ISSN:0975-9646

Deepa Malviya/ (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (5) , 2015, 4469-4474

ATM Card and Safety Chip: Embedded in Human Preventing ATM from Hackers and Frauds

Deepa Malviya
Department of Information Technology,
Suresh Gyan Vihar University, Jaipur (Raj.), India

Abstract- In this paper we have tried to overcome the risk involved due to the lost pins and pin hackers of ATM cards.

The advancement of ATMs reflects the enhancing technology of the time. The use of ATM card is increasing and blooming day by day among the humans, which is further giving rise to malicious attacks on bank accounts via ATM cards because of less security & authentication techniques. To resolve this problem, dissertation will focus at concept of a chip / micro chip that will be provided by the bank along with ATM card confidentially to the possessor / owner itself. The micro chip will be embedded into the hand of possessor, at the same time when ATM card will be given by the bank. This chip inserted inside the owner of ATM card will work with the ATM card. When possessor will swipe ATM card into machine, as soon as the ATM card will get accepted, a random PIN number will get generated and this PIN number will get transferred to the chip inside possessor via radio waves. The chip will transfer this random PIN number to the brain of possessor via nerves and senses in few seconds. The random PIN number will only be known by the possessor and cannot be copied by attackers. This will reduce ATM attacks and frauds to a great extent.

***Keywords*- ATM, ATM Cards, Pin Number, Hacker, Authentication, Micro Chip**

I. INTRODUCTION

In past days withdraw, saving cash and detail of bank account through bank was very tough work but now a day's most of people use the ATM because it's the most easiest way for withdraw the cash and check any type of details of their accounts. Many banks open its many ATMs on various places so everyone can easily withdrawal the cash and check any type of details of their accounts through any bank ATM. But in today life we have many passwords like lock, email, car radio, mobile phones, computers, bank lockers ATM card etc and users have many cards like Credit card , Debit card, Identity card, PAN Card etc, so the many problems faced by user related to ATM card and its passwords some are given below:

1. Tough work to remember lots of passwords many times user forgets its passwords and forgetting password sometimes creates the big problem like user can't withdraw the cash, view details of account and sometimes ATM card is hacked by pin hackers.
2. The problem comes around when we forget to carry the ATM card. If he/she has no cash at that time than it create the big problem.
3. Sometimes user only choose the one password of all things like email , mobile phones etc but it has also deficiencies like if anyone comes to know his password then the thief or any relative can easily use the ATM card.

Automatic Teller Machines (ATMs) are used by millions of customer's everyday to make cash withdraw from their accounts. However, the wide deployment and sometimes secluded locations of ATMs make them ideal to also for criminals to turn traceable electronic money into clean cash. The customer PIN is the primary security measure against fraud; forgery of the magnetic stripe on cards is trivial in comparison to PIN acquisition. A street criminal can easily steal a cash card, but unless he observes the customer enter the PIN at an ATM, he can only have three guesses to match against a possible 10,000 PINs and would rarely strike it luckily. Even when successful, his theft still cannot exceed the daily withdraw all limit of around $300. However, bank programmers have access to the computer systems tasked with the secure storage of PINs, which normally consist of a mainframe connected to a Hardware Security Module (HSM) which is tamper-resistant and has a restricted API such that I will only respond to with a YES/NO answer to a customer's guess.

A crude method of attack is for a corrupt bank programmer to write a program that tries all PINs for a particular account, and with average luck this would require about 5000 transactions to discover each PIN. A typical HSM can check maybe 60 trial PINs per second in addition to its normal load, thus a corrupt employee executing the program during a 30 minute lunch break could only make off with about 25 PINs.

However, HSMs implementing several common PIN generation methods have a flaw. The first ATMs were IBM 3624s, introduced widely in the US in around 1980, and most PIN generation methods are based upon their approach. They calculate the customer's original PIN by encrypting the account number printed on the front of the customer's card with a secret DES key called a "PIN generation key". The resulting cipher text is converted into hexadecimal, and the first four digits taken. Each digit has a range of '0'-'F'. In order to convert this value into a PIN which can be typed on a decimal keypad, a "decimalization table" is used, which is a many-to-one mapping between hexadecimal digits and numeric digits. [2]

