International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)) Volume 4, Issue 10, October 2015)

A Novel Approach of Card Payment to Avoid Shoulder Surfing Attacks

Akanksha Gat[1], Neha Bhosale[2], Harshada Deshmukh[3], Snehal Gore[4], Prof. Mrs.Shwetambari Chiwhane[5]

[1,2,3,4]*Pune*

[5]*NBN Singad School Of Engineering, Ambegaon, Pune-411042, India*

***Abstract*— As per the recent Reserve Bank of India Mandate, the customers who have used their credit card at an international Point of Sale (POS) terminal will have to be re-carded with a Chip+PIN credit card. A chip is a small microchip embedded in customer's credit card. Chip is encrypted so transactions are more secure on the card. The Chip+PIN card is a most superior level of security on customer's card, in line with best global practice of security of transactions. When customer uses a Chip+PIN credit card at a Point of Sale terminal, the Point of Sale (POS) machine will prompt customer for his/her PIN to be entered, you are required to enter the Credit Card or ATM PIN in the terminal and complete the transaction. To complete the transaction we need to provide 4 digit PIN number into that device. We suspect a security thread in this process. While providing PIN in front of friends, relative or unknown person, it is affected by "Shoulder attacks".**

***Keywords*— Cloud Security, Shoulder Attack, Card Payment Security**

I. Introduction

Nowadays, one of the weapon of hackers is shoulder attack .It is used to hack user's confidential information like financial records, Bank account passwords. In a shoulder attack a 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 handle this type of attacks we wanted to develop such a technique which provides more security to a user in typing his password, in a public place like malls, movie theatres etc. As existing systems are using CHIP+PIN method. CHIP+PIN enabled Credit Cards offers more security and fraud protection. As per our propose technique we wanted bank server should accept PIN from users mobile phone and not from merchants keypad. So when ever merchant swap user card for payment, bank server will notify user on his mobile to enter PIN number [4].

II. Definations

2.1 Cloud Computing:

Cloud computing is becoming increasingly important for provision of services and storage of data on Internet.

Cloud computing: It is a technology where cloud service provider provides resources to their clients to host their data and perform their computing task. However there are several challenges in securing cloud infrastructures from various attacks. Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a utility (like the electricity grid) over a network. At the foundation of cloud computing is the broader concept of converged infrastructure and shared services.

2.1.1 Challenges

- Attraction of hackers: It is becoming target of hackers because information is easily available hence can be easily hacked.
- Service provider can easily access user's data that is on the cloud at any time. So it can accidently or deliberately alter or even delete information.

2.2 Cryptography:

In cryptography technique, data is encrypted using key involving Armstrong number and colors as password. 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.

The three types of algorithms are as follows:

Secret Key Cryptography (SKC): It uses single key for encryption as well as for decryption. The common algorithms used are Data Encryption Standard (DES), Advanced Encryption Standard (AES).

- *Public Key Cryptography (PKC):* It uses different keys for encryption and decryption.. For example, RSA (Rivest, Shamir, Adleman) algorithm
- *Hash Functions:* It uses a mathematical transformation to irreversibly "encrypt" information. For example, MD (Message Digest) algorithm.

2.3 Elliptic Curve:

In cryptography, one of the technique used is Elliptic Curve (EC) for securing user's data. It was first proposed independently by Neal Koblitz and Victor Mille in 1985.

Let us assume we have two organizations Q and S. Q and S act as public clouds with data, software and applications. Q want to send data to S's cloud securely and data should be authenticated. Here we will apply digital signature and encryption to data by using elliptic curve technique, while sending that data from cloud Q to S. Suppose S wants text document from Q's cloud then S's user will place a request to Q's user. Q's user select corresponding text document from Q's cloud data storage and then apply the hash function, it will give message digest. Sign the message digest with his private key by using Q's software. It is called digital signature. Encrypt digitally signed signature with S's public key using ECC algorithm. Encrypted cipher message will be send to S. S's software decrypt the cipher message to text document with his private key and verify the signature with Q's public key [1].

2.3.1 Key generation:

1. Q selects an integer dQ. this is Q's private key.
2. Q then generates a public key PQ=dQ*S
3. S similarly selects a private key dS and computes a public key PS= dS *S
4. Q generates the security key K= dQ *PS. S generates the secrete key K= dS *PQ.

2.3.2 Generation :

Firstly message m is signed by sender of Q by using it's private key dQ. 1. HASH is a cryptographic hash function, which is used to calculate e=HASH (m) 2. Select a random integer k from [1, n − 1] 3. Calculate r = x1 (mod n), where (x1, y1) = k * S. If r = 0, go to step 2 4. Calculate s = k − 1(e + dQr)(mod n). If s = 0, go to step 2 5. The signature is the pair (r, s) 6. Send signature (r, s) to S cloud [1].

2.4 Encryption algorithm:

Suppose Q wants to send to S an encrypted message.

i. The plaintext message M is taken by Q the it encodes it onto a point PM, from the elliptic group.
ii. Q chooses another random integer, k from the interval [1, p-1]
iii. The cipher text is a pair of points PC = [(kS), (PM + kPS)]
iv. Send cipher text PC to cloud S [1].

2.5 Decryption algorithm:

For decryption of cipher text PC, the following steps will be taken by Cloud S

a. S computes the product of the first point from PC and his private key (dS). So dS * (kS)
b. S then takes this product and subtracts it from the second point from PC's

(PM + kPS) – [dS(kS)] = PM + k(dSS) – dS(kS) = PM

To get the message M cloud S cloud decodes PM . *Signature Verification:* For S to authenticate Q's signature, S must have Q's public key PQ 1. Verify that r and s are integers in [1, n − 1]. If not, the signature is invalid 2. Calculate e = HASH (m), where HASH is the same function used in the signature generation 3. Calculate w = s −1 (mod n) 4. Calculate u1 = ew (mod n) and u2 = rw (mod n) 5. Calcúlate (x1, y1) = u1S + u2PQ 6. The signature is valid if x1 = r(mod n), invalid otherwise [1].

