PIN ENTRY METHOD FOR RESISTANT SHOLDER-SURFING ATTACKS USING STEGANOPIN

Bedare Thulja Bhavani Bai[1], Dr. D. Vishnu Vardhan[2]
[1] M.tech in Embedded Systems, JNTUA College Of Engineering, Ananthapuramu
[2] Assistant Professor, Department of ECE, JNTUA College Of Engineering, Ananthapuramu.

Abstract: ***In the modern world everyone using the ATM'S (automated teller machines), digital door locking systems, debit card terminals and point of sales terminals (POS). PIN security is compromised in public places easily. User normally uses same PIN for multiple applications. The Direct PIN entries are highly affected to shoulder-surfing attacks can effectively capture user's PIN entry number by concealed cameras. Indirect PIN entry method proposed to achieve usability and security. Here, SteganoPIN is indirect practical PIN entry method. The human-machine interface between two numerical keypads, a user can generate a one-time PIN can safely enter by the plain view of attackers. The user basic interface of SteganoPIN is standard keypad with regular layout and other is a small separate keypad is challenge keypad with random key layout. The challenging keypad is vary according to the IR based Proximity Sensor. To derive fresh OTP a user must use this challenging keypad. The user first locates PIN in random key layout and subsequently maps the key locations into the standard keypad for OTP derivation. For each attempt of PIN, capture the user's picture using camera and send it to the registered authorized person's mail that person can recognize the user who are trying to attempt their account.***

Index Terms: Authentication, Human-machine interaction, Personalized identification number (PIN), One time PIN (OTP),Shoulder-Surfing.

1. INTRODUCTION

A. Personalized identification(PIN) number Security problems

Personal identification numbers (PINs) are constructed and memorized numerical passwords typically for user authentication login and different unlocking purposes widely. Their application usage is increases because of modern technology can convenient facilitate implementation of PIN entry interfacing on a various machines and devices, including ATMs, point-of-sale terminals (POS), debit card terminals on banking services, digital door-locks, smartphones, and tablet computers.

When the users are entering their PIN (personalized identification number) unfortunately, in such systems security is compromised particularly in the public places like ATMs, digital door locks, debit card terminals, and point of sales (POS) terminals. This will be happens by the nearby peoples by shoulder-surfing observations and by the concealed cameras.

Moreover, attacker who have already observed and riding shoulder-surfing attacks and collected multiple PIN, candidates can attempt to act as user. Observation from remote places is also done because of arranging high-resolution cameras are placed in application areas. Now the attackers are increasingly uses the camera-base shoulder-surfing attacks for PIN user interface.

B. Related work: Improve security to the entry measures of personalized identification number(PIN)

To handle these nontechnical attacks, for providing more security to PIN incorporating entry indirect key method to separate the visible and entry parts of secret attackers. In earlier research on password authentication various methods are introduced as BinaryPIN, is each round of entering of every key system colors randomly the half of numbers in black and the half of numbers in white so user enter the color for PIN key entering separate colored key multiple times all PIN digits were entered. ColorPIN uses set colored random challenge characters assign to numeric keypad. In every instant, three different colored characters are assigning to every key in numeric keypad with different colors. Users enter the secret colored character key of a PIN. Secret PIN is combination of color-digit. This PIN entering system is longer authentication time and difficult to remembering password.

Others also have the physical protections of visual channels studies various authentication methods to secure numeric PIN and graphical password entry with multiple techniques. Mainly this paper was based on this authentication techniques are sheildPIN, in this user puts the hand in the Γ-shape to cover the keypad and another hand used for the entering of the PIN. CoverPad, in this it will presume a gesture detection mechanism on touchscreen mobile devices. The hand covered shape and its gesture were inspired. To enter single digit in a PIN user should first access with the challenging keypad. Based on the operation of the challenging keypad the indirect key that should be entered, our method follows these approaches.

2. STEGANOPIN SYSTEM

To addressing the camera base shoulder-surfing attacks user should familiar with standardPIN entry methods over the multiple session authentication. Here, it presents novelPIN method commonly known as SteganoPIN method.

The SteganoPIN system builds on concept of the sheildPIN and CoverPad authentications. In those concepts the challenging keypad will appears under the covering of hand and it will disappears after removing it. It provides the security from the direct shoulder-surfing attacking.

