SECURITY NOTIONS SHOULDER-SURFING RESISTANT PIN-ENTRY BY USIG PIC CONTROLLER AND BASE PIN ,BASE TEXT

T.Manikandan[1] | P.Devika[2] | M.Gayathri[3] | V.Mallika[4]
[1](Department of ECE,Assistant Professor,Jay Shriram Group of Institutions, Avinashipalayam, Tirupur-638 660)
[2](Department of ECE,Jay Shriram Group of Institutions, Avinashipalayam,Tirupur-638 660)
[3](Department of ECE,Jay Shriram Group of Institutions, Avinashipalayam,Tirupur-638 660, gayathree5566@gmail.com)
[4](Department of ECE,Jay Shriram Group of Institutions, Avinashipalayam,Tirupur-638 660)

Abstract—*The main objective of this system is to develop a secure ATM in future. In general all the keypad based authentication system having several possibilities of password guessing by means of shoulder movements. Shoulder-surfing is an attack on password authentication that has traditionally been hard to defeat. This problem has come up with a new solution by following two methods of proposal idea one is designing shuffled automated teller machine keypad which displays the shuffled texts in the display which confuses person who standing near you to guess the password. Another one is to develop the GSM application between the user and Automated Teller Machine counter for communicating a password via the wireless medium. If someone tries to input the old password got by shoulder-surfing a message containing the location of ATM and time will be sent to nearest station and the ATM shutter will be closed.*

INTRODUCTION

In ATM Machine Was Commonly Used an Electronic Device. Now a days using 4 Digit Password for withdrawing money from ATM machine. This method easy to handle shoulder surfing attack. Those drawbacks are overcome by this project.to reducing surfing attack by using extra alphabets words. Another one is to develop the GSM application between the user and Automated Teller Machine counter for communicating a password via the wireless medium. If someone tries to input the old password got by shoulder-surfing a message containing the location of ATM and time will be sent to nearest station and the ATM shutter will be closed, basically here using 5 digit password for secured money transfer in ATM machine.each and every time using different password based on permanent password

RELATED WORKS:

In my projects based on those related paper.in Mun-kyu lee[1]. was developed security system in ATM money transfer. Basically here using black and white concept this project easy to implement. Those are handle by user .because here each digits are pressed 4 times by user with different black and white combination. Example in my pass word is 1221 then first we got '1' digit then to watch 1 is which color combination that is white then to press then next color will be change, after changing color then to press next combination. This will be rotating 4 times for each digit. Then to pressed 4 digit based on that above rotation. After finishing 4 digit with a each caring 4 press then our password will be pressed .this system used by Mun-kyu Lee. Alexander De Luca, Katja Hertz schuch, Heinrich Hussmann[2] wes developed secured system using red ,white, black combination.here using alphabets based on color combination buttons. Alain Forget, Sonia Chiasson, & Robert Biddle[3] proposed Eye-Gaze Entry in Cued-Recall Graphical Passwords for a user friendly method using only by human eye those are 4 digit sensor model. Amir Tayyebi Moghaddam[4] user has to verify the PIN entry cognitively, other malevolent observer also can capture the sequence of confirmation process. Amir Tayyebi Moghaddam[5] thi system provide story alignment user has to verify the PIN entry cognitively, other insufferable observer also can capture the sequence of authentication
process .those are our remaining(existing) systems

COMPONENT USE:

Power supply

The ac voltage of 220V rms is connected to a step down transformer, then the ac voltage is converted into required dc voltage by this transformer. The dc voltage is given to the rectifier circuit it provides a full-wave rectified voltage that is initially filtered by a simple capacitor filter to produce a dc voltage. This resulting dc voltage has some ac component. A regulator is used to remove the undesired ac component and also remains the same dc value even if the input dc voltage varies.

Microcontroller :

Microcontrollers are high performance RISC CPU. The Operating speed of the micro controller is DC - 20 MHz

clock input, DC - 200 ns instruction cycle andit have a memory size Up to 8K x 14 words of FLASH Program Memory, Up to 368 x 8 bytes of Data Memory (RAM), Up to 256 x 8 bytes of EEPROM Data Memory. Direct, indirect and relative addressing modes are possible. Power-on Reset (POR), Power-up Timer (PWRT) and Oscillator Start-up Timer (OST) are available modes.

