ATM APPLICATION USING MYKAD (APMY)

NABILA BINTI SHARUDIN

A thesis submitted in partial fulfillment of the requirement for the award of the degree of Bachelor of Computer Science (Software Engineering)

Faculty of Computer Systems & Software Engineering
Universiti Malaysia Pahang

MAY, 2011

ABSTRACT

This report is basically about ATM Application using MyKad. ATM Application using MyKad (APMY) is a system that upgrades the user convenience in using ATM. Besides that, in by replacing bankcard with MyKad, bankcard fraud can be reduced as Mykad is more secured. The existing ATM (Automated-Teller Machine) has weaknesses that should be overcomed. APMY is the best solution in order to prevent fraud from happening most of the time. Account holder that owns a MyKad is able to use this system. Compared to the old ATM system, APMY uses newly developed technology which is the MyKad which is more reliable than bankcard. MyKad, or Government Multipurpose Card, (GMPC) is the official compulsory identity card of Malaysia. It is regarded as the world's first smart identity card. So there is no burden in using MyKad because it must be carried around all the time. This system can only be used by Malayan Banking Berhad(MAYBANK) account holders and owns a MyKad. APMY is a standalone system which will be installed in the computer to use it. The system implementation requires usage of smart card reader such as EZ100PU, MyKad and a computer. In developing this system, Rapid Application Development (RAD) is chosen as the methodology. As a conclusion, APMY is build to improvise the user convenience in ATM usage and reduce number of cases of bankcard cloning.

ABSTRAK

Tesis ini adalah tentang ATM Aplikasi menggunakan MyKad. ATM Aplikasi menggunakan MyKad (APMY) adalah sebuah sistem yang menambahbaikkan kemudahan pengguna dalam menggunakan ATM. Selain itu, dengan menukar kad bank dengan MyKad, penipuan dan pemalsuan kad bank dapat dikurangkan kerana Mykad lebih selamat. ATM mempunyai kelemahan yang harus diatasi. APMY adalah penyelesaian yang terbaik untuk mencegah terjadinya penipuan dari semasa ke semasa. Pemegang Akaun yang mempunyai MyKad boleh menggunakan sistem ini. Dibandingkan dengan sistem ATM lama, APMY menggunakan teknologi yang baru dibangunkan iaitu MyKad yang lebih berteknologi tinggu daripada kad bank. MyKad, adalah kad identiti rasmi wajib Malaysia. MyKad merupakan kad pintar pertama di dunia. Jadi pengguna tidak dibebankan dalam menggunakan MyKad kerana MyKad sememangnya harus dibawa oleh rakyat Malaysia di mana sahaja mereka berada. Sistem ini hanya boleh digunakan oleh pemilik akaun bank di Malayan Banking Berhad (Maybank) dan mempunyai MyKad. APMY adalah sistem yang akan diintegrasikan di komputer untuk menggunakannya. Implementasi sistem memerlukan penggunaan pembaca kad pintar seperti EZ100PU, MyKad dan komputer. Dalam membangunkan sistem ini, *Rapid Application Development (RAD)* dipilih sebagai metodologi. Sebagai kesimpulan, APMY adalah untuk menambahbaikkan penggunaan ATM oleh penggunanya dan mengurangkan jumlah kes pengklonan kad bank.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Introduction

Automatic -teller Machine or known as ATM is used by nearly everyone around the world. The use of this machine is for cash withdrawal, cash transfer and many other services. In those days, there were no cases reported of stolen ATM card and unauthorized access into saving accounts. But nowadays, more and more cases have been reported. This problem can be solved by improvising the ATM system.

Automatic-teller-machines (ATM) use magnetic-strips cards to identify and authorize the person accessing them. The card contains details of the user's bank account and is protected by a Personal Identification Number (PIN). Users must enter the PIN connected with their card before they are allowed to perform any transaction with their account. The weakness in that is the only items needed to authorize the ATM transaction is the bankcard which is easily be cloned.