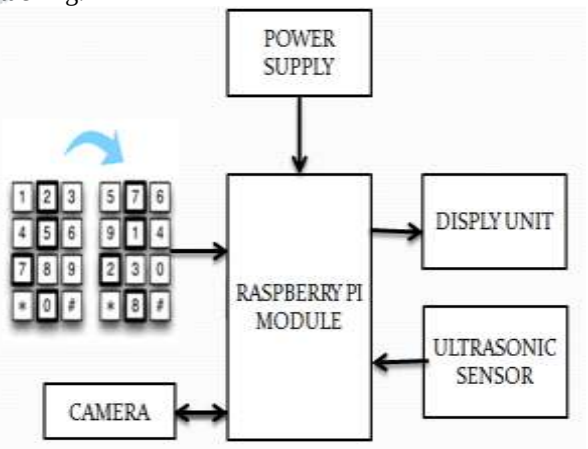

Fig1: System block representation of inter facing of two faced human-machine and Hardware components with the processor

A Usability

This concept provides the strong security, camera base shoulder-surfing attacks must resilient over multiple session authentication. With scope of challenging keypad uses the regular

numeric keypad for key entry. It provides less possibility of active guessing from attackers without any random guessing.

B Two faced Human-Machine interaction protection

The meaning of stegano is concealed or protected, in Greek. When numeric key entered by the user in plain view of attackers must be one time PIN (OTP) that can be conceal real PIN by the derivation of following. For such derivation processes incorporate with two-faced keypad interaction. To develop such systems of process against to the attackers, incorporate with human-machine interface protection method.

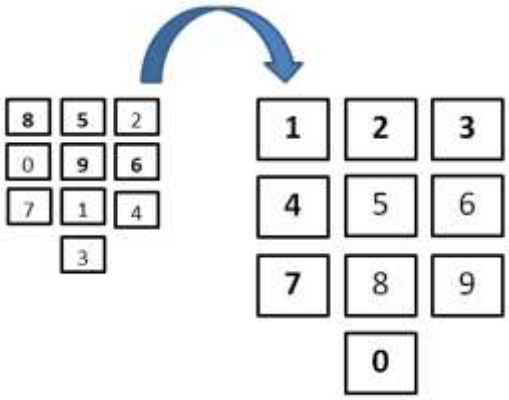

Fig2: Two-faced keypad system

In this SteganoPIN system standard keypad in regular key layout is a one numeric keypad, and another with random layout, this random key layout keypad is known as challenging keypad as in Fig2. This challenging keypad must use by user for deriving one time PIN (OTP). User first locates a PIN in random layout, simultaneously maps the PIN keys in standard keypad and relocates the location in to the regular keypad to deriving of OTP named as response keypad. Same process repeated until completion of PIN entering process. System refresh the random challenging keypad, due to mapping randomly between two keypads, system verifies the user PIN to the entered one time PIN (OTP).

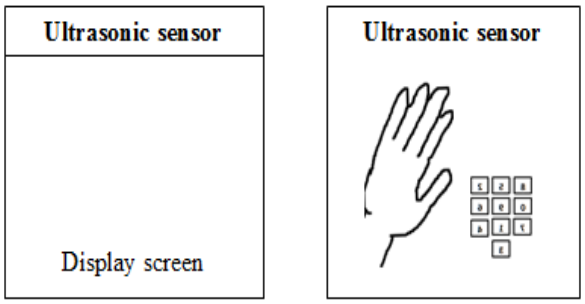

Fig3: Human-computer interactive protection

In general user interfacing with SteganoPIN, challenging keypad doesn't appear immediately only responding keypad appears with regular layout. The SteganoPIN system was displayed besides the IR based Proximity sensor arrangement, because of sensor will detect the person hand presents and it will display challenging keypad on the screen of under user covered hand. Using this system the user and machine system can interactive procedure it protect PIN from attackers. Challenging keypad is less in size with possible distance of user.

