

# Security Enhancement in Card Payment Systems

Prof. Yashwant Ingle, Ms. Dipali Gawde, Ms. Pranoti Deshmukh, Ms. Dipti Deshmukh  
Department of Computer Engineering, RMDSSOE, Pune 1, 2, 3, 4, 5

**Abstract:** All customers who have used their credit card at an international POS terminal will have to be re-carded with a Chip +PIN credit card. A chip is a small microchip embedded in our payment card. It is encrypted so transactions are more secure on the payment card. The Chip +PIN card is a higher level of security on your card, in line with best global and local practice of security of transactions. This paper starts with an examination of a previous attempt at solving the pin entry method. It had the advantage of being simple to understand and use. Our analysis takes both the theoretical and experimental approaches reveals serious shortcomings of previous method. We suspect a security thread in this process when we enter the pin in front of our friends and family members.

**Keywords:** shoulder attack, PIN, authentication

\*\*\*\*\*

## I. INTRODUCTION

The most widespread user authentication method in use today is obviously the password-based authentication, where the user enters already arranged alphabetical, graphical, and/or numerical password directly through the user interface of the authentication system. However, the password submission process is prone to direct observational attacks, such as shoulder-surfing, and this is a source for the security concerns. The entry of a password can easily be observed by nearby people in crowded places, by vision enhancing and/or recording devices like cameras, 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 flow of card payments are changed in recent months (OCT 2014) and made pin number compulsory to complete transactions.[1]

A chip is a small microchip embedded in your credit card. It is encrypted so transactions are more secure on the card. To complete the transaction we need to provide 4 digit PIN number into that device. We assume the security thread in this process. While providing PIN in front of friends, relative or unknown person, it is affected by the different attacks like "Shoulder attack". This system is applicable for all types of cards (Debit, Credit, etc). This is done to minimize the fraud and misuse of card payments.



Fig.1 Card Payment Machine

## II. SYSTEM ARCHITECTURE

- We have entered PIN in front of merchant or friends to complete transaction where those people can remember our 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.

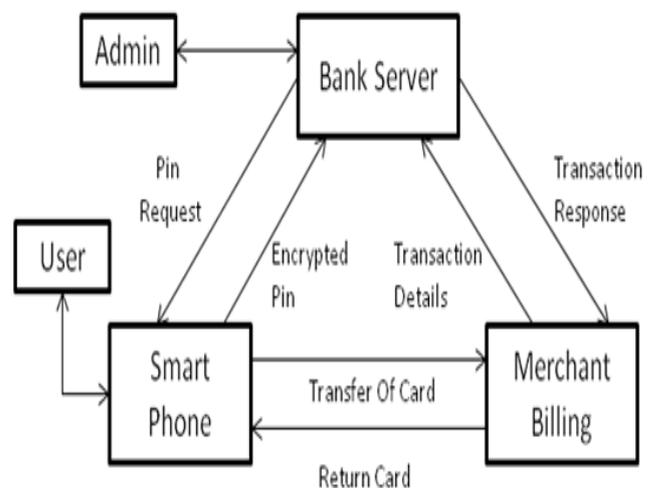


Fig.2 Architecture Of Card Payment

**The proposed Application works as follows:**

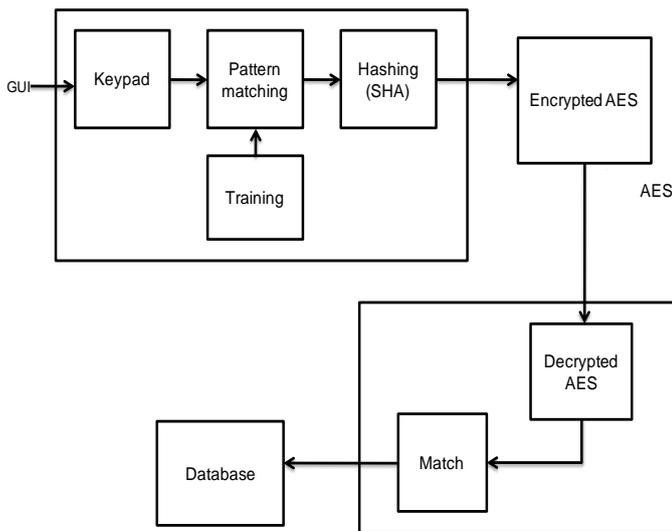


Fig.3 Proposed System

In this section, we review the related works and discuss several issues closely related to our work. In this section we are going to implement actual process of it and work on different standard algorithms which makes our system secure.

