Auto Teller Machine (ATM) System Security with User Signature Image as Password

Mais Abid Khalil
Computer and Software Engineering Department, Al-Mustansiriya University/Baghdad
Email: manarabd2@yahoo.com

Received on: 21/2/2012 & Accepted on: 8/11/2012

ABSTRACT

This Paper will discuss Auto Teller Machine (ATM) system security facts and theft problems, crimes, hacking and attacks. In this paper will Implement ATM system that use the user signature image as password beside user's PIN information, to realize more secure verification and authentication to ATM bank users, also to strength the ATM security for prevent theft and to combat ATM crime. The ATM system will implement Inquiry, Deposit, and Withdrawal transactions for users.

Keywords: ATM, Checker, GMV, PIN, Deposit, Withdrawal, Inquiry.

أمنية نظام ماكنة السحب البنكي الالي باستخدام صورة توقيع المستخدم ككلمة عبور

الخلاصة

البحث سوف يناقش الحقائق الامنية لنظام ماكنة السحب البنكي الالي ومشاكل السرقة والجرائم والقرصنة والهجمات. في هذا البحث سوف يتم تنفيذ نظام ماكنة السحب البنكي الالي مستخدمين صورة توقيع المستخدم لهذا النظام واعتباره كلمة عبور بالاضافة الى معلومة الرقم الشخصي للمستخدم لتحقيق اكثر لامنية دخول المستخدم للنظام بالتحقق من معلومات الدخول والتحقق من شخصية المستخدمين لهذا النظام البنكي كذلك لاعطاء قوة اكثر لامنية النظام لمنع السرقة ولمقاومة جرائم النظام البنكي. هذا النظام سوف ينفذ معاملات الاستعلام والايداع والسحب للمستخدمين.

INTRODUCTION

The introduction of the auto teller machine in the 80s marked the first electronic banking transaction in Malaysia. However the recent development of the internet has changed the landscape of electronic banking. More products have been offered by banking institutions, in order to lure more customers. Not only constricted to consumer banking products banks are now offering online products to its business customer. The reliance on new technology to provide services makes security and system availability the central operational risks of electronic banking , Being able

to operate beyond their geographical boundaries meant banks might not be fully versed in a jurisdiction's local laws and regulations before they begin operations. The implication can be damaging to the bank's reputation. As the internet allows services to be provided from anywhere in the world, regulation and supervision are difficult to implement if not impossible. [1]

In the banking industry, technologies such as ATM networks and transactional Internet websites allow banks to interact efficiently with customers over long distances.[2]

The increasing convergence of mobile technologies and the Internet is rapidly giving way to mobile data services (MDSs) [3]. Among various MDSs, m-banking can add more value than other services [4,5]. M-banking is defined as provision and availability of banking services

With the help of mobile telecommunication devices such as mobile phones [6]. Typical functions include viewing account balances, transferring funds from one account to another, receiving alerts and paying bills. However, m-banking cannot support all banking functions. Forinstance, cash can only be withdrawn at physical branches or at automated teller machines (ATMs)[7]Banks should also ensure safety of financial transactions on the net and ATM via authentication, authorization, data integrity, and non-repudiation. Well-protected private networks should be employed where the source of the request for payment is recorded and proven. The devices such as message integrity, digital signature, digital wallet, secure electronic transaction (SET), electronic cash (e-cash), electronic cheque, smart cards, electronic bill payment and digital certificate can be used in this regard.[8]

TERMINOLOGY – ATM

What is ATM mean and where is they at?

