.0
	agree	19	47.5	47.5	67.5
	strongly agree	13	32.5	32.5	100.0
	Total	40	100.0	100.0	

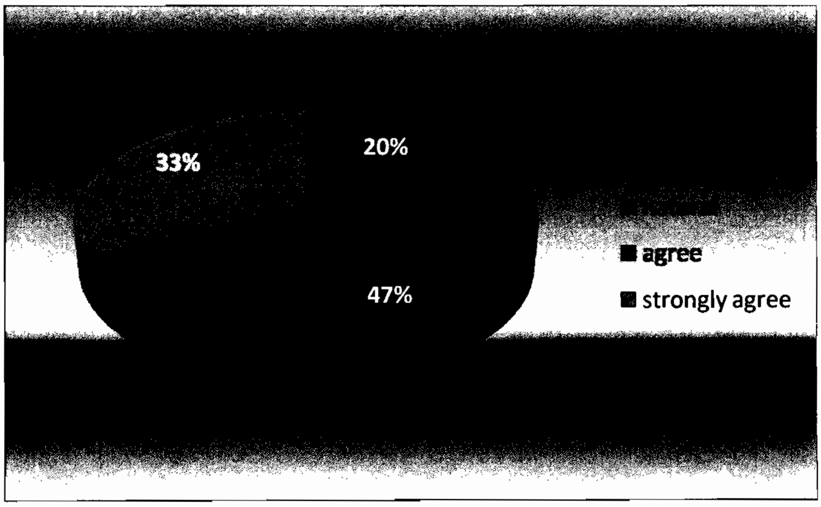


Figure 5. 12 Statistics for question twelve

5.3 SUMMARY

Evaluation takes part in an important part in the development process and can uncover usability deficits early during the design. In further works, more usability tests for the re-design application with real customer should be conducted. Interviews with these test persons and evaluation to reach more people will help to shape application and better meet the user's opinion, requirements and expectations. The overall results were encouraging but improvement is definitely needed. The Cronbach’s Alpha values range from .701 to .842 and are all above 0.7 which is considered as acceptance.

CHAPTER 6

CONCLUSIONS AND RECOMMENDED FURTHER STUDY

Beginning the chapter with a discussion of the outcome found in chapter four and it's density with prior research works that either support or disagree with result of this research labor. It's followed by conclusions that are drawn from this research labor. Several implications for both research and practice emerged and are discussed in following section, and then recommendations for future research are made, finally, the conclusion of the study.

6.1 DISCUSSION

The purpose of this research is to identify the following:

- Can develop security system for ATM machine by using fingerprint technique?

Drawing on the research result, will discusses how the finding support the objective of this study. This study highlighting on the Automatic Teller Machines (ATM) is an electronic banking outlet, which allows customers to complete basic transactions without the aid of a branch representative or teller (Qadrei & Habib, 2009). Nowadays, using the ATM which provides customers with the convenient banknote trading is very common.

However, the financial crime case rises repeatedly in recent years; a lot of criminals tamper with the ATM terminal and steal user's credit card and password by illegal means. Once user's bank card is lost and the password is stolen, the criminal will draw all cash in the shortest time, which will bring enormous financial losses to customer. How to carry on the valid identity to the customer becomes the focus in current financial circle (Yang & Mi, 2010).

Using credit card and password cannot verify the client's identity exactly. Biometrics based authentication is a potential candidate to replace password-based authentication (Uludag, Pankanti, Prabhakar & Jain, 2004). In recent years, the technique that the fingerprint recognition continuously updated, which has offered new verification, the original password authentication method combined with the biometric identification technology verify the clients' identity better and achieve the purpose that use of ATM machines improve the safety effectively. That's what the study aims to achieve

Objective 1:

In this research developed the system requirements to improve security system for ATM machine by using fingerprint technique As a result, have been identified the following requirements.

Customer enters the system by using credit card and PIN code, system will display main page with all services, it is then possible to accomplish banking transactions such as withdraw, deposit, and others. If the customer forgets PIN code or lost it, then he/she can used fingerprint technique to enter the system, when put he/she finger on the finger scan, system will verify his/her finger with the database to open the system. After customer enter the system by using fingerprint technique the system display same main page with all the services but he/she have an additional option when he/she enter withdraw page. The additional option in withdraw page is extra withdraw, extra withdraw is optimal allows the customer to withdraw huge amount (less than 15.000 RM), this optional was active when the customer enter system by fingerprint technique.

Objective 2:

Technical fingerprint gives any possibilities of an electronic high-security. The ATM system needs to be more secure to the customer by providing a high protection level for accomplish banking transactions. In this study, use the fingerprint technology on the entry of customer on the ATM system. So that means any person cannot penetrating account of any other person.

In addition, the use of fingerprint technology at ATMs give high confidence for the client to conduct banking transactions through ATM, on the other hand, the bank administration have a higher confidence about ATM protection, which makes it to allows more options on ATM. The system was implemented using ASP.net environment with C# language, and the database designed by using SQL.

Objective 3:

The security features were importance to largely for the stability and reliability. ATM system based on fingerprint recognition was give more advantages of the stability and reliability. Additional, the system also contains the original verifying methods which were inputting owner's password. The whole system was built on the technology of embedded system which makes the system more safe, reliable and easy to use.

All above depend on the evaluating of the system. The evaluation is based on usability testing by using System Usability Scale (SUS) proposed by Brooke (Bangor, Kortum & Miller, 2008). Prototype was assessed through a sample consists of thirty customers; and the results has been positive.

6.2 LIMITATION

For this research, the study was focused on construction of prototype ATM using fingerprint (ATMUFP) helps the customer to provide the best services and high protection of their accounts; additional services in this system is extra withdraw, Which gives the customer to withdraw a huge amount. Furthermore, improve security system for ATM was reducing the threats which have exposed customer accounts through ATMs.

6.3 CONTRIBUTION

This research obtained the following contributions in the ATM security, internet banking fields:

a) Use of the facilities in the area of biometric recognition technologies to development of automatic teller machines.

b) Give a picture of possible solutions to get rid of cases of theft or loss of ATM cards or password, and procedures of the bank to change the password for the client.

c) It uses the facilities in the area of information and communication technology to create stability in the electoral process in modern societies.

6.4 FUTURE WORK

The spread of the computer and the growth of the number of users quickly, putting information technology in the areas of new research and development vehicle. Accompanied by the continuous development and facility earned this area the flexibility to cope with all the sciences. Through this research was to highlight on an important aspect in the life of society through dealing with bank accounts through ATMs and problems that occur with it. It is recommended that, the future research in this field covers the followings:

a. It can be development of the ATM system and make it absorb more of the banking services that need to protect highest, and reliability by the customer and the bank.

b. The use of fingerprint technology in the ATM system could open the door to facilitate the provision of e-Government Services; through facilitating the access of older retirees paid via ATMs using the fingerprint.

