Preventing Shoulder Surfing Attack by Changing Flow of Card Payment System

Nehal Kadu
Pursuing BE IT
SKN College of Engineering,
Pune-41, Maharashtra

Suyog Akolkar
Pursuing BE IT
SKN College of Engineering,
Pune-41, Maharashtra

Mugdha Shirlekar
Pursuing BE IT
SKN College of Engineering,
Pune-41, Maharashtra

ABSTRACT

Security is provided to grant access to a legal user and to prevent the system from an illegal or non-authorized person. SHOULDER ATTACK is one of the latest weapons that are used by hackers or adversaries to hack an account or to authenticate in a secure zone. When a user uses a Chip+PIN credit card at a POS terminal, the POS machine will ask for PIN to be entered then on entering PIN in the terminal the transaction gets completed. To complete the transaction user need to provide four digit PIN number on that device. While providing PIN in front of friends, relative or unknown person, it is affected by "Shoulder Surfing attack". In a shoulder surfing attack, password can be easily obtained by simply looking at the fingers of the user or by making video while user enters the password.

So there is a need to develop a secure system for credit/debit card transactions that will avoid the SS and another similar type of attacks. The proposed system must contain minimum hardware changes and secure algorithms.

The approach is to divert the flow of current system in such a way that whenever the user needs to put PIN code, he will be using his mobile phone to type that pin-code. The user will get the request to enter the pin code on his/her phone itself. The project proposes the technology of secure authentication system to avoid shoulder surfing (SS) attack and also the problem of identity theft is resolved to increase the faith of users in the system.

Keywords

Shoulder Surfing (SS), Point Of Sale (POS), Personal Identification Number (PIN).

1. INTRODUCTION

In the modern era, people use credit or debit cards for transactions instead of cash. But according to the survey credit/debit card frauds are increasing day by day. One of the major attacks is shoulder surfing attack i.e. human or camera looking at the display while the user is entering PIN. So one can easily get the password and miss use it.A Credit card can get stolen, or the credentials from the chip of the card can be duplicated, even the credit card PIN is of four digits only, so can be easily cracked.

The flow of Card Payments are changed from OCT 2014 and PIN number is made compulsory to complete the transactions. This is applicable for all types of Cards (Debit, Credit, etc.) and is done to minimize the fraud/misuse of card payments. This method is called as CHIP+PIN methods.

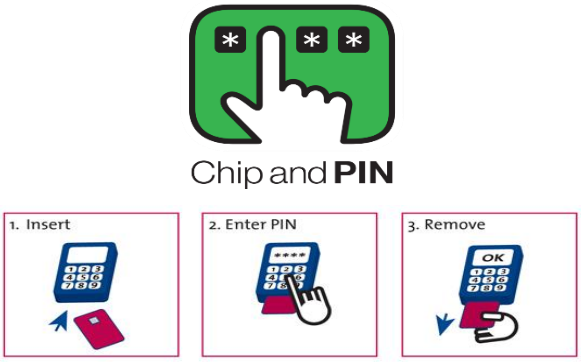

Fig 1.1: Chip+PIN method

The trust issue is also a big problem; the user feels uncomfortable to enter PIN in from of relatives or friends. So in the proposed system user can enter PIN in front of people without letting them know the correct password.

As there are many methods proposed to avoid the shoulder surfing attack, these methods change the some of the hardware of the system, but in this proposed system there is a change in the flow of existing system with minimum hardware changes to avoid the attacks. Also, in the current system password changing method is very complicated for the user, in this system user can change the password without following any complex procedure.

The Secure communication channel is established between the bank server and the Android app. So any information regarding the account or credit/debit card can be directly given to the user with fewer security concerns. So we can avoid credit card frauds that happen due to fake phone calls. Also, the application contains one panic button which will generate an alert when pressed. User can is easily able to block the card in case of stolen or lost. If the card gets stolen and the thief is trying to get money from ATM or to use it at any merchant's POS, the system will ask the user for the password on his/her phone. The user realizes that the card is stolen and then the card can be blocked immediately, and the merchant gets the alert about the theft.

