International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 04 | April - 2023 Impact Factor: 8.176 ISSN: 2582-3930

Cyber Crimes, Forensics and Incident Handling Case Study

ON

ENHANCEMENT OF ATM SECURITY

(BIOMETRICS AND IT'S SOLUTIONS)

Submitted By:

Name: Vivek Basera

Location: Haryana

Organization: Cognizant Technology Services

Abstract:

In this modern world, all the people were used ATM machines to withdrawal and transfer cash. I selected this area to increase save and secure for all customers to make easy to do the transaction. ATM is an automated teller machine which is a computerized telecommunication device that provides the customers of a financial institution with access to financial transactions in a public space without the need for the human being. In ATMs the customer is identified by inserting a plastic ATM card with a magnetic strip stripe or a plastic smartcard with a chip that contains a unique number and some secure information about the customer's bank account details etc. But nowadays it is not secure as there have been many cases reported of fraudulent activities with ATM machine and cards. I guess the way in which banking and transaction system is changing in the world, the validation, authentication and confirmation of a person is very important and should be of more concern. With the emerging technology, Fraudsters have also started using advanced tools like card skimmers to read debit and credit card data during usage, they even use to play various tricks, apply

social engineering for extracting ATM Personal Identification Number (PINs) from decent users, and once they got the PIN they can be easily hacked by the fraudster.

In order to make it more secure as high security is needed to stop the ATM frauds and to make it easy for people I think we should use retinal scans or fingerprints. It will be safe for all the customers to do the transactions. This is safer and user-friendly with users as compared to the current systems.

Introduction:

The advancement of payment system in the modern world has gone passed cash to cheques, and then to payment cards such as credit cards and debit cards. Automatic Teller Machine ATM is a terminal installed by banks or other financial institution that enables customers to perform service, like cash withdrawal or cash deposit, balance enquiry, request for bank statements, and money transfer from one account to the other. Due to rapid development in science and technology, upcoming innovations are being built-up with strong security. But on the other hand, threats are also being posed to destroy this security level. Though enhancement in automation has made a positive impact overall, but various financial institutions like banks and applications like ATM are still subjected to thefts and frauds. The existing ATM model uses a card and a PIN which gives rise to increase in attacks in the form of stolen cards, or due to statically assigned PINs, duplicity of cards and various other threats.

My main focus is to develop the better security system by using fingerprint-based ATM. Biometrics is a technology that helps to make your data extremely secure, unique all the users by way of their personal physical characteristics. Using this technology gives many advantages over the existing system. Debits cards, credit cards or other smart cards can be stolen, lost, cloned or hacked by any other person so we need this technology. As compared to other technologies fingerprint is more secure and accepted technology and easy to develop. This feature will inhibit access of account through stolen or fake cards.

Now days the ATM machines are offering excellent services 24 hours but lots of criminal's tamper with this existing system and steal user's card details and passwords by different illegal means such as social engineering, card trapping, skimming etc.

Despite the warning given by banks to customers many people don't take it seriously as share passwords and cards with other person which leads to fraudulent activities. After coming of the internet, the ATM cards can be hacked using some software and hacked by thieves. So, I think fingerprint authentication is the need of the hour as PIN and OTP doesn't verify the customer's identity exactly. To overcome these problems, we need fingerprint-based ATM machines to make it more secure and safe for people.

Existing ATM System

In today's world everyone needs to make some transactions related to money like deposit, transfer, withdrawal money etc. For all this people have to stand in big lines in banks; so, banks came out with a solution that is ATM machine for withdrawal of money whenever and wherever needed quickly. So, for those ATM machines they introduced smart cards like debit card, credit cards for customers which can be used to withdraw money from ATMs. It is great benefit for customers as it saves lot of time when they used to spend time standing in long lines but it also has a disadvantage like, smart cards and passwords etc. can be stolen, lost, replicated or PINs can be shared or can be taken out by using social engineering and ATM machines can be hacked. The banks and customers need a latest authentication system or technique to maintain security for carrying out the transactions. To overcome these problems, we need a new authentication system.

