Automatic Teller Machine System Security by Using Mobile SMS Code

Muhammad Aleem
Department of Computer Science, University of Lahore, Pakistan

Saad Bashir[2]
Department of Computer Science, University of Lahore, Pakistan

Sayyam Malik[3]
Department of Computer Science, University of Lahore, Pakistan

Muhammad Tahir[4]
Department of Computer Science, University of Lahore, Pakistan

Abstract

The main objective of this paper is used to develop a high security in Automatic Teller Machine (ATM).In these system bankers will collect the mobile numbers from the customers and then provide a code on their mobile number. In most country existing ATM machine use the magnetic card reader. The customer is identifying by inserting an ATM card with magnetic card that hold unique information such as card number and some security limitations. By entering a personal identification number, the customer is authenticated first then will access bank account in order to make cash withdraw or other services provided by the bank. Cases of card fraud are another problem once the user's bank card is missing and the password is stolen, or simply steal a customer's card& PIN the criminal will draw all cash in very short time, which will being great financial losses in customer, this type of fraud has increase worldwide. So to resolve this problem we are going to provide the solution using "Mobile SMS code" and ATM "PIN code" in order to improve the verify the security of customers using ATM system and confidence in the banking area.

KEYWORDS: ATM, PIN, Inquiry, Biometric, Magnetic Strip, Iris Recognition, Face Recognition

Problem statement

Researchers have been approved in the field of authentication and key exchange protocols which is based on passwords. Password based user authentication is low cost and easy to apply but the use of passwords has built-in flaws. The user chosen passwords are inherently weak because most users select short and easy to remember passwords [10]. The main problem in ATM machine is authentication security, which is very much week and based on just PIN code.

Objectives

[1] To research scope of Mobile SMS code authentication technique in ATM.

[2] Mobile SMS code: the Mobile SMS code is used in the ATM machine. It must verify the customer's mobile number after entering the Mobile number then give the code through Mobile SMS.

[3] Remote authentication: In which system can compare the customers mobile number and PIN code information using the remote data server

I. Introduction

1.1 What is ATM and where are they at?

An Automatic teller machine (ATM) is a telecommunication and computerized system or device that allows the customers and beneficiaries of financial institutions to carry out financial transactions without having contact with bankers and

clerks and tellers. Today's modern ATM cards are made of plastic with magnetic strip that have a unique identity or PIN number and some security information. This card is used to identify the user or customer. Security is maintained using a secret PIN number or code. Using ATM card, a customer can check status of balance and can withdraw cash and also can buy goods through credit facility. 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]. ATMs are not only placed in premises of financial institutions but also in large and medium shopping center, educational institutions and other busy locations to facilitates customers. But it is only placed at secured and safe place with reference to ATM machine as well as Customers.

ATM machine installation:

There are two types of ATM installations.

(i) On premises

On premises ATMs are advances comparatively, these are multifunctional machines that are resembles with actual bank branch in terms of cash dealings like deposit, withdraw, balance check, money transfer, transaction cancelation etc. these are more expensive machines.

(ii) Off premises

These types of machines are installed on those places where people have simple need to withdraw cash and balance inquiry and no more. These are simpler and cheap due to simple system and services as well as technology.

1.2 Why ATM Security is needed?

ATMs have been remain a part of financial institution since more than a decade and combination of technology in terms of software and hardware made it possible to carry out transactions without visiting bank branches and meeting with bankers. It also facilitated to make transaction round the clock. But since the birth of ATM it has been remain vulnerable to various threats specially security. There are two types of threats to ATM machines, first physical threat and second virtual threat. Former can be control using physical measures of security but later is very tough and difficult to overcome due to various factors. . A very general justification to protect and ask ATM secure is that it keeps a significant amount of money in its belly. It can be steal using physical force that is not possible all the time. But this money can be stealing without being suspected because machine asks just a PIN code. It never bothers whether person receiving money is authentic or not. Like a thief can be traced out using security cams and alarms but a person who mischieves and withdraw money using some ones ATM card is very difficult to stop from withdraw cash instantaneously. If someone lost his ATM card of someone any way become seceded in knowing one's PIN code. Then there maximum chances of actual customer's loss due to no mechanism to detect correct customer because PIN number is the only way to become authenticated and authorized to get money or make transaction.

I. Literature review

What is identification and authentication?