2. PROBLEM DEFINITION

To prevent human shoulder surfing and overlooking attacks by providing a secure way to enter the PIN. It provides a secure authentication, communication, and transaction process by changing the flow of the current system.

3. EXISTING METHODS

Pass Shape - Stroke based Shape Passwords [1] are used nowadays as many people remember their PINs as a shape on the number pad of the ATM instead as a combination of numbers. So in this paper, user proposed that instead of remembering the password, the user should remember the shape of the password on the keypad. The password can be replaced by their shape representation in the numeric pad. Many times users forgot their new password shape and retry with the old one repetitively.

In Formula Based Authentication [2] (FBA) a user is authenticated by finding the answer of formula. This technique is highly resistant to SS attack but sufferers from poor usability. Shakir Ullah Shah et al. explored a new factor i.e. something you processed and described its usage by minimizing the complexity of FBA to maintain the security and increasing usability. The proposed system of authentication uses the ad hoc or Bluetooth connectivity eliminating the manual steps of taking a picture of the barcode and its analysis for the authentication mechanism.

Roth et al. [3] have developed a cognitive Trapdoor game to provide protection against shoulder-surfing. Cognitive Trapdoor game is ineffective against miniatures cameras. The observer can easily derive the PIN by recording the multiple sessions of the user. This approach is also very time consuming as a user has to play several rounds of challenges for entering just four digit code.

Bogdan Hoanca [4]. Represented secure graphical password system for high traffic public areas in which user used the concept of a camera-based eye tracking system that operates as a gaze-based mouse. The user looks at an object on the screen and selects it by fixing his/her eyesight on it or by pressing a button. There is no feedback provided that the image or location was selected successfully or not. Bogdan also presented a scheme that accounts for systematic errors. This type of error is when the estimated gaze position and the actual gaze position differ by a constant translation vector.

Samiullah Afzal [5] provided a solution by using Formula Based Authentication in such a way that user is asked to submit two things that user can remember instead of the username at the time of sing up. The Password is a numeric value of 3 to 6 digits that can be easily remembered. Four letter word is a four letter word like Iran, Iraq, Imam, etc. which represents the four arithmetic operators i.e. division, multiplication, addition, and subtraction.

For example, a user chooses 321 as his pass-code, and Iran as his four letter word [6]. This four letter word will be used to perform the arithmetic operations. The sequence for arithmetic operations is as follows.

i) / (division)

ii) * (multiplication)

iii) + (addition)

iv) - (subtraction)

The four letter word will be used to perform the arithmetic operations, in their sequence .i.e. the word Iran will be used in the following way,

i = / (division)

r = * (multiplication)

a = + (addition)

n = - (subtraction)

So here arithmetic operators are hidden in the digits which only the user knows. At the time of signing in, the user will have to enter his username; the system will give the user a formula (op code) which user has to solve.

4. PROPOSED SYSTEM

The aim is to provide security against the shoulder surfing attack and also to provide security in an authentication process. At the time of the transaction, the bank server should accept PIN from user's mobile phone instead of merchant's keyboard (POS). Provides security to the PIN by following various types of patterns such as reverse, half reverse or shuffle. The user can be able to set different patterns to encrypt the PIN. Banking system makes use of secure algorithms for its communication such as AES. So in the proposed system, such secure communication can be used for the transaction. Increase the faith of users by resolving the problem of identifying theft.

Once the user swaps credit/debit card on POS, it communicates with the bank server for authentication of card's credentials. After authentication server asks for the PIN from the registered mobile number. The user enters the PIN through the mobile application that is then encrypted and sent to the server. After validation process is finished, the transaction is completed. AES algorithm is used to secure the communication channel between bank server– Android application – merchant POS. The SHA-256 algorithm is used to hash the PIN entered by the user. Also, the base-64 algorithm is used to secure the bank's database.