Magnetic-strips card faced a threat which is it can be cloned and therefore easy to be fraud. There have been many cases of bankcard fraud. The bankcard is vulnerable and it only takes few seconds to clone a bankcard using a cloning device.

In order to overcome this problem, bankcard should be replaced with a card that has better security which is MyKad. MyKad has a powerful chip that makes it harder to be cloned.

1.2 Problem Statement

More and more cases of stolen ATM cards have been reported lately. It is just not that. But later, the owner of the stolen ATM card finds out that his saving account has been emptied. This is mostly the result of bank card cloning. When the thief possess the bank card, there is no need to acquire the PIN as he has the ability to trick the system that the PIN he entered is correct although its not.

Besides that, user will have to bring around the bankcard every time he wants to use the ATM. It is inconvenient for user to bring around many cards whenever he goes out of the houses which are the identification card, license card and bankcards.

Also, in order to own a bankcard, user will have to pay some amount of money for the bankcard itself. It would save the cost if user won't have to create a new bankcard. Instead of paying for the bankcard, user could have use a card that every user has already owned.

1.3 Objectives

The objectives of this project are to:

1) Develop a prototype using MyKad for ATM application.
2) Produce a Produce Software Engineering document such as Software Development Plan(SDP), Software Requirement Specification(SRS) and Software Development Documentation(SDD) in order to develop an ATM application using MyKad.

1.4 Scope

The scopes of this project are:

1) Account holders as requested by the bank officer of Malayan Banking Berhad.
2) Users for this application are MyCard holder from the age of 12.
3) This application will be tested by 100 users.
4) The device used is EZ100PU Smart Card Reader.
5) The tools that will be used are Microsoft Visual Studio 2008 and Microsoft SQL Server 2008.
6) This system is a standalone system.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

There are many banking companies in the market nowadays. Most of the banking companies offer almost similar services such as saving accounts, loans and much more. In those days, whenever account holders want to withdraw cash, they will have to wait in such a long queue. It is such a waste of time. Then in 1939, Automated Teller Machine (ATM) was invented by Luther Simjian. However, it wasn't until the mid to late 1980s that ATMs became part of mainstream banking. [1]

An automated teller machine (ATM), also known as automatic banking machine (ABM), Cash Machine, or Cash point, is a computerized telecommunications device that provides the clients of a financial institution with access to financial transactions in a public space without the need for a cashier, human clerk or bank teller. [2] Automated teller machines (ATM) became an essential part of the banking business. [3] ATM made life much easier. People do not have to queue up and waste their time just to withdraw cash from their accounts.

2.2 Existing system

ATM system requires the account holder to slot in his bankcard. Then, after the bankcard has been detected, the customer is required to key in his Personal Identification Number (PIN). If matched, customer is now allowed to use any of the services offered.

Every banking company has their own ATM machine, uniquely designed based on their requirements. But the services offered are almost the same.

