IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 08, Issue 3 (March. 2018), ||V2|| PP 17-24

Haptic Based PIN Securing Embedded System

Miruthubashini.S[1], Mohammed Ashiq.A[2],Paul Stephen.V[3],Saranya.U[4],Dr.Vetrichelvi.G[5]
[1,2,3,4]B.E-Project Student, Jansons Institute of Technology,Coimbatore, Tamil Nadu, India
[5]Professor,Jansons Institute of Technology,Coimbatore, Tamil Nadu, India
Corresponding author: Miruthubashini.S[1]

Abstract: *Money transaction systems such as ATMs and POS work based on verification of highly confidential PIN numbers.This traditional security system is vulnerable to shoulder surfing and theft. In this paper, a new security system to overcome this vulnerability is proposed. The proposed embedded system works by verifying the inputof OTPin accordance with Haptic vibration generated in the system. This embedded system secures the original PIN from shoulder surfing and saves the payment cards from being used illegally.*

Keywords: *Embedded system, Haptic Vibration, OTP, PIN security, POS*

Date of Submission: 23-02-2018 Date of acceptance: 06-03-2018

I. INTRODUCTION

Money transaction systems such as POS (Point of sale) machines are widely used today. A POS (point of sale terminal) also called as credit card terminal is a device which accepts the payment cards to make electronic money transfers.These systems retrieve user data from bank servers and use it to verify the swiped payment card and authentication PIN number given by the user during transaction.The procedures of directly entering the PIN numbers in these machines have vulnerability of exposure to the potential attackers.This vulnerability is prevalent during transaction at supermarkets and miniature ATMs installed in public spaces.When the PIN is entered, the four digit number would be hidden in display but the keypad or touch screen interface on which the PIN is entered would still be visible to the nearby strangers in public spaces.This is a major problem when it comes to heavily populated public places.

In this proposed work, the vulnerability of the PIN exposure is shown to be overcome by using localized haptic technology. This embedded system is an advanced POS with improved security than traditional POS machines. When the card holder swipes their card for money transaction, this system would run the algorithm required to verify the validity of the swiped card.This procedure is same as traditional systems except that it initializes the Haptic vibration necessary for the OTP. The haptic vibration is randomly generated each time a valid card is swiped.

After swiping the card the system would prompt the user to enter OTP. The user adds the generated number of vibration to the PIN number to arrive at a One Time Password (OTP). This OTP is entered and the system shall retrieve the real PIN number associated with the card. The system performs the algorithm to subtract the haptic vibration number with the OTP and compare the results with the real PIN number. When the PIN is found to be correct the system gives commands to money transaction unit to proceed with the transaction. This prevents the nearby strangers to know the real PIN number due to the localized haptic vibration felt only when the palm is placed on the system by the user.

The proposed system prevents the potential attackers from using the money transaction machines for stealing the money. The system ensures the PIN security from shoulder surfing and eliminates the vulnerability to visibility. This proposed system makes sure the nearby strangers do not know the real PIN which would be known only to the user.

II. RELATED EXISTING WORK

Previously many technical researches have been carried out attempting to improve the security of the money transaction machines. They are discussed below:

In paper [1], a research which implements an illusion PIN (IPIN) for touch screen systems is published. The virtual keypad of IPIN is composed of two keypads with different digit orderings blended in a single hybrid image. The user who is close to screen is able to see and use one keypad and a potential attacker who is looking at a screen from a large distance is able to see only the fake keypad.But hybrid keypad does not secure the PIN because it doesn’t prevent the Shoulder peeking by people standing next to the user in a queue or standing close to the machine. In paper [2] & [4], a research which proposes that authentication could be carried out by drawing the characters on the touch screen of the system have been proposed. And it works, in two modes learning mode and recognition mode. In learning mode user will be able to make the system to learn the templates of any character or number by writing on a touch screen .In recognition mode the system will automatically identify the character or number drawn on the touch screen. The drawback of this technology is that nearby strangers could understand the pattern in real. In paper [3], a system to enhance the security of the user card is proposed. The proposal is that finger print recognition could be used along with pin based authentication since Biometric features are unique for every individual and hence can be widely used for enhancing the security system. But the main drawback of this robust system is when the user has any injury to their fingers then the system would fail to recognize the user due to mismatched fingerprint. Our system doesn't use biometric system to avoid this potential difficulty.