4.1 Mobile Application

After the installation and registration of the application, training is provided to the user. Training trains the user how to set the secure password to his/her credit card. The user can set any one of the available patterns.

The user will enter the password that is not the original one but is derived by applying the pattern to it. Very easily interactive GUI will be provided to the user.

4.2 Merchant POS

It consists of GUI to generate the bill for the customer. The communication manager is provided to connect to the bank server. The card reader is used for reading the credit or debit card of the customer.

4.3 Bank Server

The banking logic will be provided for the transactions made on POS machines. It also consists of database manager for maintaining the MySQL database. The administrative logic will be provided & changes will be made through web GUI.

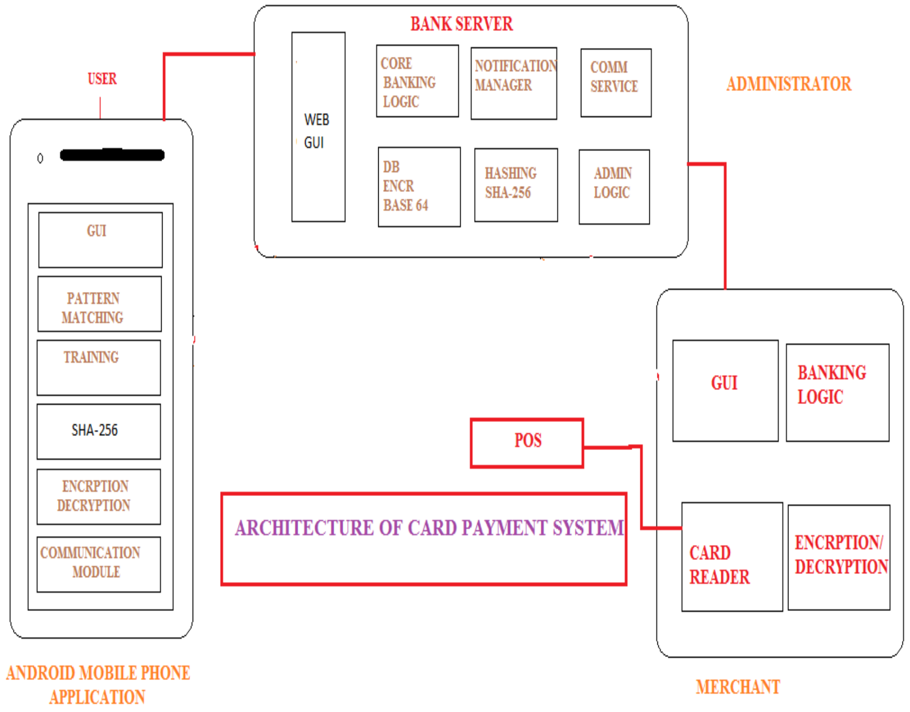

Fig 1: Architecture

Workflow:

1) The Customer swipes the card on merchant's POS.

2) Then the machine communicates with the bank server for the transaction.

3) The bank server communicates with the customer's mobile phone for the PIN entry.

4) The Customer enters the card PIN inside the android application.

PIN gets verified at the bank server, and the transaction takes place. The activity at Android app can be shown in detail as given in fig 2

