

Biometric Verification System for Automated Teller Machine (ATM)

by

Haiza Izura Binti Basri
1560

Dissertation submitted in partial fulfillment of
the requirements for the Bachelor of Technology (Hons)
(Information System)

JUNE 2004

Universiti Teknologi PETRONAS

Bandar Seri Iskandar

31750 Tronoh

Perak Darul Ridzuan

TK

7882

.056

#149

2004

1) Biometric identification

2) IT/IS - thesis

CERTIFICATION OF APPROVAL

Biometric Verification System for Automated Teller Machine (ATM)

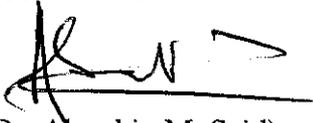
by

Haiza Izura Binti Basri
1560

A project dissertation submitted to the
Information System Programme
Universiti Teknologi PETRONAS
in partial fulfillment of the requirement for the
BACHELOR OF TECHNOLOGY (Hons)
(INFORMATION SYSTEM)

JUNE 2004

Approved by,



(Dr. Abas bin M. Said) *← Bodo hehe.*

Universiti Teknologi PETRONAS
Bandar Seri Iskandar
31750 Tronoh
Perak Darul Ridzuan

CERTIFICATION OF ORIGINALITY

This is to certify that I am responsible for the work submitted in this project, that the original work is my own except as specified in the references and acknowledgements, and that the original work contained herein have not been undertaken or done by unspecified sources or persons.



(HAIZA IZURA BT BASRI)

ABSTRACT

Biometric Verification System for Automated Teller Machine (ATM) will serve as an alternative for the current verification system that uses ATM card and personal identification number (PIN) to protect against fraud and effectively eliminating most common attempts to gain unauthorized access. With biometric technology, customer can gain access to their account through smart card approach combined with biometric technology to automatically identify individuals using their distinct physical or behavioral characteristics. The main objective of this project is to solve the problems that arise from using PIN as the base of ATM verification system. These include unauthorized access into financial accounts, stealing money, ATM fraud and many more. To ensure a reliable project output, the author had outlined the scope of study for the proposed project. It involves the study of ATM system, biometrics technology, architecture, the benefits and the drawback of each approach and the current trend in the market. The development of this system will be based on the RAD methodology.

ACKNOWLEDGEMENT

Though I would like to take credit for the concepts and ideas presented in the system, I am not alone. I would like to thank the countless number of people who have helped get this Final Year Project (FYP) into a complete success.

I am indebted to the IT Department for their concerns and technical support on this project, especially Mrs. Vivian Yong Suet Peng and Mr. Shuib bin Basri as the FYP coordinators. Many thanks go to my supervisor, Dr. Abas bin Md Said, who always been there when I need that advice and extra burst of energy to tackle yet another problem.

I also like to thanks all the lecturers who helped the system development with some guidance in a few areas where my skills were deficient. I would like to express my greatest gratitude to Bumiputera Commerce Berhad, IT & Media Services personnel and all respondents who have give me full cooperation and assistance. Their input made this project a much better product.

Last but not least, my family and friends, who always had been there for me through my hard and bad time. All your help, support and guidance are highly appreciated. I am looking forward to work together again in the near future.

TABLE OF CONTENTS

CERTIFICATION		iii
ABSTRACT		iv
ACKNOWLEDGEMENT		v
LIST OF FIGURES		ix
CHAPTER 1:	INTRODUCTION	1
	1.1 Background of Study	1
	1.2 Problem statement	2
	1.2.1 Significance of the project	3
	1.3 Objective and scope of study	3
	1.3.1 Objectives	3
	1.3.2 Scope of Study	3
	1.3.3 Feasibility of the project within the Scope and Time Frame	4
CHAPTER 2:	LITERATURE REVIEW	5
	2.1 ATM Fraud – Technical Attack on PIN key	5
	2.2 Future Direction – The idea of biometric ATM	7
CHAPTER 3:	METHODOLOGY/PROJECT WORK	10
	3.1 Data Collection Method	10
	3.1.1 Observations	10
	3.1.2 Reading/Studies	11
	3.1.3 Questionnaires	11
	3.2 Procedure Identification	12
	3.3 Project work	13
	3.3.1 Phases of project	13
CHAPTER 4:	RESULTS AND DISCUSSIONS	14
	4.1 Current ATM Security System	14
	4.2 Introduction to Biometric Identification	15
	4.3 Combining Smart Card With Biometric Technology	16
	4.4 Comparison on Biometric Measurement	16
	4.4.1 Fingerprints	17
	4.4.2 Hand Geometry	17
	4.4.3 Eye Scanning	17
	4.4.4 Face Recognition	18
	4.5 Results from questionnaires	20
	4.6 Project Design	26
	4.6.1 Process Flow	26
	4.6.2 Use Case Diagram	27
	4.6.3 Activity Diagram	28

TABLE OF CONTENTS

	4.6.4 Interface Design	30
CHAPTER 5:	CONCLUSION AND RECOMMENDATION	31
	5.1 Conclusion	31
	5.2 Recommendation	32
REFERENCES		33
APPENDICES		35
APPENDIX A	Questionnaires	36
APPENDIX B	Types of Fingerprints Sensors	39
APPENDIX C	Biometric Revenue By Technology	42
APPENDIX D	Print Screen of Designed Interface	44

LIST OF FIGURES:

Figure 3.1:	Phases of RAD Methodology	12
Figure 4.5.1:	Results from Question 1	20
Figure 4.5.2:	Results from Question 2	21
Figure 4.5.3:	Results from Question 3	21
Figure 4.5.4:	Results from Question 4	22
Figure 4.5.5:	Results from Question 5	22
Figure 4.5.6:	Results from Question 6	23
Figure 4.5.7:	Results from Question 7	23
Figure 4.5.8:	Results from Question 8	24
Figure 4.5.9:	Results from Question 9	24
Figure 4.5.10:	Results from Question 10	25
Figure 4.6.1:	Process Flow For Enrollment and Verification Process	26
Figure 4.6.2:	Use Case Diagram	27
Figure 4.6.3:	Activity Diagram	29

LIST OF TABLES:

Table 4.4:	Comparison of Biometrics	19
------------	--------------------------	----

CHAPTER ONE

INTRODUCTION

1.1 BACKGROUND OF STUDY

An automatic teller machine or ATM allows a bank customer to conduct their banking transactions from almost every other ATM machine in the world. ATM provides customers a quick and convenient way to access their bank accounts and to conduct financial transactions. In order to gain access to an ATM a customer needs a card issued by the appropriate bank and the correct Personal Identification Number (PIN) issued by the financial institution. The PIN is entirely private to the cardholder and should never be revealed or written down. The PIN is the key to the system, without it any transactions cannot be made from an ATM. We can say that it is one of the important aspects in ATM security system. The question is whether the PIN system is still reliable in today's world.

Since the first time of ATM introduction nearly 30 years ago, theft started tapping into the system. The number of ATM fraud has increased from time to time concurrently with the awareness of public on banking technology. Seems, the harder banks work to secure their ATMs against fraud, the more likely criminals are to use violence against ATM users to steal their money. The use of PIN as security means has been questioned since it can never protect one's privacy once it fell into the wrong hand. This is where biometric technology comes into the picture. The idea is to use something for identification that can't be lost, stolen or forgotten and maybe there will be less fraud.

Although biometric security in banking industry is still in early phase, it may become one of a reliable alternative to PIN system. Moving to a biometric security system translates into greater security and efficiency, while minimizing the fraud in ATM transactions. This project would serve as a good tool to understand the importance of security measures towards one's privacy. Moreover, it gives an expose towards the technology used in today's world to aid a particular system like this ATM security system in order to reach its reliability and effectiveness.

1.2 PROBLEM STATEMENT

Currently, password or personal identification number (PIN) is one of important aspects in ATM security system which is commonly used to secure and protect financial information of customers from unauthorized access. In general, PIN is sufficient to protect against fraud and effectively eliminating most common attempts to gain unauthorized access. In practice, however, PIN is often easy to defeat particularly those which are easily guessed. The most recent cases show that the thefts have used sophisticated cracking programs to steal ATM holders' money very easily. In addition, for some people who live in today's high technology society which are bombarded everyday by so many numbers such as social security number, credit card number and so on, oftentimes they are confusing or difficult to be recalled immediately which could lead to many problems. Whenever it is written down on small piece of paper or card in order to anticipate such event, the strength of PIN as a security protection is weakened since the likelihood of the code leaking to other people increase.

In summary, there are 2 main problems regarding the use of PIN system:

1. Stealing/duplication of bank card and identification number that leads to ATM fraud.
2. Users have to memorize their identification number in order to gain access to their accounts.

Responding to this matter, the author had come out with the idea to use biometrics-based identification method in replacement of personal identification number (PIN) in the ATM Security System.

1.2.1 Significance of the project

An IT solution is required to help reduce the problem of ATM fraud. The concept of Biometric Verification System is to offer the following benefits to the society:

- Convenience - Biometrics can indeed make a system easier to use since the clients no longer has to remember their identification number.
- Greater security — biometrics link a person to an action.
- Local verification—clients hold their identity information (e.g., on a Smart Card), so there is no need to verify identity via a central repository or server.
- User identity is stored safely and is tamper-free.
- Decrease error of key-in wrong identification number.

1.3 OBJECTIVES AND SCOPE OF STUDY

1.3.1 Objectives

- To learn and understand the function and the current trend of Automatic Teller Machine (ATM) especially in the security aspect.
- To propose a solution regarding the problems of the current security system (PIN).
- To search on the latest method/technology of identification system (biometric technology).
- To come out with a conceptual design of the system.
- To design the interface for the machine upfront and the screen layout.

1.3.2 Scope of Study

- Research on existing ATM security system.
- Research on biometric technology.
- Studies on the issue of biometrics technology.
- Study on conceptual design and development of a verification system.

1.3.3 Feasibility of the Project within the Scope and Time Frame.

Biometric Verification System for Automated Teller Machine ATM is a relevant project not only to the author but to the society as well. The author had used this opportunity to apply what she has learned in classes into this project. While for the society, this project will offer a great benefit by improving the security measures in daily banking transactions through ATM thus increase the efficiency and reduce frauds.

Due to time constraints, the author decided to narrow down the scope of study as well as the system's design. As for the time frame, the author has to construct the project plan and schedule to catch up with the time frame. This project should be feasible to be completed in one semester, which is about 4 months.