In paper[5], a system of brain wave based authentication which is another addition to the wide range of authentication systems has been implemented, which has many advantages over other authentication systems. Differently abled persons can't use systems which use fingerprints or retina scans but they can use system using brain-waves. This clears that using brain waves as biometric to provide authentication is very beneficial. Though the system is beneficial, the brain signal attention is calibrated to give value from 0 to 100. Also, eye blink will be counted only if the strength of eye blink signal is greater than 35. The main drawback is that the Brain wave system is complicated to implement in public places.In paper [6] two image based authentication techniques: Pair Based and Text Based Image Authentication schemes are implemented. The authentication technique consists of three phases: registration, login and verification. In the registration phase, user has to create his password. During login phase, user enters his password. In the final phase, the password entered is verified and the user is authenticated. In PIA technique, the strength of the password depends upon the user selected images and the way user paired them. If the user selects well known pairs of characters, it is easy to crack the PIN number.

Although the above discussed works have improved the security of transaction machines they have not effectively eliminated shoulder surfing attacks. The work proposed in this paper overcomes the vulnerability of shoulder surfing.

III. PROPOSED SYSTEM

The system proposed here proves to overcome the vulnerabilities in previous systems. The proposed model comprises of hardware and software components. The hardware component includes a powerful microcontroller and I/O devices such as Display and Keypad.

The payment card is first swiped in the card reader so that it is read by the controller. The system works by first verifying whether the swiped card is valid or not. If the card is found to be valid, the controller makes the Haptic vibrator to generate vibrations. The vibrations are generated with random count. It is felt when the palm is placed on the vibrating device connected to the system. The number of vibrations is counted by the user. Then the number is added to the original PIN number associated with the payment card. This gives a new 4 digit number which acts as One Time Password (OTP).

The OTP is entered into the system and the controller processes the OTP in an arithmetic algorithm. The vibration number would be subtracted from the entered OTP number. This algorithm gives the real PIN number to the system. The system would have already obtained the real PIN number via the server at the moment the card is found to be valid. The PIN number resulting in subtraction is compared with the real PIN number obtained from the servers. If the PIN is found to be matching the system proceeds with passing commands to the machine to take control of the transaction. If the entered OTP is wrong either due to mistaken count of the vibration or due to not knowing the real PIN in case of illegal usage the system blocks the card temporarily. If the card itself is found to be invalid then the system prompts to swipe the valid card.

IV. DESIGN OF THE SYSTEM

4.1 Hardware:

The hardware component of the system is described in the following block representation. The whole components can be divided into six main functional units.

