Asian Journal of Convergence in Technology Volume IV, Issue I
Issn No.:2350-1146, I.F-5.11

Securing Card Transaction Against Shoulder Surfing Attack

Dr. M.P. Dale[1], Shruti R. Gogawale[2] , Twinkle S. Deore[3]
mpdale@mescoepune.org, shrutigogawale@gmail.com, deore03sonu@gmail.com

[1](Professor,E&TC Department, MESCOE, Pune)
[2,3](Students,E&TC Department, MESCOE, Pune)

***Abstract*— In this paper author presents an approach to minimize shoulder surfing attack (SSA). Information available and security of computers are supported mostly by passwords which play the important role in verification process. The (PIN) Personal Identification Number is common certification method used in various devices like ATM's, Bank Lockers, secure door lock system and mobile devices. This method of entering pin is the main cause for shoulder surfing attack (SSA). When pin number is entered in public places, culprit observe the pin number over their shoulder. This is called shoulder surfing attack (SSA). In this project we will propose a system to prevent this SSA attack. A shoulder attack is one of the modern way used by hackers or opponent to steal the account information or to authenticate in a private region. In a shoulder attack a person is being observed by a culprit and he observes his activities that what numbers he has entered or makes a video of total transaction process and comes to know that what the password is so whenever user need to put PIN code, user will be using the mobile phone to type that pin code, using shuffling keypad prototype designed on user's Android phone.**

Keywords- SSA, PIN, ATM, prototype.

I. INTRODUCTION

Passwords are really the important part of our daily life in various system applications like online services, ATM machines, websites login, authentication in mobiles etc. The main objective for using passwords is to avoid uncertified clients to access the system. Passwords are very important but, their security can't be considered much safe for users because of more flaws in the traditional password systems. Large number of cases happens because most of the systems are based on passwords. 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.

As the number of risks are increasing day by day, certain measures should be taken to prevent ATM thefts. For this reason, certain measures are taken which are divided into 3 types, that is implementation of alarms and sensors, video supervision, and remote tracking.

1.1 **Video Supervision**- Video supervision is the constructive process implemented to detect fraud attempts at the ATMs and create awareness. It is implemented by installing Closed Circuit Television Camera(CCTV) near the ATM. Nowadays cameras are so easy to integrate in ATMs. By installing extra site cameras more security can be given to the area. For this method, the cameras must track the area continuously. But continuous supervision is a complex issue of security in many states around the world.

1.2 **Alarms and sensors**- Sensors are installed inside the ATM cabin to sense if any uncommon activity is happening, and alarms are there to alert people present over there. This type of process is mainly used to monitor different parameters which shows & records the act of robbery.

1.3 **Remote Tracking-** By using this method, the central association can manage the functionalities of ATM machine from remote location. It provides automated means to monitor our ATM network. It is useful in delivering important information regarding to the state of machine. By making development in the remote monitoring system, the current status of machine can be send to central location in terms of messages. This is the location where this status information can be acted upon.

II LITERATURE SURVEY

Paper [1] which we have referred represents Study of Fraud Analysis & securing card present transaction, it is given that when user swipe their card at shopping centers and food corners or use it at ATM to withdraw cash or pay shopping bills, users are under continuous risks of cards being stolen. Besides if they lose their card, someone can misuse it. absence of appropriate security and verification procedures in card transactions nowadays has led to millions of dollars losses, So the flaws in present card transaction system can be overcome

by making development in the present system for better security and customer satisfaction.

According to paper [2] the latest survey made by authors there are some other problems like attackers can watch directly or use some recording techniques to achieve user's private information. This problem can be overcome by using Pass Matrix, based on graphical passwords to prevent shoulder surfing attack, with login indicator, vertical and horizontal blocks covering the entire image so that no one can predict the password using camera methods or by just simply observing over user's shoulder.

According to paper [3] in current system, security improvement for magnetic data transaction in online payment and medical system is major issue, the personal data on card's magnetic stripe is not encrypted and hence transaction frauds occur so measures are taken to enhance the security of magnetic stripe data transaction.