An automated teller machine (ATM) is a computerized telecommunications device that provides the customers of a financial institution with access to financial transactions in a public space without the need for a human clerk, or bank teller. On most modern ATMs, the customer is identified by inserting a plastic ATM card with a magnetic stripe or a plastic smartcard with a chip, that contains a unique card number and some security information, such as an expiration date . Security is provided by the customer entering a personal identification number (PIN). Using an ATM, customers can access their bank accounts in order to make cash withdrawals (or credit card cash advances) and check their account balances as well as purchasing mobile cell phone prepaid credit. ATMs are known by various other names including automated transaction machine, automated banking machine, money machine, bank machine, cash machine, hole-in-the-wall, cash point, Bancomat (in various countries in Europe and Russia), Multibank (after a registered trade mark, in Portugal), and Any Time Money (in India) [9].

ATM is placed not only near or inside the premises of banks, but also in locations such as shopping centers/malls, airports, grocery stores, petrol/gas stations, restaurants, or any place large numbers of people may gather. These represent two types of ATM installations: on and off premise. On premise ATMs are typically more advanced, multi-function machines that complement an actual bank branch's capabilities and thus more expensive. Off premise machines are deployed by financial institutions and also ISOs (or Independent Sales Organizations) where there is usually just a straight need for cash, so they typically are the cheaper mono-function devices. In Canada, when an ATM is not operated by a financial institution it is known as a "White Label ATM". In North America, banks often have drive-thru lanes providing access to ATMs. Many ATMs have a sign above them indicating the name of the bank or organization owning the ATM, and possibly including the list of ATM networks to which that machine is connected. This type of sign is called a topper. [9]

Real facts on ATM security

The arrival of common computer operating systems onto the financial self-service scene, together with the use of IP networks for communications services, has resulted in a considerable increase in security risks for Automatic Teller Machines see Figure (1). Attacking ATM networks well organized and in a very highly sophisticated way, is a clear trend today in places like Eastern Europe or Latin America, and it will definitely become a very uncomfortable reality in the most advanced countries very soon.While typical attacks like skimming are little by little, being controlled, other types of attacks are beginning to rise. So, once you manage to introduce malware in the ATM, why not use it to withdraw cash? And even more, once an ATM has being infected and the cash withdrawal comes from the ATM’s inside, how can banks detect, and prevent this new type of fraud?

HOW TO COMBAT ATM CRIME

ATM, the problems

ATMs have spread like wildfire since the pioneer one in Enfield, now adding up to over 2 million around the world, offering huge advantages to both bank and customer. Right from the start, however, their security posed a tricky problem.

The valuable information contained in these devices and the fact that real cash is on hand are obviously tremendous lures for criminals. ATM hacking is now on the rise with some organized and highly sophisticated attacks. This has now become a real headache because both banks and customers are prone to heavy losses. According to figures of EAST (European ATM Security Team), the banks of 22 European countries lost between them 485 million euros in 2008 due to ATM crime.ATM attacks can be broken down into three types: theft of customer's bank card information or card skimming (magnetic stripe details and PIN), attacks on the ATM's IT infrastructure (and on the networks used to process transactions) and physical attacks at ATMs.

ATM, new threats

One of the main aims of ATM crime today is the theft of the credit card customer information. Until recently these credit cards consisted of a magnetic stripe storing the client identification information, allowing users to authenticate their identity and carry out their transactions safely. The magnetic stripe is easy to copy and falsify, encouraging thieves to perfect malicious techniques to steal this crucial information.

The commonest crime is called "card skimming"; this happens when the card's magnetic stripe details are captured at the ATM by a modified card reader called a skimming device. The captured information is then used for falsifying credit cards for subsequent fraudulent.

Technological weaknesses

Today's teller machines are pretty vulnerable. Many of them employ operating systems like Microsoft Windows (over 85% of security incidents occur on Windows systems) and use IP networks as their communication mechanism. This exposes the system to a high security risks due to the many vulnerabilities in open systems of this type, and they are also prone to malware infection.