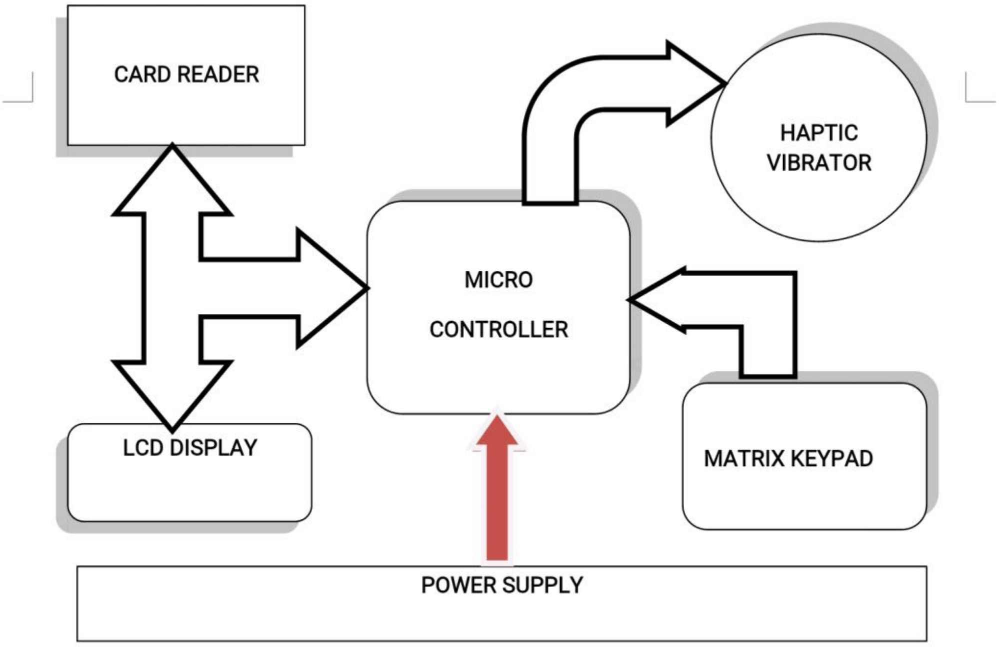

Fig 1. FUNCTIONAL BLOCK DIAGRAM

4.1.1 Card Reader:

This unit reads account information that is stored on a magnetic strip of the payment card. The magnetic strip is printed in credit/debit cards and it holds the user's account details. The data retrieved by the card reader is passed on to the implemented microcontroller, which compares the read data with the user accounts' information obtained from bank servers. Card reader is able to read magnetic strips effectively. It is connected with the microcontroller so that it sends its read data to it for comparison with the user information.

4.1.2 LCD Display:

The Display unit helps to display the prompt messages to the user. This proposed work demonstrates the system with the implementation of 16x2 Liquid Crystal Display. Any other compatible displays can also be used instead of LCD. This varies in accordance with the type of money transaction machine where the system is embedded. The display prompts the user with the message "Swipe the Card" before the card is swiped and after swiping the card ,display gives the prompt message "Vibration Generated" in case the swiped card is found to be valid. In case the card is found to be invalid the display gives the message "Invalid card". Finally the display is programmed to give "Transaction Complete" in case the supposed OTP is entered correctly.

4.1.3 Arduino Due Controller:

Arduino Due is a microcontroller used widely in embedded systems. This controller is programmed accordingly and output is taken as per the proposed model. The controller would be programmed with embedded C and interfaced with the servers so that the user information could be obtained from them. When the card is valid with correct OTP Password the controller sends commands to proceed further with money transaction. In case of wrong password the controller temporarily blocks the access of the account to prevent any unauthorized usage.

4.1.4 Keypad 4x4:

4x4 Keypad with 16 keys is used for input of the OTP password. The rows and Columns of the keypad is precisely connected to the controller. The keypad is used to initialize the system to read the card. After completion of successful transaction the '*' key is used to terminate the whole process.

4.1.5 Haptic Vibrator:

An eccentric rotating mass vibration motor (ERM) is a small unbalanced mass on a DC motor. It is used as Haptic vibrator. When it rotates it creates a force that translates to vibrations. They are also the most versatile - they can be mounted on PCBs, encapsulated, use a variety of power connections, and even be based on brushless motors. Hence this miniature motor technology is chosen for the proposed system.

4.1.6 Power Supply:

A separate power supply is given to the embedded system. The supply is fixed in accordance with the type of controller used.

4.2 Software:

The Integrated Development Environment (IDE) used is ARDUINO, to program the Arduino Due Microcontroller. Embedded C is very powerful language which could be used to program a wide range of Embedded systems. Embedded C is used here to arrive at the required algorithm for verification of the swiped card and proceeding with the PIN number verification. The following Flow chart elaborates on the algorithm being used.When the Card is swiped the algorithm checks whether the card is valid or not by reading the card.When the condition is true, random vibrations is generated. Theentered OTP is subtracted from the generated number to check whether the PIN added to the vibration count is correct or not. If the condition is true, the algorithm proceeds further by passing commands to allow money transaction. If the condition is false, the algorithm assumes the PIN to be invalid and would notproceed the transaction.