CHAPTER 2

LITERATURE REVIEW

2.1 ATM Fraud – Technical Attack on PIN key

For decades, people had used personal identification number (PIN) to protect against fraud and effectively eliminating most common attempts to gain unauthorized access. However, with the rapid changes in technology, we can't keep relying on identification number as a security means to our privacy. ATM fraud is one of the crimes that results from inappropriate way of handling PIN. A corrupt bank employee can discover your debit card pin number after just 15 attempts, according to a study by computer scientists in Cambridge. [1]

In most cases withdrawals go without a hitch but ATM fraud has started to be a growing nuisance. This type of fraud, including use of stolen cards at ATMs, has grown from £8.2 million in 1997 to £21.2 million in 2001, representing about 5% of all card fraud. Two years ago it was a London problem but it has now spread all over the country. Sandra Quinn of the Association of Payment Clearing Services (APACS) says that more recent figures are due soon and they are expected to show a sharp jump in ATM fraud. [2]

In United Kingdom, the ATM scam uses different tactics to steal money from ATM user. The scam, called the Lebanese Loop works like this: A plastic or metal sleeve is constructed that fits into the card slot of an ATM machine. When the next unsuspecting customer arrives to withdraw money the card is caught in the sleeve and doesn't completely enter the machine. You will get the screen asking you to enter your PIN number, but no matter how many times you enter the number nothing else happens. This gives a thief, standing behind you, plenty of opportunity to see you punch in your PIN. After you give up the thief uses a small tool to pull out the sleeve with your card and promptly withdraws the maximum cash from your account. [3]

ATM fraud has become more sophisticated with cracking programs to steal ATM holders' money very easily. The newest device for stealing information is a thin, transparent-plastic overlay on an ATM keypad that captures a user's identification code as it is entered. To the card holder, it might look like some sort of cover to protect the keys. In fact, microchips in the device record every keystroke. Another transparent device inside the card slot captures card data. While the cardholder completes the transaction, a computer attached to the overlay records all the data necessary to clone the card. [4]

Another method used is to distract us by spilling a drink over us or doing something like dropping a £10 and asking who owns it. While distracted, they will nab your cash or card or both, having already surfed your shoulder to get your PIN number. Sometimes those using the distraction method will take your card and quickly skim it through a machine in order to make a copy. The card is then returned to the machine, with the user being none the wiser. [2]

The newest device for stealing information is a thin, transparent-plastic overlay on an ATM keypad that captures a user's identification code as it is entered. To the card holder, it might look like some sort of cover to protect the keys. In fact, microchips in the device record every keystroke. Another transparent device inside the card slot captures card data. While the cardholder completes the transaction, a computer attached to the overlay records all the data necessary to clone the card. [5]

The secrecy of the PIN key, although necessary, is not sufficient. This is illustrated by a famous fraud, which took place at the Chemical Bank in New York in 1985. An ATM technician, who had been fired, would stand in line and watch a customer keying in his PIN. He would then pick up the discarded receipt, which contained the account number, write this number to the magnetic strip of a blank card, and use this with the observed PIN to raid the poor customer's account. He managed to steal over \$80,000 before the bank saturated downtown New York with security men and caught him in the act. Needless to say, the emergence since then of worldwide ATM networks makes such attacks much more easy to do, and extremely difficult to stop. [6]

With all the drawbacks, passwords and personal identification numbers (PINs) soon may become relics of our computer past as biometric identification technology takes over the critical task of identifying and authenticating computer users, and permitting access to secure sites, files and Intranets.[7]

2.2 Future Direction – The idea of biometric ATM

According to Roberto Torres, Frost & Sullivan automatic identification industry research analyst, "The underlying driver in the commercial arena is the business community's search for tools which can prevent fraud. Problems stemming from false identification of individuals have seriously hurt the financial industry, government agencies and business establishments for decades."

Biometrics is an old greek word for a very new concept. "Bio," meaning life, and "Metric," the measure of, so Biometrics is in essence, the measure of life. Biometrics is an emerging technology for automatically identifying individuals using their distinct physical or behavioral characteristics. Types of Biometrics can be any unique human characteristics, such as fingerprint, voice, face, iris, retina, palm, signature, wrist vein, and hand geometry. Biometrics provides a better solution for the increased security requirements of our information society than current identification methods (passwords, PIN numbers and magnetic strip cards with a PIN number) for various reasons: the person to be identified must be physically present at the point of identification; identification based on biometric techniques obviates the need to remember a password (or write it on a yellow sticky note), PIN or carry a token. Using biometric systems to identify the user of a computer, ATM, cellular phones and even credit card purchases will reduce fraud and unauthorized access. This could save the economy billions of dollars. [6]

Mark Radke of Diebold, one of the biggest ATM manufacturers in the United States, says the emergence of biometrics has been slow in part because of the technology and partly due to slow overall acceptance by the public. But that's changing, he says, to the point where credit unions, which have been more aggressive than banks about using biometrics, see the new technology as a customer draw. [5]

"Banks realize biometrics are not something to be ignored," says Jennifer Schmidt, a Meridien Research analyst and author of a study on biometrics in financial services institutions. Biometrics provide a unique advantage over other forms of security, such as user name and password, in that an individual's biometrics print is one-of-a-kind. Whether it's the pattern of blood vessels in the eye or the long-familiar thumbprint, no one else in the world has the same measurable characteristic. [8]

Bank United became the first US bank to trial a biometric-enabled Diebold ATM at three of its branches using iris technology from Sensar in the spring of 1999. The bank's customers gave positive feedback to the trial, with 98 per cent of those surveyed saying that would like to see more machines installed locally. However, Bank United has yet to install any further machines. UK building society Nationwide became the first organisation worldwide to trial iris recognition technology supplied by NCR back in 1998. The results of the pilot were very positive for the customer, with 94 per cent saying they were comfortable with the technology and 91 per cent saying they would choose iris identification in future above either PINs or signatures. [2]

Citibank is looking into the feasibility and cost of using biometrics technology as a more efficient and secure method of identifying its customers. Meanwhile, Huntington Bancshares is studying the impact of identity theft and fraud with a close eye on biometrics as a possible approach to reducing the chronic problem. Tom Connaughton, managing director of risk management at Citibank North America, in New York, said his company wants to be a leader in extending biometrics technology to customers, providing them with several types of identification options, such as fingerprint and facial-recognition technologies, so they can choose which one they're most comfortable

with. Having customers use biometrics to gain access to accounts is the only way for the bank to know for sure whom they're dealing with, Connaughton said. [9]

Bill Rogers, publisher of Biometric Digest, says things should change now that some major corporations are getting behind biometrics. "Microsoft has committed to putting biometrics in a future release of Windows. Compaq Computer has built a PC with a fingerprint scanner built into the keyboard. Visa, MasterCard and Discover are doing pilot projects where your fingerprint is put into the bar code, the merchant drops the card into the reader, you put your finger on a scanner and they know the card is yours. Once the credit card companies and Microsoft or the hardware manufacturers make them part of the standard system, it'll move faster." [5]

There is a good chance that biometric authentication and verification will become more commonplace in the near future. Enterprise implementations and specialized applications such as ATM are more likely to use biometric as an alternative. The potential of this growing technology could not be ignored since it may become one of the most anticipated technologies to ensure that human's security and privacy are well protected.

CHAPTER 3

METHODOLOGY/PROJECT WORK

3.1 DATA COLLECTION METHOD

The author used 3 types of different methods for data collection. There are:

1. Observations
2. Readings/Studies
3. Questionnaires

3.1.1 Observations

In observations, the author play two roles while gathering data - that of a nonparticipant-observer or participant observer. For nonparticipant-observer, the author collected the needed data without becoming an integral part of the system. The author observes the natural activities and behaviors of the ATM users, as well as other environment factors such as the layout of the ATM itself, especially the security aspect. For user's behavior, the author focused on the time when the users enter they PIN. Actions such as how many times they need to re-enter the PIN, the errors when entering the PIN, or whether they've written their PIN anywhere and bring it when they use the ATM were recorded. Other than that, the author observes the security measures taken by the banks for user's protection such as security's camera, guards and so on.

For participant-observer, the author also play the role of the by become part of the system user. The author used the ATM to do banking transactions and observes the flow of the verification process as well as the security measures from user's view. The author then records the weakness and the area that can be improved to increase the level of security for ATM.

3.1.2 Reading/Studies

The author had done some readings from newspapers, magazines, case studies, white papers and journals that is relevant to the topics. The area of studies includes the frauds in PIN system, biometrics issue and about verification system. Besides that, the author had also collected lots of data from searching the web sites in order to gain knowledge on biometric products in current market. The findings from this method will be discussed in chapter 4.

3.1.3 Questionnaires

During the data collection phase, the author had prepared a written set of questions to which respondents can record their answers. The questionnaires are distributed to 100 ATM users to get their feedback on the current PIN system in ATM and to test their knowledge about biometrics technology. The results from the survey will be discussed in chapter 4.

3.2 PROCEDURE IDENTIFICATION

The author choused to use the Rapid Application Development (RAD) methodology for the project work procedure. Since the schedule for the Final Year Project is only about 14 weeks, the author had to use the RAD approach because it offers the best system development methodology for this project in order to decrease time needed to analyze, design and develop a system. Using this method can help a lot on shortening the system schedule and thus results in a speedy development.

There are four phases of RAD in designing a system:

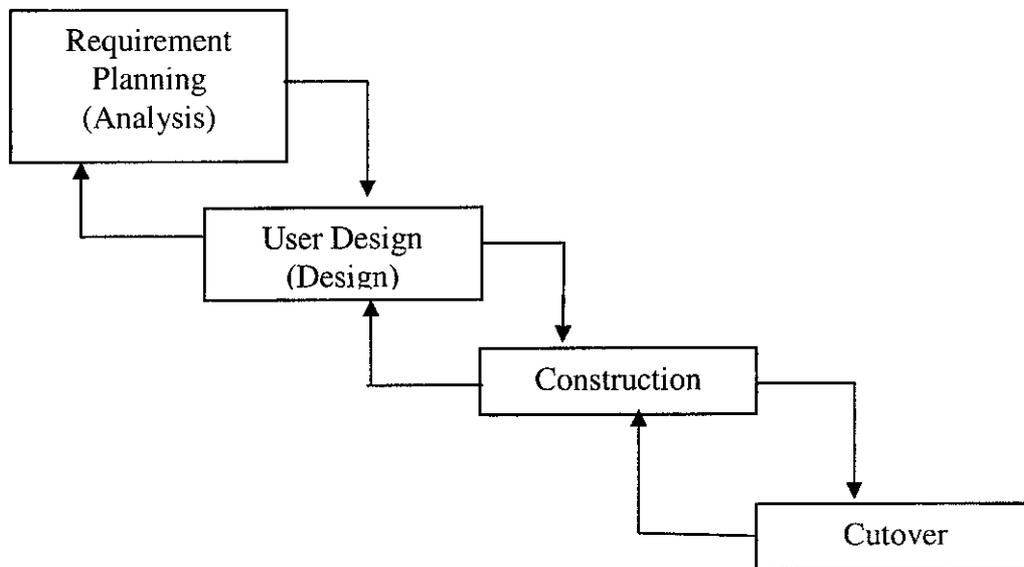


Figure 3.1: Phases of RAD Methodology

3.3 Project work

3.3.1 Phases of project

Requirements Planning Phase (Analysis) is where the author analyzes and identifies the problems regarding the PIN system. The author conducted an analysis of the ATM security system, in order to document the system and determine what problems exist with the current system. From the problem identification, the author comes out with a possible solution and set upon the objectives and significant of the project while collecting the data needed before analyzing the requirements specification for the system. During this phase, the author also determined the functions of the system and plans other phases. This phase is basically oriented towards solving business problems.

