IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 08-12

Survey Of Security Mechanisms For Atm Based Transactions

Prof. Ms. Krutika Sapkal Assistant Professor, Ms. Ankita Singh Student
Dept. of Computer Technology Priyadarshini College of Engg.Nagpur
Email- krutikasapkal@gmail.com Mr. Amit Zodape Student
Dept. of Computer Technology Priyadarshini College of Engg., Nagpur
Email- amitzodape91@gmail.com Ms. Ankita Rode Student
Dept. of Computer Technology Priyadarshini College of Engg., Nagpur
Dept. of Computer Technology Priyadarshini College of Engg., Nagpur Ms. Ankita Pal Student
Dept. of Computer Technology Priyadarshini College of Engg., Nagpur Ms. Nikita Kumari Student
Dept. of Computer Technology Priyadarshini College of Engg., Nagpur

Abstract— *In the past few years' robbery of ATM card has increased, in the present system pin number is used for ATM transaction security, which can be easily Phished, guessed or misused by many ways, with this person can lose money from his/her account without the person's authorization. The main objective of this work is to propose a system, which is used for ATM security applications. Here authorized Bank officials will register the customer details such as Mobile Number with their Official Bank Database while opening the accounts then customer can access the ATM machine with the help of the QR-Code generated and the OTP Sent on the Registered mobile number. When the customer enters ATM he must scan the QR code generated on ATM screen from his mobile phone, wherein he automatically gets a Randomly generated 4-digit code (OTP). Every time this code is sent as a message to the mobile of the authorized customer through GSM module connected to the particular ATM. The code received by the customer should be entered by pressing the keys on the keypad, after that he will be able to do for further transaction from the mobile app. If someone try to physically damage the system or try to evade the system without authorization, then the ATM shutter gets shut and locked down automatically till the Security officials arrive. This proposal will go a long way to solve the problem of ATM transactional Security.*

Keywords— *ATM, GSM module, QR-code card, OTP, Mobile*

I. Introduction

In today's fast life no-one wants to stand in long queues for banking operation, they don't want to wait for too long thus many of us use ATM machines. Fast development of banking technology has various advantages and Disadvantages to banking activities and transactions are the advent of automated teller machine (ATM). ATMs are electronic banking machines located in different places and the customers can make basic transactions without the help of bank staffs. With the help of ATM, the user can perform several banking activities like money transfer, cash withdrawal, credit card payment, paying various domestic bills like electricity, and phone bill.

The rapid development of banking technology has changed the way banking activities are dealt with. One banking operation that has impacted positively or negatively to banking activities and transactions is the advent of Automated Teller Machine (ATM). It is a computerized machine designed to dispense cash to bank customers without need of person-to-person interaction. Today the ATM users are increased in number. They use ATM cards for banking transactions like deposits, transfers, balance enquiry, mini statement, withdrawal, fast cash, etc. The ATM machine has card Reader and keys as input devices and display screen, cash dispenser, receipt printer, speaker as output devices. (Available present day security) Account information of user is stored on the magnetic strip present at the back side of the ATM card. When a person enters this card in the card reader, the card reader captures the account Information and the data that is required for the transaction. The person has to insert the ATM pin for security authorization by use of keys / touch- pad present on the system. The pin is the unique 4-digit number registered with particular ATM card given to the Account holders. The number is verified by the bank and allows the customers to access their account. The password is the only authentication required so anyone with this 4-digit pin can access the account when they have the combination of both the card and Pin. Once the card and the Pin is stolen by the culprit they withdraw money from the account with the Account Holders Authorization, it may bring huge financial losses to the Card holder.

In this paper discusses some of the techniques that involves use of QR code to prevent the fraud at the time of ATM transaction. The QR code measure is an attempt for enhancing the current security loophole of the banking

system. Here a new technology is introduced which works for QR code scanning and mobile phone and GSM technology to generate authorization. QR code scanning technology provides strong and indisputable authentication. Because QR code is unique, it can't get hacked. So we use the QR code for the identification purpose. QR code are a secure means of authentication. The QR code of the card and user details will be stored in the database of the bank when the card holder accesses the services using ATM. After the QR code is scanned they will have to enter the OTP that is automatically sent to the registered mobile number. If an unauthorized user tries break in the system unethically or if someone try to harm the system physically, then the shutter gets automatically locked down. From that same system two message gets generated one goes to users mobile alerting unauthorized access and one message to the official security to notify them about ATM money stealing.