TABLE 1.SAMPLE CASES OF PIN AND RANDOM VIBRATION

Sl.No	**Original PIN**	**Random Vibration**	**Obtained OTP**
1	1234	4	**1238**
2	1234	8	**1242**
3	1467	3	**1470**

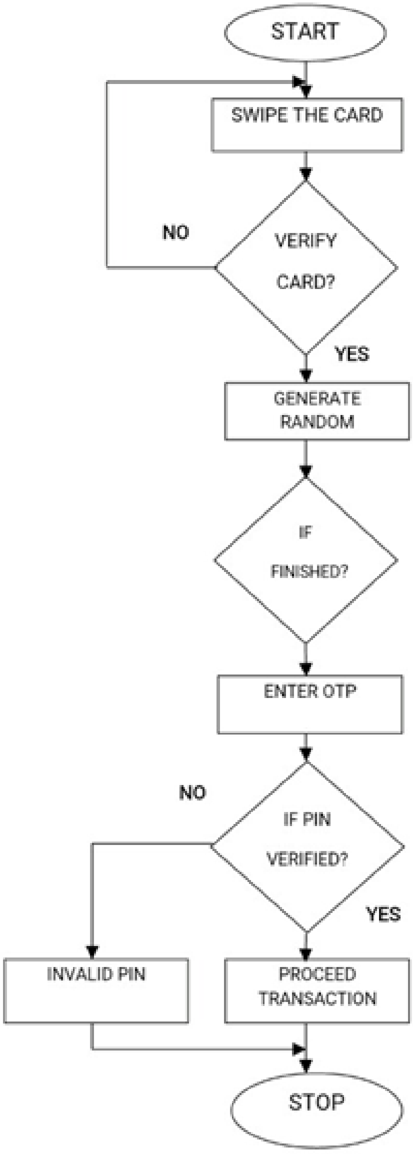

Fig 2. FLOW CHART OF IMPLEMENTED ALGORITHM.

V. RESULTS

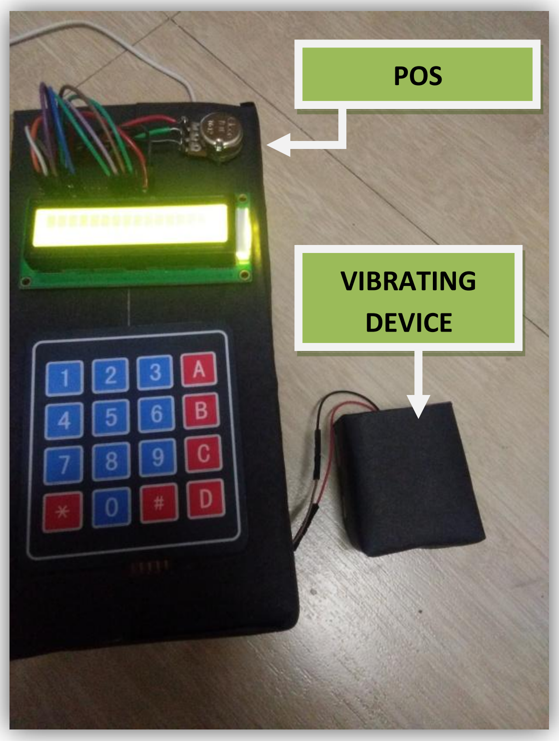

Fig 3. IMPLEMENTED WORKING POS SYSTEM.

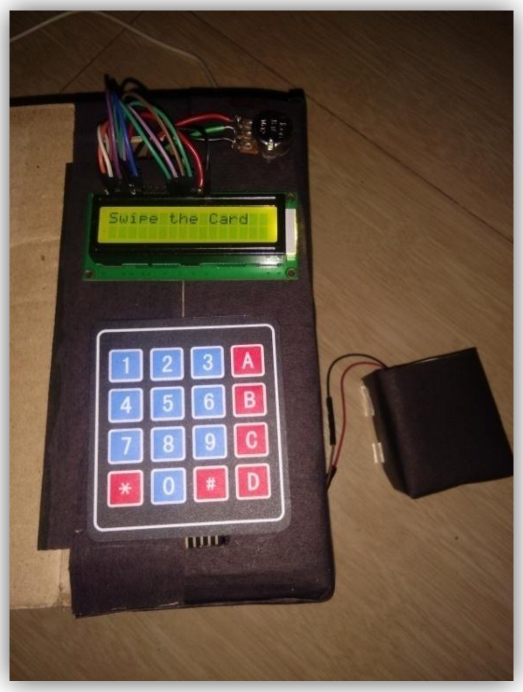

Fig 4. LCD DISPLAY PROMPT MESSAGE “SWIPE THE CARD”.