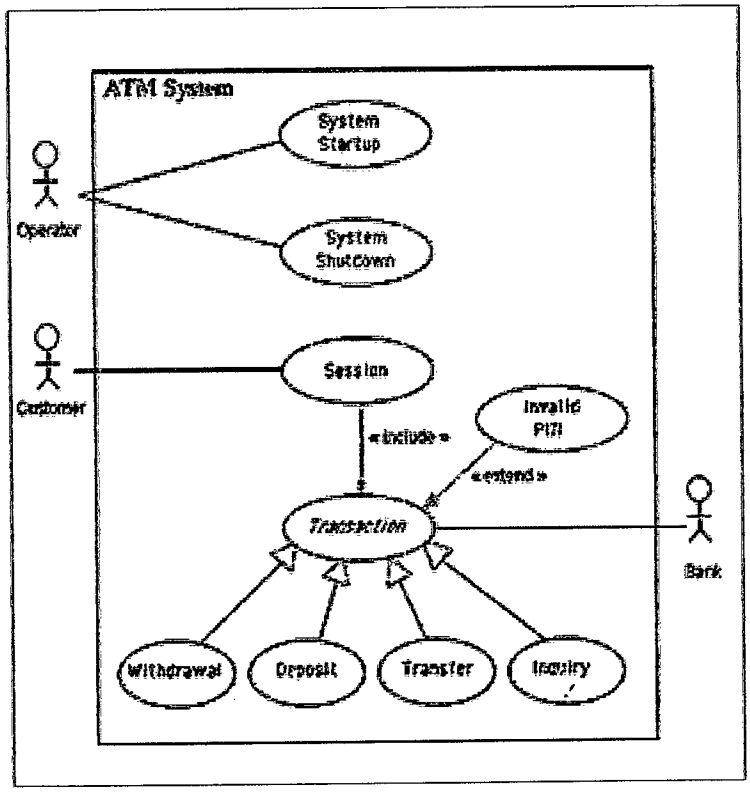

Figure 2.1 ATM use case

The services offered are usually cash dispenser, pay bills, print bank statement, balance inquiry, change of PIN and fund transfer.

