ATM PIN Verification via Smartphones: Securing the Future of Digital Banking in Pakistan

Muhammad Irfan Khan[1], Adnan Ahmed Siddiqui[2]
[1]Department of Computer Science Sir Syed University of Engineering and Technology Karachi, Pakistan
[2]Assistant Professor, HIET- FEST Hamdard University Karachi, Pakistan
[1]mirfan.khan@yahoo.com, [2]adnan.siddiqui@hamdard.edu.pk

Abstract:

Plastic money has become the most favored wayof conducting monetary transactions in most developed countries, partly due to the ubiquity and ease of access of Automated Teller Machines, but its use in Pakistan still lags largely behind. While Teller machines offer a great deal of ease when it comes to accessing personal bank accounts, checking balance, paying utility bills or performing Inter/Intra Bank Fund Transfers. However, they also pose numerous critical security challenges. For example, skimming devices only require a 4-digit Personal Identification Number to steal an individual's private information and a teller machine's hardware especially vulnerable to such tactics. This might even lead to identity theft where someone might steal a customer's account by way of recording their PIN after a valid debit/credit card transaction. This paper identifies such security concerns and suggests a method to make transactions safer and more secure by bypassing the Teller's own vulnerable hardware by way of entering the PIN from the keypad of a user's Smartphone or handheld device via a bank's digital banking app.

Keywords*—Security; Automated Teller Machine; Smartphone; Authentication; ISO 8583; PIN Verification.*

I. Introduction

Modes of carrying cash have evolved rapidly together with technology since the beginning of the 21st Century, and now people use Automatic Teller Machines (ATM) to perform tasks such as withdrawing cash, transferring funds and paying utility bills, all of which can be done with extreme ease and speed by inserting a personalized piece of plastic, called a debit/credit card, and entering a four-digit Personal Identification Number (PIN). Many countries, China being a notable example, are also adopting and offering speed internet coupled with the card and mobile payment services through their national banks; e.g., mobile financial and banking services, greatly increasing the reach and efficiency of their banking systems [3].

While modern technology has undeniably transformed ways of carrying cash, increasing the speed and efficiency with which we conduct our day-to-day monetary transactions, it has simultaneously generated new modes of vulnerability such as identity-fraud, loss of sensitive or private information, and monetary theft. This vulnerability is especially pronounced in Pakistan, whose banking sector is not well-equipped to process such fraud claims, leading to the citizens lagging behind in the use of plastic money. ATMs are the most commonly used channel of monetary transfer in Pakistan, even compared to mobile, internet, branch and Telephone banking. In the last few years, people have started gradually adopting digital banking in its myriad of forms, but ATMs are still poised to be the primary way of monetary transactions for the foreseeable future, and thus any gaps in their security have extensive consequences for the banking sector as a whole. This paper identifies one such gap in the security of the commonly used ATMs here and tries to propose a pragmatically sound solution that could be implemented with ease to this mode of banking. This will additionally allow us new opportunities to analyze transaction trends and build better systems to detect fraud in its various shapes [1].

In Pakistan, the majority of people use two types of cards; Magstripe Cards and Chip Cards. In the former, a magnetic strip stores all your personal data, while in the latter a chip performs the same function. Coupled with the numbers embossed on the plastic of a card, of which the first six digits define the BIN (Bank Identification Number) and the following six digits contain the cardholder's details. As such while the card itself contains all of a user's information, you still need a PIN for verification before performing any electronic transactions. The banks in Pakistan which offer debit or credit card services only use a PIN verification system, which is inadequate when we compare it to the banks in Europe and a few other first world countries that require both a PIN and personal signature for verification purposes while in some countries both options are available [4].

The most common manner in which fraud is committed with regards to ATM banking is by stealing a person's PIN by using methods such as shoulder surfing or skimming devices. The security measures adopted by many banks are obsolete and are severely lacking in up-to-date guidelines and an adequate Standard Operating Procedure (SOP) in case someone's PIN is compromised [2]. The PIN is not embossed on a credit or debit cards but is physically entered by the cardholder during the transaction and set by the user during the activation of the card. The PIN is the only verification step which requires user input in order to make a transaction, and in our proposed model we allow users to input their PIN using a Smartphone bypassing the ATM's hardware entirely. In effect, this means that after *inserting* the card into the ATM a user will enter their 4-digit PIN using the keypad of the Smartphone via a banking application that will then send a request to the bank's server using the code specific to that particular device on which the user is performing the transaction, allowing them to not use the embedded keypad of the ATM, which is the most likely target of

skimming devices used to extract personal information.