Identity and authenticity are very common but very important terms with reference to security in cyber world. The former term describes identitification of a person or user of the system. While the later term

describes the authority of a person or a user to use a system or account. In short, here in terms of ATM, Identity and authentication mechanisms are collectively used to secure the transaction on an ATM machine by checking that who is using ATM machine. And the person who is using a card to make transaction has any authority to carry out that transaction. Hence identity and authentication are mea measures to protect and make a transaction secure. So various measures have been implemented to make sure that the identity and authenticity of ATM users to protect bank's customers. These measures include PIN code verifications, Biometric identifications through thumb and iris detection. Bu tin this paper, we are going to add another security mechanism to further strengthen the security of transactions via ATM machines.

1. Real facts of ATM security

The common computer operating systems along with IP based networks for computer communication has made the ATM a very vulnerable cyber devise. It has considerably increased the security risks for automatic tell machines across the globe. Sophisticated attacks on ATM machines in developed as well less developed countries as a glaring trend that is getting pace with every passing day. Europe and Latin America are more vulnerable. As skimming attacks are under control but cuber attacks are still out of control. So it is very clear that whether ATM is secured or not, but people have lot benefits from ATM cash transactions. But of one skim or misuses ones PIN code then who bank or machine can detect that who is real gamer.

2. How to combat ATM crime

ATM has been spread all over the world like fire due to huge advantages to banks and customers. There are almost more than two million ATM across the world to facilitate bank's customers to carry out transactions round the clock. From beginning of the ATM, security of the atm remains a tangling problem. Two things create lure for criminals, one information of the customers and banks and second the one hand cash. This has been turned into a severe problem for banks and customers. Because ATM hacking is one of the rising criminal and cyber crime activity of the present times.

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.

3. ATM New Threats

Theft of money and user account information hacking from ATM machines is now turned into another sort of grim situation. This new threat is theft of customer's credit card number. Until recent times, credit cards consisted of magnetic type of strip which contained user information like identity and authentication to carry out a safe business or other transactions. But loopholes in magnetic strip allowed the bad minds to steal information to make misuse of credit card via internet. Theft of credit card information at time of transaction is called "card skimming". It happens often when a user inserts card into machine to make transaction then some ill will people copy data from strip and later on misuse this data. So this new threat has also added into problems of cyber transaction mechanisms.

4. Technological weaknesses

ATM machines are not secured enough both physically as well as technologically. Many ATM systems are working over operating systems like

Microsoft Windows that is not considered secure and safe for web transaction. Almost more than 80% security incidents are on the part of Microsoft Windows. Because they still uses IP based network mechanism. This lack of technological measures, ATMs are at high vulnerabilities and threats of being hacked. They are also prone to malware infections.

An Overview of previous security measures:

The above given identification and authentication measures have sole purpose to make financial transaction safe and secure through ATM machines. If a wrong person tries to make transaction, machine must be intelligent enough to detect and identify the wrong user of ATM card. PIN coed system and biometrics have been worked for ATM security. But in this era of cyber world, these security measures are too vulnerable, PIN code specially. Biometrics proved good after PIN code but it is clear from the example of iphone that was launched with unique feature of biometric security system. But unfortunately it was hacked by a hacker very next day after it was launched. Hence, no one can say these PIN and Biometric systems perfect and invulnerable.

a) PIN:

PIN code identity and authentication system is mainly based on a matching algorithm. User enters the PIN code. Machine encrypts the PIN that travels over the internet routs and reaches to Banks database. At bank's end, PIN number decrypts and it is matched with saved PIN in banks repository. If match algorithm returns true then transaction is successful otherwise failed? The only PIN number is not enough because, identity and authentication mechanisms are fail to identify the actual and authorized person. PIN code never enables the machine to retaliate against wrong user. Hence, a wrong person can easily get money from ATM if one steal PIN coed any ways.

b) Biometrics:

Biometrics encompasses all those means and measures using uniqueness of human organs that are used to implement security in information processing systems. In context of ATM machine, biometrics have special interface for biometric processing systems. User of ATM machine first get himself identified at machine as original customer. After getting identified, customer enters PIN code that is verified and transaction becomes complete. Biometric systems also based upon pattern matching algorithms. Data from biometric device is transfer to database where patterns are matched and if user is identified as true person then process proceeds to next. Otherwise machine may capture card or alarms the user. There are two main sources, fingerprints and Eye iris, are used as biometric identity verification. Biometrics is much better than PIN code system.

c) Facial recognition:

Facial recognition is also a type of security measure through biometrics but algorithms use in facial recognition is new on plate form of computer sciences. It is concept of machine learning to make our machines to intelligent enough to identify the true user of ATM or credit card.