6.5 CONCLUSION

Automatic Teller Machines is an electronic banking outlet, which allows customers to complete basic transactions without the aid of a branch representative or teller. It is an unattended computer terminal that performs basic teller functions when a cardholder inserts a card into the ATM and enters the correct PIN. Typical functions include dispensing cash, accepting deposits and loan payments, and accepting account transfers and inquiries.

When reviewing ATM security, a pragmatic approach is a risk-based one. Especially in today's economic climate, it makes little sense to spend money on ATM security measures that don't address real business risks. There are many ways for theft ATM such as skimming and card theft and so on.

A widely held concept among security professionals is that security for its own sake is not a wise business investment. Before investing in security measures, an organization should undertake a risk assessment to identify possible threats, their likelihood and their possible impact.

Biometric technology is consists of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. In computer science, in particular, biometrics is used as a form of identity access management and access control. It is also used to identify individuals. The main motivation for employing biometric technology is to efficiently and effectively control access by authenticating users via their unique biometric characteristics such as fingerprint technique.

Through this study was designed ATM system using fingerprint technique to provide the highest protection for customer accounts. System was developing by using C# language under ASP.net environment. Moreover, was evaluation based on usability testing by using System Usability Scale (SUS) proposed by Brooke and prototype was assessed through a sample consists of forty customers; and the results has been positive.

Finally, the rapid development of information and communication technology accelerates the growth of many areas provide service facilities, corresponds the need to develop protection techniques through the use of features unique to humans such as biometric technology, these features make services more stable and reliable.

REFERENCES

Abdulahi, R., & Demisse, A. (2009). Challenges of E-Payment Service in Commercial *Bank of Ethiopia.* Paper presented at the Wuhan Management and Service Science, 2009. MASS '09. , 1-4.

Alhir, S. S. (2003). *Learning UML*: O'Reilly & Associates, Inc. Sebastopol, CA, USA.

Bangor, A., Kortum, P. T., & Miller, J. T. (2008). An empirical evaluation of the system usability scale. *International Journal of Human-Computer Interaction, 24*(6), 574-594.

Beck, K., & Fowler, M. (2000). *Planning extreme programming*. Boston, MA, USA: Addison-Wesley Longman Publishing Co. Inc.

Berardi, D., Calvanese, D., & De Giacomo, G. (2005). Reasoning on UML class diagrams. *Artificial Intelligence, 168*(1-2), 70-118.

Caparroz, R., Martuscelli, P., Scherer-Neto, P., Miyaki, C. Y., & Wajntal, A. (2006). Genetic variability in the Red-tailed Amazon (Amazona brasiliensis, Psittaciformes) assessed by DNA fingerprinting. *Revista Brasileira de Ornitologia, 14*(1), 15-19.

Cavoukian, A. (1999). *Consumer Biometric Applications: A Discussion Paper*: Information and Privacy Commissioner/Ontario. Retrieved 28 November 2010, from http://www.ontla.on.ca/library/repository/mon/10000/ 211727.pdf

Cavoukian, A., & Stoianov, A. (2007). Biometric encryption. *Biometric Technology Today, 15*(3), 11.

Chung, L., & do Prado Leite, J. (2009). On non-functional requirements in software engineering. *Conceptual Modeling: Foundations and Applications*, 363-379.

Coventry, L., De Angeli, A., & Johnson, G. (2003a). Biometric verification at a self service interface. *Contemporary Ergonomics*, 247-252.

Coventry, L., De Angeli, A., & Johnson, G. (2003b). *Usability and biometric verification at the ATM interface.* Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 153-160, (New York. ACM Press).

Darwish, A., Zaki, W., Saad, O., Nassar, N., & Schaefer, G. (2010). *Human Authentication Using Face and Fingerprint Biometrics.* Paper presented at the(Liverpool, United Kingdom), Computational Intelligence, Communication Systems and Networks (CICSyN), 274-278.

Das, R. (2005). An introduction to biometrics. *Military Technology, 29*(7), 20-27.

Dedeke, A., & Lieberman, B. (2006). Qualifying use case diagram associations. *Computer, 39*(6), 23-29.

Duan, J. (2009). *An approach for modeling business application using refined use case.* Paper presented at the ISECS (Sanya. China.) International Colloquium on Computing, Communication, Control, and Management (CCCM 2009), pp 404 - 407.

Guerette, R., & Clarke, R. (2003). Product life cycles and crime: Automated teller machines and robbery. *Security Journal, 16*(1), 7-18.

Halal, W. (2006). Technology's Promise: Highlights from the TechCast Project. *Futurist, 40*(6), 41.

Han, F., Hu, J., Yu, X., Feng, Y., & Zhou, J. (2005). A novel hybrid crypto-biometric authentication scheme for ATM based banking applications. *Advances in Biometrics*, 675-681.

Hannan, T. (2007). ATM surcharge bans and bank market structure: The case of Iowa and its neighbors. *Journal of Banking & Finance, 31*(4), 1061-1082.

Hayashi, F., Sullivan, R., & Weiner, S. (2003). *A guide to the ATM and debit card industry*: Payments System Research Dept., Federal Reserve Bank of Kansas City.

Hidano, S., Ohki, T., Komatsu, N., & Kasahara, M. (2009). *On biometric encryption using fingerprint and its security evaluation.* Paper presented at the 10th International Conference Hanoi. Control, Automation, Robotics and Vision, 2008. ICARCV 2008. pp.950-956.

IBG (2005). *Biometric market and industry overview.* Retrieved November 28, 2010,from http://www.biometricgroup.com/reports/public/CBT8_Overview.pdf

Jain, A., Hong, L., & Pankanti, S. (2000). Biometric identification. *Communications of the ACM, 43*(2), 90-98.

Jang, S. H., Kim, Y. H., Cho, S. H., Lee, J. H., Park, J. W., & Kwon, Y. H. (2003). Cortical reorganization induced by task-oriented training in chronic hemiplegic stroke patients. *Neuroreport, 14*(1), 137.

Jeong, W., Cha, M. K., & Kim, I. H. (2000). Thioredoxin-dependent hydroperoxide peroxidase activity of bacterioferritin comigratory protein (BCP) as a new member of the thiol-specific antioxidant protein (TSA)/alkyl hydroperoxide peroxidase C (AhpC) family. *Journal of Biological Chemistry, 275*(4), 2924.