Proposed System

The new system is needed to increase safety and security by implementing new authentication system for ATMs that is Fingerprint system. It has a great accuracy and it also reduces the chances of ATM hacks and frauds. For this internet will play a huge role of working environment and platform to communicate with ATMs and bank servers as they store customers data like PINs, fingerprints, and other information. It also reduces fear of losing the ATM cards or PIN sharing as that will not work. For implementation of this we

banks need to store their fingerprints scans or they can take it with the help of AADHAAR number as it will be difficult for them to take everyone's fingerprints as banks have lakhs of accounts. Instead of removing the existing technology we can merge both. Whenever customers go to machine and swipes the card and scans his fingerprints if they match he can proceed otherwise there can warning or alarm as it is done by some unknown person. Its biggest benefit is that is someone loses the cards then there is no fear of unknown access to his/her account.

Issues with Exiting System (Types of ATM Attacks)

1. **Card Skimming**

   Card skimming is type of theft where any attacker uses a small device called skimmer to steal the card information. Whenever a credit card is swiped through a skimmer; it captures the all the information and details stored in the card's magnetic stripe or electronic chip. Skimmers are placed over the ATM machine where we swipe the card, but they can be placed over almost all the card readers installed by banks. Many a times attacker also hides camera to record the PIN you enter. It gives them information which is needed to make duplicate cards. Many times, restaurant workers who handle cards are recruited as a part of skimming ring.

2. **ATM Malware**

   Malware assaults require an insider, for example, an ATM expert who has a key to the machine, to introduce the malware on the ATM. Once that has been done, the aggressors can embed a control card into the machine's card pursuer to trigger the malware and give them control of the machine through a custom interface and the ATM's keypad. The malware gives culprits a chance to assume control over the ATM to take information, PINs, and money. The malware catches attractive stripe information and PIN codes from the private memory space of exchange handling applications introduced on a bargained ATM.

3. ATM Jackpotting

ATM jackpotting is the exploitation of physical and software vulnerabilities in automated banking machines that result in the machines dispensing cash. With physical access to a machine, ATM jackpotting enables the theft of the machine's cash reserves, which are not tied to the balance of any one bank account. Thieves who are successful and remain undetected can walk away with all of the machine's cash. The culprits use a portable computer to physically connect to the ATM along and use malware to target the machine's cash dispenser. In this bold public approach, an attacker will often use deception and weaker targets to limit risk, like dressing as service personnel to avoid scrutiny. Stand-alone ATMs in retail and service outlets are more likely targets, away from a bank's tighter monitoring and security. Older machines, which may not be fully up to date, are also common targets.

4. Keypad Jamming

In this attack attacker jams some buttons of ATM machines such 'Enter' and 'Cancel' buttons with some glue or by inserting some pin at edges of buttons. When the buttons don't work the customer would automatically think that machine is not working as the cancel button is also not working. In many cases customer leaves and go but the transaction they were doing is active for 30-40 seconds during which the attackers remove the pin or glue and press enter to go ahead with the withdrawal. The loss is however done to the cardholder. To people need to be made aware of this.

5. Cash shimming

The installation by a criminal of a foreign device on an ATM to capture data from the chip of a customer's card. The defining characteristic of a card shimming device is, therefore, the targeting of the data contained on the chip on the customer's card, typically by placement of the foreign device between the customer's card and the contacts of the card reader. The placement of a card shimming device by a fraudster enables a number of possible attacks such as capturing magnetic strip equivalent data, relay and other man in the middle attack.

6. **ATM Hacking**

Aggressors utilize advanced programming systems to break into sites which live on a budgetary establishment's system. Utilizing this entrance, they can get to the bank's frameworks to find the ATM database and consequently gather card data which can be utilized later to make a clone card. Hacking is likewise ordinarily used to depict assaults against card processors and different parts of the exchange handling system. A large portion of the ATM Hackings is because of the utilization of non-secure ATM programming.