Next, in the **User Design** phase, the author have to design the prototype and come out with a conceptual model for the system, The author also have to refined phase with regards to the outcomes from the Requirements Planning. The output for the design includes design on the system model, the process flow and also the interface for the system.

Construction phase will follows the Design phase. This is where the author translates the designs into codes using Microsoft Visual Basic. In this phase, the author had also tested the functionality of each components and makes some adjustments to the code before users come and test, validate and review modules as they are built.

The last phase is **Cutover**. In this phase, the author developed conversion data and system and fully test the system before preparing the final documentation and oral presentation.

CHAPTER 4

RESULTS AND DISCUSSIONS

4.1 CURRENT ATM SECURITY SYSTEM

The author has done some research on the current ATM security system. The author have found out that password or personal identification number (PIN) is one of important aspects in ATM security system which is commonly used to secure and protect financial information of customers from unauthorized access. Customers will insert their ATM card in the card slot and they will be prompted to key in their PIN to grant access to their accounts. PIN typically in a form of four or six digit combination of numbers that entered through ATM panel. The system compares the PIN code against a stored list of authorized passwords and users. If the code is legitimate, the system allows access at the security level approved for the owner of the account.

From the author's observations, in order to secure customer's PIN from ATM scam when the customer is dealing with the ATM, banks has put a yellow line few feet from the ATM so that the person who in queue will be standing in a safe distant from the ATM dealers. In some places, banks put the ATM in a glass room where only one person can enter the room to do the banking transaction through the ATM while others will have to queue outside the glass room. This way, it will prevent any ATM scam from having a peek over a bank customer's shoulder at a machine, to get the person's PIN.

In general, PIN is sufficient to protect against fraud and effectively eliminating most common attempts to gain unauthorized access. The four or six digits PIN also easy to memorize and can be typed quickly with few errors but it quite difficult to be cracked if it is managed properly. In practice, however, PIN is often easy to defeat particularly those which are easily guessed such as family member birth dates, consecutive number - 1234, phone number and so forth. Moreover, ATM scam has found more sophisticated cracking program to get customer's PIN and steal money from the ATM easily.

4.2 INTRODUCTION TO BIOMETRIC IDENTIFICATION

The idea of replacing PIN key with biometric identification system in ATM has been widely discussed as a result of the emerging technology in biometric. Biometrics means “to measure life”. Broaden definition of biometrics is the science of identifying a person by way of unique biological characteristic such as fingerprints, a handprint, pattern of an iris, and any of which are read by a scanner and matched against an electronic version of file. There are actually two types of biometrics, that is behavioral biometrics and physiological biometrics. Behavioral biometrics is by measuring the way we do something such as signature verification, keystrokes dynamics and voice recognition. Whereas, the physiological biometrics is by measuring a person’s physical characteristics such as their fingerprint, hand geometry, retina scan or face recognition.

The underlying advantages of biometric identification includes elimination of common problems such as illicitly copied keys, lost or broken mechanical locks, and forged/stolen personal identification numbers (PIN) which can lead to automatic teller machine (ATM) and checking fraud. Biometric systems can be used for identification purposes involving security access systems in management information services departments, government agencies, ATMs/banks, law enforcement, prisons, international border control, and military agencies.

How does the biometrics technology work? Actually the principal behind the biometrics data capture is simple. A biometric system must have a sensor that pick up a physical characteristic, convert it into a digital pattern, and compare it to stored patterns for identification. For example, with fingerprint imaging, a person authorized to access secure files or a system submits his or her fingerprint to a digital scanner. This digitized print is stored in a computer library for retrieval when access is requested. An authorized user places his or her finger on a reader or scanner, and the resulting image is compared to the software library image. If there's a match, access is granted. The same procedure

is generally applicable to retinal scans, voice recognition systems, and palm, face and signature identification methods.

4.3 COMBINING SMART CARD WITH BIOMETRIC TECHNOLOGY

Typically, our security solution is based on three categories of identification data. The first one, it is based on something that we **knows**, like a password or PIN; the second one is based on something we **have**, a token like a key or a smart card; and the third one is something we **are**, such as or voice, fingerprint or our facial features. Usually, users accessing classified systems had to pass checks from two of these three categories. Earlier ATM designers decided to identify users by the first two of the above criteria, which are memorized PIN and a token that is our ATM card. Recently, the common magnetic strip ATM card has been replaced with a brand new smart card which comes in a greater flexibility and security. By combining biometric verification solution with the smart card, we can utilize the use of smart card. The user's biometric template is retrieved from storage by a smart card and can quickly be compared to a live sample.

Typical system may use centralized databases that can create many security risks and can add a substantial amount of traffic to the network. If the database is compromised, the entire biometric solution may also be compromised. Storing the template locally decreases processing time but may introduce difficulties if users move from machine to machine. Using smart cards may be the best way to go because they give the user portability and do not require centralized storage.

4.4 COMPARISON ON BIOMETRIC MEASUREMENT

They are many types of biometric measurements. This includes the behavioral and physiological measures. The author would like to focus on the physiological measures. There are fingerprints, hand geometry, eye scanning (retina and iris), and face recognition. The author will summarize each of the type before making comparison on each of them.

4.4.1 Fingerprints

Fingerprint identification is the most commonly recognized and most widely applied form of Biometric technology. Fingerprint ID is based upon the fact that a person's fingerprint is completely unique to the individual. A fingerprint is made of 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 the minutiae points. It is the oldest biometrics method and has already been used for a long time.

4.4.2 Hand geometry

Hand geometry is based on the fact that virtually every person's hand is shaped differently and that the shape of a person's hand (after a certain age) does not significantly change. When the user places a hand on the hand reader, a three-dimensional image of the hand is captured. Then, the shape and length of the fingers and knuckles are measured. Depending on the data used to identify a person, hand reading technologies generally fall into one of three categories - application to the palm, the pattern of veins in the hand and the geometrical analysis of fingers.

4.4.3 Eye Scanning

Eye scanning can be divided into two different fields, which is the iris scanning and retina scanning. Iris is the colored band of tissue that surrounds the pupil of the eye. An iris recognition system uses a video camera to capture the sample while the software compares the resulting data against stored templates. The retina is the layer of blood vessels at the back of the eye. Retina scans are performed by directing a low-intensity infrared light to capture the unique retina characteristics. An area known as the fovea, situated at the center of the retina, is scanned and the unique pattern of the blood vessels is captured.

4.4.4 Face Recognition

Face recognition systems identifies an individual by analyzing the unique shape, pattern and positioning of facial features. There are essentially two methods of processing the data: video and thermal imaging. Standard video techniques are based on the facial image captured by a video camera. Thermal imaging techniques analyze the heat-generated pattern of blood vessels underneath the skin. There are various recognition methods that emphasize identification based on the areas of the face that don't change, including:

- Upper sections of eye sockets
- Area surrounding cheek bones
- Sides of mouth

In the past, fingerprints were recorded by the application of ink to the finger which was then pressed to paper to give an impression. Fingerprints have been used as human identification long ago. People are familiar with it-and they trust it. Hand geometry is even older than digital fingerprinting; it was first used for security purposes on Wall Street more than 20 years ago. However, in Malaysia, the idea of hand scanning is not very popular compared to fingerprints.

Retina biometrics is considered to be the best biometric performers. However, despite its accuracy, this technique is often thought to be inconvenient and intrusive. The retinal scan, according to some studies, is more expensive and less "user-friendly" than fingerprinting. The fact that it requires the user to place their eye near a scanning device, which then reads blood vessel patterns unique to each person, is often a cause of discomfort. The retinal scanner requires an individual to stand still while it scans the unique patterns of the retina with a low-intensity light source.

By contrast, iris scanning uses a camera and requires no intimate contact with the reader; reading the retinal information. Eye and retinal scanner are ineffectual with the blind and those who have cataracts. However, it is difficult to gain general acceptance by the end user. Some are suspicious and don't want any of their physical features saved on some

database. They are frightened of iris and retinal recognition because they believe a laser will scan and thus damage their eyes. Cost is another thing that makes banks reluctant to deploy eye biometrics on a broad scale.

Facial recognition, which compares a user's facial characteristics with the stored results of an algorithm calculation (similar to a data hash), offers the ultimate security. Some systems match two static images, and others claim to be able to unobtrusively detect the identity of an individual within a group. But facial recognition has had only very limited success in enterprise applications, such as access to nuclear facilities, because of its cost and complexity. The attraction of this biometric system is that it is able to operate 'hands-free', limiting the amount of man-machine interaction. However, this system is highly unreliable and expensive. For example, it will not distinguish twins or triplets, not recognize the user after a haircut, and not recognize a person who changes from wearing and not wearing glasses.

Although many parts of the human body can provide data for electronic identification, users remain most comfortable offering their fingertips. Fingertip scanners are the most commonly used form of biometrics -- and the least expensive and easiest to deploy -- but not all scanners are the same. Some match the ridges in a thumbprint, others are straight pattern-matching devices, and still others take unique approaches such as ultrasonic. Here are more comparisons between the biometric measurement that the author taken from *IT Professional* (January/February 2001).