Knapp, A., Koch, N., Zhang, G., & Hassler, H. M. (2004). Modeling business processes in web applications with ArgoUWE. *2004-The Unified Modelling Language*, 69-83.

Lamon, P., Nourbakhsh, I., Jensen, B., & Siegwart, R. (2005). *Deriving and matching image fingerprint sequences for mobile robot localization.* Paper presented at the Robotics and Automation, 2001. Proceedings 2001 ICRA. IEEE International Conference, Lausanne, pp. 1609-1614, (Switzerland).

Lee, M. (2006). Global ATM Security Alliance focuses on insider fraud. *ATMMarketplace, http://www. At marketplace. com/article. php? id, 7154.*

Lee, S., Choi, H., Choi, K., & Kim, J. (2008). Fingerprint-quality index using gradient components. IEEE Transactions on Information Forensics and Security, 3(4), 792-800.

Levine, D. E. (2000). Voice security: Biometrics keeps information secure. *Audio Technologies, 6*(8), 60-63.

Li, X., Liu, Z., & Jifeng, H. (2004). *A formal semantics of UML sequence diagram.* Paper presented at the Software Engineering Conference. Australia. pp168.

Matutes, C., & Padilla, A. (1994). Shared ATM networks and banking competition. *European Economic Review, 38*(5), 1113-1138.

McAndrews, J. (2003). Automated teller machine network pricing-a review of the literature. *Review of Network Economics, 2*(2), 146-158.

Nielsen, J. (2002). The usability engineering life cycle. *Computer, 25*(3), 12-22.

Olatokun, W., Gaborone, B., & Igbinedion, L. (2009). The Adoption of Automatic Teller Machines in Nigeria: An Application of the Theory of Diffusion of Innovation. *Growing Information: Part I, 6*, 373.

Overmyer, S. P., Lavoie, B., & Rambow, O. (2001). *Conceptual modeling through linguistic analysis using LIDA.* Paper presented at the (IEEE Computer Society Press, Toronto), 23rd International Conference on Software Engineering. Toronto, 12–19 Maypp. 401–410.

Peretti, K. K. (2009). DATA BREACHES: What the Underground World of "Carding" Reveals. *the Santa Clara Computer and High Technology Journal, 25*(2), 375-413.

Prabhakar, S., Pankanti, S., & Jain, A. (2003). Biometric recognition: Security and privacy concerns. *Security & Privacy, IEEE, 1*(2), 33-42.

Qadrei, A., & Habib, S. (2009). *Allocation of Heterogeneous Banks' Automated Teller Machines.* Paper presented at the (First International Conference alencia), Intensive Applications and Services, 2009. INTENSIVE '09. pp 16-24

Rhodes, K. A. (2003). *Challenges in using biometrics*. United States General Accounting Office. Retrieved 24 November 2010, from http://www.gao.gov/new.items/d031137t.pdf

Ross, A., & Jain, A. (2003). Information fusion in biometrics. *Pattern Recognition Letters, 24*(13), 2115-2125.

Sha, L., Zhao, F., & Tang, X. (2003). *Improved fingercode for filterbank-based fingerprint matching.* Paper presented at the Image Processing, 2003. ICIP 2003. Proceedings. 2003 International Conference, china.

Sommerville, I. (2007). Software Engineering. Eighth: Addison-Wesley. ISBN 0-321-31379-8.

Stavins, J. (2000). ATM fees: does bank size matter? *New England Economic Review*, 13-24.

Sugiura, A., & Koseki, Y. (1998). *A user interface using fingerprint recognition: holding commands and data objects on fingers.* Paper presented at the Proceedings of the 28th international conference on Human factors in computing systems NY, pp. 581-590, (USA).

Sullivan, R. J. (2008). Can smart cards reduce payments fraud and identity theft? *Federal Reserve Bank of Kansas City, Economic Review, 93*(3), 35-62.

Uludag , U., Pankanti, S., Prabhakar, S., & Jain, A. (2004). Biometric cryptosystems: issues and challenges. *Proceedings of the IEEE, 92*(6), 948-960.

Walsh, N. (2005). ATM fraud prompts card rethink? *Card Technology Today, 17*(2), 10.

Wang, J., Wang, W., Li, R., Li, Y., Tian, G., Goodman, L., et al. (2008). The diploid genome sequence of an Asian individual. *Nature, 456*(7218), 60-65.

Wen, C., Guo, T., & Wang, S. (2010). *Fingerprint Feature-Point Matching Based on Motion Coherence.* Paper presented at the (Second International Conference Sanya), Future Information Technology and Management Engineering, 2009. FITME '09.. pp.226-229.

Wu, J., Xie, S. J., Seo, D. H., & Lee, W. D. (2008). *A new approach for classification of fingerprint image quality.* Paper presented at the (7th IEEE International Conference, Stanford, CA), Cognitive Informatics, 2008. ICCI 2008.. pp.375-383.

Yanez, M., & Gomez, A. (2004). ATM & BIOMETRICS: A SOCIOTECHNICAL BUSINESS MODEL. *P7–9. University of Miami, School of Business Administration.* 16th January 2011 from http://www.iamot.org/conference/index.php/ocs/4/paper/view/1104/479

Yanez, M., & Gomez, A. (2004). ATM & BIOMETRICS: A SOCIOTECHNICAL BUSINESS MODEL. *University of Miami, School of Business Administration*.

Yang, Y., & Mi, J. (2010). *ATM terminal design is based on fingerprint recognition.* Paper presented at the Computer Engineering and Technology (ICCET), 2010 2nd International Conference Chengdu.

Yun, Y. (2002). The '123'of Biometric Technology. *Synthesis Journal, 2002*. Retrieved 23 November, 2010, from http://www.itsc.org.sg/synthesis/2002/biometric.pdf

Zhou, J., Su, G., Jiang, C., Deng, Y., & Li, C. (2007). A face and fingerprint identity authentication system based on multi-route detection. *Neurocomputing, 70*(4-6), 922-931.