Guaranteed Minimum Value (GMV) Solutions

To mitigate all these risks in a simple and effective way GMV has created checker ATM Security, setting up in the ATM a centrally monitored, managed and secure execution and communications environment.

checker is the first ever security product custom designed for financial self-service systems, enabling a centralized check to be kept of which applications are run on the system, which local or remote resources are accessed and which other systems are communicated with. By means of this cast-iron control checker ensures a high security ATM environment cutting off at source any infection by viruses, Trojan horses, worms or other malware, while also preventing any malicious software from being entered or run with access to sensitive ATM resources. Each ATM in which checker has been fitted has an Access Control List (ACL) giving an exhaustive definition of the processes, system resources (files and libraries) and permitted communications. Any other element not appearing on this list would be automatically blocked. The detail level of these control lists enables an exact definition to be given of what the ATM can and cannot do. Checker is topped up with a central server for managing and monitoring the ATM network on which the client checker has been fitted. Communication between the ATMs and server is end-to-end encrypted, enabling the ATM's security to be remotely managed and also ensuring that notification of any type of security event detected in an ATM is received in real time. [11]

Why using ATM checker?

Guaranteed Minimum Value (GMV) Checker ATM Security, the first Software product specifically designed for ATMs infrastructure, that will help you protect your ATM, and meet the PCI requirements quickly and effectively. **Checker ATM Security**, needless of continuous and unnecessary software updates, assures high-

security in ATM environments, rejects unauthorized network connections, restricts access to sensitive information, and controls unauthorized devices from being connected to the ATM and prevents from any malicious software being entered or run on any sensitive resource of the ATM, thanks to its innovative and lightweight performance security policy based whitelisting technology. All of these, combined with its centralized monitoring and management functionalities, makes checker ATM Security a unique product with just one single target focus, to prevent your ATM infrastructure from logical fraud.

An ATM must be compliant with a high number of requisites that makes a very difficult task to design a compact solution. ATMs must support multiple applications, each one more complex that the other, most of the times running over obsolete systems, with reduced resources and very often discontinued see Figure (2).[10]

Ideally we would require just one ATM security product that would do three simple things:

- Provides generation and management of the ATM-specific security policies, that could automatically be translated into rules for security controls.
- Enforces this rules (being it regarding execution, access, communication or any other security requirement) using one single, low footprint security product in the ATM.
- Provides centralized monitoring of compliance, including all required audit features.

Design and Implementation

The software to be designed will control a simulated automated teller machine (ATM) having a magnetic stripe reader for reading an ATM card, a customer console (keyboard and display) for interaction with the customer. The ATM will communicate with the bank's computer over an appropriate communication link. The ATM will service one customer at a time. A customer will be required to insert an ATM card and enter a personal identification number (PIN), also enter Signature password Id - both of which will be sent to the database of bank for validation as part of each transaction, if PIN and Signature matches (valid),then signature image will be displayed and The customer will then be able to perform one or more transactions see Figure (3) below.

The ATM must be able to provide the following services to the customer

1. A customer must be able to make a cash withdrawal from any suitable account linked to the card,
2. A customer must be able to make a deposit to any account linked to the card, consisting of cash and/or checks in an envelope. The customer will enter the amount of the deposit into the ATM, subject to manual verification.
3. A customer must be able to make a balance inquiry of any account linked to the card.

The ATM System provide customer with Input screen with three input values, PIN, Signature PassWord, and sum to be Deposit or Withdrawal and four commands:

Verify Passwords: to verify customer PIN and signature

Deposit and Withdrawal: for the sum to be deposit or withdrawal from customer account

Inquiry: this command will open Inquiry ATM screen according to PIN and Signature of Customer

ATM Inquiry screen: this screen will display customer inquiry information

The ATM will provide the customer with a printed receipt for each successful transaction or Inquiry, showing the signature password, PIN,ID, account name, signature image, gender, customer living address, available balance, type(deposit or withdrawal), finally sum(amount) to be deposit or withdrawal.

ATM main screen: this is banking system screen, just bank employee can open it and save Secret customer information.

