www.ioirp.com

International Journal of Innovative Research in Computer Science and Engineering (IJIRCSE)
ISSN: 2394-6364, Volume – 2, Issue – 4. April 2016

SECURE AUTHENTICATON FOR ATM IMPLEMENTING QR CODE USING MOBILE DEVICES

S.Kanimozhi, D.Revathy

Guide name: Mr.Gopirajan.V.P

Karpaga Vinayaga College of Engineering and Technology, Madurantakm

EMAIL ID: VRPreva6@gmail.com

ABSTRACT

Credit card fraud is a common problem in today's world. Financial institutions have registered major loses till today due to users being exposed of their credit card information. In the existing paper we use Shoulder-surfing or observation attacks, including card skimming and video recording with hidden cameras while users perform PIN-based authentication at ATM terminals is one of the common threats for common users. Researchers have struggled to come up with secure solutions for secure PIN authentication. In this paper, we propose Security PIN Authentication for providing security for user by using ATM by connecting Smart Phones. It is using Image Processing techniques is implemented for the user pin entry process. QR Code is the trademark for type of matrix barcode. A barcode is a machine-readable optical label that contains information about the item to which it is attached. Security PIN Authentication allows a user to scan a QR code from the screen of a point-of-service terminal and connects to the cloud based bank's server .Security PIN Authentication server to obtain secure one-time-use PIN templates. Here, a PIN template is a sequence of digits with marked positions for the user to enter the actual PIN code. The QR code scanning is done using mobile devices. The Security PIN Authentication service can also be used with a smart phones.

Keywords-ATM, Authentication, smart Card, QRcode ,webcam, TRANS_ID, PIN Template, Point-of-Service, Security.

1. INTRODUCTION

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 image.

2. RELATED WORK

Shoulder-surfing attacks, also known as observation attacks, are most common for ATM authentication. In this case, the attacker simply observes the entry procedure of the PIN by the authorized user to get hold of the secret information. Credit and debit card frauds due to identity thefts are increasing every year [10, 11]. Unfortunately, users of such banking systems are still not legally protected by the banks and card companies [12]. Additionally, there are sophisticated scam-ming techniques using fake terminals, credit card cloning, and remote relay or wormhole attacks which make the process of user protection harder [13–16].

Researchers have studied the reasons for ATM malpractices and the ways users are exposed to attackers [2]. Credit or debit cards may have magnetic strips on them to store the PIN information. Cards with magnetic strips are easy to clone with readily available and cheap card readers [17, 18]. Even though chip-based (EMV) cards are recently gaining popularity, cards still come with the magnetic strips, and it will be a while till all point-of-service devices and banks are upgraded to support only EMV cards. Unfortunately, such EMV cards are still vulnerable to cloning of the bank's certificate and relay attacks [15, 16]. Research on shoulder-surfing resistant PIN entry has not been new [19, 20]. Newer technologies, such as ubiquitous wearable devices and mobile phones have also been utilized in developing secure PIN authentication technologies [21]. However, such devices are also considered as an opportunity for more complex attacks by malicious users [22]. QR-based password using the client's certificate [21]. However, SEPIA does not rely on stored client certificates, and can be considered resistant to attacks even if the user loses the personal device. Moreover, the SEPIA service allows the users' devices to offload any security critical operations to the cloud and is highly scalable without imposing any resource- hungry operations on the personal mobile or wearable devices.

3. EXISTING SYSTEM

Shoulder-surfing attacks, also known as observation attacks, are most common for ATM authentication. In this case, the attacker simply observes the entry procedure of the PIN by the Authorized user to get hold of the secret information. Credit and debit card frauds due to identity thefts are increasing every year. Unfortunately, users of such banking systems are still not legally protected by the banks and card companies. Additionally, there are sophisticated scamming techniques using fake terminals, credit card cloning, and remote relay or wormhole attacks 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 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 has installed 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.

4. PROPOSED SYSTEM

In proposed system,a framework called the Secure-PIN-Authentications- a-Service (SEPIA) is to enable obfuscated PIN authentication for ATM using cloud connected personal mobile. SEPIA allows a user to scan a QR code from the screen of a point-of-service terminal and connects to the cloud based bank's SEPIA server to obtain secure one-time-use PIN templates. Here, a PIN template is a sequence of digits with marked positions for the user to enter the actual PIN code. The QR code scanning is done using mobile devices. The SEPIA service can also be used with a smart phone. The protocol is immune to shoulder-surfing attackers, and ensures resistance against relay and replay attacks by proving co-location with the ATM terminal to the cloud-based bank's server.

