International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 3 | Mar -2017 www.irjet.net p-ISSN: 2395-0072

Color Code PIN Authentication System Using Multi-TouchTechnology

K. Abinaya[1], T. Pavithra[2], P. Divya[3], S.Hema malini[4]

Mrs. S. Hema malini, Associate Professor, Dept. of Computer Science & Engineering, Panimalar Institute of Technology, Chennai, Tamilnadu, India

---

ABSTRACT: *Users typically use direct PIN entry method for multiple system in numerous session. Direct PIN entries are highly susceptible to shoulder surfing attacks as attackers can effectively observe PIN entry with concealed cameras and they can use it illegally. Indirect PIN entry method proposed as countermeasures to this issues. To achieve this BW method is used with MULTI-TOUCH technique. Random four colors are used for indirect PIN entry method and attackers find it difficult due to the probability of finding PIN is very complex. In addition to colors, pattern are also used like dotted, diagonal strips to help visually challenged persons. This establish a secure transaction between the mobile app and server with improved BW method. This method prevents the transaction from a well-trained perceptual grouper to crack the PIN digit entered by the user in a conventional way.*

KEY WORDS- PIN, color, attackers, server, transaction, shoulder-surfing.

1. INTRODUCTION

A. PIN ENTRY SECURITY PROBLEMS

Personal identification numbers (PIN), typically constructed and memorized, is widely used as numerical passwords for user authentication or various unlocking purposes.

Unexpectedly, when the user enters the PIN directly in public places it may lead to shoulder-surfing attack. The people nearby may or can observe the PIN entry with or without concealed cameras. The camera-based shoulder-surfing leads to more security issues. When the attackers observes the PIN entry using the cameras, the entries are noted perfectly though they are in long range. The camera-based shoulder-surfing is strong enough to note the PIN entry, when the user enters the PIN multiple times. Thus the attackers can easily use the PIN entries illegally.

B. IMPROVED PIN ENTRY METHOD

Here indirect way of PIN entry method is used by which security is enhanced. Instead of standard PIN numbers, the color code with multi-touch technology is used to enter the PIN in public places. The multi-touch technology uses four standard colors for the PIN entry purposes. The colors used are standard with the reputation of colors in the keypad.

2. RELATED WORK

[1] Designing Leakage-Resilient Password Entry on Touchscreen Mobile Devices by Qiang Yan, Jin Han, Robert H.Deng

Touchscreen devices are fast moving commodities since the user can use various services at any time anywhere. To avoid the unauthorized attack it uses the passwords for user authentication. Even though it uses passwords some passwords are poor in providing the security. Mostly the leakage is more in computer systems than in mobile devices. Since the features like touch screen is not present in basic mobiles they are used in less. In this method cover pad provides a security in this devices. This works with the conditions like time pressure, distraction, mental workload. This

condition has the common password. Test conditions are checked by user and the process is proceeded.

[2] On Limitations of Designing Leakage-Resilient Password Systems: Attacks, Principles and Usability by Qiang Yan, Jin Han, Yingjiu Li, Robert H. Deng[2]

The design of leakage-resilient password systems (LRPSes) in the absence of trusted devices remains a challenging problem today despite two decades of intensive re- search in the security community. The inherent tradeoff between security and usability in designing LRPS is investigated. Most of the existing LRPS systems are subject to two types of generic attacks - brute force and statistical attacks, whose power has been underestimated in the literature. And in order to defend against these two generic attacks, we introduce five design principles that are necessary to achieve leakage resilience in the absence of trusted devices. And also to get better understand about tradeoff between security and usability of LRPS. By decomposing the authentication process of existing LRPS systems into atomic cognitive operations in psychology, it show that a secure LRPS in practical settings always imposes a considerable amount of cognitive workload on its users are proposed.

[3] Breaking Undercover: Exploiting Design Flaws and Nonuniform Human Behavior by Toni Perkovi , Asma Mumtaz ,Yousra Javed[3]

Two attacks on Undercover, a human authentication scheme against passive observers. The first attack exploits non-uniform human behavior in responding to authentication challenges and the second one is based on information leaked from authentication challenges or responses visible to the attacker. Theoretical and experimental analyses show that both attacks can reveal the user's password with high probability with O(10) observed login sessions. And also proposed some enhancements to make Undercover secure against the attacks . First, it reemphasizes the principle of "devil is in details" for the design of security-related human-computer interface. Secondly, it reveals a subtle relationship between security and usability .To design a secure human-computer interface, designers should pay special attention to possible negative influence of any detail of the interface including how human users interact with the system.

[4] Multi-touch Authentication on Tabletops by David Kim, Paul Dunphy, Pim Briggs[4]

The introduction of the tabletops has made the user to develop the security system in the devices. The user authentication is based on something you know but it is overcome to avoid shoulder surfing. In this paper to avoid shouder surfing multi touch system is avoided and number of novel laptops is used. So improved system like the PIN and graphical passwords is used in this paper. The user can make the system convinent to the access purpose by creating the PIN and the password.