APPENDIX A

Login

```
<%@ Page Language="C#" AutoEventWireup="true"
CodeFile="Default.aspx.cs" Inherits="_Default" %>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" >
<head runat="server">
    <title>Untitled Page</title>
</head>
<body>
    <form id="form1" runat="server">
    <div>
        &nbsp;
        <table style="z-index: 101; left: 378px; position:
absolute; top: 116px">
            <tr>
                <td style="width: 111px; height: 32px;">
                </td>
                <td style="width: 100px; height: 32px;">
                </td>
                <td style="width: 90px; height: 32px;">
                </td>
                <td style="width: 239px; height: 32px;">
                </td>
                <td style="width: 239px; height: 32px">
                </td>
            </tr>
            <tr>
                <td style="width: 111px; height: 103px;">
                    <asp:RequiredFieldValidator
ID="RequiredFieldValidator1" runat="server"
ControlToValidate="TextBox1"
                        ErrorMessage="Must fill the
field"></asp:RequiredFieldValidator></td>
                <td colspan="2" style="text-align: center;
height: 103px;">
                    <asp:TextBox ID="TextBox1"
runat="server"></asp:TextBox></td>
                <td style="width: 239px; height: 103px; text-
align: right;">
                    &nbsp;<asp:ImageButton ID="ImageButton1"
runat="server" ImageUrl="~/img/1111 copy.png"
                        OnClick="ImageButton1_Click"
style="background-image: url(img/1111.png)" Height="105px"
Width="82px" /></td>
                <td style="width: 239px; height: 103px; text-
align: right">
                </td>
            </tr>
            <tr>
                <td colspan="4" style="height: 17px; text-align:
right;">
```

```
                    &nbsp; &nbsp; &nbsp; &nbsp; &nbsp; &nbsp;
&nbsp; &nbsp; &nbsp; &nbsp; &nbsp; &nbsp;
                    &nbsp;&nbsp;&nbsp; &nbsp; &nbsp; &nbsp;
&nbsp; &nbsp;&nbsp; &nbsp; &nbsp; &nbsp;
                    &nbsp; &nbsp; &nbsp; &nbsp; &nbsp; &nbsp;
                    <asp:ImageButton ID="ImageButton2"
runat="server" ImageUrl="~/img/123.png"
                        OnClick="ImageButton1_Click"
style="background-image: url(img/1111.png)" Height="54px"
Width="82px" /></td>
                <td colspan="1" style="height: 17px">
                </td>
            </tr>
        </table>
        <asp:SqlDataSource ID="SqlDataSource1" runat="server"
ConnectionString="<%$ ConnectionStrings:ConnectionString %>"
            SelectCommand="SELECT * FROM
[people]"></asp:SqlDataSource>
        <img src="img/mini-atm-machine-135.jpg" style="z-index:
100; left: 346px; width: 642px;
            position: absolute; top: 12px" />

    </div>
    </form>
</body>
</html>
```

Account Manage

```
<%@ Page Language="C#" AutoEventWireup="true"
CodeFile="Exter1.aspx.cs" Inherits="Exter1" %>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" >
<head id="Head1" runat="server">
    <title>Untitled Page</title>
</head>
<body>
    <form id="form1" runat="server">
    <div style="text-align: center">
        &nbsp;
        <asp:TextBox ID="TextBox1" runat="server" Style="z-index:
100; left: 472px; position: absolute;
            top: 226px" Width="60px"></asp:TextBox>
        <img src="img/1111%20copy.png" style="z-index: 103; left:
851px; width: 78px; position: absolute;
            top: 201px; height: 112px" />
        &nbsp; &nbsp; &nbsp;
        <asp:HyperLink ID="HyperLink4" runat="server"
NavigateUrl="~/scc.aspx" Style="z-index: 101;
            left: 626px; position: absolute; top:
221px">OK</asp:HyperLink>
        &nbsp;&nbsp;
        <asp:Label ID="Label1" runat="server" Style="z-index:
104; left: 465px; position: absolute;
            top: 187px" Text="Mix 1500 RM"></asp:Label>
        <img src="img/mini-atm-machine-135.jpg" style="width:
742px; height: 528px" /></div>
    </form>
</body>
</html>


<%@ Page Language="C#" AutoEventWireup="true"
CodeFile="Exter2.aspx.cs" Inherits="Exter2" %>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" >
<head id="Head1" runat="server">
    <title>Untitled Page</title>
</head>
<body>
    <form id="form1" runat="server">
    <div style="text-align: center">
        <asp:Label ID="Label1" runat="server" Style="z-index:
100; left: 452px; position: absolute;
            top: 191px" Text="100"></asp:Label>
        &nbsp;
        <img src="img/1111%20copy.png" style="z-index: 107; left:
851px; width: 78px; position: absolute;
            top: 201px; height: 112px" />
        &nbsp;
        <asp:Label ID="Label2" runat="server" Style="z-index:
103; left: 452px; position: absolute;
```

```
            top: 219px" Text="200"></asp:Label>
        &nbsp;
        <asp:HyperLink ID="HyperLink1" runat="server"
NavigateUrl="~/Exter3.aspx" Style="z-index: 104;
            left: 446px; position: absolute; top: 246px">Exter
Number</asp:HyperLink>
        &nbsp;
        <asp:HyperLink ID="HyperLink2" runat="server"
NavigateUrl="~/scc.aspx" Style="z-index: 105;
            left: 628px; position: absolute; top:
218px">OK</asp:HyperLink>
        <asp:HyperLink ID="HyperLink3" runat="server"
NavigateUrl="~/scc.aspx" Style="z-index: 106;
            left: 627px; position: absolute; top:
191px">OK</asp:HyperLink>
        <img src="img/mini-atm-machine-135.jpg" style="width:
742px; height: 528px" /></div>
    </form>
</body>
</html>
```