ATM Input Screen

As mentioned earlier, this screen input customer informations(PIN, Signature and deposit or withdrawal sum of money). As example, if PIN=1234, and Signature ID=12, then customer click VerifyPasswords, the output will be as in the following Figures (4, 5) shown below:

If customer want to deposit sum=500, then click Deposit button ,the customer balance will change to 1500,finally customer want to check (his/her) account by click Inquiry button, then output will be as in Figures (6,7,8) as shown below:

Here the customer Manar has balance=1500, if withdrawal sum=1250 then balance will be 250.if after some time Manar want to withdrawal sum=500, but balance=250? Massage will be displayed to tell customer Manar that the balance is not enough to complete the Transaction as shown in Figures (9, 10) below.

ATM main screen is concerned with bank side and retain customer's secret and private account informations as shown in Figure (11) below.

The ATM transactions sequence in the screen buttons VerifyPasswords, Deposit, and **Withdrawal** respectively for ATM Input Screen are mentioned below with explanation to each customer transaction and Passwords Verifications. The Inquiry transaction (mentioned earlier) is implemented with database query engine and need just PIN and Signature ID as input parameters to display customer Inquiry screen See Figure (12) below.

CONCLUSIONS

ATM has gradually become a target of crimes due to it providing direct access to safe and cash.Deposit or withdrawal fraud, also Software and network attack and thieves try to infect the machines or hack into the ATM's internal data networks to steal the account information, all these reasons make us give more attention and care to built robust and effective ATM safe system with more sophisticated PINs and in the future adapt encryption principles for secure image signatures that make ATM crime is very difficult.more safe and convenient transaction platform and channel will be built up eventually.

REFERENCES

[1]. Noor Aireen Ibrahim, Advice Giving in a health, Australian Bureau Statistics, 2008

[2]. Berger, Allen N.,DeYoung, Robert., Technological Progress and the Geographic Expansion of the Banking Industry, The Ohio State University Press, 2006.

[3]. Lyytinen, K. & Y. Youngjin, Research Commentary: The Next Wave of Nomadic Computing. Information Systems Research, 2002.

[4]. Kim, G., B.S. Shin, & H.G. Lee, Understanding dynamics between initial trust and usage intentions of mobile banking.Information Systems Journal, 2009.

[5]. Economist, Leaders: Bank In Every Pocket? Mobile Banking. The Economist, 2007.

[6]. Mallat, N., Rossi, & Tuunainen, Mobile Banking. Communications of ACM, 2004.

[7].Saifullah M Dewan, Issues in M-Banking: "Challenges and Opportunities", IEEE, 13th,364-369, 2010.

[8]. Dr. Agboola A. A., Electronic Payment Systems and Tele-banking Services in Nigeria, Journal of Internet Banking and Commerce, December 2006.

[9]. Hwasung System Co.,Ltd, "Terminology – ATM", http://www.hws-kioskprinter.com,2009.

[10]. GMV innovating solutions, ATMsecurity.com, "Cheker ATM security", 2011, www.gmv.com

[11]. GMV innovating solutions, ATMsecurity.com, "How to Combat ATM Crime", Wednesday, 31 August 2011, www.gmv.com.

Figure (1) Automatic Teller Machine system.

Figure (2) ATM checker system.

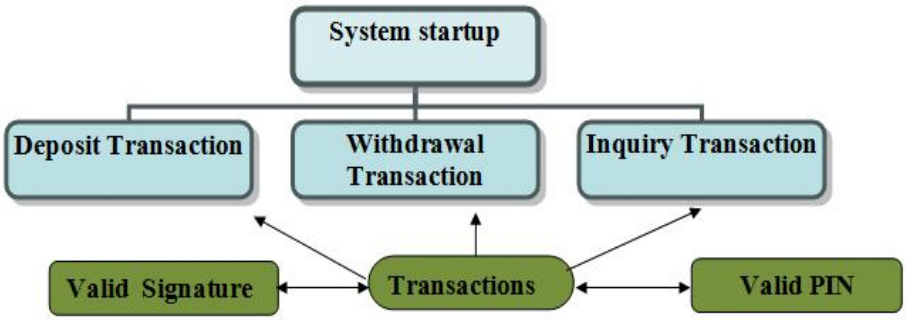

Figure (3) ATM system.