II. Background

In the existing system, every user has a 4-digit PIN for each ATM card and in order to withdraw money the user needs to verify their identity by entering a pin on the ATM interface. The PIN verification process is completed by inserting a card into the machine and entering your personal code. This pin is known only to the user and the bank. The latter uses it to get a matching code by the controller of the issuing bank using ISO 8583 standard message for transaction. After verification of the PIN, the controller sends back an approved matched response to the ATM which then allows the user to perform any further steps related to their transaction.

The debit or credit card, being a tangible entity can easily be lost or stolen and if the thief who steals the card can acquire the user's ATM PIN, then the user's bank account is severely compromised.

III. Literature Review

Advancements in payment technologies have lead to an accelerated development of the ATM services in Pakistan, making them the primary site for banking purposes. Thus, financial institutions in Pakistan should concentrate their attention on ATM security to enhance consumer loyalty [8]. The payment industry as a whole has progressed towards becoming more customer-centric and technology-driven, significantly changing how the banking activities are conducted all over the world [9]. At the same time, there has been a rise in fraudulent activities revolving around the credit or debit card, as they are often stolen and the unauthorized owner of that card often tries to use it on an ATM by randomly guessing the PIN. Many skimmers can come up with correct credentials because many people choose PIN ranging from birthdays to phone codes [10].

There are many different approaches to overcoming such security challenges presented by an ATM's PIN verification process that are being adopting by numerous banks. An example of this is biometric verification of a user based on their finger prints, which studies have shown to minimize the rate of fraudulent activities on ATM machines [5]. Similarly, other modes of biometric verification such as Iris, Face, Handprint and Retina recognition are equally valid at curbing fraud, but their drawbacks are also restricting; simple dirt and dry skin easily hamper these techniques and they also require the installation and maintenance of specialized equipment in each and every ATM. For example, a camera for Face Recognition and a fingerprint reader for print recognition, which can be costly and time consuming [6]. Another method that has been previously proposed consists of a PIN verification technique relying on a numeric keypad with two shades of the keys as painted either black or white but the limitation of this system is it requires users to go multiple steps of color identification and if a video recording of the login is made the pattern can be found out because the system still uses an embedded keypad [11].

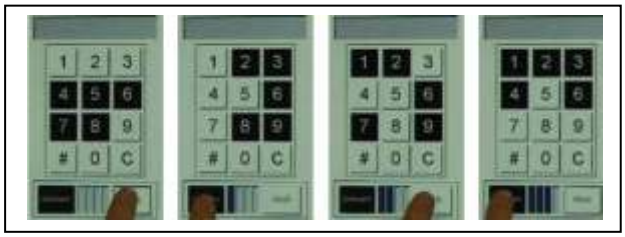

Fig. 1. PIN verification system image.

Another proposed system to prevent skimming attacks utilizes the technique of SMS verification. In this method, the user receives a temporary PIN generated by the bank's controller before each transaction. However, this approach involves complex interaction techniques and bypass the user's security as card holder requires to sends clear card data information via SMS to the bank's server for verification and the limitation, thus becoming very drawn out and repetitive and breaching a customer's privacy [12].

The password/PIN-based authentication system that is the already the norm here does not involve any complex pattern recognition techniques, such as those involved in biometric authentication, and its only requirement is that the given password must match the one already saved on the system. Thus, the PIN verification method is extremely cost and time effective since it requires no specialized hardware and only one input, and as such any improvements that we might propose should ideally capitalize on its strong-points without taking away any of its functionality [13].

Keeping all the aforementioned points in mind, this paper proposes a system that relies only on a simple, banksanctioned Smartphone application. This is an extremely viable method as according to the pilot survey conducted for this paper, 94% of people who own a debit or credit card also own a Smartphone. As such the user will only need an internet connection and a bank app through which they can access the PIN verification section. After the costumer has inserted a card into the ATM and entered the PIN through their Smartphone, the server will then send an authentication request to the ATM on which the card was inserted. Thereafter the customer's Smartphone will display the same screen as the one on the window where they will select the nature of their transaction.