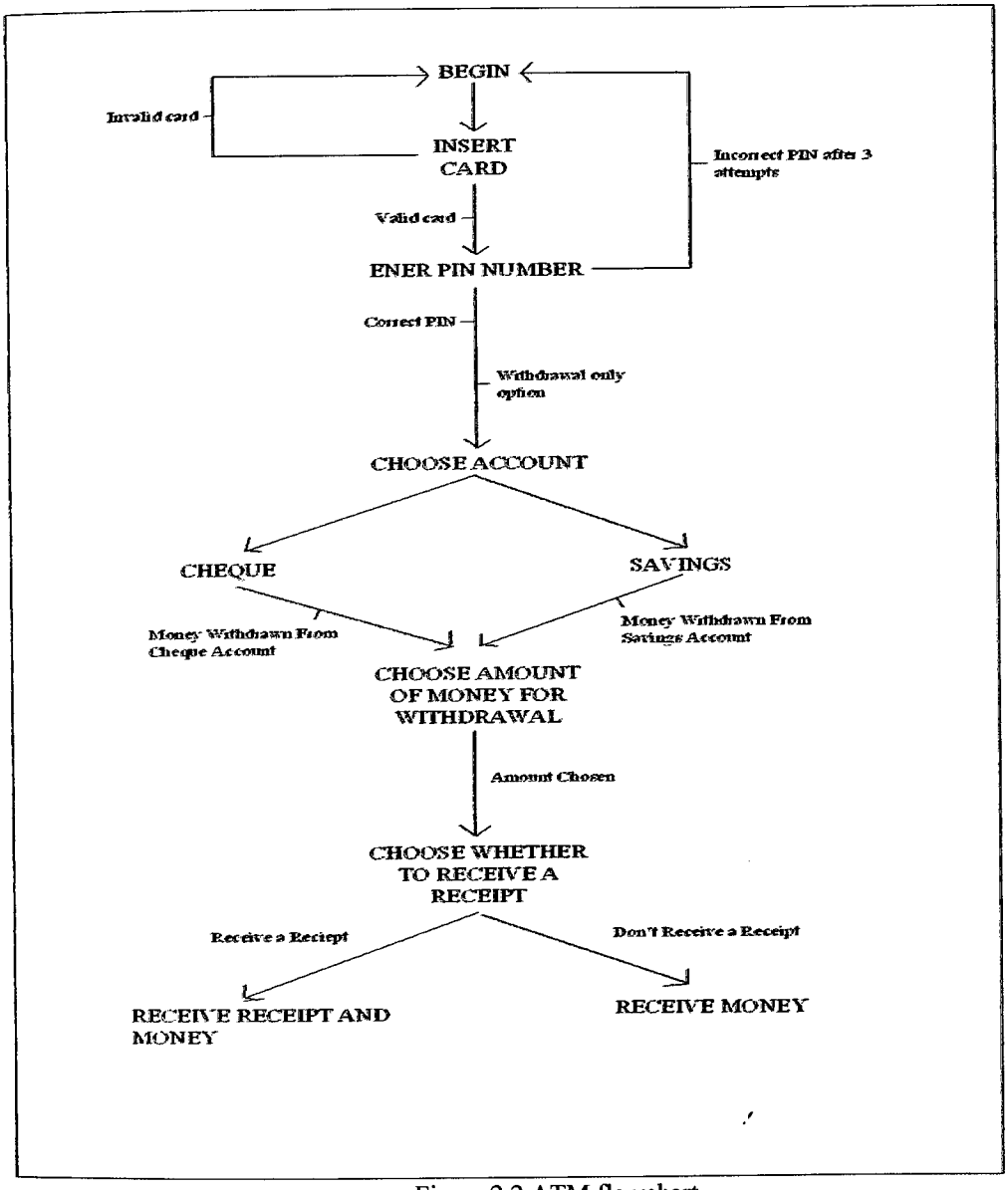

Figure 2.2 ATM flowchart

The flow of the process in using ATM machine is a simple flow. It begins with the user inserting the bankcard and keying in the PIN in order to perform the wanted task. There is no problem occur in using ATM as it is a simple process. However, the problems occur when the system can be fooled by a cloned card.

The system is unable to trace a cloned card. The cloned card which is very easy to be created has all the details of the original bankcard. All the details about the user account can be copied into a cloned bankcard. After creating a cloned bankcard, thief can acquire the PIN easily by spying on the user while he is making an ATM transaction or the thief can even cheat the system in believing that he is entering the correct PIN where else it's not the right PIN.

Every account user owns a bankcard that needs to be carried around every time he wants to use the ATM. It would be more inconvenience for users that own more than an account.

2.2.1 Magnetic stripe card

ATMs require user to slot in the bankcard and PIN in order to verify the legitimate user. The type of bankcard normal used by banking sector is the magnetic stripe card. Magnetic stripe card is a type of card capable of storing data by modifying the magnetism of tiny iron-based magnetic particles on a band of magnetic material on the card. The magnetic stripe, sometimes called swipe card or magstripe, is read by physical contact and swiping past a magnetic reading head. [4]

A magnetic stripe is the black or brown stripe that you see on your credit card, or maybe the back of your airline ticket or transit card. The stripe is made up of tiny magnetic particles in a resin. The particles are either applied directly to the card or made into a stripe on a plastic backing which is applied to the card.

The material used to make the particles defines the coercivity of the stripe. Coercivity is the measure of how difficult it is to encode information on the magnetic stripe. [6] Standard low coercivity stripes use iron oxide as the material to make the particles, high coercivity stripes are made from other materials like barium ferrite.

High-coercivity magstripes are harder to erase, and resistant to damage from most magnets likely to be owned by consumers. Therefore are appropriate for cards that are frequently used or that need to have a long life. Low-coercivity magstripes are easily damaged by even a brief contact with a magnetic purse strap or fastener. Magstripes require a lower amount of magnetic energy to record, and hence the card writers are much cheaper than machines which are capable of recording high-coercivity magstripes. Because of this, virtually all bank cards today are encoded on high coercivity stripes despite a slightly higher per-unit cost.

After a while since magnetic stripe card is in used, problems begin to occur. It turns out that this card can be easily cloned and fraud. Many people are trying hard to alter and counterfeit them in order to gain fund illegally. It only takes few seconds to clone a bankcard by using a cloning device.

2.3 Weaknesses of ATM

Although ATM is most needed in these modern days, there are drawbacks in using it. Many cash has been stolen from the ATM that causes lost of money from customer's saving accounts. Researchers who work for an Israeli computer security company say they have discovered a fundamental weakness in the system that banks use to keep debit card PIN codes secret while they are transported across bank networks – a flaw that they say could undermine the entire debit card system. [7]

There were many unexpected events happened that proves that ATM is no longer safe. Ng, 29 years old, pleaded guilty to electronically spying on people while they used ATMs. He had planted an electronic skimming device and pin-head camera in 36 ATMs in Sydney. [8]

There is also another fraud happened in the same country. A team of organized criminals is installing equipment on legitimate bank ATMs in at least two regions to steal both the ATM card number and the PIN. The team sits nearby in a car receiving the information transmitted wirelessly over weekends and evenings from equipment they install on the front of the ATM. [9]