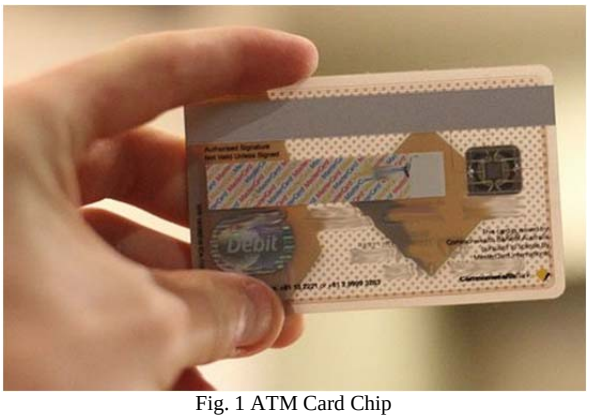

Fig. 1 ATM Card Chip

For any OLT (Online Transaction) the user 1st activates the laptop so open web-browser, accesses the net banking web site of the bank and enters the ID or Personal distinctive range (PIN) and therefore the word by victimization the keyboard or virtual keyboard. SSL (Secure Socket Layer) encode the info transmitted between client's laptop and bank's server. The bank's server decrypts the transmitted data and processes the user's authentication, account inquiry, account transfer, etc. Online banking has become progressively necessary to the profit of economic establishments similarly as adding convenience for his or her customers. Because the range of consumer's victimization on-line banking will increase, on-line banking systems have become additional fascinating targets for criminals to attack. To maintain their customers' trust and confidence in the security of their on-line bank accounts, money establishments should establish however attackers compromise accounts and develop ways to safeguard them. The distinctive facet regarding security in industry is that the protection posture of a bank doesn't rely entirely on the safeguards and practices enforced by the bank; it's equally addicted to the attention of the user's victimization the banking channel and also the quality of finish -user terminals. This makes the task for safeguarding data confidentiality and integrity a larger challenge for the industry.

Most industries have deployed net technologies as a necessary a part of their business operations. The industry is one among the industries that has adopted net technologies for his or her business operations and in their plans, policies and techniques to be additional accessible, convenient, competitive Associate in nursing economical as a trade. The aim of those methods was to supply net banking customers the facilities to access and manage their bank accounts simply and globally. [3]

Nevertheless, there are a unit inherent data security threats and risks related to the employment of net banking systems which will be diversely classified as low, medium and high. In specific the confidentiality, privacy and security of net banking transactions and private data area unit the most important considerations for each the industry and net banking customers. For instance, adware, key loggers, malware, phishing, spyware, and Trojans and viruses area unit presently the foremost common net banking security threats and risks.

At the essential level, net banking will mean putting in place of an online page by a bank to provide data concerning its products and services. At a sophisticated level, it involves provision of facilities like accessing accounts, transferring funds, and shopping for monetary product or services on-line as well as new banking services, such as electronic bill presentment and payment, which permit the purchasers to pay and receive the bills on a banks web site. This is often referred to as "transactional" on-line banking. on-line banking could be a series of processes within which a bank shopper logs on to the web site of the bank through the Web-browser that's put in on client's pc and carries out varied transactions like account transfers, bill submissions, account inquiries etc. on-line banking is applied in four major stages.[4]

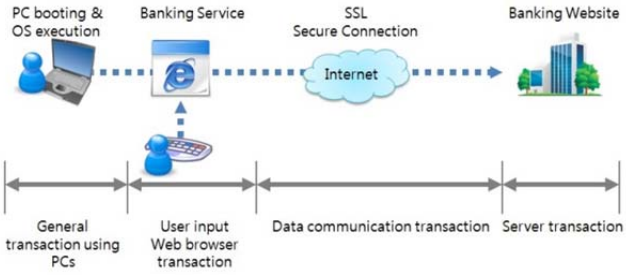

Fig. 2 Online Banking Transaction

.

II. IMPORTANCE AND RELEVANCE OF THE STUDY

ATM is one of most used machine that has changed the traditional system of exchanging money with bank. The advent of ATM changed the way of consumers to handle their money. In world of technology, most of consumers rely on ATM for money transaction, deposit and transfer, as it is easy and time consuming. The ATM card have a magnetic strip on back that record the customer's activity for the day to maintain account. Swiping of ATM card into the machine and entering a PIN number for performing any activity is getting risky day by day for consumers. Attackers may do fraud by inserting a magnetic strip inside the ATM machine keyboard that can easily trace the PIN number entered by consumer.

