Secure PIN Authentication for ATM Transaction using Mobile Application

Bharathiraja N, Ravindhar N.V, Loganathan V

***Abstract*— Automatic Teller Machines (ATMs) transactions are an important role for obtaining money using credit or debit cards; hence they need to be secure and trustworthy. Shoulder-surfing or observation attacks, including card skimming and video recording with hidden cameras while users perform transactions at point-of-service terminals is one of the common threats for common users. In the proposed system, a secure authentication protocol for performing transaction in Automatic Teller Machines (ATMs) using mobile application is developed. This approach protects the user from illegal use of credit/debit cards and partial observation attacks, and is also against to relay, replay, and intermediate transaction attacks in the transaction process. Users use an mobile application installed in their personal mobile device for scanning a Quick Response (QR) code on the screen to initiate the transaction and obtain a secure One-Time-Password (OTP) for authentication. By using this proposed system, the security is enhanced while providing less complexity on the user side.**

***Index Terms*—About four key words or phrases in alphabetical order, separated by commas.**

I. Introduction

PIN based verification is mostly done in the automatic teller machine transactions. Enhancing this security, user authentication process is an important activity. The major problems include shoulder-surfing attacks, replay attacks, card cloning, and PIN sharing. Multiple researches have also been conducted to create systems supporting card-less transactions.

These are getting popular, where users can use additional personal devices, such as mobiles phones, to perform atm transactions. Shoulder-surfing attacks, also known as observation attacks, are most common threat for ATM authentication. In this case, the attacker simply views the entry procedure of the PIN by the authorized user to get hold of the secret information. Credit card and debit card frauds due to identity thefts are increasing every year. Additionally, there are scamming techniques using fake terminals, credit card cloning, and remote relay which make the process of user protection harder.

The attacker can be standing in queue behind the authenticating person and looking at the PIN entry and execute a shoulder-surfing or observation attack. The attacker may also install a small camera on the top surface of the ATM terminal to record PIN entries of users at the point-of-service. The attacker can install a card skimming device on the ATM machine to get hold of the user's card information. Such devices fit at the card slot on ATM machines and record the card information as the user slides in their card. The security level is thus improved by providing a PIN authentication protocol for ATM using mobile applications in smart phones. Image processing technique is further used for user identity checking process when a maximum of three PIN attempts is made by the user.

II. RELATED WORK

A. *GSM based antitheft Transaction system:*

In this system GSM module is used. This project helps to overcome the problem of complexity and provides easiest way to secure the ATM transaction. Whenever person enters account number onto the ATM machine, the system requires PIN to authenticate the user. If PIN gets verified, it makes a call to the user's mobile.[12] If the user replied to make a transaction, then transaction process takes place. The proposed system uses GSM modem for call from ATM to the user and getting reply from user to ATM. If user correctly entered amount and secondary password from mobile then transaction takes place. There is no problem of lost or damaged ATM card. The drawback of the system is authentication process will take much time. It is a time consuming process.

B. *An enhanced ATM security system using second level authentication [2] :*

The objectives of this study are to propose a second-level authentication system on the existing ATM process for withdrawal, after entry of correct PIN and to propose second-level authentication system in a scenario where a customer-specified withdrawal limit is attained. To perform the transaction the pin and amount has to be entered by the user. The permanent PIN number will get verified by the bank server. If the authentication is successful then the entered amount will be verified whether the amount lies within the user specified limit. Upon successful authentication the OTP will send to the pre-registered mobile device. Some of the advantages of this system are it is cheaper than biometric authentication, practical and workable. Drawback is in case of emergency user can't withdraw huge amount of money.

C. *ATM security using Fingerprint Biometric Identifier:*

ID cards can be lost, forged or misplaced [3]; passwords can be forgotten but ones' biometric is in full control of to its owner. It cannot be borrowed, stolen or easily forged. Using the proper PIN gains access, but the user of the PIN is not verified. When credit and ATM cards are lost or stolen, an unauthorized user can often come up with the correct personal codes. Biometric authentication technology using fingerprint

Revised Version Manuscript Received on May 06, 2016.

Bharathiraja N, Assistant Professors, Department of Computer Science Engineering, Saveetha Engineering College, Anna University Chennai (Tamil Nadu). India.

Ravindhar N.V, Assistant Professors, Department of Computer Science Engineering, Saveetha Engineering College, Anna University Chennai (Tamil Nadu). India.