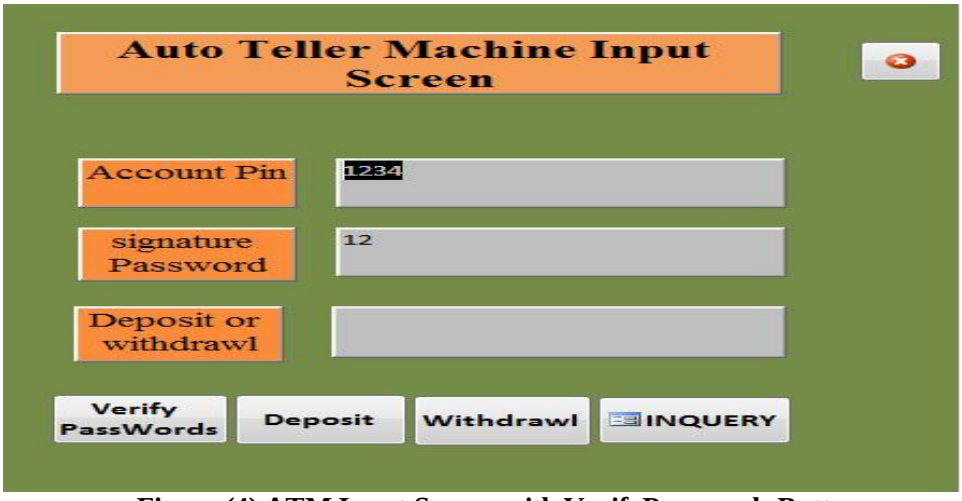

Figure (4) ATM Input Screen with VerifyPasswords Button.

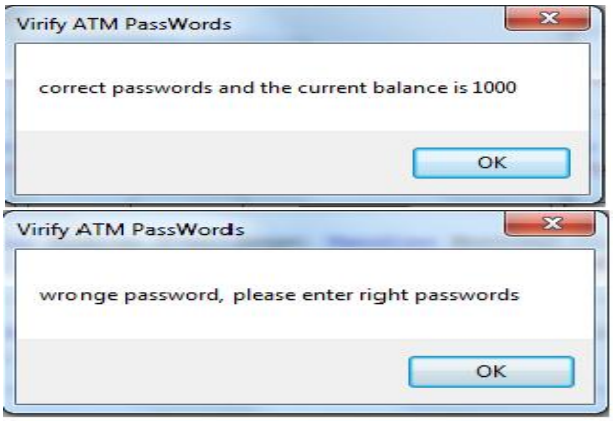

Figure (5) Verify ATM Passwords messages (Correct or wrong Passwords).