Withdraw

```
<%@ Page Language="C#" AutoEventWireup="true"
CodeFile="Exter3.aspx.cs" Inherits="Exter3" %>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" >
<head id="Head1" runat="server">
    <title>Untitled Page</title>
</head>
<body>
    <form id="form1" runat="server">
    <div style="text-align: center">
        &nbsp;
        <asp:TextBox ID="TextBox1" runat="server" Style="z-index:
100; left: 472px; position: absolute;
            top: 226px" Width="60px"></asp:TextBox>
        <img src="img/1111%20copy.png" style="z-index: 103; left:
851px; width: 78px; position: absolute;
            top: 201px; height: 112px" />
        &nbsp; &nbsp; &nbsp;
        <asp:HyperLink ID="HyperLink4" runat="server"
NavigateUrl="~/scc.aspx" Style="z-index: 101;
            left: 626px; position: absolute; top:
221px">OK</asp:HyperLink>
        &nbsp;&nbsp;
        <asp:Label ID="Label1" runat="server" Style="z-index:
104; left: 465px; position: absolute;
            top: 187px" Text="Mix 15000 RM"></asp:Label>
        <img src="img/mini-atm-machine-135.jpg" style="width:
742px; height: 528px" /></div>
    </form>
</body>
</html>
```

```
<%@ Page Language="C#" AutoEventWireup="true"
CodeFile="Figer3.aspx.cs" Inherits="Figer3" %>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" >
<head id="Head1" runat="server">
    <title>Untitled Page</title>
</head>
<body>
    <form id="form1" runat="server">
    <div style="text-align: center">
        <asp:Label ID="Label1" runat="server" Style="z-index:
100; left: 452px; position: absolute;
            top: 191px" Text="100"></asp:Label>
        <asp:TextBox ID="TextBox1" runat="server" Style="z-index:
108; left: 443px; position: absolute;
            top: 273px" Width="60px"></asp:TextBox>
        <img src="img/1111%20copy.png" style="z-index: 107; left:
851px; width: 78px; position: absolute;
            top: 201px; height: 112px" />
        <asp:Label ID="Label3" runat="server" Style="z-index:
102; left: 453px; position: absolute;
            top: 247px" Text="20000"></asp:Label>
        <asp:Label ID="Label2" runat="server" Style="z-index:
103; left: 452px; position: absolute;
            top: 219px" Text="200"></asp:Label>
        &nbsp;
        <asp:HyperLink ID="HyperLink1" runat="server"
NavigateUrl="~/scc.aspx" Style="z-index: 104;
            left: 627px; position: absolute; top:
246px">OK</asp:HyperLink>
        <asp:HyperLink ID="HyperLink4" runat="server"
NavigateUrl="~/scc.aspx" Style="z-index: 104;
            left: 626px; position: absolute; top:
272px">OK</asp:HyperLink>
        <asp:HyperLink ID="HyperLink2" runat="server"
NavigateUrl="~/scc.aspx" Style="z-index: 105;
            left: 628px; position: absolute; top:
218px">OK</asp:HyperLink>
        <asp:HyperLink ID="HyperLink3" runat="server"
NavigateUrl="~/scc.aspx" Style="z-index: 106;
            left: 627px; position: absolute; top:
191px">OK</asp:HyperLink>
        <img src="img/mini-atm-machine-135.jpg" style="width:
742px; height: 528px" /></div>
    </form>
</body>
</html>
```

Withdraw Other Amount

```
<%@ Page Language="C#" AutoEventWireup="true"
CodeFile="Finger1.aspx.cs" Inherits="Finger1" %>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" >
<head id="Head1" runat="server">
    <title>Untitled Page</title>
</head>
<body>
    <form id="form1" runat="server">
    <div>
        &nbsp;
        <table style="z-index: 101; left: 378px; position:
absolute; top: 116px">
            <tr>
                <td style="width: 111px; height: 32px;">
                </td>
                <td style="width: 100px; height: 32px;">
                </td>
                <td style="width: 90px; height: 32px;">
                </td>
                <td style="width: 239px; height: 32px;">
                </td>
            </tr>
            <tr>
                <td style="width: 111px; height: 103px;">
                    </td>
                <td colspan="2" style="text-align: center;
height: 103px;">
                    <asp:TextBox ID="TextBox1" runat="server"
Font-Bold="True" ForeColor="Red">please use
FingerPrint</asp:TextBox></td>
                <td style="width: 239px; height: 103px; text-
align: right;">
                    &nbsp;<asp:ImageButton ID="ImageButton1"
runat="server" ImageUrl="~/img/1111 copy.png"
                        OnClick="ImageButton1_Click"
style="background-image: url(img/1111.png)" Height="105px"
Width="82px" /></td>
            </tr>
            <tr>
                <td colspan="4" style="height: 17px">
                    &nbsp; &nbsp; &nbsp; &nbsp; &nbsp; &nbsp;
&nbsp; &nbsp; &nbsp; &nbsp; &nbsp; &nbsp;
                    &nbsp;&nbsp;&nbsp; &nbsp; &nbsp; &nbsp;
&nbsp; &nbsp;&nbsp; &nbsp; &nbsp; &nbsp;
                    &nbsp; &nbsp; &nbsp; &nbsp; &nbsp;&nbsp;
                </td>
            </tr>
        </table>
        <img src="img/mini-atm-machine-135.jpg" style="z-index:
100; left: 346px; width: 642px;
            position: absolute; top: 12px" />

    </div>
    </form>
</body> </html>
```

Login with Fingerprint

```
<%@ Page Language="C#" AutoEventWireup="true"
CodeFile="finger2.aspx.cs" Inherits="finger2" %>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" >
<head id="Head1" runat="server">
    <title>Untitled Page</title>
</head>
<body style="text-align: center">
    <form id="form1" runat="server">
    <div>
        <asp:Label ID="Label1" runat="server" Text="Label"
Visible="False"></asp:Label>&nbsp;

    </div>
        <table style="z-index: 103; left: 350px; width: 567px;
position: absolute; top: 113px; height: 188px;">
            <tr>
                <td style="width: 72px">
                </td>
                <td style="width: 104px">
                    &nbsp;</td>
                <td style="width: 65px">
                    &nbsp; &nbsp; &nbsp; &nbsp; &nbsp; &nbsp;
&nbsp; &nbsp; &nbsp; &nbsp; &nbsp; &nbsp;
                    &nbsp; &nbsp; &nbsp; &nbsp; &nbsp; &nbsp;
&nbsp; &nbsp; &nbsp; &nbsp; &nbsp; &nbsp;
                    &nbsp; &nbsp; &nbsp;&nbsp;
                </td>
            </tr>
            <tr>
                <td style="width: 72px; height: 21px;">
                </td>
                <td style="width: 104px; height: 21px; text-
align: left;">
                    <br />
                    <asp:HyperLink ID="HyperLink1" runat="server"
NavigateUrl="~/Exter2.aspx">Withdraw</asp:HyperLink>
                    <br />
                    <asp:HyperLink ID="HyperLink3" runat="server"
NavigateUrl="~/withdrow.aspx">Deposit</asp:HyperLink><br />
                    <asp:HyperLink ID="HyperLink4" runat="server"
NavigateUrl="~/withdrow.aspx">Transfer</asp:HyperLink><br />
                    <asp:HyperLink ID="HyperLink2" runat="server"
NavigateUrl="~/withdrow.aspx">Service</asp:HyperLink></td>
                <td style="width: 65px; height: 21px; text-align:
right;">
                    <img src="img/1111%20copy.png" style="height:
110px" /></td>
            </tr>
            <tr>
                <td style="width: 72px; height: 21px">
                </td>
                <td style="width: 104px; height: 21px">
                </td>
                <td style="width: 65px; height: 21px">
                </td>
            </tr>
        </table>
        &nbsp;&nbsp;&nbsp;
        <img src="img/mini-atm-machine-135.jpg" style="width:
650px; height: 500px" />
    </form>
</body>
</html>
```