Loganathan V, Assistant Professors, Department of Computer Science Engineering, Saveetha Engineering College, Anna University Chennai (Tamil Nadu). India.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

identifier may solve this problem since a person's biometric data is unique for every individual.[8]

III. EXISTING SYSTEM

In the process of ATM transaction, there are different aspects that should be considered. Personal identification number has been of very great importance in the overall operation. The PIN is not printed or embedded on the card but is manually entered by the cardholder during ATM transactions. In existing system, the card will be swiped. After swiping the card, the machine will ask for amount to be transacted and user's PIN. The user has to enter the necessary details. Upon entering, the transaction will take place. The transaction would get declined if incorrect PIN is entered.

A. *Limitations of Existing System:*

- Shoulder-surfing attacks.
- Complicated skimming techniques using fake terminals.
- Credit card cloning.
- Record PIN entries of users at the point-of-service.
- Customer is not having any option to block the view of PIN.
- PIN Recollection.
  Use of fake pin pad overlay

IV. PROPOSED SYSTEM ARCHITECTURE

In the proposed system, the user is able to perform ATM transaction in a secure way using mobile application. User has to log in to that application by using user name and password. During login the IMEI number of the registered mobile is automatically detected. Username, password as well as IMEI number of user mobile are used here to authenticate user. The app allows a user to scan a QR code from the screen of a ATM terminal and connects to the bank's server to obtain secure one-time-password(OTP)[12].

Checking the user identity (User profile photo) in the bank database for a minimum three attempts are allowed to the user for entering the pin in the ATM. If the user exceeds three times, the user image will be captured and sent to the bank server. The bank server will check the user image by searching in the bank account holder's image database. If the user identity is matched then the user will get the pin Re-entry option again. If the Identity is not matched, the user account and mobile application will be blocked.

The architecture consists of three key components namely user, ATM terminal and the bank server. The system model allows credit/debit card users to perform secure obfuscated PIN authentication at ATM point-of-service terminals. Bank Server : The bank server is a cloud-based server that stores the users' service profiles. The server incorporates a callable API server to communicate with the user application and the ATM terminal.

Point-of-Service Terminal: The ATM point-of-service terminal has a unique location identifier, Loc ID, which is approved and assigned by the bank. The ATM incorporates network connectivity and can communicate with the bank over secure connection. User: The user owns a personal mobile, for using the service for secure PIN authentication. The mobile application is installed on the mobile device. The mobile application requires the user to log in using the username and password. Once logged in the user can perform the transaction with his registered mobile device.

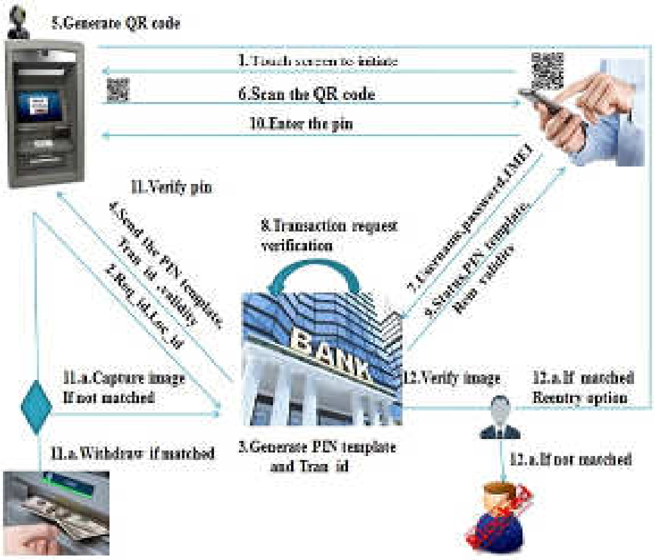
5.Generate QR code
1.Touch screen to initiate
6.Scan the QR code
10.Enter the pin
11.Verify pin
4.Send the PIN template, Tran_id, validity
2.Req_id,Loc_id
8.Transaction request verification
7.Username,password,IMEI
9.Status,PIN template, Rem_validity
BANK
11.a.Capture image If not matched
12.Verify image
12.a.If matched Reentry option
11.a.Withdraw if matched
3.Generate PIN template and Tran_id
12.a.If not matched

Figure.1.Proposed System Architecture

V. MODULES

Figures There are three modules in the process of the proposed system. Each process is dependent on the previous process.