Soon, more and more fraud happened and became headlines nearly every day:

i) $500,000 taken in skimming at a Sovereign Bank in New York City;
ii) 600 ATM customers hit in Nashville, TN;
iii) Three ATM skimming operations in Maryland, Illinois and Georgia netted thieves more than $120,000;
iv) 300 credit union members in North Carolina were victims of a skimming scheme;
v) A skimming operation in Houston, TX cost one bank $200,000;
vi) Three men arrested in Boston, MA on charges of ATM [10]

Next reported case is five Namibia men charged of having been part of a fraud ring that allegedly cloned 474 bank credit and debit cards and gift cards and then used the cards at automated teller machines throughout Namibia to withdraw large amounts of cash alleged to total some N$1,467 million from the accounts of customers of British bank Barclays PLC. [11]

There is also the most famous modus operandi used by bandits. When an unsuspecting customer inserts his or her card and enters their PIN, a message instructing the user to reenter the PIN is displayed because the machine cannot read the card's magnetic strip.

After several unsuccessful attempts to reenter the PIN, the user finds that he or she cannot remove their card and, in many cases, leaves the machine mistakenly believing that the machine has malfunctioned and retained their card.

In reality, the thief, posing as another customer pretending annoyance over the malfunctioning machine, was able to memorize the user's PIN following the unsuccessful entries, before leaving the area. After the unsatisfied user leaves, the thief returns to the machine, removes the plastic sleeve containing the user's card, reinserts the card without the sleeve, enters the user's PIN and empties their account. [12]

Figure 2.3 shows that another slot is being inserted in order to retained the user's bankcard and made user believed that the ATM has malfunctioned. [13]

Figure 2.4 shows that a camera is being set up in order to record the user's PIN. [14]

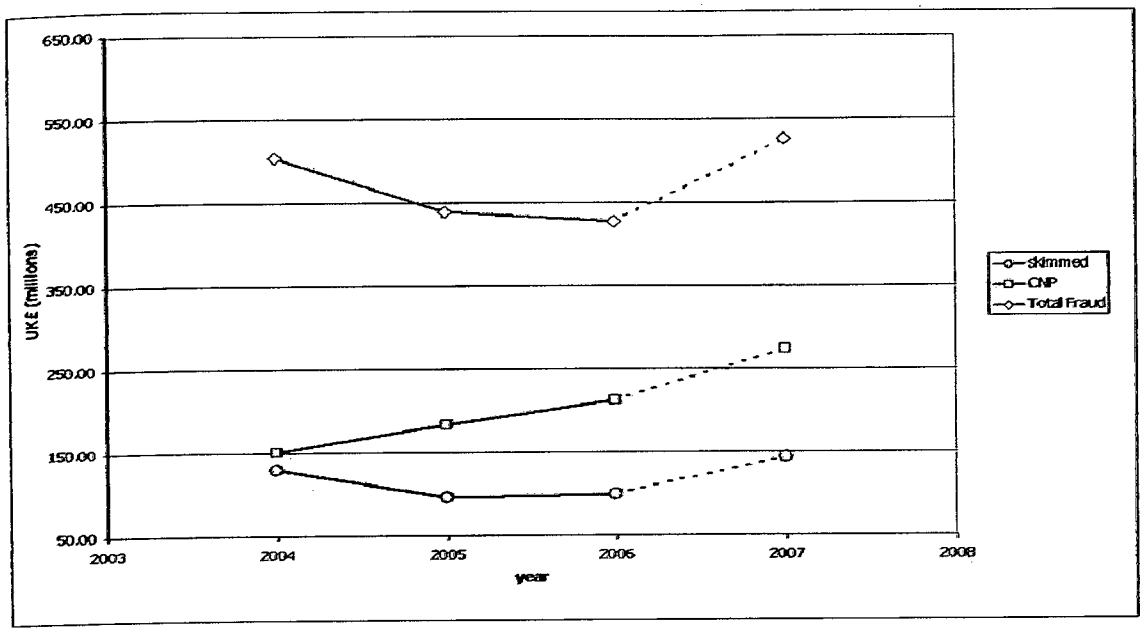

Figure 2.5: The proportion of skimming fraud in overall UK card fraud according to APACS (2007 figures are estimates based on Q1-Q2). [15]

This proves that the skimming of ATM has reached the critical level and actions must be taken in order to prevent more of unwanted things happen.