2.6 Black and white method :

The basic model 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 with TM service mobile app Black and white method is selected according to the user's key entry in each round B&w method consists of four iterations.each iteration refers to pin entry of single pin[3].

2.7 Card Payment Steps:

The card payment is also affected by same attack. If we look into STEPS of card payment :

Step 1: Firstly your card will be inserted by merchant at a PIN enabled Point of Sale terminal.

Step 2: He enters the transaction amount

Step 3: The machine prompts for a PIN to be entered by you.

Step 4: You enter your Credit Card PIN in the machine

Step 5: On entering the correct PIN the transaction is confirmed and completed

Step 6: For terminals without PIN authentication support, your new Chip+PIN credit card shall continue to support the regular signature mode.

III. Proposed System

From above mentioned card payment steps, in step no.5, we have entered PIN in front of merchant or friends to complete transaction where those people can remember my PIN number. So to handle such type of attacks we wanted to developed such a technique which provides more security to a user in typing his password, in a public place, and in case that user is in critical position. As per our propose technique we wanted bank server should accept PIN from users mobile phone and not from merchants keypad. So whenever merchant swap user 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. We will be using Encryption and Decryption security system for communication between bank server, mobile application and Merchant hardware.

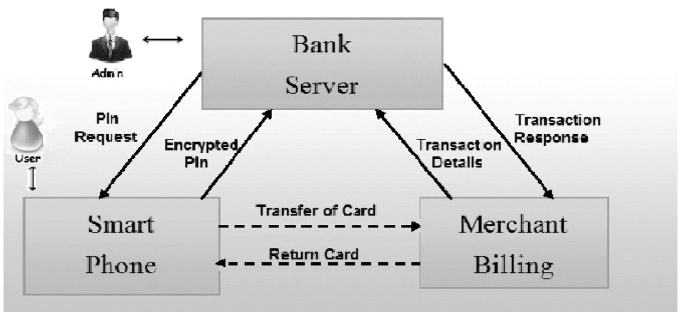

Fig 1: Architecture of card payment security

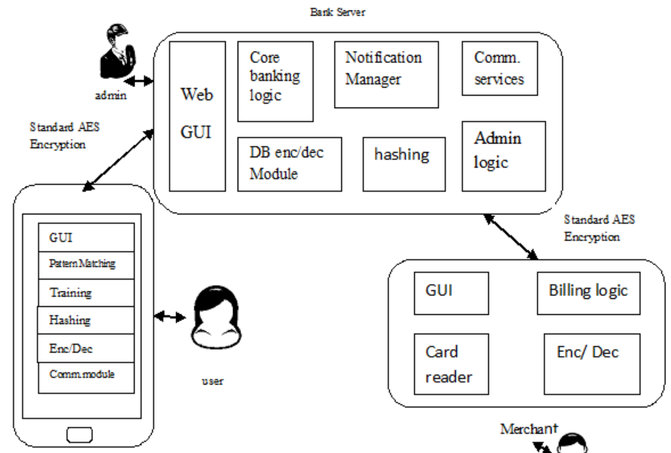

Fig 2 : Architecture of card payment

1. Keypad Circuit:-

Keypad Circuit will provide Numerical keypad for typing an amount.

2. Communication Manager:-

Communication Manager will handle the communication between client side and server side.

3. Web GUI:-

It means that the majority of the logic runs on the server side.

4. Banking Logic:-

Banking logic will handle the payment and transactions.

5. Card Reader:-

Card reader will 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 module will handles all encryption and decryption logic.

3.1 Armstrong Number

The combination of substitution and permutation technique is used to ensure data security. We perform substitution by assigning ASCII equivalent to characters. By using different Armstrong numbers and matrices Permutation process is performed. In above technique, the initial step is to each receiver is assigned with a unique color and no two receiver has same color . Each color is represented with a set of three values i.e values for Red, Green and Blue colors respectively. For example Rose pink color is represented in RGB format as (255,174,201). Assigning a set of three key values to each receiver Armstrong number is the next step. For ensuring more security to data that provides authentication, usage of colors as a password is beneficial. User can only access the actual data , when the colors at the sender's and receiver's side match with each other[2].

3.2 RGB Color Model :

Any color is the combination of three primary colors Red, Green and Blue in fixed quantities. A color is stored in a computer in form of three numbers representing the quantities of Red, Green and Blue respectively. Typically, 24 bits are used to store a color pixel. This is usually apportioned with 8 bits each for red, green and blue, giving a range of 256 possible values, or intensities, for each hue [2].

IV. CONCLUSION

A simple and effective system which solves the problem under study has been developed. Card payment security system help to solve shoulder surfing attack and gives simple solution to avoid shoulder attack problem.

REFERENCES

[1] Veerraju Gampala, Srilakshmi Inuganti, Satish Muppidi,"Data Security in Cloud Computing with Elliptic Curve Cryptography", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume 2, Issue 3, July 2012.

[2] 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.

[3] J.Rajalakshmi and V.Valarmathi Assistant Professor, "Preventing Human Shoulder Surfing and to Provide Resistence Against Pin Entry" International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 0976-1353 Volume 13 Issue 1, March 2015.

[4] Mun-kyu,"Security Notions and Advanced method for Human Shoulder- Surfing Resistant PIN entry",IEEE Transactions on Information Forensics and Security, Volume 4,No 4,April 2014