International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 04 | April -2020 ISSN: 2582-3930

A Novel method to enhance the Security of Automated Teller Machine

Shine Rajesh D
HOD / Assistant Professor, Dept of IT
Bethlahem Institute of Engineering
Karungal, India

JiniMol G
Assistant Professor
Arunachala College of Engineering
Tamil Nadu, India

Jebin Bose S
ME/CSE
Noorul Islam Centre for Higher Education
Kumaracoil, India

***Abstract*—In Automated Teller Machine cyber-crime rate is increasing day by day. Many people are using new technologies for looting money. The security needs to be high for money transactions. The proposed system involves a shuffled key and color method for improving security of ATM pin. On examining the complete reason behind the ATM looting, the problem shows that the looting may happen because of the standard numeric PINauthentication. The normal numeric standard PIN does not provides any of the security in ATM against recording attacks. The complete security on the PIN entry is based upon the corresponding card holder activities. From this we come to the point to improve security. This system presents a color PIN selection methodwhich providescolored and shuffled keysforsecured PIN selection by the card holder. The system will be more secure when compared with the normal standard PIN selectionby providingsecured authentication and fast transaction systems and also provides higher security features for overcoming the recording attacks.**

Keywords—PIN;security; authentication.

I. INTRODUCTION

In olden days, the user's having account at bank are allowed to deposit or withdraw the cash only by means of moving onto the bank and through written statements. This has been overcome by a hardware machine known as ATM, where all the customer's having an account on authorized bank will have ATM card along with four digit numeric secret PIN. With the help of the ATM card and four digit numeric PIN, the account holder can withdraw, deposit, transfer or request for mini statement on all time whenever they are in need.

In ATM authentication is performed by using four digit secret numerical password that verifies the card along with the PIN the user enters using the keypad. Here PIN selection leads to recording attacks. The PIN entry can be easily noted by the persons standing behind with the help of recording devices or by means of vision enhancement and all the user data will be looted.

The ATM transaction developed on the basis ofuser havinga ATM card and a secured four digit numeric secret PIN. Whenthe card details and PIN are verified, user will be enabled with a pattern and the user have to select the button that has beenenabled in the pattern using the color choice. The PIN, that has four numerical digits, may easily be identified or easily be noted down by the persons standing behind or can easily be recorded because of the simplicity of PIN as well as ten digit keypad[11]. Since ATM PIN's are widely used in various automated teller machine, information as well as the PIN can easily be subjected to attacks. Various secured PIN entry methods have been proposed to overcome the attacks, but maintaining the usability as well as the security is always a challenging task.

Various previous works focus on the simple PIN entry method on providing the secured authentication. In this paper we will refer Tictoc PIN entry method to be the basic scheme. The basic Tictoc PIN entry method presents five decimal keypad for a single PIN entry where the user have to select the colors preceded on the third and fifth keypad based on the vibration and simulated sound.In first keypad a short vibration occurs were colors appears in the left boxes. In second keypad a simulated sound occurs in which colors appear on the right boxes.In the third keypad four color input keypad containing white, black, blue, red will be enabled at the bottom were user selects the first key that has been notified with vibration. The fourth keypad will be enabled with two vibration sounds that will be continued by a normal vibration where the colors appears on left, middle and right boxes. In the fifth keypad three color input keypad appears with white, black, blue at the bottom in which user selects the first key color buttonthat has been notified with the vibration.

Even though the work presented by [5] provides a secured PIN Entry scheme the Tictoc PIN Entry method provides its security, we focus the issues on security and usability. On analyzing [23] the Tictoc PIN entry method provide following results.

- The Identification of Vibration as well as the simulated sound can't easily be identified by the user.
- User finds very much difficulty in identifying the color within particular time period.
- Tictoc PIN entry method is more slower than other standard PIN entry techniques.
- Tictoc PIN entry method is more error prone when compared with other standard PIN entry techniques.

On finding the above insights we intent to strengthen the

security and usability of PIN's (ATM) from Tictoc PIN entry method into a Multi Color Key Shuffling Scheme (MCKS).

In Section II, we reviewed and analyzed the Tictoc PIN Entry Method. In Section III, we introduced the improved MCKS and evaluated the security features and its usability. The related works has been discussed in Section IV and concluded in Section V.

II. EXISTING SCHEME

A. Review of Tictoc PIN entry method

The Tictoc PIN entry method [23] can be used for entering the PIN based on color.Here user's have clearly identify the vibration and simulated sound that occurs on certain time period and the users have to enter their PIN based on the color. In this method the user's have to select the colors instead of standard PIN's.The user's have to select two colors for a single PIN entry from a set for five keypads. The user finds very much difficulty in finding the colors as well as the vibration and simulated sound that occurs on a particular time period. It takes more time for a single PIN to be entered using two stages. The Tictoc method provides security for some attacks and does not able to overcomesome of the recording attacks [23].