This method can also be applied to make monetary transactions on a single ATM using the credit or debit card of various different banks as well. All ATM transactions are based on response codes from 00 to 99, where the '00' code refers to a withdrawal notice. In terms of the controller, it means that approved transactions on an ATM are always routed through a bank's own secure server, handling all the various status checks and securing connectivity, while the point of sale (POS) only builds a connection when a user initiates a transaction. As such the entire communication between Bank-1 and Bank-2 can be done using a ISO 8583 in such a way that if a card holder of Bank-1 inserts a card into the ATM of Bank-2

the card can be used to initiate a request message using ISO standard message format to the controller of Bank-2 ATM which will further route to the controller of Bank-1 for verification. After receiving an approval or successful response from the controller of Bank-1 the user can expect to receive the desired cash which they requested from the ATM. Finally, Bank-2 will mark the transaction as successful and send a successful response back to the controller [7].

IV. Methodology

In order to calculate the impact of the proposed system a survey was conducted with a sample size of 50 participants in order to analyze the result and responses were conducted over the time period of one month. The results of the survey are presented in tables 1-2. Table 1 shows the nature of participants who took part in this survey and figure 1 shows their age range (from 19 to 41 years) and clearly demonstrates that most participants owned either a credit or debit card. Table 2 shows their comfort and confidence in using an ATM in Pakistan. According to question one, while 92 percent of the respondents do own a credit or debit card, 30 percent of them still fear for the security of their private information.

On the other hand, the other questions show that 54 percent of people have prior experience in internet banking, just not in conjecture with ATMs and 52 percent of people also have 4G internet continuously enabled on their Smartphone. As such, the security method suggested by this paper can be adopted quite easily. It has the potential to replace the existing transaction method which is quite risky and to overcome the security gap as represented in figure 2 which also validates the hypothesis of this study.

Table 1: Survey Participants Profile

No.	Profile	Details
1	Age	20 - 41 years old
2	Gender (Male/Female/NA)	36:13:1(NA)
3	Profile	The majority respondent owns multiple accounts in multiple banks and owns debit/credit cards.

Table 2: Questionnaire

No.	Question	Responses (Yes/ No)		Total	Percentage (Yes/No)	
1	Do you have an ATM card?	46	4	50	92	8
2	Do you feel secure using ATM in Pakistan?	31	19	50	62	38
3	Do you have a Smartphone?	47	3	50	94	6
4	Have you ever used an internet banking App on your Smartphone?	27	23	50	54	46
5	Do you have a 4G speed internet data enabled on your phone?	26	24	50	52	48
6	Do you feel your information is secure while using ATM?	35	15	50	70	30
7	Have you previously used any other method of authentication on ATM such as Biometric?	13	37	50	26	74

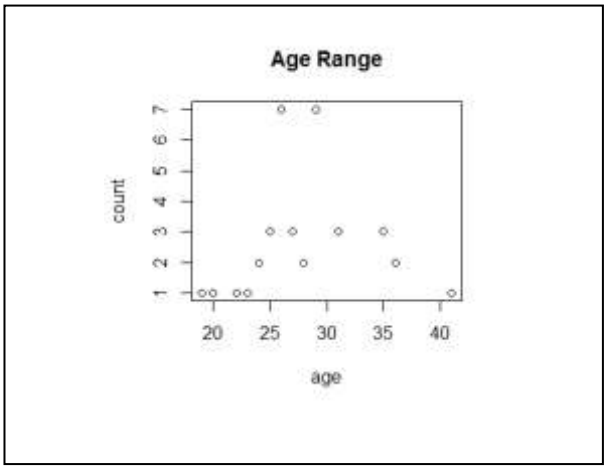

Fig. 2. Graph shows the age range of the participants.

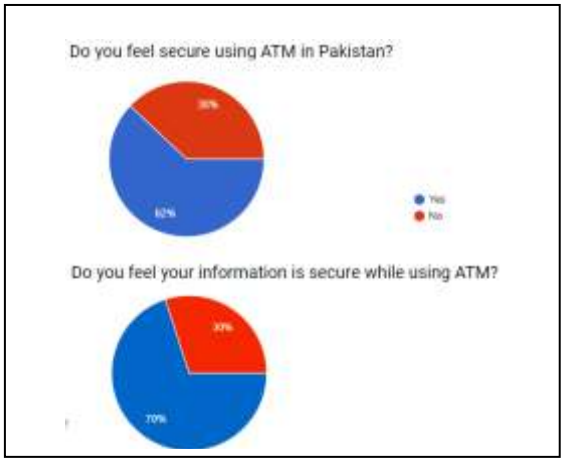

Fig. 3. The above figure show the percentage of question 2 and 6.