Withdraw with Extra Amount

```
<%@ Page Language="C#" AutoEventWireup="true"
CodeFile="fingermas.aspx.cs" Inherits="fingermas" %>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml11/DTD/xhtml11-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" >
<head id="Head1" runat="server">
    <title>Untitled Page</title>
</head>
<body>
    <form id="form1" runat="server">
    <div>
        <img src="img/loading.gif" style="z-index: 100; left:
415px; width: 358px; position: absolute;
            top: 159px; height: 327px" />
        &nbsp; &nbsp; &nbsp; &nbsp; &nbsp; &nbsp; &nbsp; &nbsp;
&nbsp; &nbsp; &nbsp; &nbsp;
        &nbsp; &nbsp; &nbsp; &nbsp; &nbsp; &nbsp;&nbsp; &nbsp;
&nbsp; &nbsp; &nbsp; &nbsp;
        &nbsp; &nbsp; &nbsp; &nbsp;<br />
        <br />
        &nbsp; &nbsp; &nbsp; &nbsp; &nbsp; &nbsp; &nbsp; &nbsp;
&nbsp; &nbsp; &nbsp; &nbsp;
        &nbsp; &nbsp; &nbsp; &nbsp; &nbsp; &nbsp; &nbsp; &nbsp;
&nbsp; &nbsp; &nbsp; &nbsp;
        &nbsp;&nbsp; </div>
    </form>
</body>
</html>
```

```
<%@ Page Language="C#" AutoEventWireup="true"
CodeFile="mass.aspx.cs" Inherits="mass" %>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml11/DTD/xhtml11-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" >
<head runat="server">
```

```
    <title>Untitled Page</title>
</head>
<body>
    <form id="form1" runat="server">
    <div>
        <img src="img/loading.gif" style="z-index: 100; left:
415px; width: 358px; position: absolute;
            top: 159px; height: 327px" />
        &nbsp; &nbsp; &nbsp; &nbsp; &nbsp; &nbsp; &nbsp; &nbsp;
&nbsp; &nbsp; &nbsp; &nbsp;
        &nbsp; &nbsp; &nbsp; &nbsp; &nbsp; &nbsp;&nbsp;<br />
        <br />
        &nbsp; &nbsp; &nbsp; &nbsp; &nbsp; &nbsp; &nbsp; &nbsp;
&nbsp; &nbsp; &nbsp; &nbsp;
        &nbsp; &nbsp; &nbsp; &nbsp; &nbsp; &nbsp; &nbsp; &nbsp;
&nbsp; &nbsp; &nbsp; &nbsp;
        &nbsp;&nbsp; your account Number :
        <asp:Label ID="Label1" runat="server"
Text="Label"></asp:Label></div>
    </form>
</body>
</html>
```

Extra Withdraw

```
<%@ Page Language="C#" AutoEventWireup="true"
CodeFile="massager.aspx.cs" Inherits="massager" %>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" >
<head runat="server">
    <title>Untitled Page</title>
</head>
<body style="text-align: center">
    <form id="form1" runat="server">
    <div>
        <asp:Label ID="Label1" runat="server" Text="Label"
Visible="False"></asp:Label>
        <asp:SqlDataSource ID="SqlDataSource1" runat="server"
ConnectionString="<%$ ConnectionStrings:ConnectionString %>"
            DeleteCommand="DELETE FROM [people] WHERE [MatricNO]
= @MatricNO" InsertCommand="INSERT INTO [people] ([MatricNO],
[user name], [Address]) VALUES (@MatricNO, @user_name, @Address)"
            SelectCommand="SELECT [user name], Address FROM
people WHERE (MatricNO = @mm)"
            UpdateCommand="UPDATE [people] SET [user name] =
@user_name, [Address] = @Address WHERE [MatricNO] = @MatricNO">
            <SelectParameters>
                <asp:ControlParameter ControlID="Label1"
Name="mm" PropertyName="Text" />
            </SelectParameters>
            <DeleteParameters>
                <asp:Parameter Name="MatricNO" Type="Int32" />
            </DeleteParameters>
            <UpdateParameters>
```

```
                <asp:Parameter Name="user_name" Type="String" />
                <asp:Parameter Name="Address" Type="String" />
                <asp:Parameter Name="MatricNO" Type="Int32" />
            </UpdateParameters>
            <InsertParameters>
                <asp:Parameter Name="MatricNO" Type="Int32" />
                <asp:Parameter Name="user_name" Type="String" />
                <asp:Parameter Name="Address" Type="String" />
            </InsertParameters>
        </asp:SqlDataSource>

    </div>
        <table style="z-index: 103; left: 351px; width: 567px;
position: absolute; top: 113px; height: 188px;">
            <tr>
                <td style="width: 72px">
                </td>
                <td style="width: 104px">
        <asp:GridView ID="GridView1" runat="server"
AutoGenerateColumns="False" DataSourceID="SqlDataSource1"
            Style="text-align: center;" Width="287px"
BackColor="LightGoldenrodYellow" BorderColor="Tan"
BorderWidth="1px" CellPadding="2" ForeColor="Black"
GridLines="None">
            <Columns>
                <asp:BoundField DataField="user name"
HeaderText="user name" SortExpression="user name" />
                <asp:BoundField DataField="Address"
HeaderText="Address" SortExpression="Address" />
            </Columns>
            <FooterStyle BackColor="Tan" />
            <PagerStyle BackColor="PaleGoldenrod"
ForeColor="DarkSlateBlue" HorizontalAlign="Center" />
            <SelectedRowStyle BackColor="DarkSlateBlue"
ForeColor="GhostWhite" />
            <HeaderStyle BackColor="Tan" Font-Bold="True" />
            <AlternatingRowStyle BackColor="PaleGoldenrod" />
        </asp:GridView>
                </td>
                <td style="width: 65px">
                    &nbsp; &nbsp; &nbsp; &nbsp; &nbsp; &nbsp;
&nbsp; &nbsp; &nbsp; &nbsp; &nbsp; &nbsp;
                    &nbsp; &nbsp; &nbsp; &nbsp; &nbsp; &nbsp;
&nbsp; &nbsp; &nbsp; &nbsp; &nbsp; &nbsp;
                    &nbsp; &nbsp; &nbsp;&nbsp;
                </td>
            </tr>
            <tr>
                <td style="width: 72px; height: 21px;">
                </td>
                <td style="width: 104px; height: 21px; text-
align: center;">
                    <asp:HyperLink ID="HyperLink1" runat="server"
NavigateUrl="~/withdrow.aspx">Withdraw</asp:HyperLink><br />
                    <asp:HyperLink ID="HyperLink2" runat="server"
NavigateUrl="~/withdrow.aspx">Deposit</asp:HyperLink>
                </td>
                <td style="width: 65px; height: 21px; text-align:
right;">
                    <img src="img/1111%20copy.png" style="height:
110px" /></td>
```

```
            </tr>
            <tr>
                <td style="width: 72px; height: 21px">
                </td>
                <td style="width: 104px; height: 21px">
                </td>
                <td style="width: 65px; height: 21px">
                </td>
            </tr>
        </table>
        &nbsp;&nbsp;&nbsp;
        <img src="img/mini-atm-machine-135.jpg" style="width:
650px; height: 500px" />
    </form>
</body>
</html>
<%@ Page Language="C#" AutoEventWireup="true"
CodeFile="scc.aspx.cs" Inherits="scc" %>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" >
<head runat="server">
    <title>Untitled Page</title>
</head>
<body>
    <form id="form1" runat="server">
    <div>
        <br />
        <br />
        <br />
        <br />
        <br />
        <img src="img/post8_success.jpg" style="z-index: 100;
left: 368px; position: absolute;
            top: 111px" />

    </div>
    </form>
</body>
</html>
```

