ISSN 2395-1621

Card Payment Security

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

[1]akankshagat@gmail.com
[2]nehabhosale77@gmail.com
[3]deshmukhharshada26@gmail.com

[#12345]NBN Singad School Of Engineering, Ambegaon, Pune-411042,India

ABSTRACT

Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. It is an effective way to get information in crowded places because it's relatively easy to stand next to someone who's entering a PIN number. When customer swipes his credit/debit card at merchant's terminal then merchant's system will communicate with bank server for customer's bank server for customer's bank account details. Bank server will further notify to customer's mobile phone for entering PIN and customer will enter his pin from his mobile phone rather than merchant's keypad. To secure communication between bank server and customer, we will use security algorithms such as Brute Force algorithm,MD5 Hashing algorithm and Base64 algorithm. Our proposed technique will secure card payment flow.

Keywords: Cloud Security, Shoulder Attack, Card Payment Security, Security algorithms.

ARTICLE INFO

Article History

Received :6th April 2016

Received in revised form :

8th April 2016

Accepted : 10th April 2016

Published online :

13th April 2016

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. To secure communication, we have used AES algorithm, MD5 hashing and Brute Force algorithm.

II. DEFINATIONS

2.1 Card Payment Steps:

- Merchant will login into system and initiate a payment transaction of amount 'a' for card no 'c
- .Data will get encrypted and sent to bank server .
- Bank server will search users session to send him notification
- User get notification on his/her mobile
- Client application will randomly shuffle keys of KEYPAD before user start giving input his/her PINs
- Once user done with input post processing starts
- System apply user pattern on given PINs
- Apply pattern matching algorithm on finally created PIN
- Get MD5 of the final PIN
- Apply AES on PIN and send this to server

- Server fetches encrypted PINs
- It will decrypt PIN using AES
- Now server will fetch user PIN from his database
- It will apply MD5 to that PINs
- verify if both PIN are same
- Accordingly server will take further action

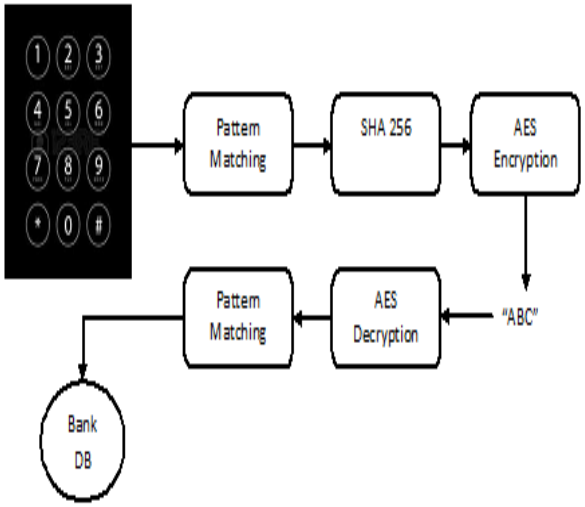

Figure 1: Flow of algorithms

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 Brute Force Algorithm

This algorithm is used for input PIN pattern matching. Requires a verification algorithm following a possible match to verify if a true match occur. In preprocessing phase the space and time complexity is O (m). In searching phase the time complexity is O (n+m),where n is the length (size) of the file and m is the length of the pattern.

2.4 Base64

Is a group of similar binary-to-text encoding schemes that represent binary data in an ASCII string format. By translating it into a radix-64 representation. The general strategy is to choose 64 characters that are both members of a subset common to most encodings, and also printable. The particular set of 64 characters chosen to represent the 64 place-values for the base varies between implementations. The ratio of output bytes to input bytes is 4:3 (33% overhead). Specifically, given an input of n bytes, the output will be 4/3 bytes long, including padding characters .We used this algorithm to encrypt users password which is saved present in server database.

2.5 MD5 hashing

Producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. We encrypt users given PIN using MD5 before sending that PIN to server.MD5 is a one-way function; it is neither encryption nor encoding. It cannot be reversed other than by brute force attack. The input message is broken up into chunks of 512-bit blocks (sixteen 32-bit words).The message is padded so that its length is divisible by 512.

III.PROPOSED SYSTEM

From 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.