II. Literature Review

A. Research Background

The increase of ATM (Automated Teller Machine) frauds has actuated the development of new authentication mechanisms to overcome security problems of personal identification numbers (PIN)[1]. For example, fingerprints are rare and unique but they are not secrets. We leave them everywhere with everything we touch, therefore, they can easily be forged with a film. The fingerprints on a person can get damaged and also, it changes with age. In addition to this, another serious disadvantage with the fingerprints is that the theft of a person's biometric leads to some serious issues as re-enrollment is not possible unlike the resetting or changing of PIN.[2]

Crime at ATM's has become a worldwide problem that faces not only by customers, but also by bank and this financial crime case rises repeatedly in recent years. A lot of criminal's tamper with the ATM terminal and steal customer's card details by illegal ways.[3] Once user's bank card is lost and the password is stolen, the user's account is easy to attack Passwords and PINs can be unethically acquired by direct covert observation.[3] When credit and ATM cards are lost or stolen, an unauthorized user can often come up with the correct personal codes. Despite warning, many people continue to choose easily guessed PINs and passwords - birthdays, phone numbers and social security numbers. Recent cases of identity theft have increased the need for methods to prove that someone is truly who he/she claims to be.[4]

B. Action in case of Physical damage to the system

Traditional ATM systems authenticate generally by using a card may be credit, debit, or smart card and a password or PIN which no doubt has some defects. The prevailing techniques of user authentication, which involves the use of either passwords and user IDs or identification cards and PINs (personal identification numbers), suffer from several limitations.

1) Card Skimming

It remains the number one threat globallybut the one that is on the wane, thanks to deployment of anti-skimming solutions, EMV technology and ATM contactless functionality. Essentially, skimming refers to the stealing of the electronic card data, enabling the criminal to counterfeit the card. Consumers experience a normal ATM transaction and are usually unable to notice a problem until their account is defrauded.[5]

2) Card Trapping

Trapping is the stealing of the physical card itself through a device fixed to the ATM. In a pre-EMV or chip- and-signature environment, the PIN does not need to be compromised. Again, contactless capability can help. For example, NCR helped launch the world's first tap and pin ATM with ANZ using EMV contactless technology.[1]

3) Transaction Reversal Fraud

Transaction Reversal Fraud involves the creation of an error that makes it appear as though the cash had not been dispensed. The account is re-credited the amount 'withdrawn' but the criminal pockets the money. It could be a physical grab (similar to cash trapping) or a corruption of the transaction message.[6]

4) Cash Trapping

Normally relatively low value, the fraudster will use a device to physically trap the cash that is dispensed and come to collect once the customer has left the ATM location.[7]

5) Shared ATMs

There are different methods used in shared ATM with regards to the decipherment of PIN and message authentication among them which is called as "ZONE ENCRYPTION". In this method, a trustful authority is appointed to operate on behalf of a group of banks so as they could interchange messages for ATM payment approvals.[5]

C. Security for Authorization of the transactions

The authentication mechanisms are usually assessed based on speed, security, and memorability in comparison

with traditional PIN entry systems. The biometric authentication technique seems to be the most popular alternative mechanism as against PIN-based ATM authentication. This authentication technique however has its own disadvantages.[8]

III. Proposed Work

Basically ATMs are networked and connected to a centralized computer, which controls the ATMs. The use of QR-code scanning is possible at an ATM. Here first all the information of user or client is to be stored at a bank branch or Network Provider at the time of opening the account and then only user can access the ATM. Typical ATM has two input devices (a card reader and keypad) and four output devices (display screen, cash dispenser, receipt printer, and speaker). Invisible to the client is a communications mechanism that links the ATM directly to an ATM host network. The ATM functions much like a PC, it comes with an operating system (usually OS/2) and application software for the user interface and communications.

ATM display a QR code that the customer scans on their smart phone. The advantage of this approach is that it doesn't require the ATM to contain a barcode scanner. QR code-based ATM transactions require a software upgrade at the ATM. A QR code-based ATM transaction involves the withdrawal of cash from a mobile wallet that is linked to a bank account. Customers begin by authenticating themselves for their mobile

TABLE I. SUMMARIZATION OF THE PREVIOUS SECURITY PRACTICES

S.No	YEAR	TECHNIQUES	IDEOLOGY	LIMITATIONS
1	2016	Iris Recognition and Palm Vein (IRPV) recognition technology[1]	• Proposed using the Iris Recognition and Palm Vein recognition technology to prevent card duplication.	• The system was not built to overcome over the current system.
2	2014	A combination of fingerprint biometric token and GSM technology[2]	• Proposed a system architecture that incorporates both the finger print and GSM technology into the existing PIN-based authentication process.	• A nominee or third party's finger print was incorporated in the architecture.
3	2013	Finger print biometric token[9]	• Developed an ATM based fingerprint verification and simulated it for ATM operations by incorporating the fingerprints of users into the bank's database.	• The system developed was inefficient because there was no finger print matching algorithm. • The system developed was not built as an enhancement of the existing system.
4	1998	Advanced Encryption Standard (AES) algorithm[6]	• The Advanced Encryption Standard (AES) algorithm was adopted to improve the security level of ATM Banking Systems.	• AES in counter mode is complex to implement in software taking both performance and security into consideration.
5	1992	Short Message Service (SMS) verification.[6]	• Developed an algorithm for enhancing ATM authentication system using Short Message Service (SMS) verification. • Conducted a usability testing of the proposed system	• The developed algorithm only considered a minimum withdrawal amount.