7. **Eavesdropping**

The installation by a criminal of a foreign device on an ATM to capture data from a customer's card. This is typically achieved via a wiretap, sniffing the functionality of the card reader, or connection to a magnetic read head within the card reader. The defining characteristic of an eavesdropping device is the use of the legitimate card reading functionality of the card reader to capture the customer's card data.

8. **Shoulder Surfing**

Shoulder surfing is nothing more than the act of direct observation as a person taps onto an ATM PIN pad. Criminals typically position themselves close but not in direct proximity to legitimate ATM customers and watch covertly as the customer enter his or her PIN. A more sophisticated take on shoulder surfing is accomplished through the installation and use of miniature video cameras aimed to record PIN entry.

9. **Phishing/Vishing Attack**

Phishing tricks are intended to allure the client to give the card number and PIN for their bank card. Regularly, an assailant utilizes email speaking to them as a bank and guaranteeing that client account data is inadequate, or that the client needs to refresh their record data to keep the record from being shut. The client is requested to tap on a connection and is redirected to some proposed site. The connection anyway is fake and guides the client to a site set up by the aggressor and intended to resemble the client's bank. The site guides the client to enter touchy data, for example, card numbers

and PINs. The data is gathered by the cheats/culprits/programmers and used to make false cards. Traditionally, after a fruitful phishing assault, the criminal would extricate the required data and go into the online record and expel the casualty's bank reserves. They go to the check picture page, where they take a duplicate of the casualty's check. Numerous money related establishments are currently offering check pictures as a feature of their web-based saving money administrations to their clients. The checks contain the casualty's financial balance number, signature, address, telephone and so on. The aggressor can either take the duplicate and make paper fake checks or take that data and make PayPal accounts or other online installment accounts that will leave the casualty on the snare for any buys.

10. Spoofing

There is a possibility that, when a user enters the PIN during the transaction process, a hacker fakes as the authorized site and prompts the user to re-enter PIN due to a system error. When a user complies with the instruction the hacker stores the data and uses it for his future peccadillo's intentions. This man-in-the-middle (hacker) attack is futile because new password is temporarily assigned in every new transaction.

11. False ATM Presenter

This fraud is performed through the addition of bill traps or false presenters in front of ATM dispensers. These traps are placed over to disguise the normal dispensing operation of the ATM. During the course of an otherwise normal transaction, an ATM will dispense notes into the trap; however, those notes are never presented to the customer. Assuming the ATM has malfunctioned, the customer leaves. After that, the criminal returns, removes the bill trap or false presenter, and leaves with cash that was intended for the customer. The simplest form of bill trap involves the placement of adhesive tape in a manner which blocks the cash dispenser, holds delivered banknotes, and prevents cash retraction. A more sophisticated approach employs a motorized device designed to deliver banknotes into a dedicated, hidden bin, thus simulating a more natural, "real" withdrawal of banknotes.

Proposed Solution for Existing Issues

Fingerprints

The use of fingerprints as a biometric is both the oldest mode of computer-aided, personal identification and the most prevalent in use today. In the world today, fingerprint is one of the essential variables used for enforcing security and maintaining a reliable identification of any individual. Fingerprints are used as variables of security during voting, examination, operation of bank accounts among others. They are also used for controlling access to highly secured places like offices, equipment rooms, and control centers and so on.

Moreover, Finger prints are the unique curves and curl lines on our hands and toes, it has been observed from studies that each individual has a distinct and unique curves as ridges; this means it can be used as a medium for security and identification to our system.

Why fingerprints:

- Uniqueness.
- Surety over the Cards and Keypads.
- Against to Cards Duplication, misplacement and improper disclosure of password.
- No excuses for RF/Magnetic Cards forget ness.