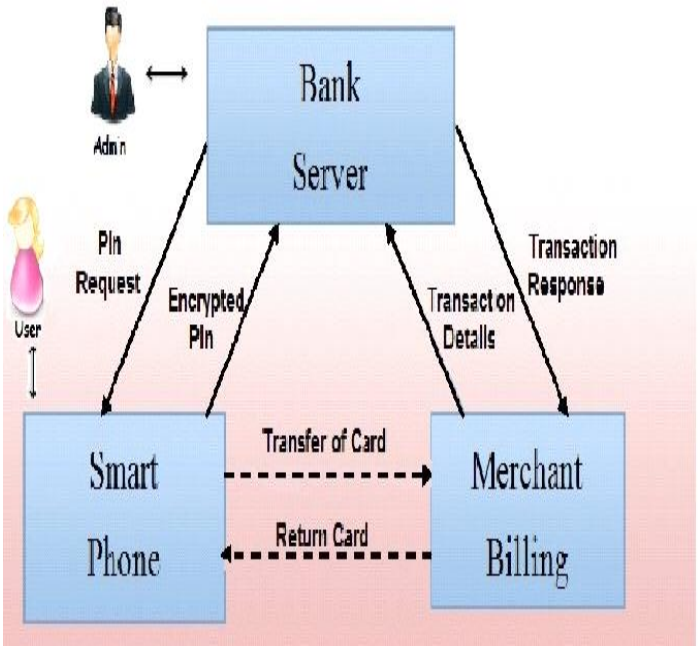

Figure 2 :Architecture of system

- Merchant POS:

  This is provided for the merchant so that he can start payment transactions. He needs to enter the amount & card users' number into system. System will connect to back server for further payment transaction. This module will help merchant user to initiate payment transaction.
- Web based GUI:

  Server will be web based application and this module will be responsible to take inputs from admin. The guiis developed in HTML and Java-script.
  Banking server input will be taken through this GUI where proper validations are supported. This includes new user registration, user account creation etc.
- Database Manager:

  This module will help to handle all database related activity. All the SQL queries will be taken care in this module. A database connection polling system will be present to avoid repeatedly opening and closing database connection. The JDBC driver manager ensures that the correct driver is used to access each data source. The driver manager is capable of supporting multiple concurrent drivers connected to multiple heterogeneous databases.
- Communication Manager:

  Communication Manager will handle the client server communication part. We have used REST over HTTP Standard communication technique for communication. REST stands for Representational State Transfer. (It is sometimes spelled "ReST".) It relies on a stateless, client-server, cacheable communications protocol -- and in virtually all cases, the HTTP protocol is used. REST is an architecture style for designing networked applications. The idea is that, rather than using complex mechanisms such as CORBA, RPC or SOAP to connect between machines, simple HTTP is used to make calls between machines.
- Banking Logic:

  This module handles all Banking logic and transactions. It also uniquely maintains each transaction sessions so that it can differentiate each system user. It takes help of database manager to complete all its transaction related database commits.
- System Configuration:

  The configuration manager which will be holding IP address of the entire client will be singleton in nature. The singleton pattern is a design pattern that restricts the instantiation of a class to one object. This is useful when exactly one object is needed to coordinate actions across the system.
- Encryption/Decryption Module:

  Total 3 different types of encryption/decryption technique have been implemented in system. Base64, MD5 hashing & AES algorithm. This module will handle all encryption and decryption logic of all types. It basically present in all of our 3 sub application.
- Keypad shuffle logic:

  This module takes care of randomly generating Keypad when users get PIN input notification on his/her mobile.

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. Proposed a new secure hash algorithm based on the previous algorithms, MD5 and SHA-256 that can be used for secure communication.

REFERENSES

[1] J .Rajalakshmi and V .Valarmathi Assistant Professor, "PREVENTING HUMAN SHOULDER SURFING AND TO PROVIDE RESISTANCEAGAINST PIN ENTRY", International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 0976-1353 Volume 13 Issue 1 –MARCH 2015.

[2] R. Roshdy, M. Fouad, M. Aboul-Dahab , "DESIGN AND IMPLEMENTATION A NEW SECURITY HASH ALGORITHM BASED ON MD5 AND SHA-256 ", International Journal of Engineering Sciences & Emerging Technologies, . ISSN: 2231 – 6604 Volume 6, Issue 1, August 2013

[3] Priyanka Walia ,Vivek Thapar," IMPLEMENTATION OF NEW MODIFIED MD5-512 bit ALGORITHM FOR CRYPTOGRAPHY"',International Journal of Innovative Research in Advanced Engineering (IJIRAE),. ISSN: 2349-2163 Volume 1 , Issue 6,(July 2014)

[4] Akanksha Gat, Neha Bhosale, Harshada Deshmukh, Snehal Gore, Prof. Mrs.Shwetambari Chiwhane,"A NOVEL APPROACH OF CARD PAYMENT TO AVOID SHOULDER SURFING ATTACKS", International Journal of Recent Development in Engineering and Technology, (ISSN 2347 -6435 (Online)) Volume 4, Issue 10,October 2015)