A. Purposed System

This facilitates user to enter PIN using their Smartphone without using the embedded keypad of ATM device in order to minimize the risk of PIN getting skimmed by a skimmer device and this will enable the user to withdraw cash from the account after successful authentication of the corresponding PIN number which enters via Smartphone's keypad.

B. Abbreviations and Acronyms

ATM, PIN, ISO, IBFT, CBS, EMV

C. Server

The server manages the user account details and include details such as the user's account balance, account number and citizen ID and PIN code.

D. ISO 8583

The ISO 8583 is an industry standard protocol for financial communication between the user and the bank which can be understood in terms of a sender and receiver. Each financial message then comprises of three parts; the header, application information, and the trailer.

The header and trailer encompass the application information and are utilized for directing and message integrity.

The application information comprises of ISO message including message type pointer.

Example: We have an ATM that can accept credit/debit card to withdraw money. This can be done through ISO 8583 using following steps:

x100 message sent to bank's server to authorize the PIN. After a successful match, it will initiate the transaction and verify the availability of amount and this done by the core banking system.

x200 The CBS will generate a response message to the server to withdraw the amount after checking the balance.

x220 The server will forward the same to the bank to complete the transaction, or x420 to the bank to cancel the authorization if the x200 failed.

E. Transaction Routing

The controller, core-banking system, and switches make cash withdrawal possible from any ATM. Apart from cash withdrawal, people can perform multiple types of transactions on ATMs for instance fund transfers, utility bill payment, conduct account inquiries. The role of switches in this is to enable customers of Bank-1 to withdraw cash from an ATM of Bank-2 where they do not have an account.

All the user must do is insert their card in an ATM and open up the banking application on a mobile device with an enabled keypad. The user will then tap the ATM transaction window on the app, which will prompt the ATM to connect to the application on your device. This will finally allow you to use your device's keypad to enter your security PIN, which the app will send as a verification request via mobile banking app to the bank's controller or modules which manage PIN verification and if matched it will send an 'approve' response to the ATM terminal. If you accidentally enter a wrong code or in case of a timeout, the transaction window will appear on the device's screen with a generated code explaining the reason for the declined transaction, simultaneously sending a signal to the ATM to eject your card and then you can simply try again. The entire communication can be done using the ISO 8583 message standards and thus require no new hardware or software upgrades on the ATM itself thus making this solution economical and easy to implement.

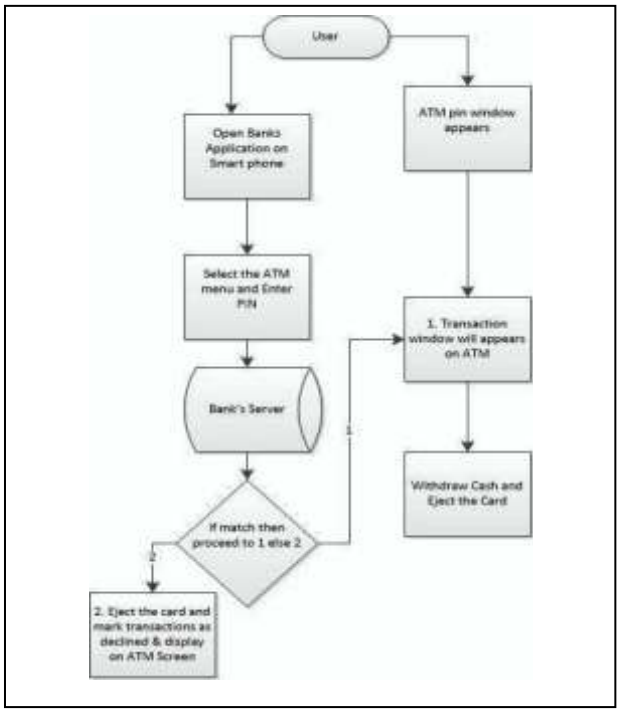

Fig. 3. DataFlow Diagram.