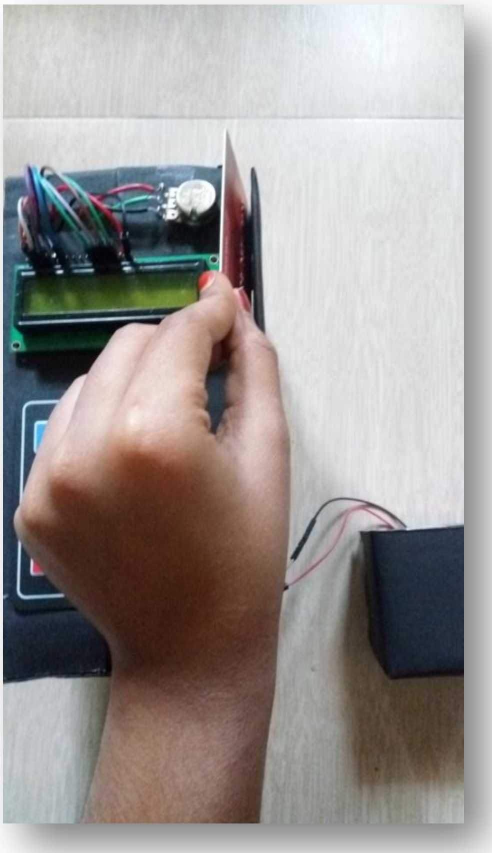

Fig 5.SWIPING THE PAYMENT CARD (DEBIT/CREDIT CARDS**)**

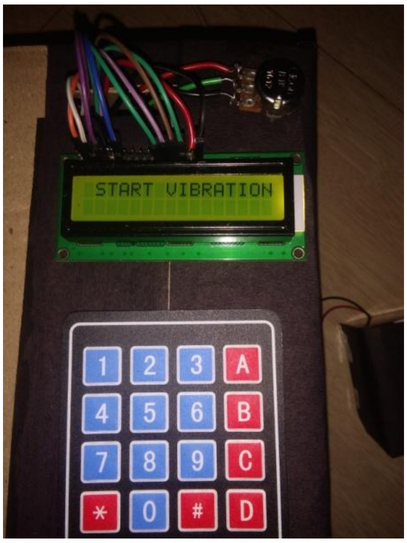

Fig 6. “START VIBRATION” Alert

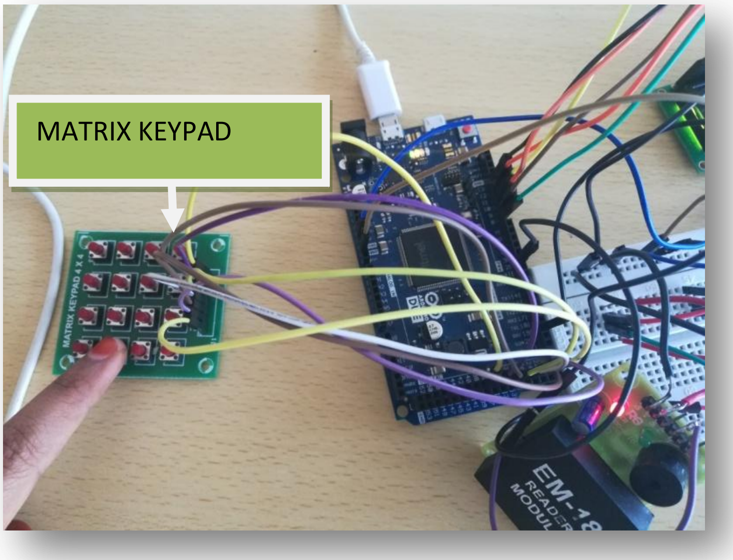

Fig 7. ENTERING THE OTP (SYSTEM WITHOUT ANY ENCLOSING)

