International Journal of Innovative Studies in Sciences and Engineering Technology (IJISSET)

ISSN 2455-4863 (Online) www.ijisset.org Volume: 2 Issue: 2 | February 2016

Preventing Shoulder Attack to Secure Card Payments

S. A. Bhure[1], N. D. Gaikwad[2], S. R. Dadge[3], V. V. Amale[4], I. S. Savant[5]

[1]Student, Computer engineering, MMCOE, karvenagar, Pune, Maharashtra, India
[2]Student, Computer engineering, MMCOE karvenagar, Pune, Maharashtra, India
[3]Student, Computer engineering, MMCOE karvenagar, Pune, Maharashtra, India
[4]Student, Computer engineering, MMCOE karvenagar, Pune, Maharashtra, India
[5]Assistant professor, Computer engineering, MMCOE karvenagar, Pune, Maharashtra, India

Abstract: *As per recent 2015 news of RBI Mandate, all credit card (Plastic card) users who used their cards at international point of sale(POS) terminal are replaced with a new CHIP+PIN card. A chip is a small microchip embedded in your credit card (Or in any plastic cards). It is encrypted so transactions are more secure while using the card. The CHIP+PIN card provides a superior level of security to your card, in addition with best global practice of security of transactions. When you use a CHIP+PIN credit card at a POS terminal, the POS machine will notify you for your PIN to be entered , you are required to enter the 4 digit Credit Card PIN number on the terminal to complete the transaction. We found a problem when user is typing his/her PIN number in front of merchant, friends, relative or unknown person, it is affected by "Shoulder attack or overlooking attack".*

Keywords: *Paytm, Shoulder Attack, CHIP+PIN, Point of sale (POS), Merchant*

1. INTRODUCTION

The flow of Card Payments are changed in recent months that is after inserting CHIP+PIN card at POS machine you have to enter private PIN number provided by bank to complete the transaction. This is applicable for all types of plastic cards (Debit, Credit, etc). This is done to minimize the fraud/misuse of card payments. Nowadays, one of the weapon of hackers is shoulder attack .It is used to hack user's confidential information like transactional records, Bank account details and also includes passwords which must be confidential. In a shoulder attack attacker person is watching the user while he is typing the password and reads his fingers that what he has typed for acquiring password. We wanted to address this problem. To cope with this problem we wanted to develop such a technique which provides more security to a user in typing his password in a public place like petrol pumps, supermarkets, malls, movie theatre, etc[2]. As per our proposed technique we wanted bank server should accept PIN from user's mobile phones and not from merchants POS terminal.

2. LITERATURE SURVEY

2.1 Payment by Cash

In early days when cards were not available then every person used to pay bill payment by cash. In this hand to hand payment was available so there was confidentiality. But problem was that person has to take cash along with him although the cash amount is more.

2.2 Manual card payment

If we look into STEPS of manual card payment:

Step1: The merchant inserts your card at POS terminal

Step2: He enters the transaction amount

Step3: The merchant removes the card

2.3 Application (Paytm)

Paytm is a mobile application used by lot of people now-a-days. In Paytm application we can do all types of online bill payment. This consists of login id and password which can be only customized by that specific person. This is very handy application and is easy to use. But most of the people used to keep remember login id and password in that application. This is characteristic of mobile application that every time there is no need to type login id and password. But there is drawback that we need internet connection and have to keep mobile with us every time.

2.4 CHIP+PIN payment

The entry of a password can easily be observed by nearby adversaries in crowded places, aided by vision enhancing and/or recording devices, and the information that should be kept secret is leaked in a relatively non-technical manner. Even partial information leakage can be greatly harmful, since users tend to use similar or even identical passwords on multiple systems, some of which may be more important than others. The whole secret PIN could be leaked through even a single authentication session. Since PINs are so popularly used in a variety of common devices, such as smart phones, automated teller machines (ATM), and point of-sale (POS) terminals, there is a great need for a secure PIN entry scheme that does not significantly sacrifice usability. Various security enforcement methods have been proposed, but achieving both security and usability still remains a challenging goal.

Steps in CHIP+PIN card payment are as follows:-
Step1: Insert CHIP+PIN card into POS terminal.
Step2: Enter 4 digit PIN.
Step3: Remove card.