F. Algorithm

a) The user inserts a card into the ATM and PIN input window will appear.

b) The user is then required to open the digital banking app on their smartphone, the user will then enter the PIN in the ATM transaction window on digital banking app after verifying the location of the ATM in which the user has inserted the card.

c) The application will send a request to the server using ISO 8583 financial request message format and the PIN validation will be performed at server's end.

d) The successful match of PIN the server will send an approved response to ATM response code "00" after a successful approval/completion PIN verification is valid.

e) Incase of an unsuccessful match, ATM will eject the card and transaction will be marked as declined.

f) The ATM then send an acknowledgment message to the host and marks the transaction as completed. A new transaction window will appear on the ATM screen and in case of timeout or incorrectly matched the server will send a response to ATM to eject the card and generate a reason code of declined transaction.

V. Advantages

a) Banks in Pakistan can introduce Smartphone technology with digital banking, which people are already familiar with thus no extensive training is required.

b) Security of the PIN code can be ensured by implementing algorithm based verification.

c) Data analytics techniques can be incorporated by using the proposed system to analyze transaction trends and to detect fraud and theft.

Conclusion

This paper identifies security concerns regarding PIN verification methods used at ATMs and suggests a method to make transactions more safe and secure by bypassing the Teller's vulnerable hardware by entering the PIN from the keypad of a user's Smartphone or handheld device via bank's digital banking app.

The proposed system is designed to be more immune to hardware-based attacks such as PIN decoding, which is easily performed through illegally embedded keypads on the ATM device. Additionally, the given model has the capability to assemble user-generated data for further trend analytics. As such, adopting this method will undoubtedly enhance the security infrastructure of the banking system in Pakistan.

Future Work

This study enables future research opportunities by integrating multiple bank cards on a single PIN and by enabling biometric verification using a Smartphone screen to avoid the installation of biometric devices on every ATM.

References

[1] J. Zhong, "A Comparison of Mobile Payment Procedures in Finnish and Chinese Markets," 22Nd Bled Econference-eEnablement Facil. an open, Eff. Represent. esociety, pp. 79–96, 2009.

[2] K. Sridharan, "Multi bank atm family card : integration of multi bank multiple user in single card with user behavior monitoring using hmm & formula verification," Int. Res. J. Eng. Technol., vol. 4, no. 3, pp. 2391–2394, 2017.

[3] R. Anderson and S. J. Murdoch, "Emv," Commun. ACM, vol. 57, no. 6, pp. 24–28, 2014.

[4] M. Jacob, R. M. Jose, and N. Mathew, "QR based Card-less ATM Transactions," vol. 2, no. 2, pp. 81–83, 2016.

[5] V. M. Kumbhar, "Customers ' Satisfaction in Atm Service: an Empirical Evidences from Public and Private Sector Banks in India," Manag. Res. Pract., vol. 3, no. 2, pp. 24–35, 2011.

[6] N. Velankar Himani Saxena Devendra Sharma, Financial Matters In Global Perspective Financial Matters in Gloabal Perspective, Customers Perception towards ATM Services: A Study of Indian Banks Priyanka Sisodia, Roshni Gupta, Richa Dube, p-234- 243, 2016.

[7] M. Okechukwu and I. Majesty, "ATM Security Using Fingerprint Biometric Identifer: An Investigative Study," Int. J. Adv. Comput. Sci. Appl., vol. 3, no. 4, pp. 68–72, 2012.

[8] V. Padmapriya and S. Prakasam, "Enhancing ATM Security using Fingerprint and GSM Technology," Int. J. Comput. Appl., vol. 80, no. 16, pp. 43–46, 2013.

[9] D. Mahansaria, "Secure Password Entry Scheme in ATM Network which Is Resistant to Peeping Attacks," vol. 1, no. 2, pp. 142–145, 2009.

[10] V. Roth, K. Richter, and R. Freidinger, "A PIN-entry method resilient against shoulder surfing," Proc. 11th ACM Conf. Comput. Commun. Secur. - CCS '04, p.236, 2004.

[11] Anil K. Jain, Fellow, IEEE, Arun Ross, Member, IEEE, and Sharath Pankanti, Senior Member, IEEE, "Biometrics: a Tool for Information Security,"IEEE transactions on information forensics and security, Vol. 1, no. 2, June 2006.

[12] J. Zinman et al., "Auto Teller Machine (ATM) Fraud – Case Study of a Commercial Bank in Pakistan," J. Bank. Financ., vol. 2, no. 2, pp. 43–45, 2014.