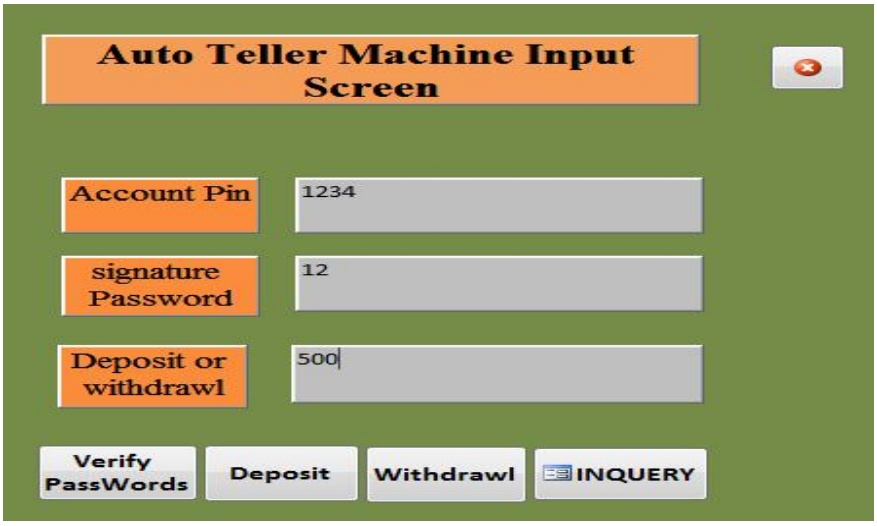

Figure (6) ATM Input screen with Deposit Transaction.

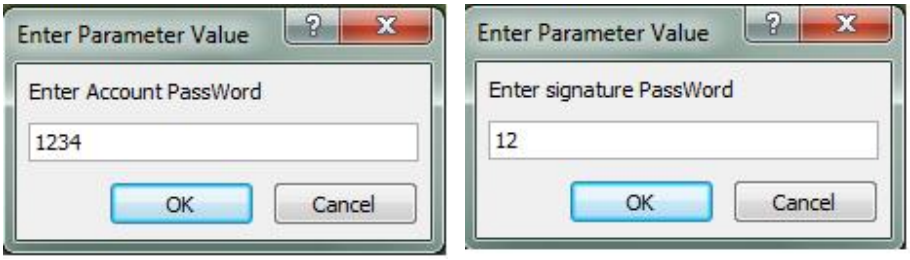

Figure (7) ATM Deposit messages with the new Customer Balance (PIN and Signature Password for Inquiry).

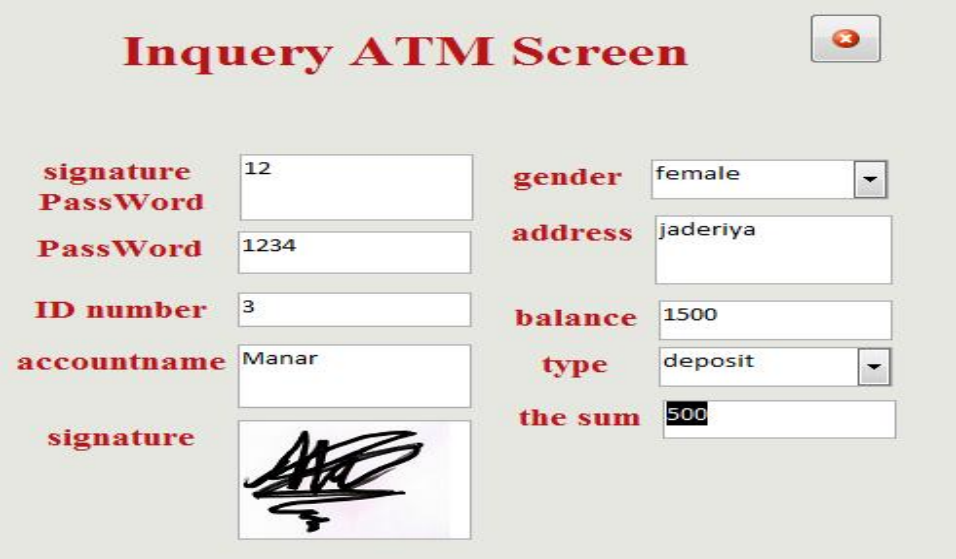

Figure (8) Inquiry ATM Screen (Customer Information).