3. SYSTEM STRUCTURE

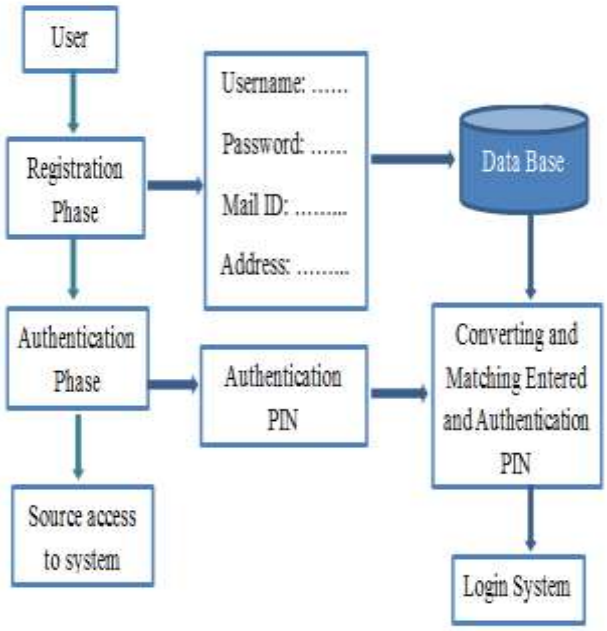

Fig4: Over all background structure of proposed system

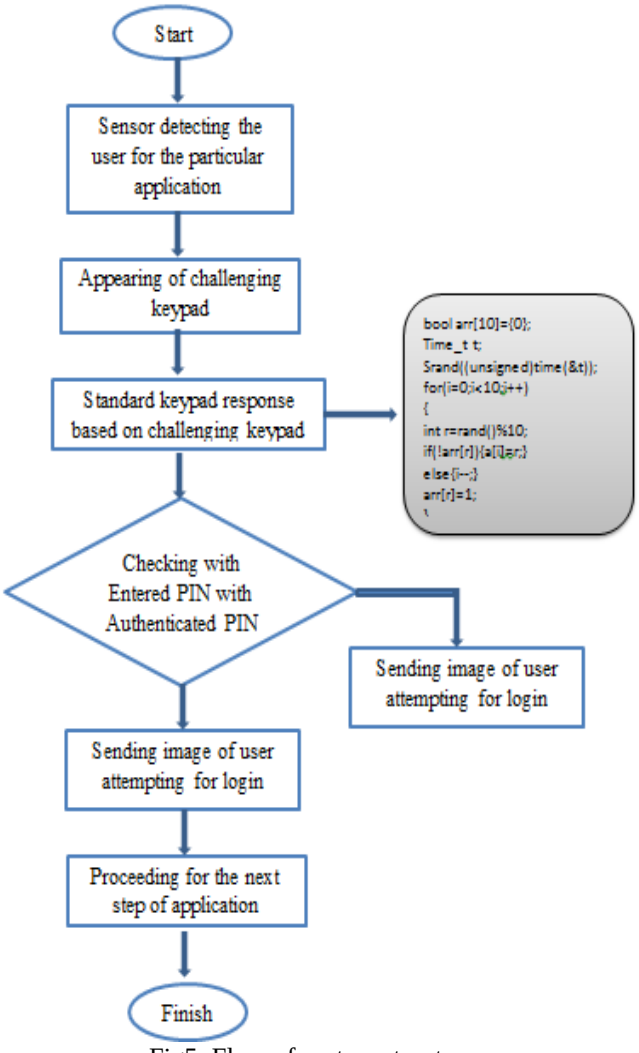

Fig5: Flow of system structure

4. SYSTEM HARDWARE

System hardware components are ARM1176JZF-S Processor, Ultrasonic sensor, Display unit, and UVC driver camera.

ARM1176JZF-S

ARM is a 32-bit RISC processor, architecture developed by the ARM Corporation. ARM is a combination unique of features, it makes ARM processor most popular in todays embedded architecture. Compared to other general-purpose processors, ARM core is very simple they can be less number of transistors comparatively. Typical ARM chip have more number of peripheral controllers, Digital signal processor (DSP), and on-chip memory with ARM core. Pipeline and ARM ISA designs are aimed for less energy consumption in embedded systems.

The Raspberry Pi board is a family of ARM11,700 MHz processor, it has a Broadcom controller BCM2835 system on a chip (SoC), with memory of ROM 1GB and RAM 512MB GPU Video Core IV, and was shipped originally with 256 megabytes RAM, upgraded to 512 MB. It doesn't include solid-state drive or built-in hard disk, but SD card used for booting and storage purpose. It supports for 8-stage pipeline architecture.

IR based Proximity sensor

The IR based Proximity sensor used to determine the nearby objects. This sensor uses Infrared radiation which is invisible.