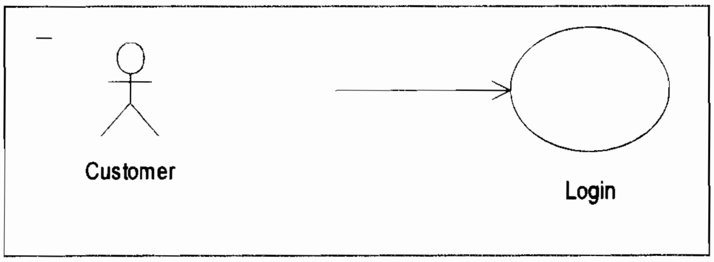
Successful Operation Interface

```
<%@ Page Language="C#" AutoEventWireup="true"
CodeFile="withdrow.aspx.cs" Inherits="withdrow" %>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" >
<head runat="server">
    <title>Untitled Page</title>
</head>
<body>
    <form id="form1" runat="server">
    <div style="text-align: center">
        <asp:Label ID="Label1" runat="server" Style="z-index:
100; left: 452px; position: absolute;
            top: 191px" Text="100"></asp:Label>
        &nbsp;
        <img src="img/1111%20copy.png" style="z-index: 107; left:
851px; width: 78px; position: absolute;
            top: 201px; height: 112px" />
        &nbsp;
        <asp:Label ID="Label2" runat="server" Style="z-index:
103; left: 452px; position: absolute;
            top: 219px" Text="200"></asp:Label>
        &nbsp;
        <asp:HyperLink ID="HyperLink1" runat="server"
NavigateUrl="~/Exter1.aspx" Style="z-index: 104;
            left: 446px; position: absolute; top: 246px">Other
Number</asp:HyperLink>
        &nbsp;
        <asp:HyperLink ID="HyperLink2" runat="server"
NavigateUrl="~/scc.aspx" Style="z-index: 105;
            left: 628px; position: absolute; top:
218px">OK</asp:HyperLink>
        <asp:HyperLink ID="HyperLink3" runat="server"
NavigateUrl="~/scc.aspx" Style="z-index: 106;
            left: 627px; position: absolute; top:
191px">OK</asp:HyperLink>
        <img src="img/mini-atm-machine-135.jpg" style="width:
742px; height: 528px" /></div>
    </form>
</body>
</html>
```

APPINDIX B

USE CASE SPECIFICATION FOR ASKST

1. Use case: Home Page



BRIEF DESCRIPTION

This use case is initiated by the customer. This use case will enable the customer to login during use credit card and PIN code..

PRE-CONDITIONS

The customer must be having credit card.

CHARACTERISTIC OF ACTIVATION

Event Driven (on user's demand)

FLOW OF EVENTS

Basic Flow (ATM_UFP _01)

- This use case begins when the user enter credit card and PIN code.
- The systems will Verification from credit card and PIN code and then display main page.

- If the customer enter invalidate credit card or wrong PIN code , system display wrong message and give customer twice chance.
- If the customer lost all the PIN code chance he/she can used fingerprint to login the ATM

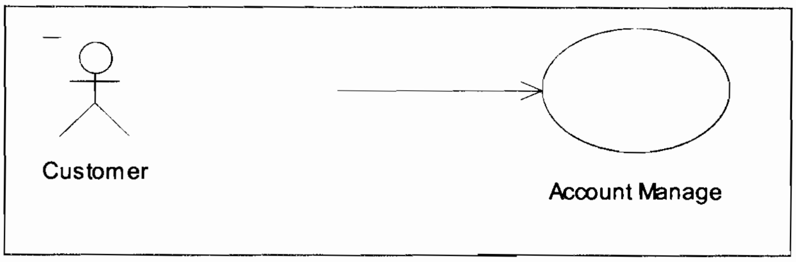
Exceptional Flow

E-2: the credit card or PIN code in not correct..

POST-CONDITIONS

User will be able to proceed to other activities

2. Use case: Account Manage



BRIEF DESCRIPTION

This use case is initiated by the customer. This use case will enable the user to manage his/her account.

PRE-CONDITIONS

The user must be login.

CHARACTERISTIC OF ACTIVATION

Event Driven (on user's demand)

FLOW OF EVENTS

Basic Flow (ATM_UFP _02)

- This use case begins when the user login the system.
- System will display for the customer all the available services.
- Customer could be requesting any available services by click on services button

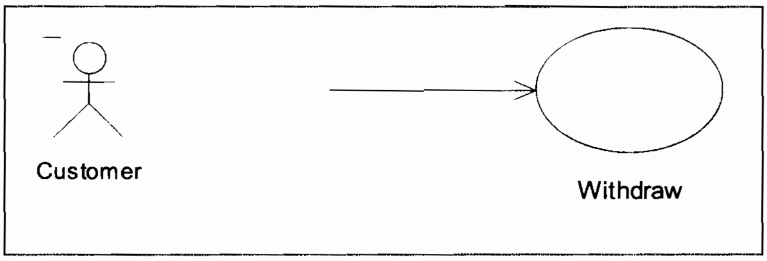
Exceptional Flow

E-2: the username or password in not correct.

POST-CONDITIONS

User will be able to proceed to other activities

3. USE CASE: MANAGE ASSESSMENT



BRIEF DESCRIPTION

This use case is initiated by the customer. This use case will enable the customer to withdraw money from his/her account via ATM.

PRE-CONDITIONS

Already the user login into the system.