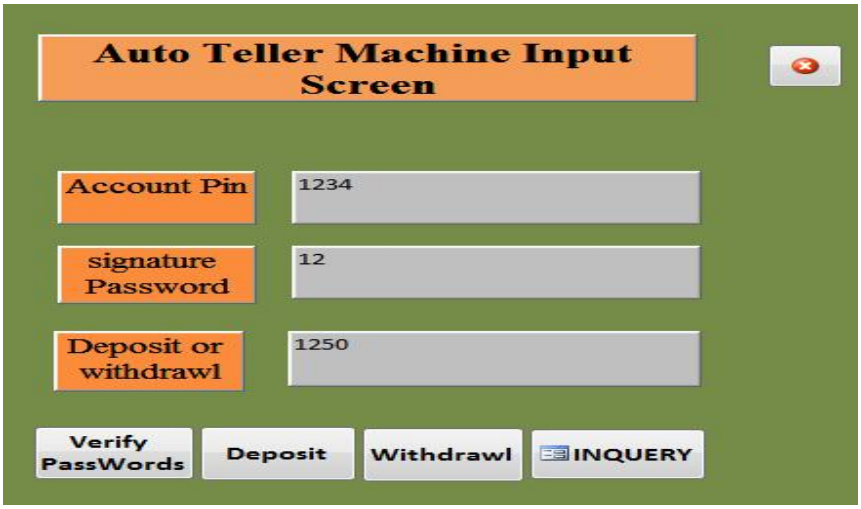

Figure (9) ATM Input Screen with Withdrawal Transaction.

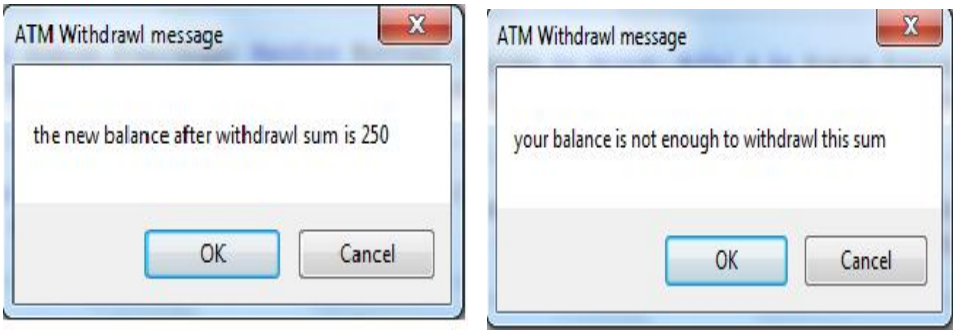

Figure (10) ATM Withdrawal messages with the new Customer Balance.

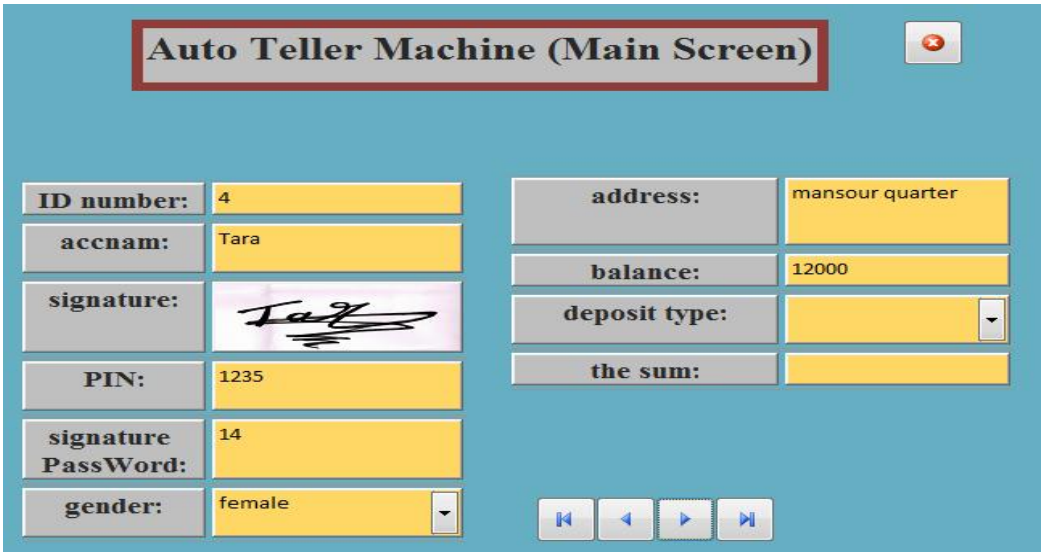

Figure (11) ATM Main Screen (Bank side).