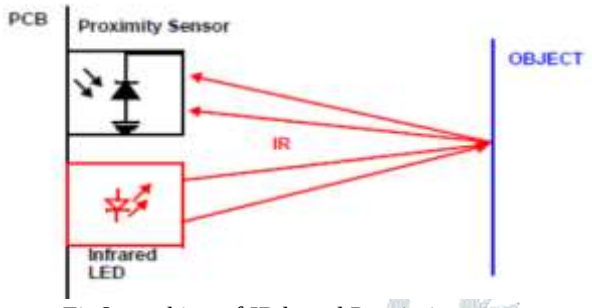

Fig6: working of IR based Proximity sensor

LED emits IR radiation that bounces off on nearby object surface. An IR receiver detects the reflected ray which is placed next to the emitter. Based on the distance and obstacles sensor intensity of light falling on the receiver varies.

Display unit

High Definition Televisions and LCD monitors are connected by using full-size male HDMI cable, and inexpensive adaptor of DVI. HDMI 1.3 and 1.4 are supporting versions and a version 1.4cables is recommended most. The RaspberryPi outputs of video and audio can supports HDMI, but it doesn't support for HDMI input.

UVC driver camera

A UVC (Universal Video Class) driver is a USB-category driver. This driver can enables a device like webcam, for communicating with computer's operating system. USB is common type of connection which allows high-speed data transfer. UVC driver enables the webcam to plug and play. Webcam with a UVC driver doesn't need additional software to work. Most current operating systems support UVC and relatively new format.

5. IMPLEMENTATION AND RESULTS

The current system application initially user registration and process of authentication with user details and PIN completes shown in Fig4. The user details and authentication of PIN is stored in to the current system application database, user when enters PIN the current system checks with the authentication PIN.

Present application of SteganoPIN system of process against of attack as follows.

Step1: when user ready to present for attempting the PIN, the sensor will detect the nearby object of user hand and system displays random layout challenging keypad.

Fig7: ARM board with interfacing of sensor UVC driver camera and display unit

Step2: Random layout can generates automatically for the every user with different random layouts. The different random layouts generates by the internal software process in Fig5.

Step3: After displaying of random layout user sequent maps the PIN keys relocates into the regular layout regular keypad in Fig2.

Step4: Repeat same process until the completion ofPIN entering. And system will compare PIN number with authentication PIN number from current supporting database shown in fig4.

Fig8: Output of the current protocol in raspberrypi

Step5: After completing of PIN entering, proposed system can sends the image of user who are trying to enter PIN in current application system by using UVC driver camera.

Fig8: Sending of picture to the Authorized mail

6. CONCLUSION

This system has been designed for the providing security to the personalized identity number, with the multiple PIN authentication sessions. Particularly with the challenging keypad, random layout generates the standard keypad response. And sending the every approach of PIN attempt to user authorized mail. It has beging developed by integrating features of the hardware components and software used.

7. REFERENCES

[1] Taekyoung Kwon and Sarang Na, "SteganoPIN: Two-Faced Human–Machine Interface for Practical Enforcement of PIN Entry Security," 2015 IEEE.

[2] V.Roth, K. Richter, and R. Freidinger, "A PIN-entry method resilient against shoulder surfing," in *Proc. ACM Computer.Commun. Security*, 2004, pp. 236–245.

[3] A. De Luca, M. Langheinrich, and H. Hussmann, "Towards understanding ATM security—A field study of real world ATM use,"in *Proc. ACM Symp.Usable Privacy Security*, 2010, pp. 1–10.

[4] A. De Luca, E. von Zezschwitz, and H. Hussmann, "Vibrapass – secure authentication based on shared lies," in *Proc. ACM CHI Conf. Human Factors Comput. Syst.*, 2009, pp. 913–916.

[5] D. Kim, P. Dunphy, P. Briggs, J. Hook, J. W. Nicholson, J. Nicholson, and P. Olivier, "Multi-touch authentication on tabletops," in *Proc. ACM SIGCHI Conf. Human Factors Comput. Syst.*, 2010, pp. 1093–1102.

[6] Q.Yan, J. Han,Y. Li, J.Zhou, and R.H.Deng, "Designing leakage-resilient password entry on touchscreen mobile devices," in *Proc. 8th ACMSIGSAC Symp. Inform.Comput.Commun. Security*, 2013, pp. 37–48.

[7] T. Kwon and S. Na, "SwitchPIN: Securing smartphone PIN entry with switchable keypads," in *Proc. IEEE Int. Conf. Consumer Electron.*, 2014,pp. 27–28.

[8] N. Cowan, "The magical number 4 in short-term memory: A reconsideration of mental storage capacity," *Behavioral Brain Sci.*, vol. 24,no. 1, pp. 87–114, 2001.