It's Working

A fingerprint-based ATM cashbox accessing system implemented. Initially we store the fingerprint of bank manager and that will be verified with the fingerprint that we are giving when the time of authentication. In this system, we stored all the data in SQL database. If the fingerprints are matched then ATM cashbox will open, otherwise buzzer will give alarm. The system consists of Arduino Microcontroller Unit, Fingerprint module, LED indicators and a buzzer alarm system and microcontroller that collect data from the fingerprint module. As it is based on the fingerprint authentication there is no chance of disclosing of password or pin to the third parties. In this system, we are mainly concentrates in customer security and usage. By introducing Fingerprint based ATM system all the people can use the ATM because of user friendly. Using this system,

the customer can use their fingerprint to do their transaction. It's very difficult to make any duplicate fingerprint. Its shows that it is more secure than the old system. At the end of this research Fingerprint biometric system prove more percentage of security and safe system to develop our system.

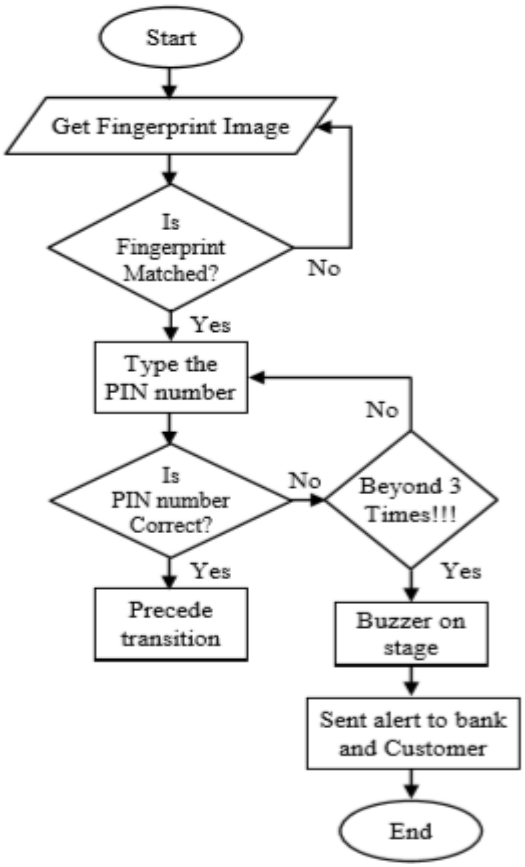

Fig. Flowchart for Fingerprint Based ATM

Biometrics	Cost	Accuracy	Performance	Flaws	Stability
Iris	High	High	High	Lighting	High
Retina	High	High	High	Glasses	High
Face	Medium	Medium	Medium	Beard, glasses, age	Medium
Fingerprint	Low	Medium	Medium	Dirt, dryness	High

Fig. Comparison of biometric technologies

Advantages

- Biometric traits cannot be lost or forgotten (while passwords can).
- Biometric traits are difficult to copy, share and distribute (passwords can be announced in crackers‟ websites).
- They require the person being authenticated to be present at the time and point of authentication.
- The advantage of enhancing ATM security using fingerprint are Low educated people can access easily.
- When our ATM card is misplaced then no one use or access, it automatically blocks, no one can hack the pin code.
- It which makes the system safer, reliable and easy to use. This will be most promising technology at electronic money transaction.

Disadvantages

- Biometric systems can be costly to implement, which might exclude many companies or organizations from implementing it.
- Since fingerprint recognition software only reads one section of a person's finger—it is prone to error. Manually repositioning fingers to get the right reading can be time-consuming.
- Biometric systems—especially lower cost systems—are prone to errors; including failing to identify an authorized person and incorrectly identifying unauthorized people.
- While an increasing number of available technologies are "plug and play", they still require some user education. Users need to know how to position their finger, face, and eye. Additionally, implementers will need training on proper installation and maintenance of biometric systems.

General Preventing Measures

1. **Video Surveillance**

   The essential strategy used to expand mindfulness and prevent extortion endeavors at the ATM is the establishment of shut circuit TV cameras mounted on display or a close to the ATM. No place does this kind of computerized security offer more advantage than in the reconnaissance of off-premises ATMs, which present clear difficulties as to upkeep and security. Cameras can be effectively incorporated into the belt of most ATM machines, and improved security can be accomplished by introducing extra site cameras close by the premises. The accessibility of remote video observation administrations makes computerized video a significantly increasingly alluring security choice, in light of the fact that numerous ATMs and their encompassing regions can be legitimately checked from a solitary, focal area.