2.4 Solutions

Since the existing ATM that uses bankcard and PIN starting to lose the ability of securing the information and cash, other alternative should be implemented in order to stop more unwanted events from happening. A better card in terms of security is needed as a replacement of the bankcard. MyKad is the best replacement as it has higher security level that makes it harder to be cloned.

Also, as MyKad replaces bankcard, the benefit goes to the user where he does not have to carry around bankcard and he does not need to pay for the bankcard. Every citizen of Malaysia owns a MyKad which should be carried around all the time. Therefore, user can simply use the MyKad to make an ATM transaction.

2.4.1 Smart card technology

Magnetic stripe technology remains in wide use in the United States. However, the data on the stripe can easily be read, written, deleted or changed with off-the-shelf equipment. Therefore, the stripe is really not the best place to store sensitive information. To protect the consumer, businesses in the U.S. have invested in extensive online mainframe-based computer networks for verification and processing. [16] In Europe, such an infrastructure did not develop instead, the card carries the intelligence.

Smart cards are credit card-sized plastic cards that contain relatively large amounts of information in an imbedded micro-chip. [17] Smart cards differ from magnetic stripe cards in two ways: the amount of information that can be stored is much greater, and some smart cards can be reprogrammed to add, delete or rearrange data.

Smart cards are the technology of choice when fairly large databases must travel with an individual or an object. [18]For instance, a version of smart card technology is used to record service histories for automobiles. The data travels on a small tag on the owner's key ring. It can be reprogrammed, updated and accessed whenever the vehicle is serviced with any of that company's dealers.

As there is a microprocessor on the card, various methods can be used to prevent access to the information on the card to provide a secure environment. [19]This security has been made as the main reason that smart cards will replace other card technologies.

The microprocessor type smart card comes in two flavors - the contact version and the contactless version. Both types of card have the microprocessor embedded in the card however the contactless version does not have the gold plated contacts visible on the card. [20] The contactless card uses a technology to pass data between the card and the reader without any physical contact being made. The advantage to this contactless system is there are no contacts to wear out, no chance of an electric shock coming through the contacts and destroying the integrated circuit, and the knowledge that the components are completely embedded in the plastic with no external connections. The disadvantage to this is that there are some limitations to the use of the smart card.

For the ATM feature, there are two keys for security checks of MyKad – one is a bank key and one is a government key, so the card cannot be cloned. [21] That's what makes MyKad more secured compared to bankcard.

The possible benefits of the acceptance of smart card technology depend on the application in use. However, the ability to move large amounts of data with little or no increase in the security of the data will lead to many new applications being created that haven't been developed yet.

2.4.2 Types of smart card

There are two types of smart card. The first is really a "dumb" card which only contains memory. [22] These cards are used to store information. Examples of this might include stored value cards where the memory stores a dollar value which the user can spend in a variety of transactions. Examples might be pay phone, retail, or vending machines. Another example of a "dumb" card is the memory that is plugged into a Personal Computer (PC Card - used to be called PCMCIA).

The second type of card is a true "smart" card where a microprocessor is embedded in the card along with memory. Now the card actually has the ability to make decisions about the data stored on the card. The card is not dependent on the unit it is plugged into to make the application work. A smart purse or multi-use card is possible with this technology.

2.4.3 Identification card (MyKad)

"Malaysia will have the world's first national multi-purpose smart card. One card will have the individual's identification and electronic signature and access to government, banking, credit, telephone, transport and medical services." These are the words told by Dato' Seri Dr. Mahathir Mohammad, Prime Minister of Malaysia, speaking at the launching of the Multimedia Super Corridor on 1st August 1996. [23]