International Journal of Research
ISSN: 2348-6848 Vol-3, Special Issue-6
National Conference on Recent Engineering Trends
NCRET- 2016
Held on 16th March 2016 organized by **Institute of Knowledge College of Engineering, Pune**, **India.**

Securing PIN Entry through User's Own Touchscreen Devices to Prevent Shoulder Surfing Attacks

Jyoti Chikane
jyoti.chikane999@gmail.com
SP's Institute of Knowledge College Of Engineering
Gaikwad Priyanka
priyagaikwad7795@gmail.com
SP's Institute of Knowledge College Of Engineering
Kishor funde
mailmekishor.funde@gmail.com
SP's Institute of Knowledge College Of Engineering
Prof. Ritesh Thakur
hodcomp@iokcoe.ac.in
SP's Institute of Knowledge College Of Engineering, Department of computer Engineering,

Abstract:

A chip is a small microchip embedded in your credit card. It is encrypted so transactions are more secure on the card. The Chip+PIN card is a superior level of security on your card, in line with best global practice of security of transactions. When you use a Chip+PIN credit card at a POS terminal, the POS machine will prompt you for your PIN to be entered, you are required to enter the Credit Card 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 attack". Shoulder attacks is one of the latest weapons used by hackers or adversaries in an organization to hack an account or to authenticate in a secure zone. In a shoulder attack a person is watching the user while he is typing the password and reads his fingers that what he has typed or makes a video of him typing the password and so comes to know that what the password is. We wanted to address this problem. 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.

Keywords: Shoulder Surfing; Authentication; Security; SS7.0; Shoulder Attacker; password entry.

INTRODUCTION:

The flow of Card Payments are changed in recent months (OCT 2014) and made PIN number compulsory to complete the transactions. This is applicable for all types of cards (Debit, Credit, etc).This is done to minimize the fraud/misuse of card payments. 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.

Problem Statement:

- We found a problem when user is typing his/her PIN number.
- He / She has to enter PIN in front of merchant or relatives or any other person.
- This is a type of Overlooking / Shoulder Attack.

Goals and objectives:

- 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.

Statement of scope:

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.

Proposed System:

The merchant inserts your card at a PIN enabled POS terminal. He enters the transaction amount. Then the bank server will notify user on his android mobile phone 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. After entering pin number bank server will do the authentication, check whether user is valid or not and also he has a sufficient balance to pay. After checking bank server will transfer the amount in merchant’s account.

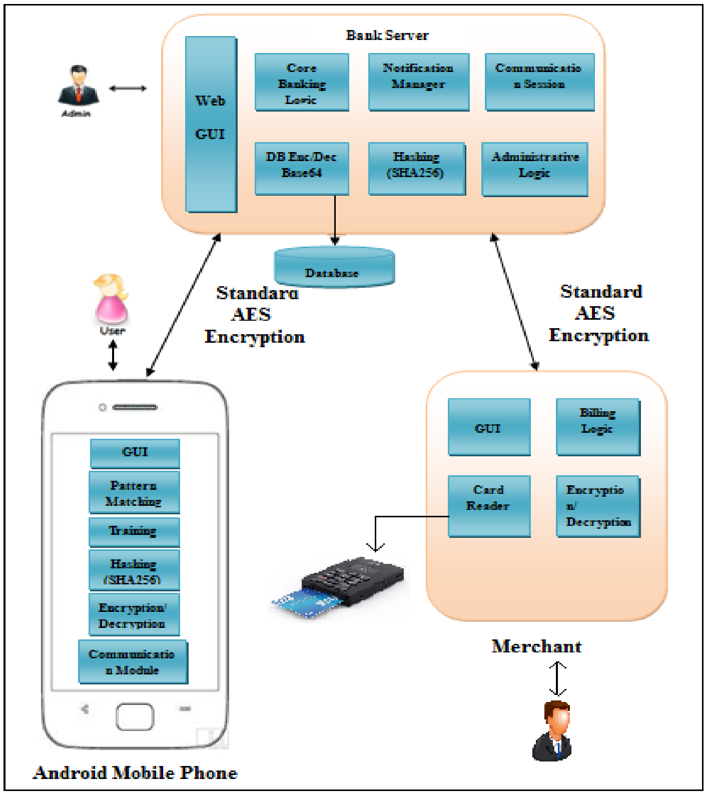

Figure : Architecture diagram

Modules:

Server Module

Bank Server

1. Admin page
2. Welcome page
3. Configuration page

Client Module

Customer

1. Mobile Device
2. Credit Card
3. Mobile Application
4. Login Page

Merchant

Credit Card Machine or Card Reader

Features and scope:

- More Secure
- Easy deployment
- Low cost
- Used in hotels, shopping malls.
- Fast deposit of funds

Name of algorithms:

- **Use of hash function, SHA256, to create hash of password.**

The SHA (Secure Hash Algorithm) is one of a number of cryptographic hash functions. A cryptographic hash is like a signature for a text or a data file. SHA-256 algorithm generates an almost-unique, fixed size 256-bit (32-byte) hash. Hash is a one way function – it cannot be decrypted back.

- **AES algorithm for communication.**

The Advanced Encryption Standard or AES is a symmetric block cipher to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data. This new encryption algorithm would be unclassified and had to be "capable of protecting sensitive government information well into the next century."

Hardware Interfaces:

- Processor – Intel Core2Duo, Pentium –III/i3
- Speed – 2.4 GHz
- RAM - 1 GB (min)
- Hard Disk -50GB
- Android 2.3 enable handset

Software Interfaces:

- Operating System : Windows 7
- Front End : Java 7
- Back End : MySQL 6
- Tomcat 7
- JDK 1.7
- Android SDK
- Eclipse Indigo

Acknowledgement:

We take the opportunity to thank our project guide and Head of the Department Prof. Thakur Ritesh B. for his valuable guidance and for providing all the necessary facilities, which were indispensable in the completion of this project report. We are also thankful to all the staff members of the Department of Computer of Institude of Knowledge College of Engineering, Pune for their valuable time, support, comments, suggestion and persuasion. We would also like to thank the institute for providing the required facilities, Internet access and important books.

Conclusion:

In this paper, we minimize the fraud/misuse of card payments. The main motive behind implementing this project is avoid the shoulder attacks. As per our propose technique bank server will 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. Then user can 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.

References:

[1] Analysis and Improvement of a PIN-Entry Method Resilient to Shoulder-Surfing and Recording Attacks Taekyoung Kwon, Member, IEEE, and Jin Hong- IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY.

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

[3] 2010 IEEE Symposium on Security and Privacy Chip and PIN is BrokenSteven J. Murdoch, Saar Drimer, Ross Anderson, Mike Bond University of Cambridge Computer Laboratory Cambridge, UK http://www.cl.cam.ac.uk/users/{sjm217,sd410,rja14,mkb23}.

[4]ColorPIN – Securing PIN Entry through Indirect Input Alexander De Luca, Katja Hertzschuch, Heinrich Hussmann Media Informatics Group, University of Munich, Amalienstr. 17, 80333 Munich, Germany {alexander.de.luca, heinrich.hussmann} @ifi.lmu.de,hertzschuch@cip.ifi.lmu.de.

[5] IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 1, Ver. II (Jan – Feb. 2015), PP 58-65 www.iosrjournals.org DOI:10.9790/0661-17125865 www.iosrjournals.org 58 | Page Moving ATM Applications to Smartphones with a Secured PinEntry Methods Kavitha V 1, Dr. G. Umarani Srikanth 21,2,(Department of PG studies, S.A. Engineering College, India).

[6] Hindawi Publishing Corporation Scientific World Journal Volume 2014, Article ID 838623,12 pages http://dx.doi.org/10.1155/2014/838623 Research Article Preventing Shoulder-Surfing Attack with the Concept of Concealing the Password Objects' Information.