2. **Remote Monitoring**

   Remote indicative administrations give a computerized intends to screen and oversee ATM systems. Remote observing can convey significant messages that may show hardening with a machine. Remote diagnostics, checking, and the board give improved uptime and decreased hazard. These administrations advance dispatch shirking and empower a gathering of focal help partners to control console and mouse activities of ATMs legitimately from remote PCs. Through ATM checking capacities, status messages from an ATM can be sent to a focal area where those messages are followed up on dependent on a pre-characterized plan. Focal help partners can rapidly recognize issues and security concerns dependent on the messages they get. For instance, the constant notice of a card pursuer disappointment or an intense decrease in exchanges at a generally bustling area may be a sign of altering. Remote symptomatic administrations additionally add to the wellbeing and security of staff appointed to take a shot at ATMs, by giving these partners remote access and the capacity to oversee occasions from secure area.

3. **Awareness and consumer Education**

   Prevention of potential misrepresentation endeavors can be accomplished by a joint exertion including banks, the shopper and ATM makers/specialist co-op. Banks should pressure the

significance of mindfulness at the ATM to their clients and advance watchfulness in announcing any anomalies in the appearance and task of the ATM. Numerous clients utilize similar ATMs in their day by day or week by week banking schedules. Constantly utilizing similar ATMs furnishes for acclimation with style for a unit. A mindful shopper that notification sporadic items or any connected notes proposing bizarre working directions ought to promptly report the disparity to the banks number situated on the ATM. Banks ought to affirm that their branch faculty, ATM administrations suppliers, and money handlers, just as, are prepared to perceive the most recent ATM extortion systems. Administration specialists ought to be prepared to direct a point-by-point assessment of key ATM segments at each visit to guarantee there has been no altering or augmentations to the ATM. They ought to likewise be especially perceptive of proof that may uncover the utilization of accomplish tape on or close working point, for example, card pursuers, PIN passage gadgets, and apportion focuses. It ought to be prescribed to clients to painstakingly survey their month-to-month account explanations. The above dialog incorporates the procedures and anticipating proportions of ATM fakes however it has been seen that more often than not ATM fakes occur because of the carelessness of banks and clients. Subsequently it ends up important to investigate a few safety measures to be taken by banks, branches and clients.

ESSENTIAL PRECAUTIONS TO BE TAKEN

To minimize or prevent ATM frauds and crimes, banks, branches, and users should, at a minimum, implement the following security measures with respect to their automated teller machine facilities:

At Bank Level:

- Banks should keep an eye on the cards in circulation-check the logo, uniformity of card number, date of expiry, their shape and other parameters.
- One way to find out if an ATM card is counterfeit is to try and peel off the magnetic strip and signature panel on its back. It does not peel off in genuine cards.

- Banks can procure the anti-fraud software that keeps track of ATM users' spending habits and flags unusual transactions.
- Banks can also use another anti-fraud software, tries to catch geographical anomalies- say if a card is used to pay for shopping in Chicago, then for other purchases in India hours later.
- Banks should lay down minimum standards for ATM lighting, and prescribe procedures for evaluating the safety of ATMs.
- Banks should implement ATM programming enhancements like masking/non -printing of card numbers.
- Banks should educate the customers by advising them regularly of risks associated with using the ATM and how to avoid these risks.
- Banks should conduct and document periodic security inspection at the ATM location, and make the pertinent information available to its clients.