[5] ColorPIN- Securing PIN Entry Through Indirect Input by Alexander De Luca, Katja Hertzschuch, Heinrich Hussmann

Automated Teller Machine (ATM) thefts are large in number now a days. The main reason for this type of theft increasing is that the PIN number used is itself not providing a improved security mechanism. The security is maintained only by the user. Its user's duty to maintain the PIN security. to overcome this color PIN authentication is the specified new way. The color PIN is based on one-to-one relationship which uses the number of clicks to use them. The user should know that color PIN is more secure than the standard PIN mechanism.

3. COLOR CODE PIN ENTRY SYSTEM

A. Concept

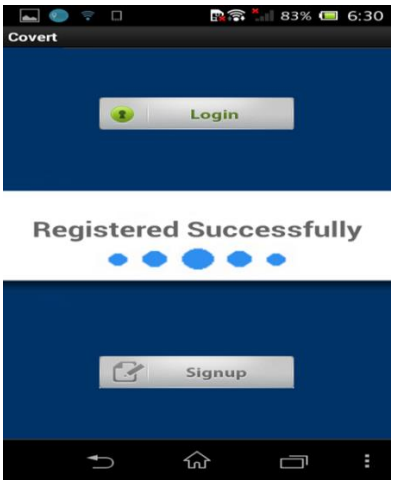
In this paper, a secured PIN authentication is done through color keypad in various devices. The proposed algorithm uses the generated four digit PIN in which each digit block is separated with the combination of two colors to prevent shoulder

surfing attack by extracting PIN digit after all user iterations got completed.

In this method, the single numeric digit is divided into two different color, in which the user can choose either of two colors that fulfils his or her PIN digit key in each round. In this session, totally four rounds are executed for PIN authentication where each digit is authenticated four times individually to enhance security in mobile banking.

B. User Registration

User Registration is done and after that the user is able to access the ATM application in their mobile phones. Once the User Registration is Complete, User will be provided with a Unique PIN Sent to their respective Mail ID. Once it got validated a User will be able to access our Application by entering the Username and Password Chosen at the time of Registration. If the PIN is entered illegally without the users knowledge, an mail is sent to the user stating about the illegal process that had took place.



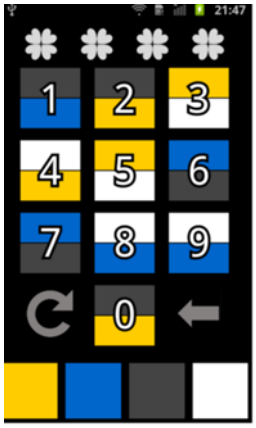
C. BW Method

In this Method, the new Strategy is actualized that will totally disregard Shoulder Surfing. Indeed, even a Well-Trained Perceptual Grouper couldn't Crack the PIN Digit Entered by the User expectedly. Give P a chance to indicate an arrangement of four hues and additionally designs adaptable. Let P = {black, blue, white, yellow} or P = {black, white, specked, corner to corner stripes}, for a visually challenged individual. Generally, the enhanced technique keeps running as takes after: The framework shows an arrangement of ten digits, A = {0, 1,2,3,4,5,6,7,8,9}, on the consistent numeric keypad with two split hues, browsed P, in each numeric key; and the four shading keys underneath.

A shading is picked aimlessly from P and fills four arbitrary parts of unmistakable keys; each split could be either upper or lower one. The rest of the hues fill four parts, separately, similarly. The client takes care of the PIN digit and enters both of its shading through the shading key. The client and the framework rehash this strategy for four adjusts that the PIN digit is recognized by convergence, and until the whole PIN digits are distinguished

Each of the digit is split into two different halves in which two different colors are filled. These colors keeps changing in every iteration, so that the probability of finding the secret four digit PIN number becomes complicated. In this session, each PIN digit is iterated or authenticated for four times with color change for each iteration. Since

two or more different digits have repeated colors either in their upper-half or lower-half, which makes the system more strong enough and provides security for transaction and authentication purpose. This makes the hacker difficult to crack the PIN digit and enter into the account illegally and do the transaction without the user's knowledge.



(a)

Color code PIN entry system

4. INVISIBLE PIN ENTRY SYSTEM

The challenge keypad does not appear immediately. Only the response keypad appears in its regular layout and size. It shows the challenge keypad only when a user cups a hand on the circle with the grip circularly closed in a ρ-shape. The challenge keypad then shows up after a small delay and disappears immediately when the user releases the cupped hand.

The user interface of SteganoPIN, one numeric keypad is a standard keypad in regular layout and the other is a small separate keypad in a random layout. The random layout keypad is called the challenge keypad because it permutes ten numeric keys as a random challenge, as in. A user must use this challenge keypad to derive a fresh OTP. The user first locates a long-term PIN in regular layout and subsequently maps the key locations into the challenge keypad for OTP derivation. The user then enters the OTP on a regular layout keypad called the response keypad.