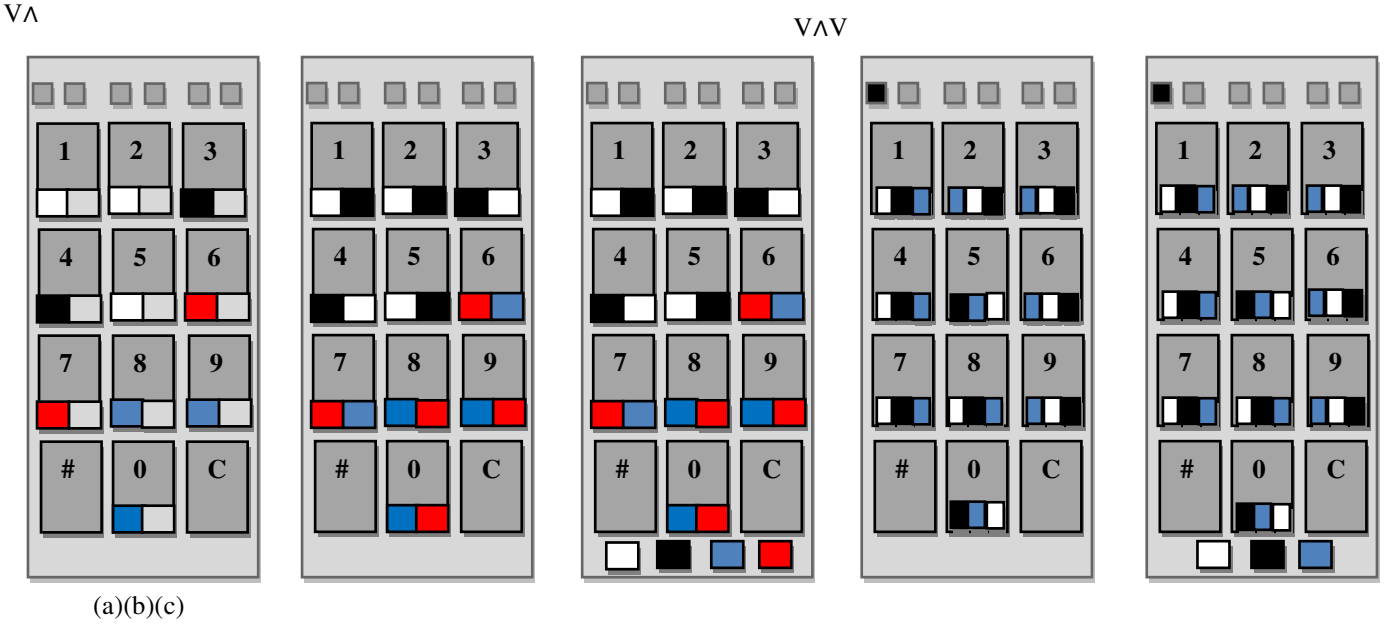


Fig. 1. Tictoc PIN Entry Method – Example on selecting digit 1 by the useron two round process. Here V determines vibration while the marking ∧determines a simulating sound. (a) A short vibration occurs were colors appears in the left boxes. (b) A simulated sound occurs in right boxes are filled with colors. (c) The input keypad containing four colors will appear at the bottom were theuser selectsthe color white under the first key that has been notified with vibration. (d) Enables with two vibration sounds that will be continued by a normal vibration where the colors appears on all the three boxes (e) Three colorswill appear at the end in whichselection will be blue, the first color button that has been notified with the vibration.

• Tictoc PIN Entry: Here the rounds are limited to two of five stages when compared to previous methods. The four sets L1 with white, L2 with black, R1 with blue R2 with red are arranged in random sequence for first round. Three colors (white, black and blue) will be arranged for the second round. Each color selection on two rounds is collected and confirmation is made.