PIN number cannot remain confidential as it can be easily traced by attackers and further can be used to make out money from that card number and PIN number. To keep PIN number confidential from attackers, the dissertation is providing an alternative better idea where possessor will be provided a micro chip with ATM card. This micro chip will be embedded into the hands of possessor, which will be contacting ATM card through radio waves. Each time the possessor will swipe the card, a new number will be generated. This random number will act as a PIN for that transaction, and will be known by possessor of that card only. The number will be known in mind of possessor through the chip. Whenever the possessor will swipe ATM card into machine, each and every time a new number will get generated, and that will only be known to the possessor itself. This will eliminate the chance of fraud and malicious attacks from ATMs.

Usually a permanent PIN number is provided by the bank for each ATM card, which is used during every transaction. Remembering PIN number might get difficult for some people, and they choose to write it somewhere on

a piece of paper or in mobile phones. This way can help attackers to steal PIN number easily, and can do fraud transactions multiple times. A new approach of generating random PIN number at each transaction will reduce the burden of remembering PIN number.

Often, ATM card cum Debit Cards are also used for online payment and transfer. With Internet access, all the details of the card can be recorded by hackers online when card details are being entered by card owner during any online transaction. This may lead to a great loss to the consumer. But, a new concept can change the phenomenon by generating random PIN number every time whenever the ATM card cum Debit card is being accessed.

Traditional client access systems have operated in closed personal networks accessed through dedicated phone, phone lines; banks and their customers were happy to use these services as long as sure core knowledge security considerations were allayed. These knowledge security needs were sometimes represented in terms of the requirement for confidentiality, integrity and authentication.

The need for confidentiality that is of specific importance within the company banking arena prescribes that knowledge can't be taken by anybody apart from the causing or receiving parties. The confidentiality of pc knowledge will be simply protected through a regime of information encoding.

Sometimes knowledge are deliberately or accidentally amended throughout transmission and its common apply thus to use scientific discipline strategies to be ready to notice these amendments. These techniques, referred to as Hash or Message Digest functions, are an awfully reliable suggests that of guaranteeing knowledge integrity.

Whenever the communication is between multiple parties there's an extra demand for guarantees that every entity is "who he says he is". Extra encoding method, supported public-key cryptography, permits every user to use his own digital signature to a transmission. Typically the digital signature method is increased by the employment of digital identity certificates "signed" by a sure Certification Authority. A Certification Authority may be an element in a very Public Key Infrastructure or PKI.

One common rule of thumb is that "when you're connected to the web, the web is connected to you." For this reason, several net applications assume the presence of the information security precautions represented on top of, however even wherever systems will guarantee knowledge security they typically fail to ordain for once one thing truly will get it wrong.

For example, as a result of the ever present nature of the web, there's the theoretical risk that anybody anyplace will conceive to attack a web banking service; these attacks will manifest themselves within the sort of ancient burglary makes an attempt, faux websites or by "denial of service" attacks.

III. IMPLEMENTAION

ATM is one among most used machine that has modified the standard system of exchanging cash with bank. The arrival of ATM modified the approach of customers to handle their cash. In world of technology, most of customers trust ATM for cash dealing, deposit and transfer, because it is straightforward and time intense. The ATM card have a magnetic strip on back that record the customer's activity for the day to keep up account. Swiping of ATM card into the machine and coming into a personal identification number for playacting any activity is obtaining risky day by day for customers. Attackers might do fraud by inserting a magnetic strip within the ATM machine keyboard that may simply trace the personal identification number entered by client.

PIN variety cannot stay confidential as it is simply copied by attackers and anyone can easily figure out cash from that card number and PIN number. To stay PIN number confidential from attackers, the thesis is providing an alternate higher plan wherever person is provided a small chip with ATM card. This small chip is embedded into the hand of person, which is able to be contacting ATM card through radio waves. This random variety can act as a PIN for that group action, and can be renowned by person of that card solely. The quantity is renowned in mind of person through the chip. Whenever the person will swipe ATM card into machine, each and every time a replacement variety will get generated, which can solely be renowned to the person itself. This can eliminate the possibility of fraud and malicious attacks from ATMs.

Usually a permanent PIN is provided by the bank for every ATM card, which is employed throughout each dealing. Basic cognitive process PIN may get troublesome for a few folks, and that they like better to write it somewhere on a bit of paper or in mobile phones. This fashion will facilitate attackers to steal PIN simply, and might do fraud transactions multiple times. A brand new approach of generating random PIN at every dealing can scale back the burden of basic cognitive process PIN.