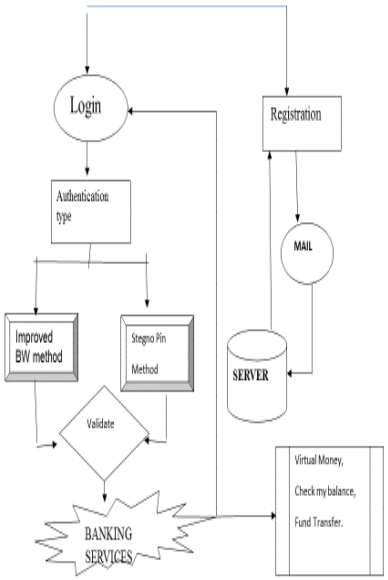


Fig a.Data Flow Diagram

In this method, the main function is to close the proximity server, so that the invisible numeric keypad appears on the screen. The challenge keypad have digits in shuffled manner. When the position is misplaced the challenge keypad gets disappeared from the screen.

The challenge keypad involves in producing shuffled numeric digits every time when the iteration occurs. The process leads to a difficult state for the hacker to find the PIN number as the shuffling takes place every time when it is iterated. The probability of finding the PIN number is not possible for the hacker.

The user makes the PIN entry transaction more secured using this challenge keypad. They help the user to keep the account details in a secured manner. This session involves in producing a high security for the transaction purpose through the mobile devices.

The challenge keypad method is another method like the color code method which gives security for transaction purpose through mobile devices. This method provides the security in mobile banking safely. To avoid the PIN number being hacked by the hacker these methods are used to improve their security while the need arises.

5. RESULTS

By implementing these methods, the user experiences, a unique security wall while doing the transaction through mobile devices.

Here general banking services are done with greater security by using PIN authentication method. Services like money transfer, deposit, withdraw, balance enquiry are made with intent security.

By implementing this method, the user can access the banking services through the mobile devices easily without any form of disturbances in public places.

The user can access the banking services in two different methods as implemented in this paper. Those two different methods are improved BW method and Invisible PIN method.

The paper indicates the ease of use through mobile devices. By accessing these methods, the user can attain the banking in relaxed manner without any kind of stress like standing in bank for banking purposes.

The implementation of this method makes the hacker difficult in hacking the user's PIN when using in mobile devices. The process leads to a good result which shows about the development of digital India.

It is 24*7 hour process, so that the user can use it efficiently.

REFERENCE

1. Q.Yan,J.Han,Y.Li,J.Zhou,and R.H.Deng,"Designing leakage resilient password entry on touch screen mobile devices,"inProc.8thACMSIGSAC Symp. Inform., Comput. Commun. Security, 2013, pp. 37–48.

2. Q. Yan, J. Han, Y. Li,R. H.Deng, "On limitations of designing leakage-resilient password systems: Attacks, principles and usability," in Proc. 19th Internet Soc. Netw. Distrib. Syst. Security Symp., 2012, pp. 1–16.

3 A. Bianchi, I. Oakley, and D. S. Kwon, "Counting clicks and beeps: Exploringnumerosity based haptic and audio pin entry," InteractingComput.,vol. 24, pp. 409–422, 2012.

4. T. Perkovic, A. Mumtaz,Y. Javed, S. Li, S. A. Khayam, and M. Cagalj, "Breaking undercover: Exploiting design flaws and non uniform human behaviour,"in Proc. 7th Symp. Usable Privacy Security, 2011, pp. 1–15.

5. A. Bianchi, I. Oakley, and D. Kwon, "Spinlock: A single-cue haptic andaudio PIN input technique for authentication," in Proc. Haptic AudioInteraction Design, 2011, pp. 81–90.

6. A. Bianchi, I. Oakley, V. Kostakos, and D. Kwon, "The Phone Lock: Audioand haptic shoulder-surfing resistant PIN entry methods for mobiledevices," in Proc. 5th Int. Conf. Tangible, Embedded, Embodied Interaction,2011, pp. 197–200.

7. 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.

8. A.De Luca, K. Hertzschuch, and H. Hussmann, "ColorPIN–Securing PIN entry through indirect input," in Proc. ACM CHI Conf. Human Factors Comput. Syst., 2010, pp. 1103–1106.

9. H. J. Asghar, S. Li, J. Pieprzyk, and H. Wang, "Crypto analysis of the convex hull click human identification protocol," in Proc. 13th Int. Conf. Inf. Security, 2010, pp. 24–30

10. 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.

11. A. De Luca, E. von Zezschwitz, and H. Hussmann,"Vibrapass-secure authentication based on shared lies," in Proc. ACM CHI Conf. HumanFactors Comput. Syst., 2009, pp. 913–916.

12. D. Weinshall, "Cognitive authentication schemes safe against spyware," in Proc. IEEE Symp. Security Privacy, 2006, pp. 295–300.

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

14. T. Matsumoto and H. Imai, "Human identification through insecure chan- nel," in Proc. Adv. Cryptol., 1991, pp. 409–421.

15. G. A. Miller, "The magical number seven, plus or minus two: Somelimits on our capacity for processing information," Psychol. Rev., vol. 101,no. 2, pp. 343–352, 1956.