B. Analysis of Tictoc PIN entry method

The Tictoc PIN entry method undergoes delayed oracle choices method in which the keypad is partitioned into two stages of five patterns. The first round contains two stages. Each PINon numeric keypad is will have two boxes. Let us consider C1 will be black C2 will be white arranged onrandom sequence, and letC3 will be blueand C4 will be red arranged onrandomsequence. For first PIN entry in first stage, the boxes in the left L1, L2, R1, R2 are filled with colors C1, C2, C3, C4. The second stagefor the first PIN entry begins with a delay of 500 msec. Here the left boxes will be displayed with colors and the right boxes of L1, L2, R1, R2 are filled with colors C2, C1, C4, C3. To receive user input, keypad containing four colors will be displayed in random manner after a delay of 500 msec. Among the two stages one stage will be chosen at the period of execution that provides vibrotactilevibration with a delay of 30 msec. This round will be enabledtill the user selects the input. The second round of first PIN entry consists of three stages with 500 msecdelayon one among them, that can be preceded by 30 msecvibrotactile vibration. Three small boxes will be enabled on the keys of numerical keypadthat are colored from left to right. Let us consider C5, C6, andC7 be black, white, and blue, randomly. The colors C5, C6, C7 will be assigned to the left boxes of Q1, Q2, Q3 on the first stage of the second round. The center boxes of Q1, Q2, Q3will be assigned withcolors C6, C7, C5 on the second stage. The third phase adds colors C7, C5, C6 to the boxes on the right. A three color keypad appears in random order. The three color keypad will remain stable until user selects the input.

III. MULTI COLOR KEY SHUFFLING SCHEME (MCKS)

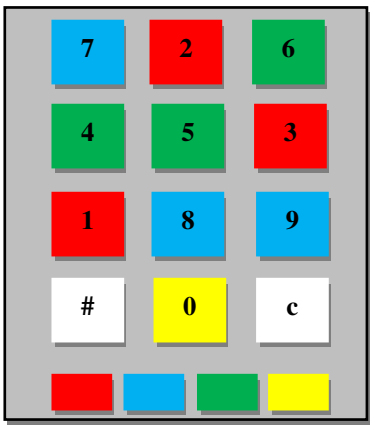
The ingenuity of the Tictoc PIN Entry method in assigning colors to PIN and to provide Vibration and Simulated sound to receive each PIN digit from the user provides various drawbacks. Our proposed security methodprovides four colored shuffled PIN entry that are explained below. In short, two round for a single PIN entry has followed.

On entering each PIN, the user have to select the color button below the keypad based on the respective PIN. Two rounds for single PIN entry will be carried out. So for completing 4 digits of entry 8rounds are used. After

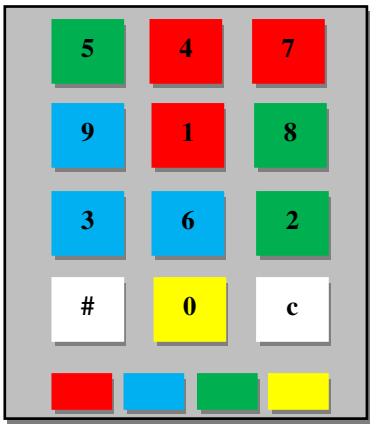
completion of the PIN entry, Administrator performs the computation for giving privilege to access the ATM for transactions.

Algorithm : Multi Color Key Shuffling

1. $Let\ (I,J) =$ All primary sets $= \{I,J,K,L\}$
2. $(I,J) \leftarrow \gamma(\pi(I))$
3. $(K,L) \leftarrow \gamma(\pi(I))$
4. $(W,X) \leftarrow (\emptyset,(\emptyset,)$
5. $(Y,Z) \leftarrow (\emptyset,(\emptyset,)$
6. For $i = 1,\cdots,m$ do
7. Let (i,j,k,l) = All permutation of colors
8. $(i,j,k,l) \leftarrow \rho\ (P)$
9. View $(I \cup X\ and\ J \cup W)\&\&(K \cup Z\ and\ L \cup Y)$
10. Input option $\in i,j,k,l$
11. if option $= i$ then
12. {
13. $(Y,Z) \leftarrow \gamma(\pi(W \cup X \cup J))$
14. $(W,X) \leftarrow \gamma(\pi(W \cup X \cup J))$
15. $(K,L) \leftarrow \gamma(\pi(I))$
16. $(I,J) \leftarrow \gamma(\pi(I))$
17. }
18. else if option $= j$ then
19. {
20. $(Y,Z) \leftarrow \gamma(\pi(W \cup X \cup I))$
21. $(W,X) \leftarrow \gamma\ (\pi(W \cup X \cup I))$
22. $(K,L) \leftarrow \gamma(\pi(J))$
23. $(I,J) \leftarrow \gamma(\pi(J))$
24. }
25. else if option $= k$ then
26. {
27. $(W,X) \leftarrow \gamma(\pi(Y \cup Z \cup L))$
28. $(Y,Z) \leftarrow \gamma(\pi\ (Y \cup Z \cup L))$
29. $(I,J) \leftarrow \gamma(\pi(K))$
30. $(K,L) \leftarrow \gamma(\pi(K))$
31. }
32. else
33. {
34. $(W,X) \leftarrow \gamma(\pi(Y \cup Z \cup K))$
35. $(Y,Z) \leftarrow \gamma(\pi(Y \cup Z \cup K))$
36. $(I,J) \leftarrow \gamma(\pi(L))$
37. $(K,L) \leftarrow \gamma(\pi(L))$
38. }
39. end if
40. end for
41. return I



(a)



(b)

Fig. 2. MCKS - (a) User selects the PIN by selecting the color at the bottom (b) User selects the same PIN at the bottom .