Description of DC Motor:

An electric motor converts electrical energy into mechanical energy. It is based on the principle of Fleming's left hand rule. The Fleming's left hand rule tells, when a current-carrying conductor is placed in a magnetic field, it experiences a magnetic force in the left hand direction.When a motor is switch on the torque is developed .This will cause mechanical rotation. DC motors are like a generators such as shunt wound or series wound or compound wound motors.

GSM:

The GSM standard has offer benefits to both consumers (who benefit from the ability to roam and switch carriers without switching phones) and also to network operators (who can choose equipment from any of the many vendors implementing GSM). GSM also gives a low-cost (to the network carrier) alternative to voice calls, the Short message service (SMS, also called "text messaging"), which is now supported on other mobile standards as well. Another advantage is that the standard includes one worldwide Emergency telephone number 112. This facilitate international travelers to connect to emergency services without knowing the local emergency number.

RELAY DRIVER

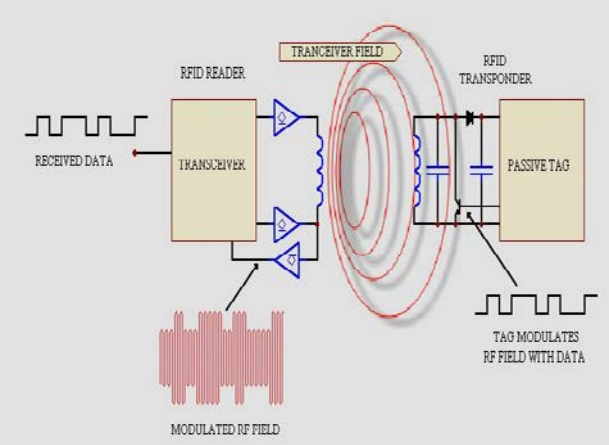
A Relay is a electromagnetic switching device which has three pins. They are Common, Normally close (NC) and normally Open (NO).

The relay driver have four relays as relay1, relay2, relay3, relay4. The pair of switching transistors control the position of these relays (ON and OFF). The common pin of two relay is connected to positive and negative terminal of motor through snubbed circuit respectively. The relays are connected in the collector terminal of the transistors T2 and T4.When high pulse signal is given to either base of the T1 or T3 transistors, the transistor is conducting and shorts the collector and emitter terminal and zero signals is given to base of the T2 or T4 transistor. So the relay is turned OFF state.

When low pulse is given to either base of transistor T1 or T3 transistor, the transistor is turned OFF. Now 12v is given to base of T2 or T4 transistor so the transistor is conducting and relay is turn ON. The NO and NC pins of two relays are interconnected so only one relay can be operated at a time. The series combination of resistor and capacitor is called as snubbed circuit

RFID:

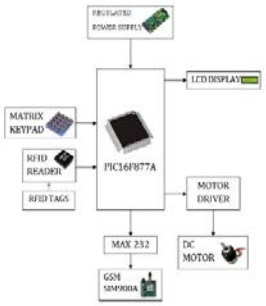
RFID stands for Radio Frequency Identification. In RFID system, there are two parts such as Reader, and one or more Transponders, also known as Tags. RFID systems evolved from barcode labels for automatically identify and track products and people.



Transceiver diagram of RFID

PROPOSED METHOD ARCHITECTURE:

A base letter and pin method is used to prevent shoulder surfing attacks, this way there is no requirement for extra hardware and is easy to implement on the existing framework



In my permanent password :3241
Display Words :pink ,bound, hall, apple, cat
To select : **[apple-5 letters]**
then to add 5 with my password (in each 4 digit number)

3 2 4 1 +
5 5 5 5
8 9 7 6

this is our new password

Those calculations are mind calculation. now our real password is 8796but a permanent password is 3241…those are our new proposed concept to prevent shoulder surfing attack for secured money transfer by using ATM

CONCULSION:

In this electronic systems are proposed in our projects provide meaningful description. this system easy to implement and also very much security proved to money transfer in ATM and also this systems used to prevents shoulder surfing attack and use as user friendly. This was possible by effectively

increasing the memory required this system easy to implemented and also used for door , home money locker in future requirement's by using PIC controller. Three sponsors were neutral .