At Customer Level

- Customer must always sign on the signature panel of ATM card as soon as received it.
- At the earliest, after receiving the card and PIN, customer must change the PIN and destroy the PIN matter.
- Customer must avoid the obvious when selecting a PIN-name, telephone number, date of birth, vehicle number.
- Customer must memorize PIN. If he/she writes down PIN on paper then, do not keep it in purse or along with the ATM card.
- If customer forgets PIN, should contact card issuing bank and intimate them of the same. The bank will then send a new card with a new PIN.
- Customer should sign new cards as soon as they arrive and cut up old cards when they expire.
- If a customer card ever gets stuck in the ATM, customer need not reveal PIN even to the concerned bank official/institution. It would suffice to let him/her know that his/her card has got stuck in the ATM.
- Use only secure internet sites.

- Never divulge ATM card information to strangers for opinion polls in internet.
- Customer must check sales vouchers/charge slips including purchases amount when sign them keep copies of sales vouchers and ATM receipts.
- Customer must check amount statements at regular intervals.
- Customer must always know that who has access to his/her cards. If his/her ATM card is borrowed by a family member (spouse, child, parent), with or without knowledge, he/she may be responsible for his/her purchase /cash withdrawal.

Outcome

After analysis of the existing system, it is concluded that the ATM system has become very important to the society. Many of the people are dependent on the ATMs. They feel no need to travel by carrying a large amount of money with them because of ATMs. ATMs provide the facility of doing transactions at anywhere anytime. Even, the amount stored in ATMs is converted into the other currency if the user wants to withdraw to money in other currency than it is stored. It provides many facilities to its users. The user can even withdraw money from any of the bank ATM that is in the network of the cardholder's ATMs bank.

Future Scope

In the existing ATM system, the people are identified with the PIN only. Now a day, the crimes at ATMs have been rapidly increasing. There may be chances to forget the PIN as it is not an easy task to remember it. There is also a possibility of hacking password (PIN) as many of the people are in habit of writing their Personal Identification Number in their diary or mobile phone in order to remember it. This shows that the existing system is not as secure as it should be. There is a need to implement some other new techniques to be more secured while using ATMs. Various techniques that can be used for enhancing ATM security is-

- Finger print recognition
- Iris recognition
- Retina recognition
- Face recognition
- Voice recognition
- Google verification code
- Gestures recognition and so many

Conclusion

ATMs have become more important to the society. There is millions of money transactions that happen in a single day through ATM. ATMs have become the necessity of people lives. As it does the transactions in just few minutes and are much faster than going to the bank and waiting in the queue. Though the existing ATM is based on PIN only, there is a need to enhance the security of the ATM. The system security can be enhanced by adoption some modern techniques that are listed /proposed above.

So, the implementation of ATM security by using fingerprint also contains the original verifying methods, which were inputting customer fingerprint, which is send by the controller and verified properly. The security Features were enhanced largely for the stability and reliability of owner recognition. The whole system was built on the fingerprint technology, which makes the system safer, reliable and easy to use. This will be most promising technology at electronic money transaction.

References

1. http://www.naavi.org/cl_editorial_04/praveen_dalal/atm_frauds_feb19.htm
2. https://www.researchgate.net/publication/299537500_A_Constraint-based_Biometric_Scheme_on_ATM_and_Swiping_Machine
3. https://www.topicsforseminar.com/2014/02/biometric-atm.html
4. https://www.veridiumid.com/blog/finally-were-safe-with-biometrics-or-are-we/
5. Anil K. Jain, Jianjiang Feng, Karthik Nandakumar, "Fingerprinting Matching", IEEE Computer Society 2010, pp.3644,0018-9162/10.
6. SHUBHRA JAIN "ATM FRAUDS – DETECTION & PREVENTION" International Journal of Advances in Electronics and Computer Science, ISSN: 2393-2835
7. Priyanka Jindal, Dr. Rajeev Kumar, "Analysis of Security System for ATM" CCSIT, Teerthankar Mahaveer University, Moradabad
8. https://www.aresearchguide.com/1steps.html
9. https://www.powershow.com/view/a25f5ZGZkY/Improving_ATM_Security_via_Facial_Recognition_powerpoint_ppt_presentation
10. https://www.thehindu.com/news/national/eaAADHAAR-valid-proofs-of-identity-address/article4869807.ece