banking app, and then using the app to pre-stage a QR code- based cash withdrawal. System which work on QR code scanning by which the person who is going in ATM is get authenticated by inputting the OTP generated after scanning the QR code, if in this method the person tries to interrupt the transaction by inputting wrong pin or try to steal money from ATM machine then the shutter gets locked down automatically.

The GSM modem connected to the ATM generates the 4- digit code that will be sent to the Card holder's mobile number. The account holder can access the account after he/she enters the One-Time Password (OTP), post this they can begin the transactions. The Account holder can perform the transactions that he/she desires like deposits or withdrawal of cash, balance enquiry, mini statements etc. After completion of the transaction the card will be ejected out of the ATM. This helps to minimize the chances of fraud occurring due the misuse of ATM.

IV. Methodology

- **QR code: -** A barcode is a machine-readable optical label that contains information about the item to which it is attached. A QR code uses four standardized encoding modes (numeric, alphanumeric, byte/binary, and kanji) to efficiently store data; extensions may also be used.

- **GSM Module: - GSM/GPRS module** is used to establish communication between a computer and a **GSM-GPRS system**. **Global System for Mobile communication (GSM)** is an architecture used for mobile communication in most of the countries. **Global Packet Radio Service (GPRS)** is an extension of GSM that enables higher data transmission rate. **GSM/GPRS module consists of a GSM/GPRS modem assembled together with power supply circuit and communication interfaces** (like RS-232, USB, etc.) for computer.

- **Microcontroller**: - Microcontrollers are used in automatically controlled products and devices, such as automobile engine control systems, implantable medical devices, remote controls, office machines, appliances, power tools, toys and other embedded systems. By reducing the size and cost compared to a design that uses a separate microprocessor, memory, and input/output devices, microcontrollers make it economical to digitally control even more devices and processes.

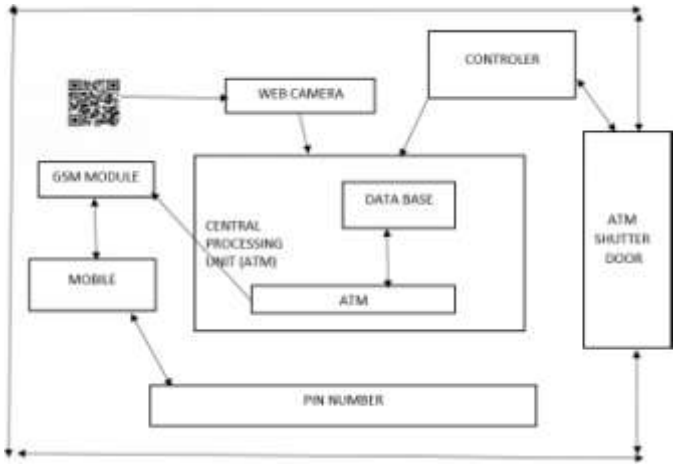

Fig. 1. Block Diagram

V. Conclusion

In all over the countries Automatic Teller Machines have become a mature technology which provides financial services to different area and different client. Thus it is very important to make the process more secure and reliable. Thus by implementation of ATM security by using QR-code and GSM MODEM took advantages of the stability and reliability of QR-code scanning. The system also contains the original verifying methods which were inputting owner's password which is send to client. When this system is fully deployed will definitely reduce the rate of fraudulent activities on the ATM machines such that only the registered owner of a card and nominee, access to the bank account, and the nominee user also will do the transaction so it is more comfortable in case of emergency. Thus the systems become more safe, reliable and easy to use.

VI. Future Scope

Card less Cash Access provides added security to standard ATM use by dramatically reducing the threat of skimming and shoulder-surfing. Additionally, consumers Are more likely to quickly detect a lost or stolen phone than a lost or stolen card. The app requires a PIN and possibly a second code if the smart phone is locked. Additionally, Pre- ordered transactions are "live" for only a specified period of time, no payment data is stored on the smart phone, and security alerts for activity are tied into the app.

Card less Cash Access provides convenience by allowing consumers to keep the familiar user interface present on their smart phones. Additionally, receipts are automatically sent to the smart phone. Finally, the QR code scans from 6 to 8 feet away, which can help with accessibility concerns.