- Bank Account Registration
- Transaction Process
- PIN Re-entry process

A. *Bank Account Registration*

Initially the users should register in the bank with the mobile application by installing in smart phones. The user should submit his personal details such as user name, password, date of birth, address, email id, mobile number, International Mobile Station Equipment Identity (IMEI) number, user image. The user's mobile IMEI number is automatically detected and sends to the bank while completing the registration process. The IMEI is registered so as to validate the user mobile identity each time he tries to access the ATM machine. Thus the bank database stores all the necessary details about each user. The image provided by the user will be cropped using HAAR technique.

B. *HAAR Technique*

HAAR is a technique which is used to recognize the face region in an image. A window is moved over the given image to detect only the face region. The input image is divided into two images namely positive image (image with face) and negative image (image without face). Having more number of positive and negative images will normally cause a more accurate classifier.

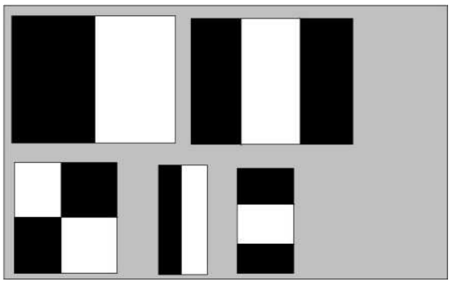

Figure.2.Moving window

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

In Figure.2, The window consists of black region and white region which moves through the entire image. It detects the positive image and negative image. The pixel value of each region is obtained and that is used to subtract the pixel value under white region and pixel value under black region. Finally a single value is obtained after subtracting the pixel values. The value is then compared to the value of training data that separates non-face from face.

C. Transaction Process

The user, along with the personal mobile approaches the ATM to perform a secure transaction. The ATM screen displays a " Touch to begin " information screen by default. The user touches the screen to initiate the transaction. At this point, the ATM sends an ATM_TRAN_REQ message to the bank's secure server. The structure of the message is defined as:

ATM_TRAN_REQ ⟹ [Req_ID,Loc_ID]

Here the Req_ID is a request identifier which is generated by the ATM for this current transaction request. The Loc ID is the unique and verified identifier for the particular ATM point-of-service assigned by the bank. Upon receiving the ATM_TRAN_REQ message from the ATM, the bank generates a transaction identifier, Tran ID, for this particular ATM transaction request. The bank then generates an one-time-password for the transaction to be made at the ATM. Finally, the bank creates a record, REC, for the received ATM TRAN REQ message, and stores it on the local database.

REC⇒ [Req ID,Loc ID,Tran ID,Validity, OTP,TS,IsUsed]

Here, TS is the timestamp at which the ATM TRAN REQ message was received by the bank from the ATM. The bank can specify a time limit for OTP. The bank stores the Validity for the maximum period of time within which the PIN template has to be used. Additionally, the IsUsed flag is set to FALSE and is saved to keep track if the particular transaction request has been successfully completed or not.

Next, the bank server responds to the transaction request made by the ATM using an ATM TRAN RES message. The structure of the message is defined as:

ATM TRAN RES⇒ [Tran ID,Validity, OTP]

Here, the Tran ID is the identifier generated by the bank for this particular transaction request. The bank also sends the Validity token, a timer for the maximum allowed time limit for the particular OTP and transaction request for the current user.Once the ATM receives the ATM TRAN RES message, it extracts the Tran ID, and generates a quick response (QR) code. The QR code is generated from the following context:

QR Code⇒ [Loc ID,Req ID,Tran ID].

Here, the Loc ID, Req ID, and Tran ID are the location, request, and transaction identifiers respectively. The QR code is then displayed on the ATM screen.

D. QR CODE

QR code (abbreviated from Quick Response Code) is the trademark for a type of matrix barcode (or two-dimensional barcode). 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. A QR code consists of black modules (square dots) arranged in a square grid on a white background, which can be read by an imaging device (such as a camera, scanner, etc.) and processed using Reed–Solomon error correction until the image can be appropriately interpreted. The required data are then extracted from patterns that are present in both horizontal and vertical components of the image. At this point, the user is able to see the QR code displayed on the ATM screen. The user then uses his personal mobile device which consists of the SEPIA application to scan the QR code. Upon a successful QR code scan, the Loc ID, Req ID, and Tran ID are transferred to the user's device from the ATM screen.