In this secured PIN entry scheme we have used 4 colors for 10 decimal digits. The colors of Red, Blue, Green and Yellow present on the keys will be available at the button. The keys # and c will also be available along with the 10 decimal digits.

Here all the digits with multi colors are shuffled on random manner, so that identification of PIN or recording of PIN is impossible for the user's standing behind. This provide more security to each and every transaction through ATM when compared with the standard PIN entry technique.

• MCKS Partitions: The partition of MCKS beA1={ 1,.,9,0} to four subsets R1 ={1,2,3}, G1={4,5,6}, B1 ={7,8,9}, and Y1={0}. The partition of A2 into the four subsetsR2={1,4,7}, G2={2,5,8},B2={3,6,9} and Y2 ={0}.The same partition can be used in all stages, with change in position of PIN. All the Keys will be shuffled randomly.

• Two-Round PIN Entry: In this system two rounds of PIN entry will be carried out. In the first round, the four sets (R1, G2, B1, Y2) be assigned with colors (red, green, blue, yellow) in randomsequence. The colors red for R2, green for G2, blue

for B2, and yellow for Y2will be assigned for second round.The colors collected at the two rounds is combined and PIN entry is confirmed

A. MCKS PIN Entry Example

The MCKS PIN entry has been explained here using the example by Figure 2, thatdetermines the PIN entry 2 through MCKS scheme.

Figure 2 (a) – User selects red, the color on the PIN 2. (b) – Here user selects green, the color on the PIN 2.

The 1st PIN 2 will be entered to the system successfullyusing two round procedure.The remaining PIN entry will also be fallowed through same technique.

B. Security Measures on MCKS

As the rounds of PIN entry has been made to two for a single entry the security has been increased. And also shuffling of keys randomly provides more security. The coloring sequence will also vary on each and every iterations. Here no user information is leaked or recorded through any devices or through any other medium.

IV. RELATED WORKS

Here, we provides feedback onall related works and analyzetheovercomeof our work.

To overcome PIN attacks, users makes their prevention through varioussecurity measures. Since the seminal work [1]and [2]describes completely about the security. The objectivedetermines an indirect PIN entry for security purposes by means of separating the standard PIN entry procedure. Various previousworksfocus on graphical password method [7], [6], and for PIN entry [18], [14], [5], [3].

Weexplain the scheme, created at [10], that uses graphical passwords. Here graphical as well as tactile challenges has been performed and delivered by means ofa device namely haptic. Our system, MCKS, provides more security against all the recording attacks that overcomes the process at [5].

Our proposed system determines on elaborating the work at [22], thatdeals with shoulder surfing attacks. Awell trained attacker can easily find all the details about the user whether the enters the PIN directly or through colored series .On analysing results we intent to determine why such attacks occurs. Moreover, our proposed system elaborates the work at [22] by providing higher security.

Here we describe then work at [23], that uses vibration and simulated sound. Five patterns containing two rounds for a single PIN entry makes the user to wait for a long time. Rather the color series can't easily be identifiable to the users. The user have to wait and notify the vibration and sound as well as the color that has been displayed during the vibration and sound. Our Multi Color Key Shuffling scheme, which uses multiple colors as well as shuffled key provides a secured authentication among the user's for their secured money transactions.

V. CONCLUSION

The Tictoc method, proposed by Taekyoung Kwon[23], determines an PIN entry method that specifies interacting with colors over five rounds based on vibration and simulated sound. In our work, we analyzedTictoc method and notedvarious issues, such as errors in identifying the vibration and simulated sound, difficulties for color selection, and system slowdown. To overcome Tictoc PIN entry method and to resolve the issueswe proposedMCKSmethod. The MCKSmethod requires two rounds of PIN entrythat has multiplecolor along with shuffled keys.

The MCKS method shows a secured PIN selectionmethod that provides authentication by providing secured way of transaction in less time . The detailed description proves that, the method is user friendly. Here the attacker can't easily find the user's login details as all the keys will be shuffled and arranged in random order.. In future, plan to extend our techniques is to secure and saving time. We can use embedded programming to fast up the process.