Often, ATM card humour Debit Cards also are used for on-line payment and transfer. With net access, all the main points of the cardboard will be recorded by hackers on-line once card details are being entered by card owner throughout any on-line dealing. This might result in a good loss to the patron. But, a brand new thought will provide modification by generating random number anytime whenever the ATM card humour charge account credit is being accessed.

In this new approach, ATMs can work as a knowledge terminal with inputs and outputs. The input that ATMs can take would be simply the swipe of ATM card, PIN number through keyboard and selection of choosing choices like money withdrawal, balance inquiry, transfer cash, etc. As presently because the card is going to be accepted, the host processor connected with ATM will contact to the bank of that ATM card. Bank will generate random PIN number and send it to host processor. The host processor will transfer the number generated to ATM card that's swiped into machine, and therefore the small chip embedded within the person will return to grasp the random PIN number via radio waves. Chip will currently pass the PIN number to brain of person through senses. This PIN number is going to be proverbial to the person solely, and he/she will enter the PIN number for that specific dealings. Since, every time a brand new random PIN number are

going to be generated by the bank system, the possibilities of fraud can minimize oftentimes. As, hackers can ne'er return to grasp PIN number of ATM cards. The person can simply perform dealings multiple times with multiple PIN's generated in each swipe of ATM card. Record of all transactions are going to be unbroken by bank through magnetic strip behind every card.

In the implementation part we have created the project in two sections:

A. For the Client or the User Usage
B. For the Bank Administration

A. For the Client or the User Usage

This section will operate like ATM machine where the user will swipe the card and make it able to access the bank facilities via the pin which is generated in the human chip.