REFERENCES

[1]C. S. Kim and M.-K. Lee, "Secure and user friendly PIN entry method,"
in Proc. 28th Int. Conf. Consum. Electron., 2010, p. 5.1–1.
[2] V. Roth, K. Richter, and R. Freidinger, "A PIN-entry method resilient against shoulder surfing," in Proc. CCS, 2004, pp. 236–245.
[3] G. T. Wilfong, "Method and apparatus for secure PIN entry," U.S. Patent
5 940 511, May 30, 1997.
[4] M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd, "Reducing shoulder-surfing by using gaze-based password entry," in Proc. SOUPS, 2007, pp. 13–19.
[5] J. Thorpe, P. van Oorschot, and A. Somayaji, "Pass-thoughts: Authenticating with our minds," in Proc. NSPW, 2005, pp. 45–56.
708 IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 4, APRIL 2015
[6] A. D. Luca, K. Hertzschuch, and H. Hussmann, "ColorPIN: Securing PIN entry through indirect input," in Proc. CHI, 2010, pp. 1103–1106.
[7] F. Tari, A. A. Ozok, and S. H. Holden, "A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords," in Proc. SOUPS, 2006, pp. 56–66.
[8] A. Bianchi, I. Oakley, V. Kostakos, and D.-S. Kwon, "The phone lock: Audio and haptic shoulder-surfing resistant PIN entry methods for mobile devices," in Proc. TEI, 2011, pp. 197–200.
[9] A. Bianchi, I. Oakley, and D.-S. Kwon, "Counting clicks and beeps: Exploring numerosity based haptic and audio PIN entry," Interact. Comput., vol. 24, no. 5, pp. 409–422, 2012.
[10] M. G. Kuhn. (1997). Probability Theory for Pickpockets, ee-PIN Guessing [Online]. Available: http://www.cl.cam.ac.uk/~mgk25/
[11] D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in Proc. 13th Conf. USENIX Security Symp., 2004, pp. 151–164.
[12] J. Bonneau, S. Preibusch, and R. Anderson, "A birthday present every
eleven wallets? The security of customer-chosen banking PINs," in Financial Cryptography (LNCS), New York, NY, USA: Springer-Verlag, 2012, pp. 25–40.
[13] Q. Yan, J. Han, Y. Li, and R. H. Deng, "On limitations of designing leakage-resilient password systems: Attacks, principles and usability," in Proc. NDSS, 2012, pp. 50–58.
[14] R. Kuber and W. Yu, "Tactile vs graphical authentication," in EuroHaptics (LNCS). New York, NY, USA: Springer-Verlag, 2010, pp. 314–319.
[15] H. Sasamoto, N. Christin, and E. Hayashi, "Undercover: Authentication
usable in front of prying eyes," in Proc. CHI, 2008, pp. 183–192.
[16] A. D. Luca, E. von Zezschwitz, and H. Hußmann, "Vibrapass: Secure authentication based on shared lies," in Proc. CHI, 2009, pp. 913–916.
[17] A. Bianchi, I. Oakley, J. K. Lee, and D.-S. Kwon, "The haptic wheel: Design & evaluation of a tactile password system," in Proc. CHI, 2010, pp. 3625–3630.
[18] A. Bianchi, I. Oakley, and D.-S. Kwon, "The secure haptic keypad: A tactile password system," in Proc. CHI, 2010, pp. 1089–1092.
[19] A. Bianchi, I. Oakley, and D.-S. Kwon, "Spinlock: A single-cue haptic
and audio PIN input technique for authentication," in HAID (LNCS). New York, NY, USA: Springer-Verlag, 2011, pp. 81–90.
[20] A. Bianchi, I. Oakley, and D.-S. Kwon, "Open sesame: Design guidelines for invisible passwords," IEEE Comput., vol. 45, no. 4, pp. 58–65,
Apr. 2012.
[21] M. Bell and V. Lovich, "Apparatus and methods for enforcement of policies upon a wireless device," U.S. Patent 8 254 902, Aug. 12, 2012.
[22] (2013). Photographing Sound of Mobile Phone Camera [Online]. Available:
http://www.tta.or.kr/data/ttas_view.jsp?rn=1&pk_num=TTAK.KO-06.0063/R1