Once the user scans the QR code on the ATM screen, a USR_TRAN_REQ message is created and sent to the bank server over secure communication channel. The structure of the USR_TRAN_REQ message is as follows: USR_TRAN_REQ⇒ [Username, Password, Loc ID, Req ID, Tran ID].

In this message, the Loc ID, Req ID, and Tran ID had been obtained from the QR scan, and the username and password are the user's personal SEPIA service settings which have been previously saved on the bank's website. The bank's cloud-based server receives the USR_TRAN_REQ message from the user's personal mobile.

E. PIN Re-Entry Process

Given that the user received a success status in the USR_TRAN_RES message, the One Time Password(OTP) is then displayed on the user's mobile. The user then enters the OTP on the ATM's input screen. The ATM machine gets the user's OTP input on the screen. The OTP which the ATM received earlier in the ATM TRAN RES message is then used by the ATM to authenticate the user credentials and completes the transaction.

After the pin validation by the ATM machine, if it is successful that user should be asked to enter the transaction amount. Once the transaction successful the user will get the SMS alert about remaining balance. If the transaction amount exceeds than the available balance, the ATM machine will shows the error message. Then the current available balance is sent to the user's mobile.

If the user wrongly enters the PIN he/she will be given three attempts for properly entering the pin. The user image will be captured and send to the bank server, after three consecutive unsuccessful attempts. The bank server will check the user image by searching in the bank account holder's image database. If the user identity is matched then the user will get the pin Re-entry option again. If the Identity is not matched, the user account will be blocked.

VI. CONCLUSION

ATM authentication using PIN-based entry is highly susceptible to shoulder- surfing or observation attacks. In this system, we propose the Secure-PIN- Authentication, OTP-based authentication service for ATMs using Mobile devices. The protocol does not require any additional hardware support for currently operating ATM machine terminals and employs offloaded computation from the mobile device for verifying the transaction requests.

FUTURE ENHANCEMENT

The system is designed in such a way that it offers secured PIN authentication for ATM machine using smart phone. Future work involves applying this service to newer application fields such as, PIN-enabled doors and visual authentication mechanisms [4].

REFERENCES

1. Alhassan M.E,Ganiyur S.O,Muhammad-Bello B.L," An enhanced ATM security system using second level authentication",International journal of computer application(0975-8887),vol 111-no 5,feb 2015.
2. A.Gera,N.sethi, "A revived survey of various credit card fraud detection techniques," International Journal of Computer Science and Mobile Computing, vol. 3, no. 4, pp. 780 – 791, April 2014
3. G. Stanley, "Card-less financial transaction," Apr. 21 2014, US Patent App. 14/257,588.
4. Gajjala Askok,Sai Venupradhap, Sivakumar, "Design and Implementation of security based ATM theft Monitoring System", International Journal of Engineering Inventions , vol 3,2013.
5. E. Weise, "Home depot's credit cards may have been hacked," Online at http://www.usatoday.com/story/tech/2014/09/02/home-depot-credit-cards-hack-russia-ukraine/14972179/, Sep 2014, us TODAY.
6. M.-K. Lee, "Security notions and advanced method for human shoulder- surfing resistant pin-entry," IEEE Transactions on Information Forensics and Security, vol. 9, no. 4, pp. 695–708, April 2014.
7. S. Schaible, "How thieves clone your credit cards," Online at http: //www.wfla.com/story/26074193/credit-cards-cloned, Jul 2014, wFLA News Report.
8. J. Langer,M.Ronald, "Cloning credit cards: A combined pre-play and downgrade attack on emv contactless." in Proceedings of The 7th USENIX Workshop on Offensive Technologies, 2013.
9. Soundar raj,"A Third Generation Automated Teller Machine using universal subscriber module with iris recognition", International Journal of Innovative Research in computer and communication Engineering,vol 1, 2013
10. H. Nam, M.K. Lee, "Secure and usable pin-entry method with shoulder-surfing resistance," in HCI International 2013-Posters Extended Abstracts. Springer, 2013, pp. 745–748.
11. Gajjala Askok,Sai Venupradhap,Sivakumar,"Design and Implementation of security based ATM theft Monitoring System", International Journal of Engineering Inventions , vol 3,2013
12. S. N. White, "Secure mobile-based financial transactions," Feb 2013,