A Critical glance at PIN, Biometrics and Facial Recognition

Currently, PIN code is mostly using to make ATM transactions all over the world. Biometrics and facial

recognition are also being used as part to identify and authenticate users and users. Lets us discuss the loopholes in these three security mechanisms of ATM transactions. First: PIN code is a four number digits code that is generated by computer and assign to customer for ATM transactions. A person to withdraw cash from ATM machine is just need ATM card and pin code. Hence security measures are enough fool proof. One may lost his ATM card, or one's card may b misused b y some one other who knows the PIN code anyways. Second: biometrics is many times securing mechanism to identify and authenticate a genuine customer but it undergoes two issues. One is that if one causes an injury on thumb or hand or lost his print impressions some way. Then it becomes impossible to get oneself to be identified at machine. Moreover in case of any disability, he can't send any one else to withdraw cash from ATM machine due to strict biometrics identity mechanisms. Second factor involve in biometrics critics is cost of machine to implement biometrics hardware and software systems. Hackers have successfully hacked biometrics systems. Third: facial recognition is also comes under criticism because in today's time of style and fashion, youngsters even professional people have started to become trendy in fashions. As they adopt no facial style or beared, hears, any surgery etc. they would have to go to bank to submit their new picture to be identified at ATM machine. Moreover, system to implement facial recognition is also an expensive and high maintenance task at ATM centers.

5. Parts of Proposed ATM machine

I. Insert card

First and for most step in ATM transaction is to insert card in machine and then the remaining processes continues if the credentials of card are valid and verified

II. Enter PIN code

After the card is valid in terms of account and date, machine interface asks customer to enter a secret PIN number or password of atm. The PIN number is processed over the network by creating contact with bank's database. If PIN number is correct then machine proceeds to next step.

III. Enter a machine generated Code from mobile phone

This is the additional step that is added into this paper. Machine sends a automatically generated code via SMS to user's mobile phone. This code is entered user in machine. Machine verified this code and the machine steps towards next process

IV. Deposit and withdrawal

Machine after identifying and verifying customer through PIN code and Mobile code, asks the customer about nature of the transaction. Machine asks about deposit and withdrawal options.

V. ATM input screen

As ATM user selects his option, machine asks for the amount that customer wants to deposit or withdraw.

VI. Withdrawal or Deposit

Customer or user deposits or withdraw amount as per his choice and bank's principals regarding financial transactions.