References

[1]. S. Bhagat, V. Singh, N. Khajuria, and B. E. Student, "ATM Security using Iris Recognition Technology and RFID (2017)," *Int. J. Eng. Sci.*, vol. 11486, no. 5, pp. 11486–11488, 2017.

[2]. M. Dutta, K. K. Psyche, and S. Yasmin, "ATM Transaction Security Using Fingerprint Recognition American Journal of Engineering Research (AJER)," no. 8, pp. 41–45, 2017.H. Leitold, "ATM Security," vol. 6, no. 4, pp. 35–44, 2012.

[3]. L. Lai, S. W. Ho, and H. V. Poor, "Privacy–Security Trade-Offs in Biometric Security Systems—Part I: Single Use Case," *IEEE Trans. Inf. Forensics Secur.*, vol. 6, no. 1, pp. 122–139, 2011.

[4]. A. Singla and N. Jain, "Website : www.ijirset.com Fraud Reduction in ATM Machines using Voice Recognition- A Review," pp. 7525– 7530, 2017.

[5]. S. N. Kumar, A. M. Arif, and S. N. Kumar, "Two Factor Authentication for High," no. 9, pp. 33–41, 2015.

[6]. R. Begum and V. Pujari, "Security of ATM System Using Biometric and OTP," *Int. J. Innov. Res. Comput. Commun. Eng.*, pp. 72–77, 2017.

[7]. Milind Godase & Anil N. Barbole, "Biometric Security Systems: A Comparative Review," *Int. J. Comput. Networking, Wirel. Mob. Commun.* , vol. 2, no. 3, pp. 13–26, 2012.

[8]. A. K. Ojha, "ATM Security using Fingerprint Recognition," vol. 5, no. 6, pp. 170–175, 2015.

[9]. S. N. Kumar, A. M. Arif, and S. N. Kumar, "Two Factor Authentication for High," no. 9, pp. 33–41, 2015.

[10]. R. Begum and V. Pujari, "Security of ATM System Using Biometric and OTP," *Int. J. Innov. Res. Comput. Commun. Eng.*, pp. 72–77, 2017.

[11]. S. Bhagat, V. Singh, N. Khajuria, and B. E. Student, "ATM Security using Iris Recognition Technology and RFID (2017)," *Int. J. Eng. Sci.*, vol. 11486, no. 5, pp. 11486–11488, 2017.

[12]. A. Singla and N. Jain, "Website : www.ijirset.com Fraud Reduction in ATM Machines using Voice Recognition- A Review," pp. 7525– 7530, 2017.

[13]. Milind Godase & Anil N. Barbole, "Biometric Security Systems: A Comparative Review," *Int. J. Comput. Networking, Wirel. Mob. Commun.* , vol. 2, no. 3, pp. 13–26, 2012.

[14]. W. Puech, O. Strauss, I. Tkachenko, J.-M. Gaudin, C. Guichard, and C. Destruel, "Two-Level QR Code for Private Message Sharing and Document Authentication," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 3, pp. 571–583, 2015.

[15]. L. Lai, S. W. Ho, and H. V. Poor, "Privacy–Security Trade-Offs in Biometric Security Systems—Part I: Single Use Case," *IEEE Trans. Inf. Forensics Secur.*, vol. 6, no. 1, pp. 122–139, 2011.

[16]. A. K. Ojha, "ATM Security using Fingerprint Recognition," vol. 5, no. 6, pp. 170–175, 2015.

[17]. J. Galbally, S. Marcel, and J. Fierrez, "Image quality assessment for fake biometric detection: Application to Iris, fingerprint, and face recognition," *IEEE Trans. Image Process.*, vol. 23, no. 2, pp. 710– 724, 2014.

[18]. A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: A tool for information security," *IEEE Trans. Inf. Forensics Secur.*, vol. 1, no. 2, pp. 125–143, 2006.

[19]. R. Munjal, "A comparative study of different biometric technologies," *Int. J. Comput. Sci. Commun.*, vol. 2, no. 4, pp. 1–7, 2014.

[20]. H. Leitold, "ATM Security," vol. 6, no. 4, pp. 35–44, 2012.

[21]. S. W. Wang, W. H. Chen, C. S. Ong, L. Liu, and Y. W. Chuang, "RFID applications in hospitals: A case study on a demonstration RFID project in a Taiwan hospital," *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, vol. 8, no. August, 2006.

[22]. M. Dutta, K. K. Psyche, and S. Yasmin, "ATM Transaction Security Using Fingerprint Recognition American Journal of Engineering Research (AJER)," no. 8, pp. 41–45, 2017