[23] G. A. Alvarez and P. Cavanagh, "The capacity of visual short-term memory is set both by visual information load and by number of objects," Psychol. Sci., vol. 15, no. 2, pp. 106–111, 2004.
[24] G. A. Miller, "The magical number seven, plus or minus two: Some limits on our capacity for processing information," Psychol. Rev., vol. 63, no. 2, pp. 81–97, 1956.
[25] T. Kwon, S. Shin, and S. Na, "Covert attentional shoulder surfing: Human adversaries are more powerful than expected," IEEE Trans. Syst., Man, Cybern., Syst., pp. 1–12, to be published.
[26] T. Perkovi´c, M. Cagalj, ˇ and N. Raki´c, "SSSL: Shoulder surfing safe
login," in Proc. Int. Conf. Softw., Telecommun. Comput. Netw., 2009, pp. 270–275.
[27] A. De Luca, E. von Zezschwitz, N. D. H. Nguyen, M.-E. Maurer, E. Rubegni, M. P. Scipioni, et al., "Back-of-device authentication on smartphones," in Proc. CHI, 2013, pp. 2389–2398.
[28] Q. Yan, J. Han, Y. Li, J. Zhou, and R. H. Deng, "Designing leakageresilient password entry on touchscreen mobile devices," in Proc. ASIACCS, 2013, pp. 37–48.
[29] K. Kobara and H. Imai, "Limiting the visible space visual secret sharing
schemes and their application to human identification," in ASIACRYPT (LNCS), 1996, pp. 185–195.
[30] A. D. Luca, E. von Zezschwitz, L. Pichler, and H. Hussmann, "Using fake cursors to secure on-screen password entry," in Proc. CHI, 2013, pp. 2399–2402.
[31] D. S. Tan, P. Keyani, and M. Czerwinski, "Spy-resistant keyboard: More
secure password entry on public touch screen displays," in Proc. 17th Austral. Conf. Comput. Human Interaction OZCHI, 2005, pp. 1–10.
[32] R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords:
Learning from the first twelve years," ACM Comput. Surveys, vol. 44, no. 4, article 19, pp. 1–41, 2012.
[33] W. Moncur and G. Leplâtre, "Pictures at the ATM: Exploring the usability of multiple graphical passwords," in Proc. CHI, 2007, pp. 887–894.
[34] D. Weinshall, "Cognitive authentication schemes safe against spyware
(short paper)," in Proc. IEEE Symp. Security Privacy, May 2006, pp. 295–300.
[35] S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," in Proc. AVI, 2006, pp. 177–184.
[36] H. Zhao and X. Li, "S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme," in Proc. AINA Workshops, 2007, pp. 467–472.
[37] P. Golle and D. Wagner, "Cryptanalysis of a cognitive authentication scheme (extended abstract)," in Proc. IEEE Symp. Security Privacy, May 2007, pp. 66–70.
[38] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge
attacks on smartphone touch screens," in Proc. 4th USENIX Conf. Offensive Technol. WOOT, 2010, article 1–7, pp. 1–10.
[39] E. von Zezschwitz, A. Koslow, A. D. Luca, and H. Hussmann, "Making
graphic-based authentication secure against smudge attacks," in Proc. IUI, 2013, pp. 277–286.
[40] (2013). iPhone 5s: About Touch ID Security [Online]. Available: http://support.apple.com/kb/HT5949
[41] (2013). iPhone 5S Fingerprint Sensor Hacked by Germany's Chaos Computer Club [Online]. Available: http://www.theguardian.com/technology/2013/sep/22/apple-iphone-fingerprint-scanner-hacked
[42] T. Kwon and S. Shin. (2011) HAM: A Study of Human Adversary Modeling via Predictive Human Performance Modeling Tools [Online]. Available: http://islab.yonsei.ac.kr/index.php?mid=publication
[43] D. Amitay. (2011). Most Common iPhone Passcodes [Online]. Available: http://danielamitay.com/blog/2011/6/13/most-commoniphone-passcodes