VII. Receipt Generation

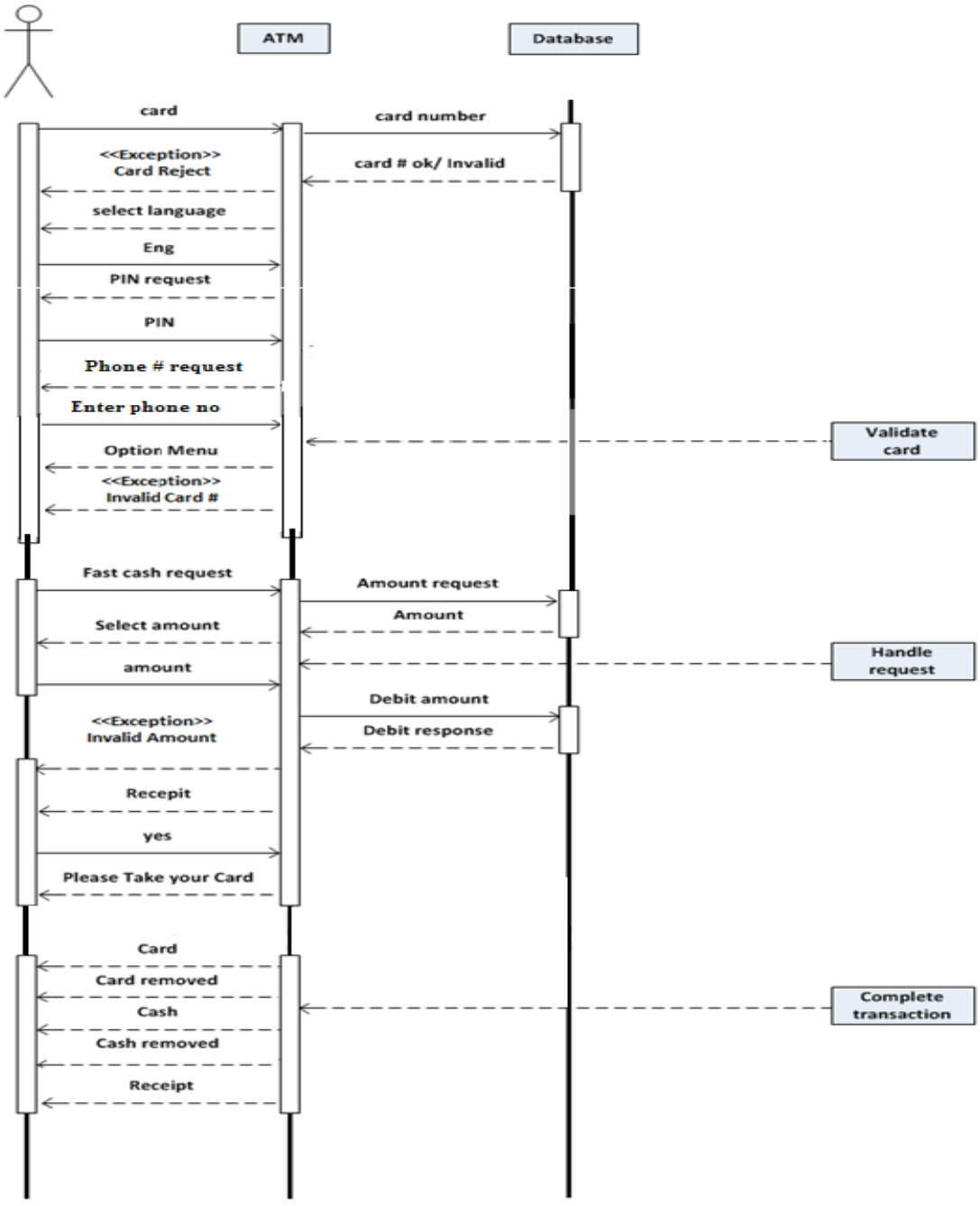
A receipt is generated from ATM machine that gives physical record of financial transaction.

VIII. Transaction SMS

User of ATM card receives a truncation alter via SMS from bank that verifies that "Fast Cash" transaction has been successfully completed.

II. Proposed Solution

The solution of the Automatic Teller Machine (ATM) is that mobile SMS code. Through mobile SMS code we will provide a high security in ATM machine. Mobile SMS code will linked to the bank account details in which the customer provide their mobile numbers to the bankers. When customers will insert their ATM card into ATM machine. The ATM



machine firstly ask the PIN code, if the PIN is correct then it will go to the next screen in which ATM machine is demanding the customers mobile number, customers enter their number on the screen then from the back end it will match their mobile number to their existing record then will send a code through to the customers mobile. So we can handle the ATM security through the mobile SMS code.

III. Conclusion

Automatic Teller Machine has emerged as blessed service on the part of banks and its advantages are enormous. It has given an easy to financial transactions as well as made banking possible round the clock. But ATM has always been remains vulnerable to security threats like theft of cash, skimming of cards and mischievous transactions. At present times, ATM is hot cake for hackers. PIN code identity and authenticity mechanisms are not enough while merging of biometrics and facial recognition also not much suitable in terms of cost and other factors. So coupling of PIN code with Mobile SMS code, as proposed in this paper, is much suitable in terms of cost and convenience to secure ATM transactions. In future, we are working to forward software and hardware implementation of the same proposal.

Reference

[1] M.subha and S.Vanithaasri "A STUDY ON AUTHENTICATED ADMITTANCE OF ATM CLIENTS USING BIOMETRICS BASED CRYPTOSYSTEM" Vol. 4, Issue 2, 2012

[2] Mais Abid Khalil "Auto Teller Machine (ATM) System Security with User Signature Image as Password" Vol 31, 2013

[3] Aru, Okereke Eze, Ihekweaba Gozie "Facial Verification Technology for Use In Atm Transactions" Vol 2, issue 5, 2013

[4] Abhijeet S. Kale1and Sunpreet Kaur Nanda "Design of Highly Secured Automatic Teller Machine System by using Aadhaar card and Fingerprints" vol 1,issue 2, 2014