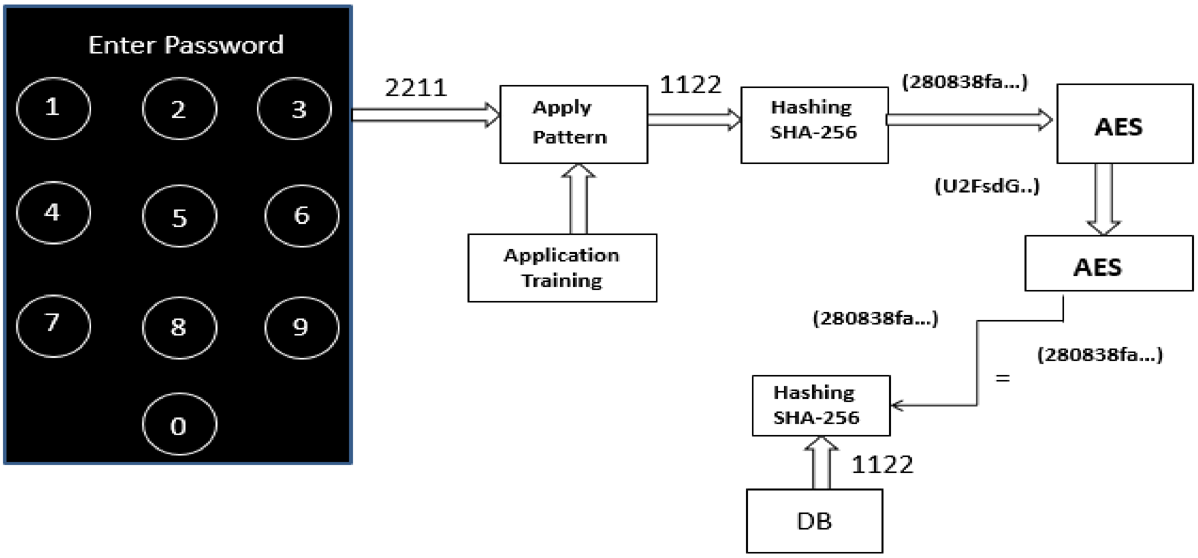

Fig 2: Workflow

1. The keyboard provided is virtual keypad i.e. the position of the numbers changes randomly at each time while entering the password.

2. After that pattern is applied to the user input, in this example reverse pattern is applied, and the original password is obtained.

3. Then SHA-256 hashing technique is applied, to the obtained password and digest is obtained.

4. AES encryption is applied to the message digest and then it is forwarded to the bank server.

5. At the bank server received a message is decrypted, and digest is obtained.

The password of that user is then obtained from the database and hashing is applied to it. So the digest obtained and the digest received are compared. If both the digest is similar, then the transaction is proceeded further else error message is sent to the user.

5. ACKNOWLEDGMENTS

We are extremely grateful to Asst-Prof. S.A.Nagtilak our Project Guide, who helped us from the very beginning and contributed towards the development of the project.We would also like to thank our friends and family for their love and support.

6. CONCLUSION

The overall study proposes a secure system against shoulder surfing and overlooking attacks. The secure authentication process is obtained which is resistant to password guessing and brute force attack. The system achieves more security without changing the hardware. The difficult task of remembering the difficult formulas is made simple. A thief can get caught red handed at the merchant’s POS by providing the alert system.

7. REFERENCES

[1] Alexander De Luca, Roman Weiss, Heinrich Hussmann, 2007."Pass Shape - Stroke based ShapePasswords"OZCHI '07.

[2] Lev Ginzburg, Rockaway,"User Authentication System and Method", NJ (US), 2006.

[3] V. Roth, K. Richter, and R. Freidinger, “A PIN-entry method resilient against shoulder surfing”. In CCS '04: Proceedings of the 11th ACM conference on Computer and communications security, pages 236-245, New York, NY, USA, ACM, 2004.

[4] Bogdan Hoanca, Kenrick Mock 2006. "Secure graphical password-a system for high traffic public areas," ETRA '06

[5] Shakir Ullah Shah, Fazal-e-Hadi, Fahad Bin Muhaya,”Secure User Authentication in Multimedia Systems”, Peshawar, Pakistan, IEEE, 2010.

[6] Syed Shabih ul Hasan Naqvi, Samiullah Afzal, ”Operation Code Authentication”, Peshawar, Pakistan,IEEE,2010.