Checking the user identity (User profile photo) in the bank database minimum three attempts are allowed to the user to a maximum 6 attempts for entering the pin in the ATM. If the user exceeds three times, the user image will be captured and send to the bank server. The bank server will check the user image by searching in a bank account holder image database. If the user identity is matched then the user will get the pin reentry option again. If the Identity is not matched, the user account and android application will be blocked.

A net banking application is also implemented as web application for

1. Fund transfer
2. Fund transfer history and
3. ATM transaction history.

5. MODULE DETAILS

a. **Bank account Registration**

b. **ATM Pin Template generation**

c. **Transaction Process**

d. **Net Banking Process.**

5.1 Bank account Registration:

The users should be register in the bank with android application. The user should upload the valid passport size photo for the bank while registering. The user mobile imei number are automatically detected and send to the bank while register. The IMEI is registered so as to validate the user mobile identity each time he tries to access the ATM.

If the user wants to fund transfer, the user should be logged in a net banking to transfer the money from his/her account to another account. Once the logged in, they have the ability to see the fund transfer history, ATM transaction history and also checking the availability of the balance. If the user want to transfer the amount, the onetime verification will be send to the user mobile through SMS and then user have to enter that OTP for a successful fund transfer.

5.2 ATM Pin Template generation:

The user should initiate the transaction using the smart card. The smart is connected to the system through com port. Now the user can swipe in that card with the smart card reader device. After reading the card identity, the atm will generate the request id for that transaction and the location of the atm id (REQ_ID, LOC_ID) is sending to the bank server. Then the bank server generate the pin template and the transaction id for that transaction and then the bank server send the response(TRANS_ID,Pin template, validity) to the atm.

5.3 Transaction Process:

Now the server sends the response to the a ATM with the pin generated pin template and transaction ID.Then ATM will generate a QR Code for that data (LOCID, REQID, and TRANSID).Now the QR Code will be shown on the ATM Monitor .Once the user can see the QR code on the ATM he should login with the banking android application, With is credentials. Once the user logged in, they will scan the QRcode. The scanned QR data and the username and mobile IMEI are sending to the bank server.Now the bank server will cross validate the data with the request id and the received transaction id and send the one time pin for the pin template to the user mobile.

5.4 Net Banking Process:

Now the pin is directly viewed with the pin template in which it can be later shown in a google glass for improved security. The user enters the OTP received in the pin template to the ATM machine for pin validation.

After the pin validated by the ATM, 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 and also send to the user registered email address. If the transaction amount is exceeds than the available balance, the ATM will shows the error message. Then the current available balances are sending to the user mobile. In the android application also the user has the ability to see the fund transfer history, atm transaction history and also checking the availability of the balance.

If the user wrongly enters the pin he can 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 a bank account holder image database. Surf algorithm is used for matching the face comparison. If the user identity is matched then the user will get the pin reentry option again. If the Identity is not matched, the user account will be blocked.

6. ALGORITHM

- Surf Algorithm
- Transaction Request Verification Algorithm
- HAAR Cascade Algorithm

Surf Algorithm

Running some test on the SIFT SURF en FAST algorithm for logo detection on smartphones

- The Fast detector is much faster than the SURF detector,and even detects almost twice
- The next step though is not a predicted result.
- Using 180 ang 319 keypoints.

Transaction Request Verification Algorithm

- The secreat key Transaction authentication for DNS
- Protocol provides a transaction
- Application host server to bank server is in encrypted format.

HAAR Cascade Algorithm

- **HAAR**-feature based object detection algorithm
- This algorithm has been used face detection
- The image is partitioned into a set of overlapping windows

7. CONCLUSION

In this project, Secure-PIN-Authentication-as-a-Service (SEPIA), a secure obfuscated PIN authentication protocol for ATM and other point-of-service terminals using cloud connected personal mobile devices.
A proof-of-concept prototype implementation was used to perform experimental analysis and a usability study. Results show that users are easily adapted to the process of template-based authentication.

REFERENCES

1.T. Kwon, S. Shin, and S. Na, "Covert attentional shoulder surfing: Human adversaries are more powerful than expected," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 44, no. 6, pp. 716–727, Jan. 2014.

2. N. Sethi and A. Gera, "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. M.-K. Lee and H. Nam, "Secure and usable pin-entry method with shoulder-surfing resistance," in *HCI International 2013-Posters Extended Abstracts*. Springer, 2013, pp. 745–748.

4.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.