International Journal of Latest Trends in Engineering and Technology
Vol.(13)Issue(2), pp.070-072
DOI: http://dx.doi.org/10.21172/1.132.13
e-ISSN:2278-621X

SHUFFLING KEYPAD FOR SMART PAYMENT TRANSFER

Prakash M.Mainkar[1], Vaidehi Prabhune[2]

Abstract—Password plays vital role in the authentication process by providing information and computer security. We use common authentication method such as Personal Identification Number (PIN) in various devices ATM's, mobile devices and electronic door locks. This PIN entry method is not safe. When user enters their PIN in popular place, attacker observes the PIN over their shoulder. This is called shoulder surfing attack (SSA). In this project we will propose a method to prevent this SSA attack. Whenever we need to enter PIN code, we will be using our mobile phone to type that pin code.
Keywords—PIN-authentication, Shoulder-surfing.

1. INTRODUCTION

Today in the banking system has got wide popularization. It provides 24 hours service for customer. In this technology, ATM (Automated Teller Machine) card is the important part of our life. To have transaction ATM pin no is necessary and it must be secured. The existing banking system has got very high popularity with 24 hours service. Use of ATM is helpful for money transaction. The flow of card payments are changed in recent months 2014 and made PIN number compulsory to complete the transactions. Passwords are necessary but, still they are not considered much safe to provide the security to the users because of many flaws in the conventional password systems. The major aim for using passwords is to restrict unauthorized user to access the system [7]. A large number of attacks on many systems are related to the password. This type of attack most probably occurs in the case of cash credit cards. While entering the password in mall or any shops the surrounding people may predict our password accidently or purposely. To avoid this and make the transaction safer this system gives more security to the ATM/Debit /Credit cards. The entry of a password can be easily 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 [9].

The personal identification no PIN, typically consisting of four decimal digits, is especially susceptible to observational attacks, due to its short length and simplicity of the ten-digit keypad [3]. The whole secret PIN could be leaked through even a single authentication session. Since PIN's are so popularly used in variety of common devices, such as smart phones, ATM's 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 to deal with this situation, but achieving both security and usability still remains a challenging goal.

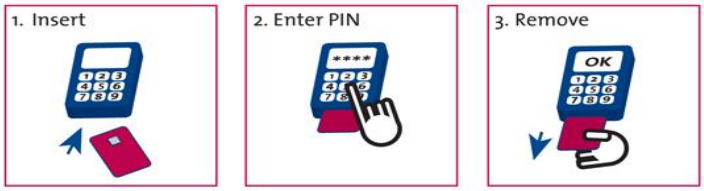
2. METHODOLOGY

Current Methodology

The current Scenario of transaction includes following steps:

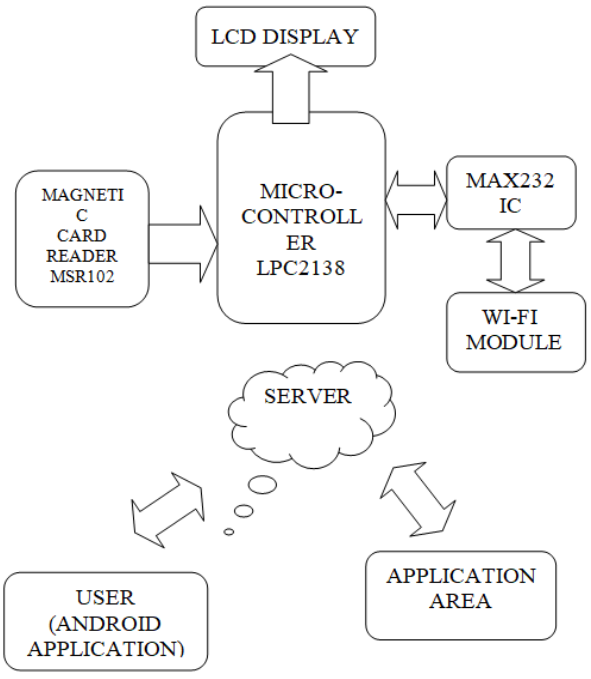
Step1: The merchant inserts your card at a PIN enabled POS terminal.
Step2: He enters the transaction amount.
Step3: The machine prompts for a PIN to be entered by you.
Step4: You enter your credit card ATM PIN in the machine
Step5: On entering the correct PIN the transaction is confirmed and completed.
Step6: For terminals without PIN authentication support, your new chip +PIN credit card shall continue to support the regular signature mode.