Characteristic	Finger-prints	Hand Geometry	Retina	Iris	Face
Ease of use	High	High	Low	Medium	Medium
Reasons for error	Dryness, dirt, age	Hand injury, age	Glasses	Poor lighting	Lighting, age, glasses, hair
Accuracy	High	High	Very High	Very High	High
User Acceptance	Medium	Medium	Medium	Medium	Medium
Required security level	High	Medium	High	Very High	Medium
Long-term Stability	High	Medium	High	High	Medium

Table 4.4: Comparison of Biometrics

From the analysis and comparisons between the biometric measurement, the author has come to a conclusion that accuracy, convenience (of user acceptance) and cost is among the main criteria in choosing which biometric measurement should be implemented in a particular system. The author thinks that fingerprint biometric is most suitable for ATM because it has high accuracy, can generally be accepted by user because it is convenience and many people are familiar with it. Moreover, the cost for the devices is affordable. Refer to Appendix C for statistic on biometric revenue. In order to get user respond towards this idea, the author has distributed a set of questionnaires to 100 ATM users. The data has been gathered and the author has come out with the results from the questionnaires.

4.5 RESULTS FROM QUESTIONNAIRES

Question 1: How many ATM card do you have?

A. 1 B.2 C.3 D.4

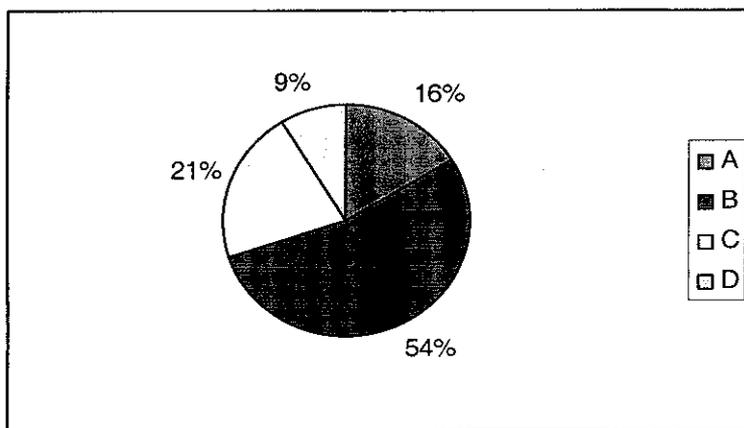


Figure 4.5.1: Results from Question 1

Question 1 was asked in order to know the average number of accounts owned by a person. From the pie chart, we can see that the average ATM card or accounts owned by a person is 2 cards that is 54%. The respondent for the questionnaires are taken among the UTP students and this may be the reason why the author get such result for the above question. If the respondent is taken from outsiders such as working people, the result may differ from this one.

Question 2: Can you recall your PIN easily whenever you use ATM service?

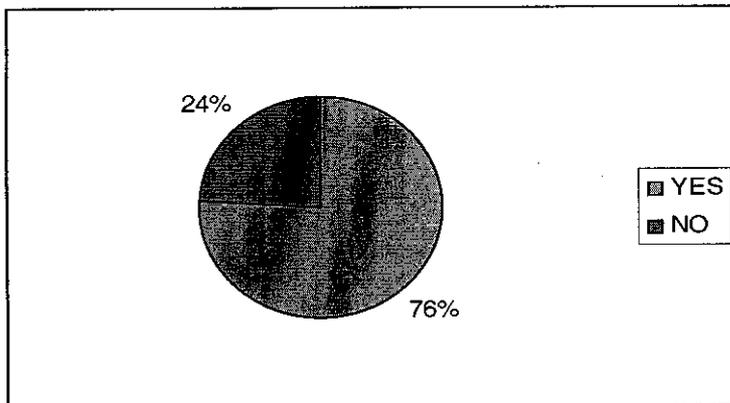


Figure 4.5.2: Results from Question 2

76% of the respondent can recall their PIN easily because most of them have used the same ATM card and PIN for years and they have only 1-2 cards. Another 24% of the respondent answer NO. This may be because they have many accounts and PIN to remember or the PIN has mixed up with other number

Question 3: Have you ever forgotten your PIN?

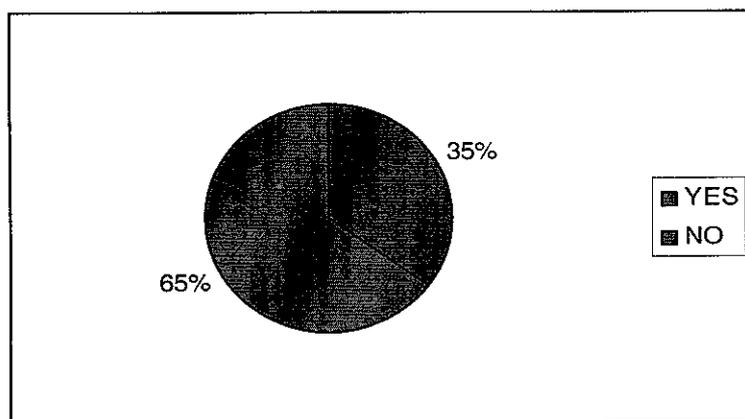


Figure 4.5.3: Results from Question 3

Only 35% of the respondent have experienced forgotten their PIN while another 65% answers that they never forgot their PIN. Again, this results may be due to demographic factor where students are still young and can remember number and codes easily compared to older people.

Question 4: Do you think the PIN system is still reliable?

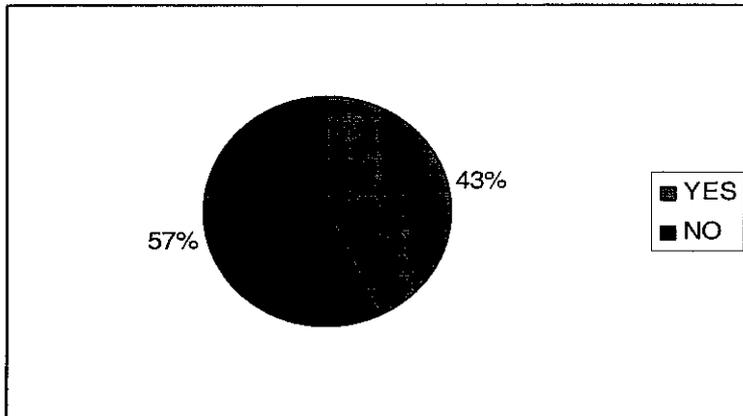


Figure 4.5.4: Results from Question 4

More than half the number of respondents, which is 57% thinks that the PIN system is not reliable in today's world. Most of them think that with the movement of technology, people shouldn't rely on PIN or password to protect their privacy. Most of them hate memorizing numbers. While 43% of the respondents think that PIN is still reliable because it is easy to use and because it has been used and trusted for a long time.

Question 5: Do you agree if the PIN system is replaced with biometric identification system (for example, fingerprint scanning) in order to gain access to your account in ATM?

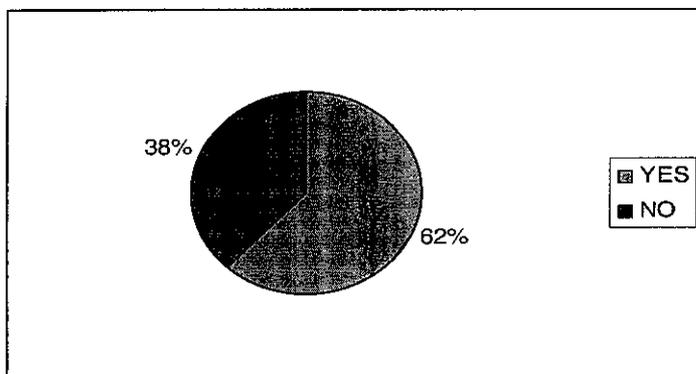


Figure 4.5.5: Results from Question 5

The author gets a very good feedback from this question. Most of the respondents agree that the PIN system should be replaced with biometric. 62% of them can accept the idea

and are looking forward for the new ATM features. Only 38% of the respondents rejected the idea and still favor the typical version of ATM.

Question 6: What kind of biometric that you find most comfortable with?

- A. Fingerprint
- B. Iris/Eye scanning
- C. Face
- D. Voice

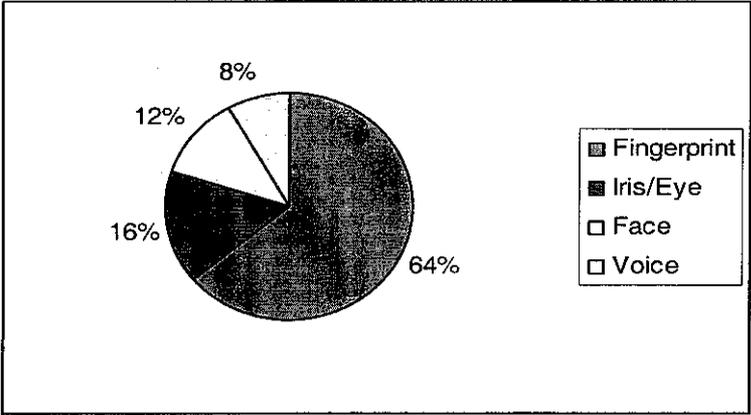


Figure 4.5.6: Results from Question 6

This question is to get user feedback on what biometric measurement that they comfortable with. From this question, the author can conclude that most users are comfortable with fingerprint biometric. 64% choose A for fingerprints biometrics. 16% favor iris/eye scanning. This respondents may be well known with biometrics technology and choose iris/eye scanning because they know it is most accurate. Another 12 % choose face and 8% choose voice recognition.

Question 7: Do you write your PIN anywhere?

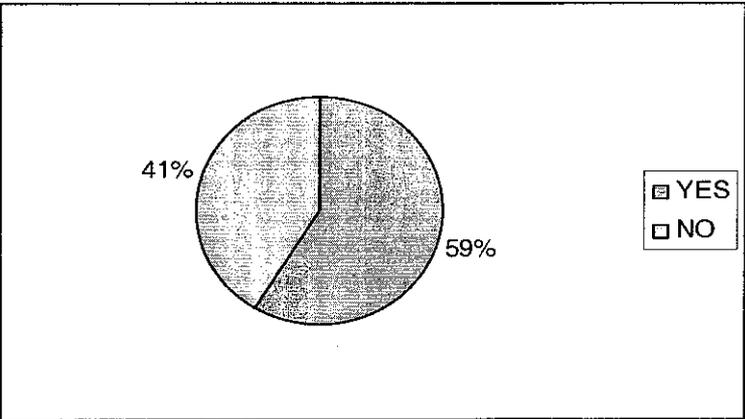


Figure 4.5.7: Results from Question 7

It is not surprising that 59% of the respondent have written down their PIN. This maybe happening to prevent them from forgetting the numbers or when they asked someone else to withdraw their money. 41% answers NO for this question.

Question 8: Would you asked your friend/family to withdraw your money from the ATM?