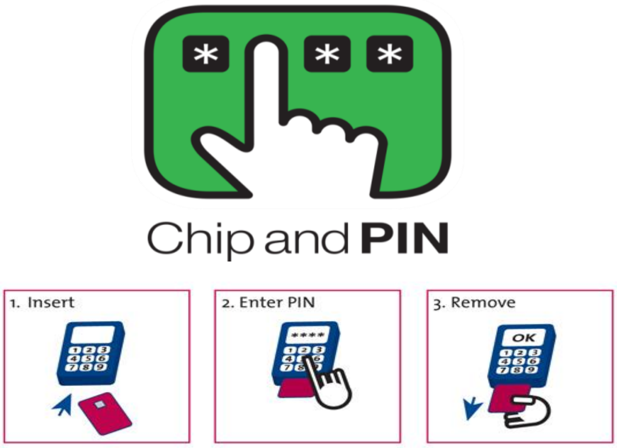

Fig no:-2.1

3. PROPOSED SYSTEM

3.1 System architecture

If we look into STEPS of card payment:-

Step1: The merchant inserts your card at a PIN enabled POS terminal.

Step2: He enters the transaction amount

Step3: The machine prompts for a PIN to be entered by you.

Step4: You enter your Credit Card ATM PIN in the machine.

Step5: On entering the correct PIN the transaction is confirmed and completed.

Above we have mentioned card payment steps, in step5, we have entered our private PIN in front of merchant or friends to complete transaction on POS terminal where they can see my password. So to prevent such type of attack we are proposing a system which is more secure than the existing system such that whenever we want to do the card payment after inserting the card on the POS terminal the bank server will notify on users mobile phones instead of asking on merchant's device. User can now safely enter PIN using his/her mobile. Even user is free to provide any pattern which he can change on daily or monthly basis. We are using Cryptography and Hashing security for communication between bank server, mobile application and merchant hardware.

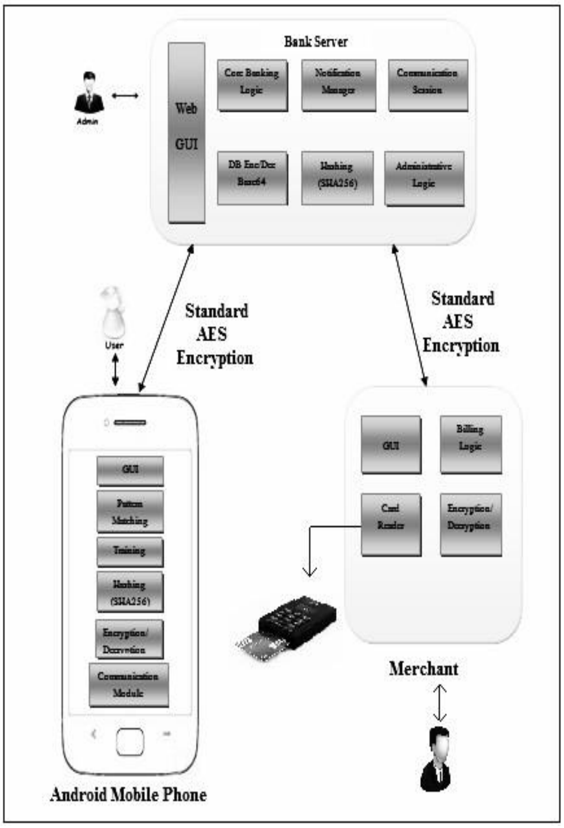

Fig no 3.1.1: *System Architecture*

1.GUI:

GUI will provide Numerical keypad for typing the transaction amount.

2. Communication Manager:

Communication Manager is for communication between client side and server side.

3. Core Banking Logic:

It is banking logic runs at the server side.

4. Hashing:

It is nothing but the encrypted message sent from the user's phone which contains some specific hash value which is already stored at the bank's database.

5. Card Reader:

It is for scan a card.

6. Database Manager:

Database manager manages the database of the system.

7. System Configuration:

System configuration handles all the configuration files of the system.

8. Encryption/Decryption Module:

This will handle all encryption and decryption logic.

9. Notification Manager:

It will notify user about his bank transactions and any other remainder messages.

10. Billing logic:

It is applicable only when any discounts are offered by the merchant.

3.2 Proposed Algorithm

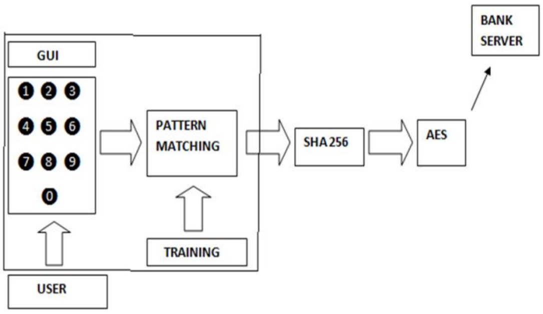

Fig no 3.2.1: *Algorithmic block diagram*

In our proposed technique user have to create his own GUI system on his or her android mobile phone. In GUI system there are three modules number pad, pattern matching and training center.