- In card payment process GUI (graphical user interface) is user friendly. This is the advantage of our system. User can enter his pin through the keypad. Even user is free to provide number as YES/NO or any pattern which he can change on daily or monthly basis. After user entered his/her pin no on keypad Merchant sends request to bank server through dedicated network.
- So pattern made by user recognize by the pattern matching algorithm which is already trained for such conditions.
- Here after pattern matching in back end bank check the particular user active is not if it is active it will send the all details of user to the merchant.
- Here to secure our payment we are using hashing technique in which 4-digit pin number after shuffling algorithm can be transferred into the hash code of fixed length which represents the original string. In hashing we cannot covert hash code into again original string.
- After conversion of pin into hash code this send to bank server for matching the details of user. Some time bank server is not safe so network spoofing can be happened over the bank network so to avoid the network spoofing we use the encryption standard algorithm AES(advance Encryption standard). It is the symmetric block cipher in which sensitive data of that person get protected. Cipher has one private key which used to encrypt the data.
- Encrypted information again decrypted by using DES algorithm(Data encryption standard) decryption can be done using private key which is used in the encryption.

- After decryption original string which is in hash code get matches using matching function through the database of bank.
- If string get matched transaction will process successfully but for next 30 sec if user not enter his password then transaction will be cancelled automatically.

### III. MERITS AND DMERITS

#### 1. Secure -

This type of technology card payment is secure because it uses the encryption, decryption and main secure hashing technique which is more secure than the previous technology magnetic strip plays important role in card payment system which can be read by card readers.

#### 2. Easy to transport -

Due to its comapctibility we can carry smart cards anywhere in the world it gives the holder freedom to carry large amount of money with him without feeling nervous and depressed about having the money stolen. In case of smart card if card get stolen then we can contact with the helpline to block the services of the card but when cash get stolen we can't get it back and it is impossible to trace the cash.

#### 3. Fraud prevention -

Benefits of card using for the identification by government to prevents the social frauds another advantage for smart card is that some countries use the smart card to identify short term workers who have been given work permit by government this secures the smart card system and frauds related to them. .

#### 4. Slow environment Adoption-

If we used the smart card in store or in hospital, restaurant they don't have the hardware compulsory to use the cards because it is very expensive to use it therefore the stores apply basic chares for using card payment, more than cash.

#### 5. Possible Risk of frauds-

Whenever we use the secure the system there are some drawbacks of that system, card fraud completely cannot be vanished there are some chances of fraud.

### IV. CONCLUSION

A Novel Approach of Card Payment is to avoid Overlooking & Shoulder Surfing Attacks. So when ever 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.

In this paper we show the new approach of card payment. Attacks and frauds can be avoided using this approach. For secure card payment we also focused on different standard algorithms like pattern matching,

shuffling, encryption and decryption techniques and its working principle.

Paper also discussed advantages and disadvantages of it. We mainly stressed the importance of secure transaction in PIN based transaction. Finally this secure card payment implemented using frequently pattern change of PIN which is helped to prevent the card payment frauds.

## V. ACKNOWLEDGEMENT

Behind Every successful work there are some people and it becomes the duty of author to express deep gratitude for the same. We take this opportunity to express my deep sense of gratitude towards my esteemed guide **Prof. Yashwant Ingale** for giving us this splendid opportunity to select an present “Security Enhancement in Card Payment Systems” Project and also gave facilities for successful completion. We thank **Prof. Vina Lomate**, Head of Department of Computer Engineering, for the tentative and supportive behaviour towards student and help them to complete their seminar report, all the staff members, for their support, suggestions and for most valuable time lent as and when required. With all respect and gratitude, I would like to thank all the those people, who have he support me directly or indirectly. We also thank my friends for their help in collecting information without which this Project not have seen the light of the day.

## REFERENCES

- [1] Analysis and advance method of a PIN-Entry Resilient to Shoulder-Surfing and Recording Attacks Taekyoung Kwon, Member, IEEE, and Jin Hong
- [2] Multipurpose Smartcard System Aditya Bodake<sup>1</sup>, Viraj Baviskar<sup>2</sup>, Ashwini Bodake<sup>3</sup>, Shital Bhoite<sup>4</sup> Prof. N. J. Kulkarni<sup>5</sup> 1,2,3,4Students of Dnyanganga College Of Engineering And Research Pune
- [3] SMARTCARD FRAUD DETECTION USING SECURE ONETIME MOBILE PASSWORD Assistant professor, Computer Science & Engineering, SR Engineering College, Warangal, India.