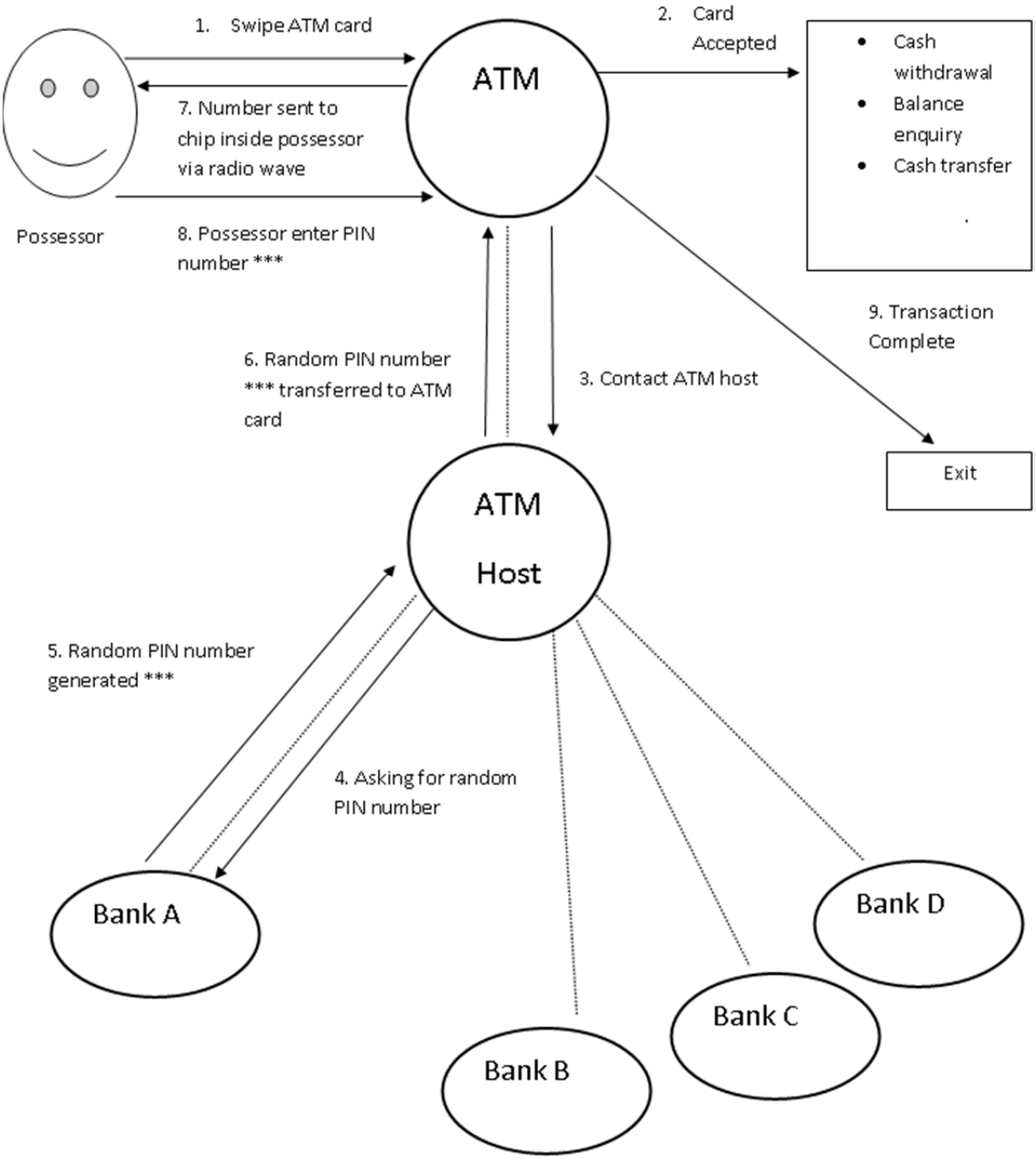

Fig. 3 Work Plan

Fig. 4 Welcome Screen

In this screen the user can swipe the card, in our case the user can enter the ATM card range. And therefore the card range is then searched within the database to see out its existence and so a singular pin is mechanically generated and holds on in another table to simulate the machine pin generation in human chip.

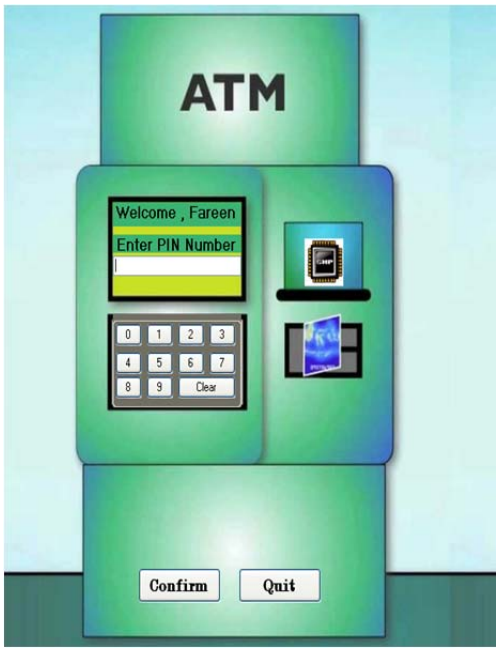

Fig. 5 Pin Number Confirmation

Using this form we will enter the pin number, which is generated automatically. When we click on “CHIP” button, it will show the password or pin number which is currently generated.

B. Server Part or Admin Part

This part will deals with the management of the tables or the data which will be required for processing the client or user section working.

In this section we have first authenticated the user which is admin to validate his or her credentials by providing the valid username and password and after the validation is done, then the admin services are available to the admin.

Fig. 6 Admin Welcome Form

IV. CONCLUSION

The advancement of ATMs reflects the enhancing technology of the time. The use of ATM card is increasing and blooming day by day among the humans, which is further giving rise to malicious attacks on bank accounts via ATM cards because of less security & authentication techniques. To resolve this problem, dissertation has focused at concept of a chip / micro chip that will be provided by the bank along with ATM card confidentially to the possessor / owner itself. The micro chip will be embedded into the hand of possessor, at the same time when ATM card will be given by the bank. This chip inserted inside the owner of ATM card will work with the ATM card. When possessor will swipe ATM card into machine, as soon as the ATM card will get accepted, a random PIN number will get generated and this PIN number will get transferred to the chip inside possessor via radio waves. The chip will transfer this random PIN number to the brain of possessor via nerves and senses in few seconds. The random PIN number will only be known by the possessor and cannot be copied by attackers. This will reduce ATM attacks and frauds to a great extent.

REFERENCE

[1]http://www.sciencepub.net/researcher/research0403/007_8414research0403_33_37.pdf.
[2]http://akshitkumar.heck.in/decimalisation-table-attacks-for-pin-cra.xhtml
[3]http://ijecs.in/issue/v4-i8/68%20ijecs.pdf
[4]https://www.isc2.org/uploadedfiles/(isc)2_public.../isc2_wpiv.pdf