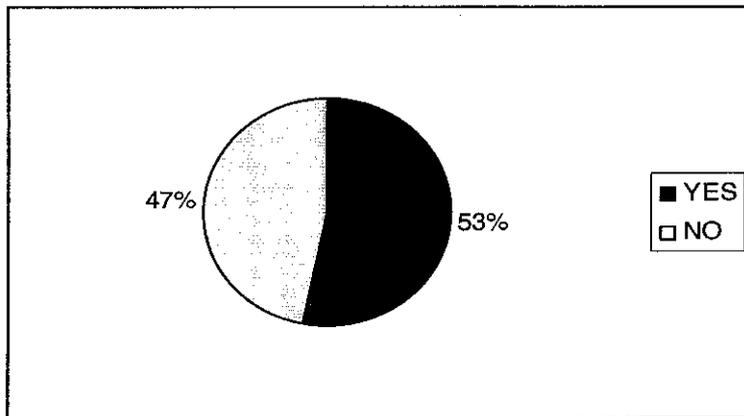


Figure 4.5.8: Results from Question 8

It is a common thing for the users to ask someone else that they could trust on to withdraw their money or doing other financial activities for them. That is why 53% of the respondent answer YES while 47% of the respondent would not ask anyone to withdraw their money.

Question 9: Would you feel threatened if you lost your ATM card?

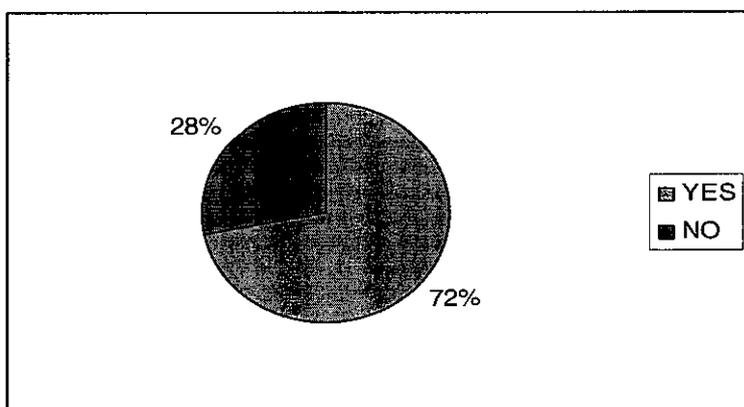


Figure 4.5.9: Results from Question 9

Most of the respondent answer YES for this question. They feel threatened and insecure when they lost their ATM card because they think that their money could be steal and

that their privacy is at risk. Only 28% of the respondents are not feeling threatened if their ATM card is lost because they trust the security measures taken by the bank to secure their money.

Question 10: Do you think the current ATM interface needs improvement? If yes, please state the improvement needed.

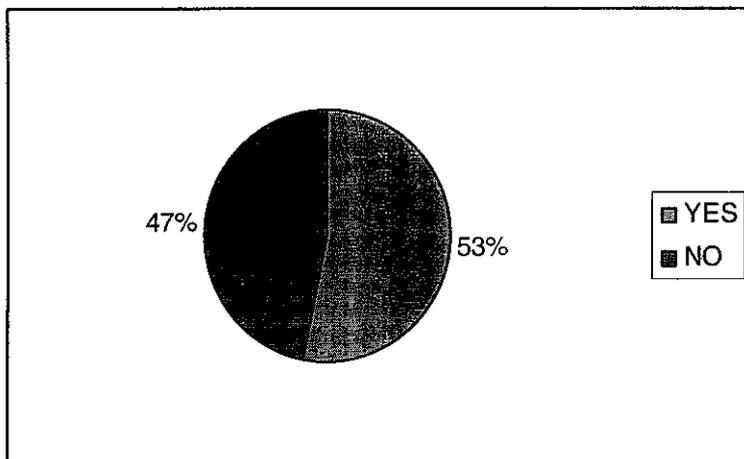


Figure 4.5.10: Results from Question 10

The response to the final question is quite balanced. 53% of the respondents request for improvement while 47% of them are comfortable with the current interface and don't really bother on how it should look like. For the comments on areas to be improved, most of them want the interface to be more user-friendly and interactive and want it to be more colorful and have more graphical user interface (GUI). Some even complained that some ATM screens are difficult to read due to the lighting effect. Some said that the ATM display screen is too high and difficult to reach. There are also complaints on the keypad which is too hard and is difficult to press.

From the results, the author found out that there's a need for improvement in the ATM verification system in order to ensure a reliable and effective security protection for ATM users. Biometric verification is the most suitable alternative for the PIN system, with fingerprint scanning as the favorable method selected by the respondents. Please refer to Appendix B for more options on fingerprint sensors.

4.6 PROJECT DESIGN

4.6.1 Process Flow

This is the process flow that the author designed for the enrollment and verification process in ATM transactions.

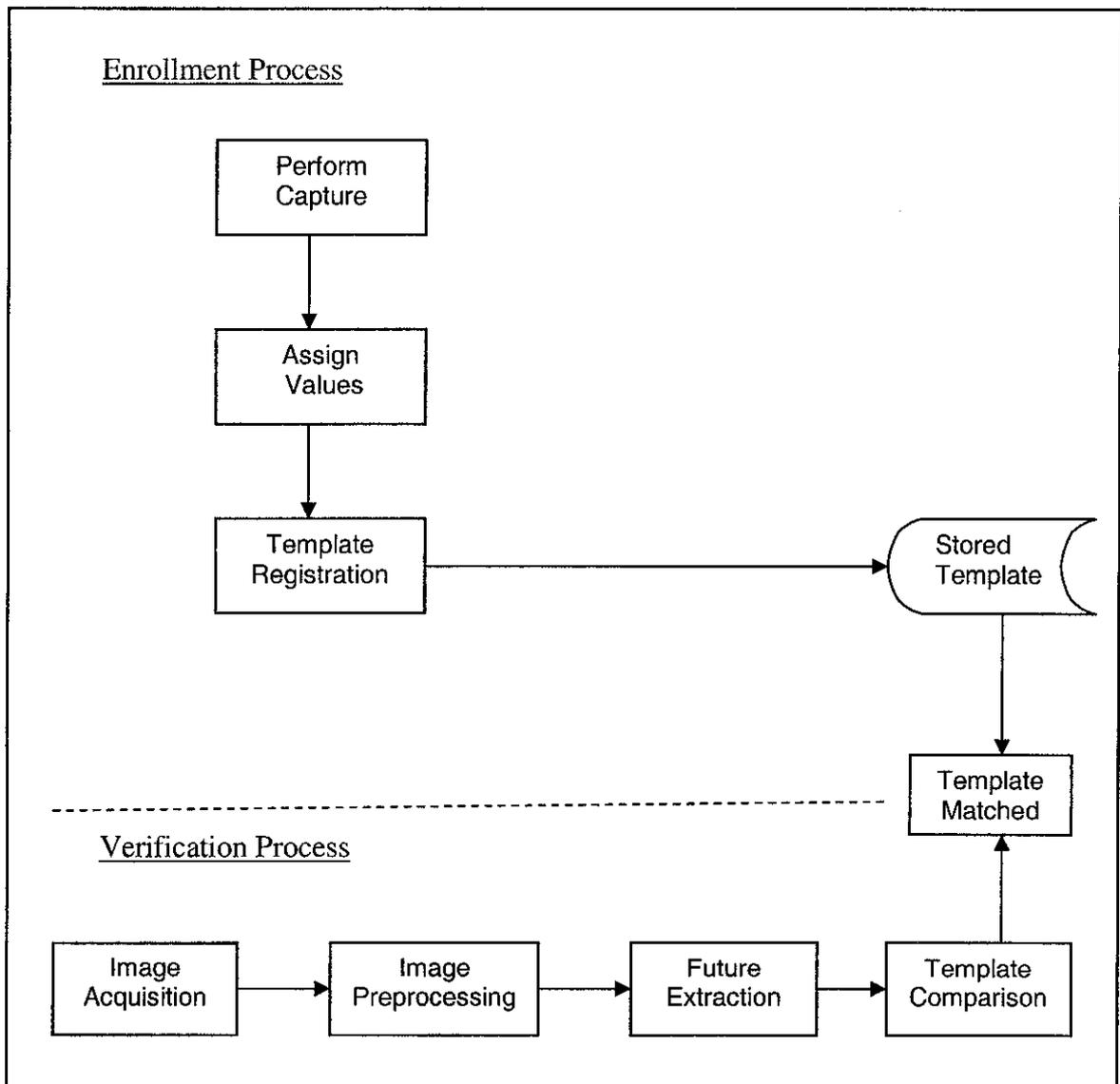


Figure 4.6.1: Process Flow for enrollment and verification process

Based on the ATM process that we have familiar with, the author had come out with her own process flow and activity diagram for the proposed system. Refer to figure 4.2 for the process flow and Appendix B for the activity diagram. There are 2 phases in the process flow that is the enrollment phase and verification

phase. In the enrollment phase, a first time user must be enrolled into the system before he or she can do any banking activity. The whole process starts with sample capture. In the capture process, scanner capture the biometric image and software will assigns values to a biometric image. These values will be considered as the template and is registered to the customer as their ID in the smart card.

During verification, when the customer initiates a transaction, the system scans the client's fingerprint for image acquisition, extracts the main features from the image, compare and matches this scan against the stored template, and approves or rejects it. It sends this result to the business software to either proceed with or halt the client's transaction.