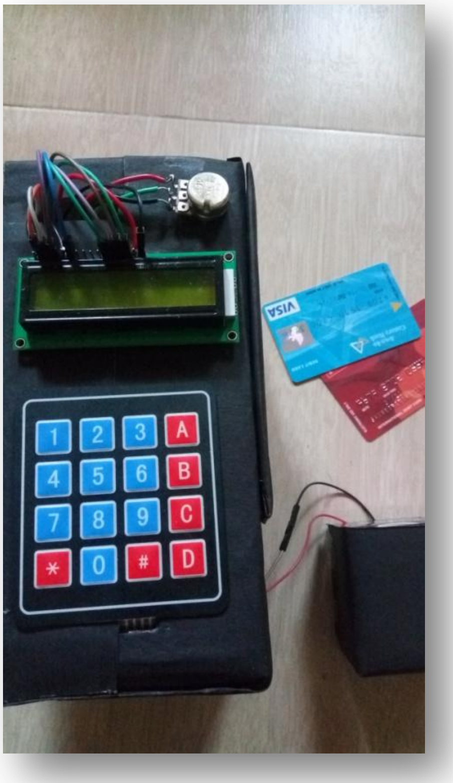

Fig 8.ENCLOSED IMPLEMENTED POS.

VI. CONCLUSION AND POSSIBLE EXTENSIONS IN FUTURE

Thus a high security POS system which prevents the illegal use of payment cards such as Credit/Debit cards has been proposed. The threat of shoulder surfing as well as card theft could be reduced to great extent when this new security system is implemented. This new system is highly secured up to the point that the authorized card holders could safely use the card in open places such as supermarkets without any fear of shoulder surfing and card theft.

This system also has potential to be upgraded and interfaced with other systems in Future. Security of Multi-Platform personal devices such as smart phones could possibly be improved with our proposed system.

REFERENCES

[1]. Athanasios Papadopoulos, EmreDurmus, Illusion PIN: shoulder surfing resistant authentication using hybrid images, IEEE Transactions on Information Forensic and Security, Volume: 12, Issue: 12, Dec 2017

[2]. SiddheshashokVaidya, Prof.VarshaBhosale, Invisible touch screen based PIN authentication to prevent shoulder surfing, Issue, IEEE Transactions on Information Forensic and Security, Issue: 19, Jan 2017

[3]. PriyaTawde, Dr.G. PrasannaLakshmi, Enhancing Micro-ATMs and POS terminals authentication system using advanced biometric techniques, IOSR Journal of computer engineering (IOSR-JCE), Volume 19, issue 4, ver.I JUL-AUG2017.

[4]. Toan Van Nguyen, Napa Sae-Bae, NasirMemon ,Finger Drawn PIN Authentication on Touch Devices, New York University Polytechnic School of Engineering, New York, USA.

[5]. Yashraj S. and Prof Dr.V.V. Shete Biometric user authentication using brain waves, Inventive Computers and Technologies, Volume: 3, 26 Aug 2016.

[6]. KrishanTuli&GurpreetKaur, ATM safety & security, International Journal of Advanced Research in IT and Engineering , Vol 2,Issue 2, February 2013.

[7]. N.Selvaraj&G.Sekar, A method to improve the security level of ATM banking systems using AES algorithm ,International journal of computer applications(0975-8887)volume 3-no.6.,june 2010.

[8]. Zharkova&Ipson, Valentina& Stan, Survey of Image Processing Techniques, EGSO-5-D1_F03- 20021029, 3, 2003.

[9]. Renjith, Arya S& Jasmine Yesudasan, ATM Security Using Virtual Password,International Journal of Advanced Research in Computer and Communication Engineering, Vol. 5, Issue 2, February 2016.

[10]. M Sreelatha, M Shashi, M Roopteja, M Rajasekar and K Sasank, Intrusion Prevention by Image Based Authentication Techniques, IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011 MIT, Anna University, Chennai. June 3-5, 2011.

Miruthubashini.S1" Haptic Based PIN Securing Embedded System "IOSR Journal of Engineering (IOSRJEN), vol. 08, no. 3, 2018, pp. 17-24.