In Paper [4] they have implemented a system for securing ATM cards by using virtual shuffling keypad and wireless password communication for proving secure login authentication technique.

III METHODOLOGY

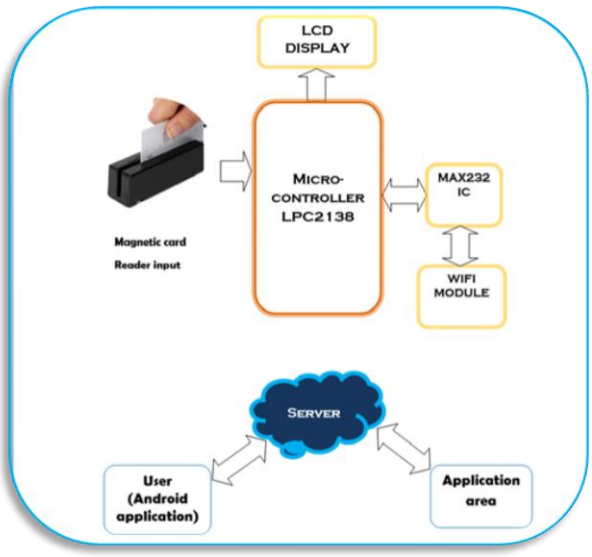

Fig. 1. Overview of the Proposed System

The system designed is based on the Microcontroller LPC 2138. Magnetic card reader reads the inserted card data and send it to the Android phone server where server is designed via Wi-Fi module interfaced in the proposed 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 at server side. 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 implementation, so no one is able to correctly predict the password what user is typing in keypad. At the server side when pin number is checked and is verified and then only transaction will be taken place for that application.

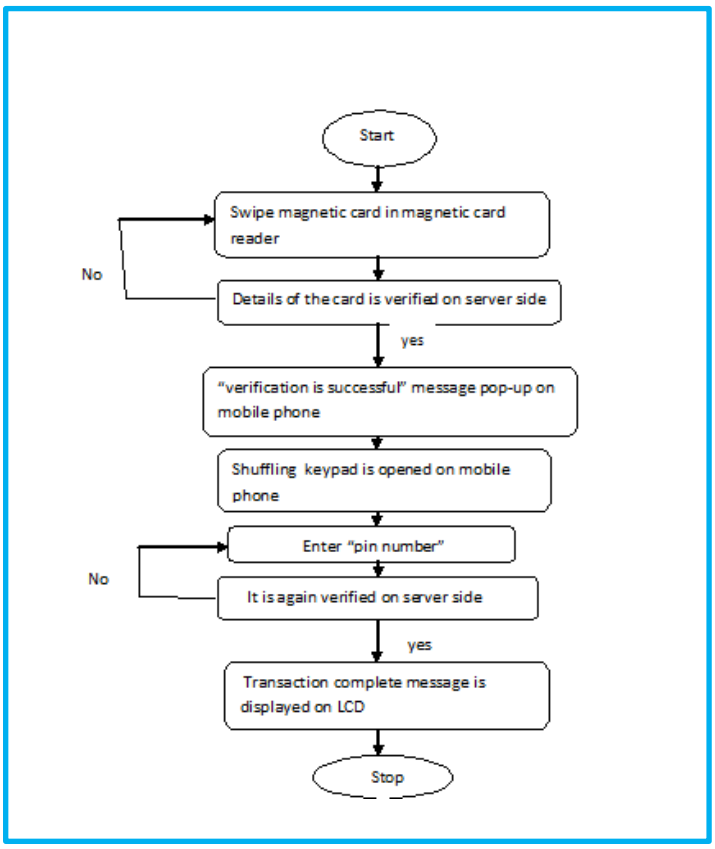

Fig. 2. Flow Chart of Proposed System

The working of proposed system is explained in the flowchart shown in fig.2

3.1 Magnetic Card Reader

Fig.3 Magnetic Card Reader for card swipe

MSR102 magnetic card reader reads the data present on the card when the user swipes the card. Recording capacity of this card reader is 79 characters, it operates at 5V DC and power consumption is 65mA.