4.6.2 Use Case Diagram

Here is the use case diagram that the author designs for the system:

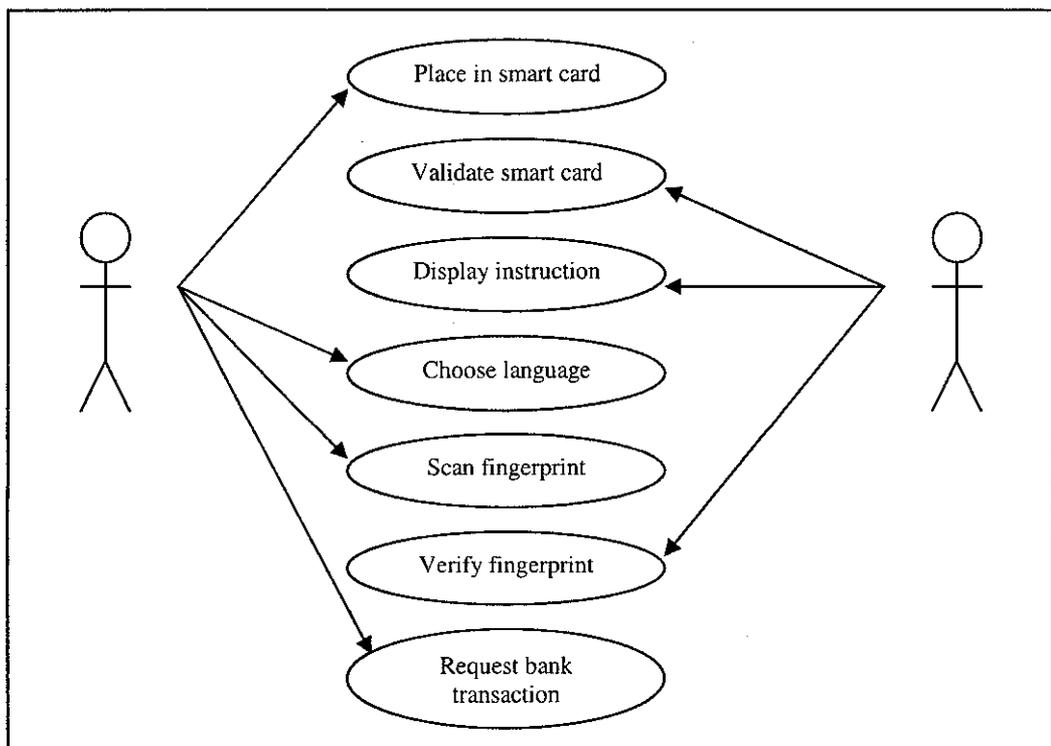


Figure 4.6.2: Use case diagram

The author designs a use case diagram for this system to show the interaction between the external entities which is in this case, the customer (ATM user) and the system itself. From the use case diagram, the customer interacts with the system by giving input (smart card and fingerprint) and by requesting bank transactions once they have been verified and approved by the ATM. On the other hand, the system interacts with the user by giving output which is the instructions and information retrieved from the user's smart card and by granting access to the user.

4.6.3 Activity Diagram

Activity diagram was designed to analyze the activities involved during the ATM's verification system take place. The activity should start when a customer/user initiate a banking transaction at the ATM. When the customer entered an automated branch to complete a transaction, the smart card was placed into an integral reader at the ATM. The customer information was read from the smart card, and the ATM screen would instruct the person, by name, to place a finger on the fingerprint reader. If the customer's live fingerprint matched the fingerprint template stored on the smart card, access to the customer's account was granted. The customer can then proceed with the banking activity. Here is the activity diagram designs by the author:

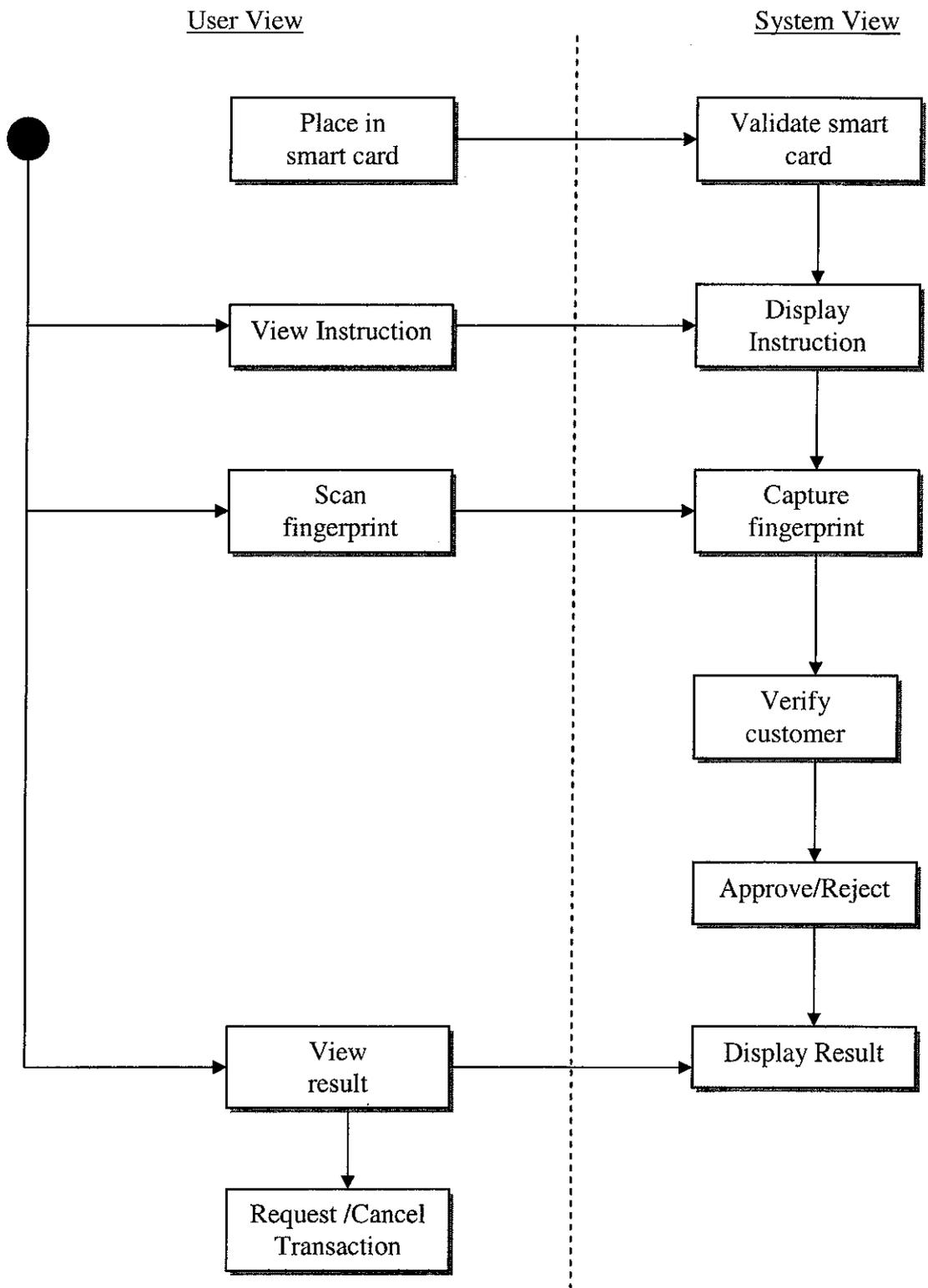


Figure 4.6.3: Activity Diagram

4.6.4 Interface Design

For the prototype, the author had also developed some interface with the ATM users as the target user. The prototype should enable the user to view and follow the step by step instructions in using the biometric devices and to make them understand how the verification system works. Besides that, the interface should also follow the basic guidelines for a good interface. A good interface is essential because a good interface will increase product credibility and acceptance. It will enable users to achieve their goals while reducing operation expenses and costly rebuilds. Some of the steps that were taken into consideration when designing the interface:

- Research customer expectations and needs.
- Review competitive and analogous products and services.
- **Design** solution concepts based on customer requirements.
- Build prototypes and test them.
- **Design** visual interfaces that support user interaction and product's functions.

The interface itself will help a lot in showing how the verification process with biometric technology takes place. Refer Appendix D for the layout of the interface.

CHAPTER 5

CONCLUSION AND RECOMMENDATION

5.1 CONCLUSION

The "Biometric Security System In ATM Transactions" is an idea that was proposed in consideration with the current trend of security measures as a result of the advance development of information technology in today's world. The whole concept is to make ways for biometrics technology as an alternative for the common personal identification number (PIN) in ATM security system. Major aim of this project is to fulfill the needs of greater security and protection from ATM fraud in order to reduce unnecessary lost.

The idea of combining smart card with biometric technology in accessing bank account at ATM may not been used widely in the world especially in Malaysia. However, the needs for a reliable security system and the advance development of technology must not be ignored. This project will adhere to the most basic requirements of ATM that suits the needs of Malaysians culture and ethical issue. This is how this system differentiate with other systems that were already exists in the market. The author put full hope that this project will be a successful one and may contribute to the efficiency of security for the society.

5.2 RECOMMENDATION

For future project work, the author would like to suggest that the research areas and the system features to be expanded. The research areas should include the numbers and statistics of ATM frauds especially in Malaysia in order to support the relevancy of the project. It is also recommended that the real technology be implemented so that it can really integrate with the system. Other recommendation is to upgrade the system's feature so that it will offer more services to the users besides what we already have nowadays.

Proposing the design, the author may try to design a duo-verification system so that user can have a choice whether to use a card along with the biometric or only use biometric to gain access to their account. This way, users may not depend on cards or any other tokens for verification because their selves are the key to the verification system.

The author also suggests that the prototype interface should maintain a user-friendly environment and a good navigation as well. Therefore, it is much hope that by enhancing the system, it could give new idea especially to Malaysian society the importance of biometric solution for effective and efficient verification and security process.

REFERENCES

- [1]. Nic Rigby, Wed 26 Feb 2003, "Concern over pin number fraud study", BBC News Online, <http://newsimg.bbc.co.uk>
- [2]. Sean Jackson, November 2000, Banking Technology Magazine, <http://www.bankingtech.com/archive/features/2000/11-shtml>
- [3]. ATM Scam: Lebanese Loop, <http://hoaxinfo.com/atmscam.htm>
- [4]. Chris Richard, July 21 2003, "Guard Your Card: ATM fraud grows more sophisticated", <http://www.csmonitor.com/2003/0721/p15s01-wmcn.html>
- [5]. Laura Bruce, March 2 2001, "Face-scanning, fingerprinting ATM's gain ground", <http://www.bankrate.com/brm/news/atm/20010302a.asp>
- [6]. Lim Dong-hun, "Biometrics, as a New Technology – Identifying oneself by using unique human characteristics", http://maincc.hufs.ac.kr/~argus/no343/t_c2.htm
- [7]. Marc Davis, "Biometric ID Technology Keeps an Eye on your Security Authentication Needs", <http://www.insight-mg.com/insight/00/08/art-06.htm>
- [8]. Maria Bruno, "Biometrics Are Too Hot to Handle, Despite high hopes, bankers are still all talk when it comes to identification technology", <http://www.banktechnews.com/btn/articles/btnsep01-1.shtml>

- [9]. Lucas Mearian, Jan 14 2002, “ Increasing security and fraud renew interest in alternate password methods”,
<http://www.pcworld.com/news/article/0,aid,79424,tk,dn011402x,00.asp>
- [10]. Jeffrey L. Whitten, Loannie D. Bentley, Kevin C. Dittman, System Analysis And Design Methods, 5th Edition, Mc Graw Hill.
- [11]. Donal Flynn, Information Systems Requirements: Determination & Analysis, 2nd Edition, Mc Graw Hill.
- [12]. Emmet A. Dulaney, Visual Basic 6.0 brief course, Glencoe McGraw Hill.
- [13]. Uma Sekaran, Research Methods For Business – A Skill Building Approach, Fourth edition, John Wiley & Sons Incorporated.