REFERENCES

[1] T. Matsumoto and H. Imai, "Human identification through insecurechannel," in Advances in cryptology, Berlin, 1991, pp. 409–421.

[2]Chih-Hung Wang, T. Hwang, and Jiun-Jang Tsai, "On the Matsumoto and Imai's human identification scheme," in Advances in Cryptology, Berlin, 1995, pp. 382–392.

[3] G. T. Wilfong, "Method and apparatus for secure PIN entry," U.S. Patent, Aug. 17, 1999.

[4] Luca, E. Von Zezschwitz, L. Pitcher, and H. Hussmann."Using fake cursors to secure on-screen password entry", in Proc.CHI,pp.2399-2402, 2013.

[5] V. Roth, K. Richter, and R. Freidinger, "A PIN-entry method resilient against shoulder surfing," in Proc. 11th ACM Conf. Compu. Commu. Secure. (CCS), Feb. 2004, pp. 236–245.

[6] S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," in Proc. ACM Int. Working Conf. Adv. Vis. Inter., 2006, pp. 177–184.

[7] D. Weinshall, "Cognitive authentication schemes safe against spyware," in Proc. IEEE Symp. Secur. Privacy, May 2006, pp. 294–300

[8] Christo Ananth, A. NasrinBanu, M. Manju, S. Nilofer, S. Magesdhwari, and A. PeratchiSelvi, "Efficient Energy Management Routing in WSN", International Journal of Advanced Research in Management, Architecture, Technology and Engineering, Vol. 1, Aug 2015, pp. 16-19.

[9] Mun-Kyu Lee, "Security Notions and Advanced Method for Human Shoulder Surfing Resistant PIN Entry", IEEE Trans. On Information Forensics and Security, vol. 9, Apr 2014, pp. 1556-6013

[10] H. Sasamoto, N. Christin, and E. Hayashi, "Undercover: Authentication usable in front of prying eyes," in Proc. ACM SIGCHI Conf. Human Factors Comput. Syst. (CHI), 2008, pp. 183–192.

[11] J. Long, No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing. Boston, MA, USA: Syngress, 2008.

[12] HongGuo, Bo Jin, " Forensic Analysis of Skimming Devices for credit fraud detection", IEEE Conf. on Information and Financial Engineering, Jan. 2010, pp. 542-546.

[13] A. Rahman Alhothaily, A.Alrawais, X. Cheng, R.Bie, "A novel verification method for paying card systems", in springer, London, vol. 19, oct. 2015, pp. 1145-1156.

[14] T. Perkovic, M. Cagalj, and N. Rakic, "SSSL: Shoulder surfing safe login," in Proc. Int. Conf. Softw., Telecommu. Comput. Netw. Sep. 2009, pp. 270–275.

[15] K.Jain, A. Ross, S. Prabhakar, "An Introduction to Biometric Recognition",IEEE Trans. On Circuits and Systems for video technology, vol. 14, Jan. 2004, pp. 4-19.

[16] Vivek, K. Singh, Tripathi S.P, Agarwal, " Formal Verification of Finger print ATM Transaction through Real Time Constraint Notation (RTCN)" Int. Jour. Of Comput. Scie., Vol. 8, May. 2011.

[17] Sharma, Vijay Singh Rathore, "Role of Biometric Technology over Advanced Security and protection in Automated TellerMachine Transaction", Int. Jour. Of Engg. And Tech., Vol. 1, Aug. 2012.

[18] 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.

[19] Zaid Imran, and RafayNizami, "Advance Secure Login" Int. Jour. Of Sci. and Rese. Publi, Vol. 1, Dec. 2011.

[20] Prasant Kumar Gajar, Arnab Ghosh, Shashikant rai, "Bring your own Device (BYOD): Security Risks and Mitigating Strategies", Jour. Of Globa. Resea. In Com. Scie, vol. 4, apr. 2013.

[21] Kavitha. V and G. Umarani Srikanth, "Moving ATM Applications to smart phones with a secured Pin-Entry Methods", Jour. Of Comp. Engg.,Vol. 17, Feb.2015.

[22] T. Kwon, S. Shin, and S. Na, "Covert attentional shoulder surfing: Human adversaries are more powerful than expected," IEEE Trans. Syst., Man, Cyber., Syst., vol. 44, no. 6, pp. 716–727, Jan. 2014.

[23] T. Kwon and J. Hong, "Analysis and Improvement of a PIN-Entry Method Resilient to Shoulder-Surfing and Recording Attacks," in Proc. IEEE Trans. on Inform. Forensics and Sec., vol. 10. No.2, Feb 2015