1. Number pad

   In number pad system we give the random function to swap the position of the numbers after every transaction [3].

2. Training center

   In training center we can apply various patterns such as reverse, yes/no, +1, -1, etc to the mobile device.

3. Pattern matching

   It is matches the pattern from user entered PIN and the training center then it will convert into the actual pin.

SHA-256:

We are using SHA algorithm to convert four digit PIN number into 256 bit unique number. To provide better security we used AES encryption algorithm.

Bank Server:

After reaching to bank server PIN number is decrypted and compared with already saved username and password in the server database. If it is valid then server will notify at merchant's POS terminal and bill will be generated. If PIN number is not valid then it will notify at merchant's POS terminal that PIN number is not valid.

4. DEFINITIONS

4.1 Cryptography

In cryptography technique, data is encrypted using key involving Armstrong number and colors as password[4]. Encryption is the technique in which transformation of data into some unreadable form and its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended. Decryption is the technique reverse of encryption; it is the transformation of encrypted data back into some intelligible form. Decryption and encryption require the use of some secret information, usually referred to as a key. The data which is to be encrypted is called as plain text. The encrypted data obtained as a result from encryption process is called as cipher text. Authentication and Access Control: When user sends data from one cloud to another, then Authentication requires for securing user's data. One time password and biometrics should be implemented in this manner. Digital signatures are used for authentication.

4.2 Black and white method

The basic model of black and white method consists of horizontal of digits from 0 to 9 and randomly arranged colors. Black and white method divides 10 digits in two halves. It play when user will have TM service mobile app then Black and white method is selected according to the user's key entry in each round Black and white method consists of four iterations each iteration refers to pin entry of single pin[2].

5. CONCLUSION

So whenever merchant swap user's card for payment, bank server will notify user on his mobile to enter PIN number. User can now enter PIN using his/her mobile.

Even user is free to provide number as YES/NO or any pattern which he can change on daily or monthly basis. Hence we overcome shoulder attack/Overlooking attack problem in our proposed technique.

ACKNOWLEDGEMENT

We have made this paper on topic "PREVENTING SHOULDER ATTACK TO SECURE CARD PAYMENTS", We have tried our best to elucidate all the relevant detail to the topic to be included in the paper. While in the beginning we have tried to give a general view about this topic. Our efforts and wholehearted co-operation of each and everyone has ended on a successful note. We express our sincere gratitude to Prof. Ila Savant who assisted us throughout the preparation of this topic. We thank her for providing us the reinforcement, confidence and most importantly the track for the topic whenever we needed it.

REFERENCES

[1] International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 2, February 2014 Credit Card Fraud Detection System Using Hidden Markov Model and K-Clustering

[2] PREVENTING HUMAN SHOULDER SURFING AND TO PROVIDE RESISTANCE AGAINST PIN ENTRY, International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 0976-1353 Volume 13 Issue 1 –MARCH 2015

[3] Designing leakage-resilient password entry on touchscreen mobile devices, Singapore Management University Institutional Knowledge at Singapore Management University Analysis and Improvement of a PIN-Entry Method Resilient to Shoulder-Surfing and Recording Attacks, IEEE 2014 Taekyoung Kwon, Member, IEEE, and Jin Hong- IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY

[4] Gayatri Kulkarni , Pranjali Gujar, Madhuri Joshi, Shilpa Jadhav,"Message Security Using Armstrong Numbers and Authentication Using Colors", International Journal of Advanced Research in Advance Computer Science and Software Engineering ISSN:2277 128X, Volume 4, Issue 1, January 2014.

AUTHORS' BIOGRAPHIES

Shubhangi A. Bhure persuing BE in Computer engineering at marathwada mitra mandal's college of engineering, karvenagar, Pune.

Neha D. gaikwad persuing BE in Computer engineering at marathwada mitra mandal's college of engineering, karvenagar, Pune.

Shital R. Dadge persuing BE in Computer engineering at marathwada mitra mandal's college of engineering, karvenagar, Pune.

Vikrant V. Amale persuing BE in Computer engineering at marathwada mitra mandal's college of engineering, karvenagar, Pune.

Ila S. Savant assistant professor in Computer engineering at marathwada mitra mandal's college of engineering, karvenagar, Pune.