APPENDICES

APPENDIX A:
QUESTIONNAIRES

QUESTIONNAIRES FOR THE ATM USERS IN UTP

Question 1: How many ATM card do you have?

- A. 1 B.2 C.3 D.4

Question 2: Can you recall your PIN easily whenever you use ATM service?

- A. YES B.NO

Question 3: Have you ever forgotten your PIN?

- A. YES B.NO

Question 4: Do you think the PIN system is still reliable?

- A. YES B.NO

Question 5: Do you agree if the PIN system is replace with biometric identification system (for example, fingerprint scanning) in order to gain access to your account in ATM?

- A. YES B.NO

Question 6: What kind of biometric that you find most comfortable with?

- A. Fingerprint B. Iris/Eye scanning C. Face D. Voice

Question 7: Do you write your PIN anywhere?

- A. YES B.NO

Question 8: Would you asked your friend/family to withdraw your money from the ATM?

- A. YES B.NO

Question 9: Would you feel threatened if you lost your ATM card?

A. YES

B.NO

Question 10: Do you think the current ATM interface need improvement? If yes, please state the improvement needed.

A. YES

B.NO

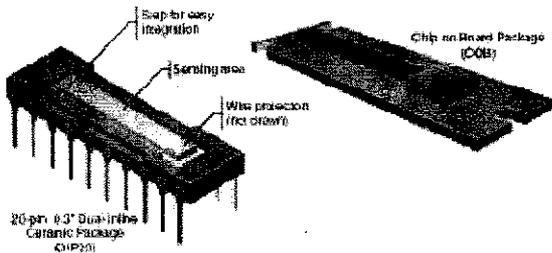
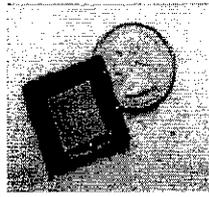
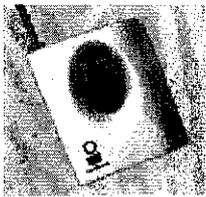
- THANK YOU -

APPENDIX B:
TYPE OF FINGERPRINTS
SENSORS

TYPES OF FINGERPRINT SENSORS :

5 types of sensors:

- Optical Sensor
- Capacitive Array Sensor
- Thermal Array Sensor
- E-field Array Sensor
- Electro-luminescent Sensor



Selection criteria:

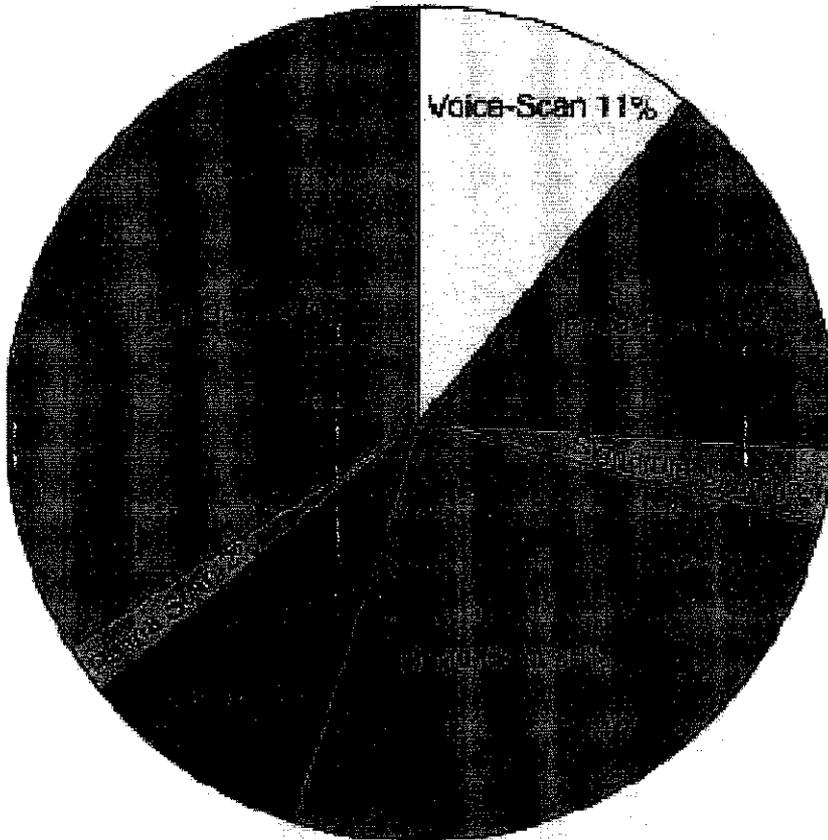
- Cost
- Size
- Durability
- Electro-static Discharge

COMPARISONS BETWEEN FINGERPRINTS SENSORS:

	Cost	Size	Durability	ESD
Optical	Low	Large	Fair	Good
Capacitive	Medium	Small	Poor	Poor
Thermal	Medium	Small	Poor	Fair

APPENDIX C:
BIOMETRIC REVENUE BY
TECHNOLOGY

1999 Biometric Revenue By Technology



© Copyright, International Biometric Group

Total 1999 Revenue: \$58.4 Million

Projected 2003 Revenue: \$594.0 Million

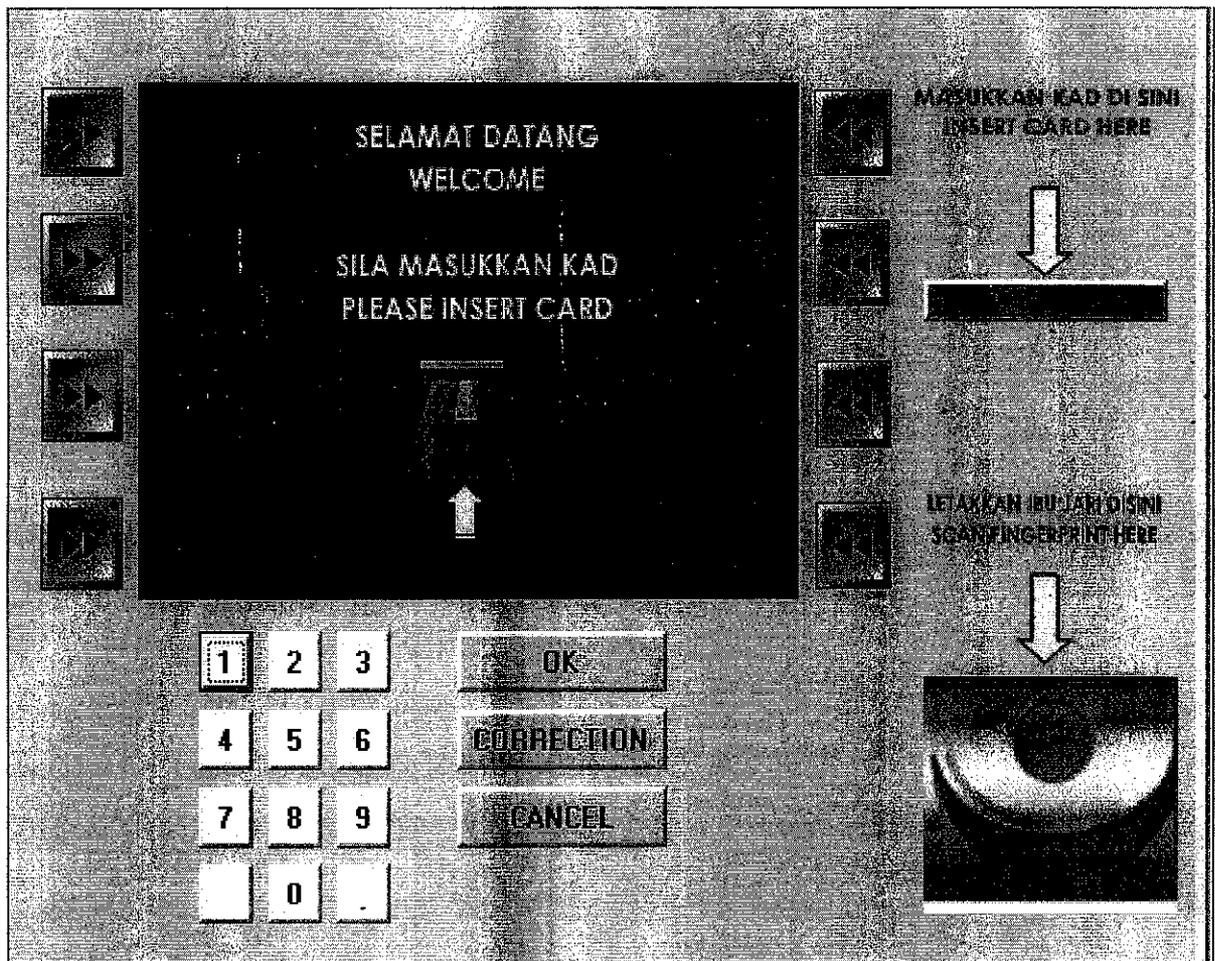
(revenue numbers do not include AFIS Systems)

APPENDIX D:

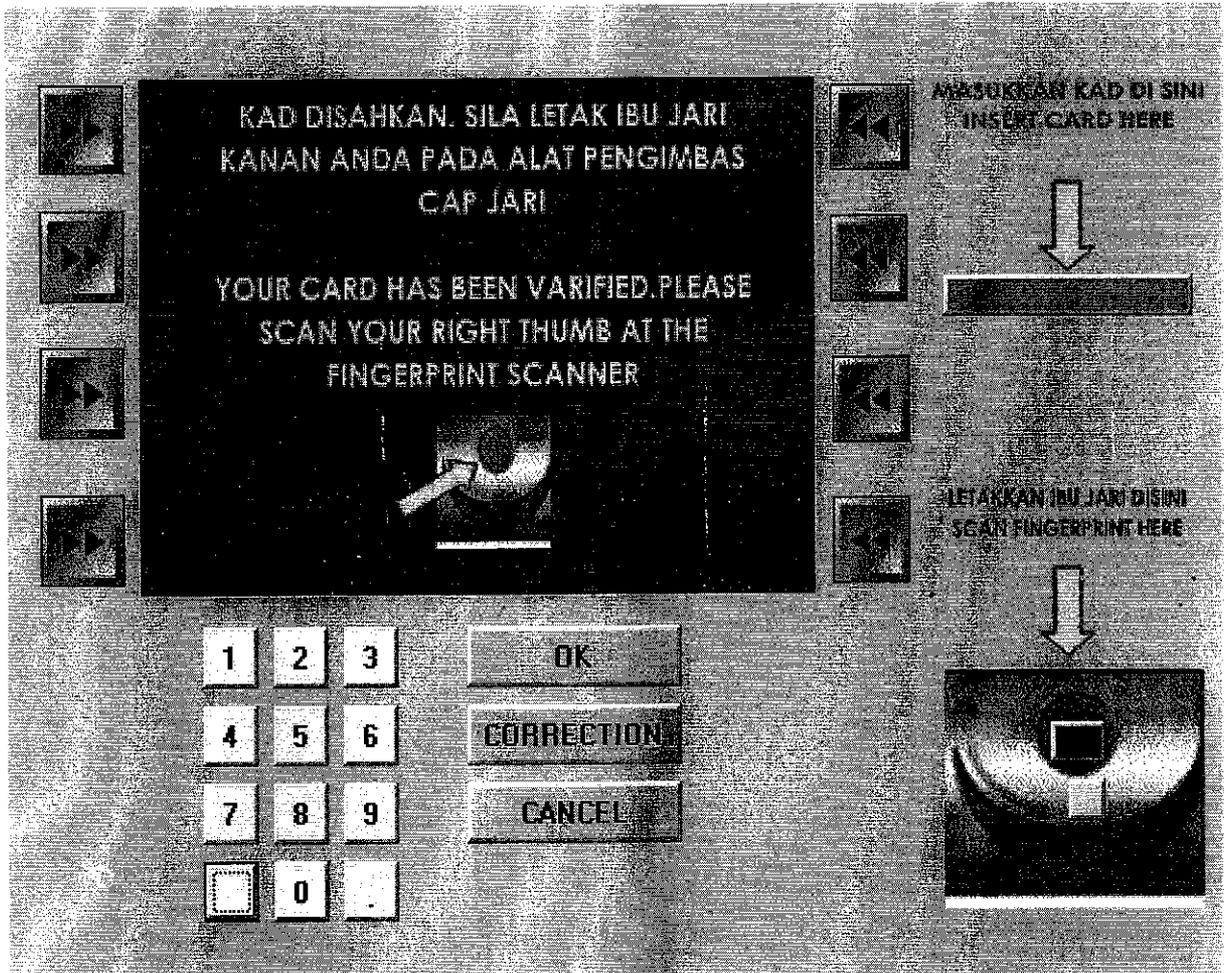
PRINT SCREEN OF DESIGNED INTERFACE

PRINT SCREEN FOR THE DESIGNED INTERFACE

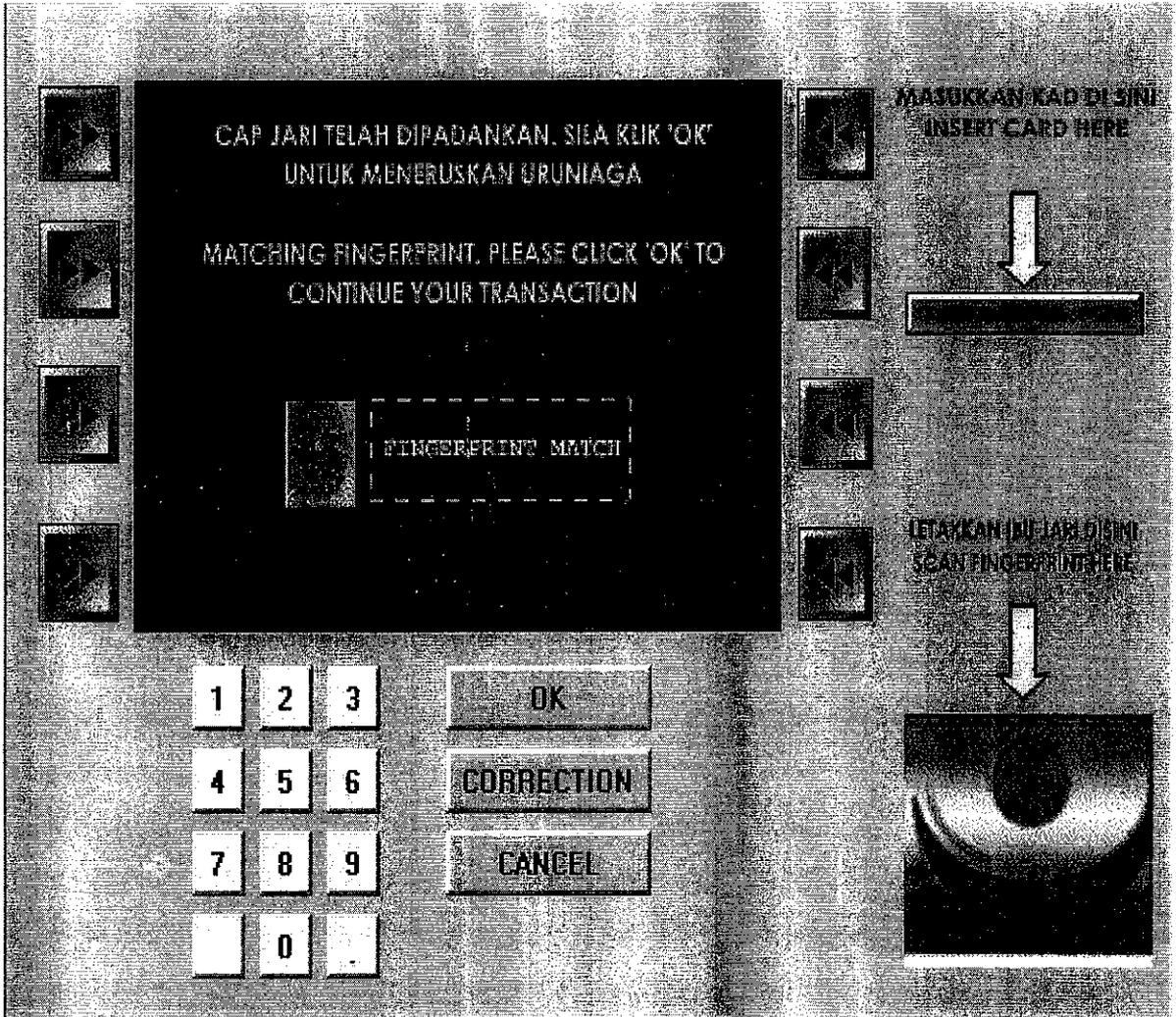
1. Main Screen



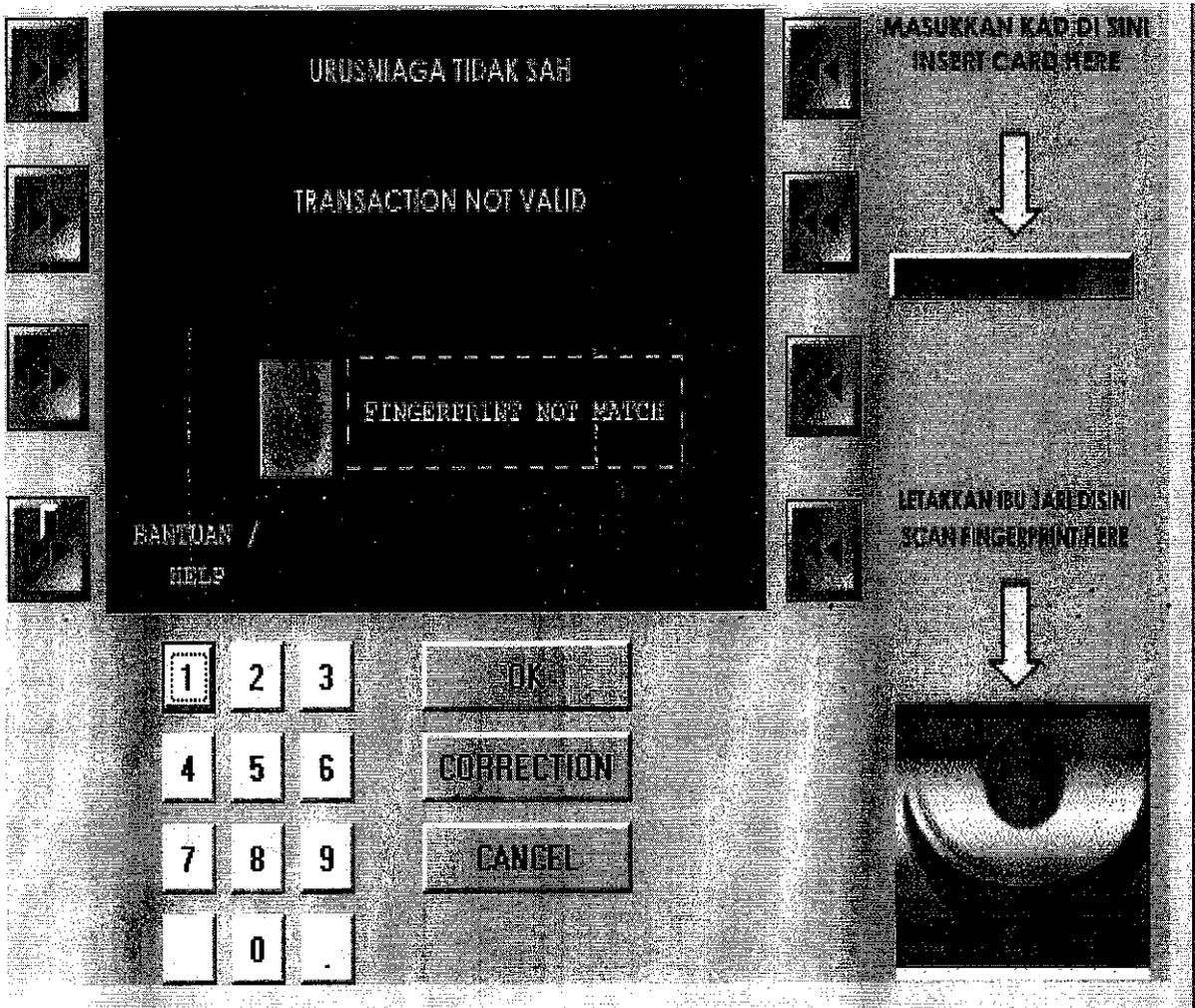
2. Instruction to scan fingerprint



3. Screen layout for a successful verification process



4. Screen layout for an unsuccessful verification process.



5. Help screen