CHARACTERISTIC OF ACTIVATION

Event Driven (on user's demand)

FLOW OF EVENTS

Basic Flow (ATM_UFP _03)

- This use case begins when the user press "withdraw" button.
- The system will display withdraw page.
- The customer could be requesting any available amount.
- The customer press Yes button when he finish
- If the customer need withdraw unavailable amount, he/she can press "other amount" button.
- System will display other amount page to customer.
- Customer can enter any amount less than 1500 RM.
- The customer press Yes button when he finish
- System will display successful massage.

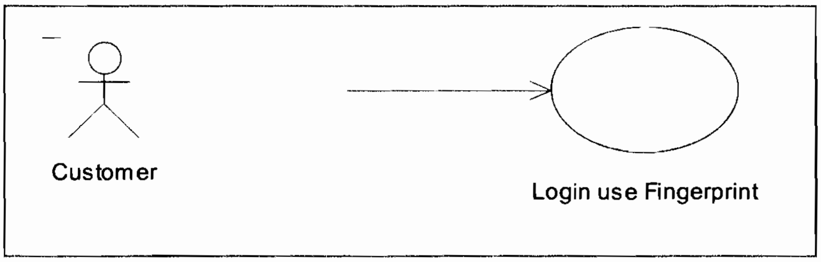
Exceptional Flow

E-2: the customer's account in unavailable.

POST-CONDITIONS

User will be able to proceed to other activities

4. Use case: Login use fingerprint



BRIEF DESCRIPTION

This use case is initiated by the user (customer). This use case will enable the customer to login the ATM system by using fingerprint.

PRE-CONDITIONS

The customer must be having credit card.

CHARACTERISTIC OF ACTIVATION

Event Driven (on user's demand)

FLOW OF EVENTS

Basic Flow (ATM_UFP _04)

- This use case begins when the user enter credit card and put his/her finger on finger-scan to login the system.
- The systems will Verification from credit card and recognition the finger image then display main page.

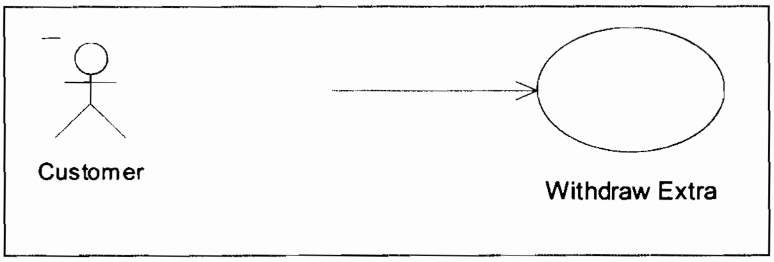
Exceptional Flow

E-2: the fingerprint in not correct finger.

POST-CONDITIONS

User will be able to proceed to other activities

5. Use case: Print Result



BRIEF DESCRIPTION

This use case is initiated by the user (customer). This use case will enable the customer to withdraw huge amount from ATM.

PRE-CONDITIONS

Already the user login into the system.

CHARACTERISTIC OF ACTIVATION

Event Driven (on user's demand)

FLOW OF EVENTS

Basic Flow (ATM_UFP _05)

- This use case begins when the user press "withdraw" button.

- The system will display withdraw page.
- The customer could be requesting any available amount.
- The customer press Yes button when he finish
- If the customer need withdraw unavailable amount, he/she can press “Extra Withdraw” button.
- System will display extra withdraw page to customer.
- Customer can enter any amount less than 15000 RM.
- The customer press Yes button when he finish
- System will display successful massage.

Exceptional Flow

E-2: the customer’s account in unavailable.

POST-CONDITIONS

User will be able to proceed to other activities

APPENDIX C

COLLEGE OF ATRS AND SCIENCES
UNIVERSITY UTARA MALAYSIA

Implementing Additional Security Measure On ATM through Biometric

I am Master of Science (Information Technology) student at final semester in University Utara Malaysia. Currently, I am performing this questionnaire to help me gain an understanding of the user who used ATM. This questionnaire aims to understand general information about system user's and the usability of the system. The results from this questionnaire will help me to understand the system requirements for developing an ATM prototype system by using fingerprint technique.

All your information will be held in strictest confidence and it will be used for research purpose only. Your insights a feedback in making this study successful is highly appreciated. If you have any queries or if you like to know the result of this study, please do contact me at 014-9003485or through the e-mail: s802829@student.uum.edu.my . This questionnaire consists of two sections:

- Section A - General Information
- Section B - System Usability

This questionnaire is adopted from Brooke (Bangor, Kortum & Miller, 2008) System Usability Scale (SUS).

Thank you for your valuable time and help in completing this questionnaire.

MSc. IT Candidate

Hayder Hussein

QUESTIONNAIRE

System to Be Evaluated:

AUTOMATIC TELLER MACHINES USING FINGERPRINT TECHNIQUE (ATM_UFP)

Objective:

Obtain your view on the evaluation of ATM_UFP.

Please answer **all** questions from each segment.

1) General Information

This segment is about your background information. Please fill up the blanks and mark [√] where appropriate.

1. Gender: [ ] Male [ ] Female

2. Age: ____________ Years.

3. Education background

[ ] High school [ ] Diploma [ ] Degree [ ] Master [ ] Ph.D.

2) Automatic Teller Machines Using Fingerprint Technique Prototype Evaluation

Please rate the usefulness and ease of use of Automatic Teller Machines Using Fingerprint Technique (ATM_UFP)

1 = Strong disagree, 2 = Disagree, 3 = Natural, 4 = Agree, 5 = Strong agree.

	PERCEIVED USEFULNESS	1	2	3	4	5
Q1	Using ATM_UFP helps me to be more effective	O	O	O	O	O
Q2	Using ATM_UFP helps me to be more productive.	O	O	O	O	O
Q3	Using ATM_UFP saves my time when I use it	O	O	O	O	O
Q4	Using ATM_UFP would enhance my effectiveness	O	O	O	O	O
Q5	Using ATM_UFP would make it easier to do my tasks	O	O	O	O	O
Q6	ATM_UFP was competency increased security of ATM system	O	O	O	O	O
	PERCEIVED EASE OF USE	**1**	**2**	**3**	**4**	**5**
Q7	ATM_UFP is simple to use.	O	O	O	O	O
Q8	ATM_UFP is very friendly to use	O	O	O	O	O
Q9	It requires the fewest steps possible to accomplish what I want to do with it	O	O	O	O	O
Q10	I can use it without written instructions	O	O	O	O	O
Q11	I don't notice any inconsistencies as I use ATM_UFP	O	O	O	O	O
Q12	I can use ATM_UFP successfully every time.	O	O	O	O	O