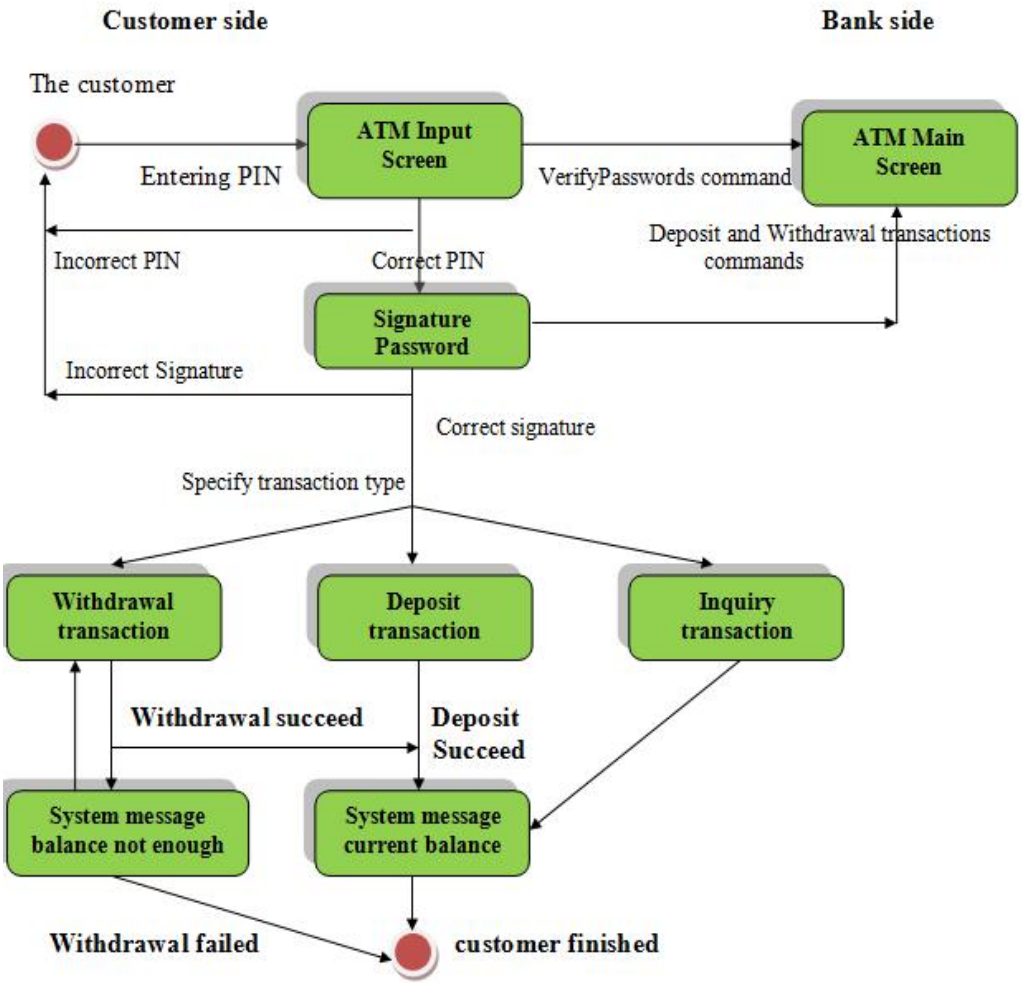

Figure (12) ATM transactions sequence and Implementation diagram.