3.2 WIFI-MODULE

Fig.4 Wi-Fi Module for wireless connection

ESP8266 is a serial WIFI trans receiver module to connect any small microcontroller platform wirelessly to internet. ESP8266 has powerful on-chip processing and storage abilities which allow it to be integrated with different devices through its GPIOs. WIFI trans receiver module is addressable over SPI and UART. User can connect any microcontroller to this module and can send data wirelessly.

3.3 SHUFFLING KEYPAD

In recent world customers are using keypads at different places and their finger movements can put them at risk because of password stealing which is happening around the world. For this problem the proposed system is designed using Shuffling Keypad on Android Phone. So that nearby people would not be able to detect the passwords. Use of this Shuffling keypad will confuse the offender and they could not predict the password which is providing more security to the users. Every time when user tries to enter password, key arrangement will change on the keypad.

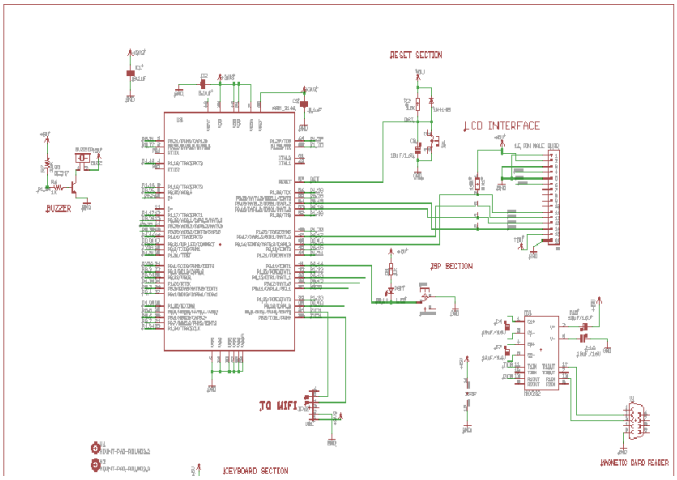

Fig.5 Circuit Diagram

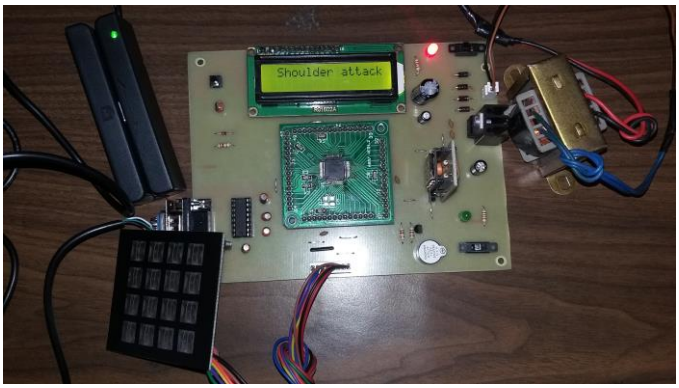

Fig.6 Hardware Implementation of Proposed System

IV CONCLUSION

The main focus of the proposed system is to give more security to PIN entering process for common user. It gives authentication with high utility, precise output and cost effectiveness (no additional hardware). In this system, the shoulder surfing attack is prevented and a more secure transaction between the Android App and server is established.

V REFERENCES

1) Hung-Min Sun,Shiuan-Tung Chen , Jyh-Haw Yeh and Chia-Yun Cheng, "A Shoulder Surfing Resistant Authentication System", November 10,2009.
2) Lakshmisha Honnegowda, Syin Chan, and Chiew Tong Lau," Security enhancement for Magnetic Data Transaction in Electronic Payment and Healthcare Systems", IACSIT International Journal of Engineering and Technology, April 2,2013.
3) Mohammad Asim, Jamal Mohommad Aqib, Khaja Moizuddin Mohammed, "The Study of Fraud Analysis & Security Card Present Transactions" , International Journal of Engineering Research and Development, June 9, 2012.
4) Prof. S.S.Punde Takle Nikhil Thakare Samadhan "Virtual Shuffling Keypad and Wireless Password Transfer for Secure ATM Transaction", IOSR,Journal of Electronics and Communication Engineering,