[1] MIT-WPU Pune,India
[2] Electronics And Telecommunication MIT, Kothrud, Pune, India



Card payment System includes following things:
1. User/Customer-They are the people who desires to purchase the goods using credit card.
2. Authorization Service-
Validate the credit card payments to ensures that the card number is valid and the card has not expired.
Deposit processing to apply the deposit payment to the card.
Prepare credit card transaction reports that show authorization codes, amounts, and error/success messages.

3. SYSTEM ARCHITECTURE



.

4. WORKING

The system designed is based on the microcontroller LPC2138.Magnetic card reader reads inserted card data and send it to the Android phone where server is designed via Wi-Fi module interfaced in the porposed system..At the same time the user connect to the server via Wi-Fi connectivity.At the server side,verification of card number is done and after successful verification,the authentication signal will be sent to the registered mobile number of the user .Here android application in the user's phone will be pop upped at the user side to enter the pin number on the mobile.When user enter pin number that will be send to the server.Here we are providing a different keypad or we can say shuffling keypad format through the Android Application designed for our system implemention,so no one is able to correctly predict the password what we are typing on keypad. At the server side when pin number is checked and is then only transaction will be taken place for that application.

5. ALGORITHM

Input: PIN Notification
Output: Payment Transaction
Let 'm' be the merchant ,'u' be the user ,'a' be the amount,
'c' be the card number &'p' be the pattern set by user.

STEPS:
Merchant will login into system and initiate a payment transaction of amount 'a' for card no 'c'.
Data will get encrypted and send to the bank server.
Bank server will search user's session to send him notification.

User gets 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.

Following are some algorithm which we use in our system:
1. 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 occurs.
- 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.Base 64
- Is a group of similar binaries–to-text encoding schemes that represent binary data in an ASCII string format.
- By translating it into 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 64place-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 use this algorithm to encrypt user's password which is saved present in server database.

3. 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.

6. FUTURE SCOPE

The input method of PIN can be made stronger using NFC technologies.

7. REFERNCES

[1] Alexander De Luca, Roman Weiss, Heinrich Hussmann, 2007."Pass Shape - Stroke based ShapePasswords"OZCHI '07.
[2] Lev Ginzburg, Rockaway, "User Authentication System and Method", NJ(US), 2006.
[3] V. Roth, K. Richter, and R. Freidinger, "A PIN-entry method resilient against shoulder surfing". In CCS `04: Proceedings of the 11th ACM conference on computer and communication securiety, pages 236-245, New York.
[4] Athanasios Papadopoulos, Student Member , IEEE, Toan Nguyen, Student Member, IEEE, Emre Durmus, Student Member, IEEE and Nasir Memon, IEEE,2017." IllusionPIN: Shoulder-Surfing Resistant Authentication Using Hybrid Images"
[5] Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh and Chia-Yun Cheng,2016,"A Shoulder Surfing Resistant Graphical Authentication System",China.
[6] R.J.Bolton and D.J.Hand, "Unsupervised profiling methods for fraud detection",Department of Mathematics Imperial College London {r.bolton,d.j.hand} @ ic.ac.uk.
[7] Tackyoung Kwon and Jin Hong, Member, IEEE,"Analysis and Improvement of a PIN-Entry Method Resilient to Shoulder Surfing and Recording Attacks ", 2014.
[8] G.T.wilfong, "Method and Apparatus for Securied PIN Entry", U.S Patent 5940511 , August 17, 1999.
[9] Lee, Mun-Kyu, "security notions and advanced method for human shoulder –surfing resistant PIN entry", Information Forensicks and Security, IEEE Transaction on 9.4(2014) : 695-708.
[10] Q.Yan, J.Han, Y.Li, J.Zhou, and R.H.Deng, "desinging leakage resilient password entry on touchscreen mobile devices, " in Proc.ASIA CCS, 2013, pp.37.48.