Generating hybrid pictures for enhancing cyber security in ATM using PIN authentication method

SAURABH SINGHAL[1], ASHISH SHARMA[2],

[1]Department of Computer Engineering and Application
GLA UNIVERSITY, MATHURA
saurabh.singhal@gla.ac.in

[2]Department of Computer Engineering and Application
GLA UNIVERSITY, MATHURA
ashish.sharma@gla.ac.in

Abstract: Present process of ATM has a lot of fraud malicious money transactions and thefts that are occurred by lack of privacy protection. Through introducing false impression PIN, a PIN-based confirmation mechanism that runs on touch screen computers, users fix the issue of shoulder surfing attacks on authentication schemes. PIN uses the hybrid picture method to combine two keys of opposite numerical order such that the button-closer can use one keyboard to reach the Lock, while the intruder from a larger distance is staring at the computer so only the other keyboard is available. The client keyboard is mixed in each effort at authentication because the aggressor can save the pressed digit spatial understanding. Because of the reliability of the Illusion PIN and the creation of an algorithm focused on human visual interpretation, the analyst can't read the key virtually unlikely to pick up the PIN of a Mobile consumer while an IPIN is used by the surveillance camera. The OTP authorization method is also incorporated in the new scheme. This increases the protection related to the computer ATM system keyboard. The idea of ATM security, including OTP authentication, was then suggested.

1. INTRODUCTION

There are several security systems for clients for various reasons. Our emphasis in present paper is based on the authentication regimes dependent on personal identification number (PIN). Authentications systems depend on PIN are widely deployed. PIN-based passwords are commonly embraced or used depending on their convenience and sophistication. They have a short password field, just digits 0 to 9. They are simple. The length of the password is usually four to six digits. The error rate is also small as there is a restricted password space and the shorter password length. From the security standpoint review of PIN authentication schemes shows that their usability adversely affects their reliability. Increasing types of PIN entry are open for different kinds of assaults, including spontaneous guessing and shoulder surfing. The number of failed login attempts can be limited to a minimum amount, such as 3, 4 or 5 to reduce the chance of a brute force attack. However, the shoulder surfing assault remains a big obstacle for numerous authentication systems that have to be fully neutralized. Shoulder surfing is a virtual application to obtain details, such as Click, passwords and other sensitive knowledge while gazing over the shoulder of the perpetrator. A very typical example of a shoulder surf assault is an individual in the line of an ATM system standing immediately behind a machine. The attacker will quickly search over a person's shoulder for a PIN or password to rob. This is also true for someone who enters his PIN or password in a crowded subway and public place while unlocking his mobile phone. The concealed cameras and tracking systems will even enable a shoulder navigator to snatch a user's PIN or password. This work is motivated by the development of a PIN entry system to increase resistance to shoulder surfing attack and improve user safety and comfort. The reality that shoulder wave attacks occur is well known, but the consumer is not taken seriously. Shoulder surfing is a matter of concern, because consumers have just one pin code in several instances, which is used frequently and for different purposes. A new graphical pin entry system has been proposed by the paper user which provides resistance to human shoulder surfing and, to some extent, to recording based shoulder surfing attacks. Lee mentioned that a shoulder surf attack based on recording cannot be catered for until some of the information is not hidden from the attacker in the login process. In order to alleviate a shoulder surfing attack, the user can use secondary channels. But on the channel because the usability of the day system will be reduced. In our scheme and a consumer report, our scheme has demonstrated that protection and usability are fairly matched.

2. PROFILE BASED PERSONALIZATION

Proposed a PIN-based solution immune to a small degree to shoulder surf assault. Two black and white color keys are used to separate the keypad. The color is randomly distributed. The user enters a key with the same color as the set, depending on the number belonging to the PIN under verification. In order to enter one single digit, it requires four rounds of PIN input and similarly sixteen rounds of PIN input are needed for a four-digit PIN code. Two out of three versions of this authentication scheme are not capable of capturing a shoulder surf attack. If the intruder has more than one authentication method information Shi et al introduced an alternative PIN-based authentication method. The designer's scheme shows a set of co-centered spinning wheels L (number of digits present in the password), which are also divided into 10 sections. Increasing sector is uniformly defined by a numerical digit from 0 to 9, and every digit is displayed in each circle exactly once. Either clockwise or counterclockwise, circles may be rotated. To access the Slot, all Slot numbers must be arranged into the appropriate series in one line.

3. SYSTEM ARCHITECTURE

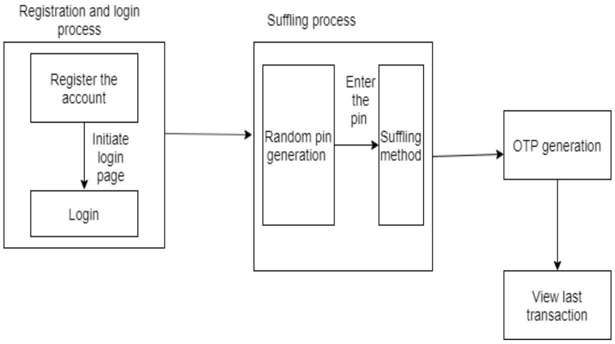


Fig 1. Architecture diagram

The user first registers the account and admin generate the random 4 digit pin then the user was enter the pin the keyboard was shuffled and the user receive the OTP from mail and enter the OTP finally the user see our transaction

Stagno PIN is an indirect pin input system designed to react to challenges through a user interface. The Stagno PIN design comprises of two keys. The first is a standard and open keyboard, the second is a random keyboard hidden from the opponent. The user will hide the view from the attacker by using one of his hands. Every digit on the secret keyboard will be tested by the user and the correct digit on the open key box will be inserted. A new pin is then inserted against a set long-term pin for each login session on the accessible keypad. The latest button is called the "OTP" module.The consumer will secure the keypad by cupping it with one of his hands and entering with his other hand the PIN code on the open keyboard. When both hands are used simultaneously, a lot of unwanted physical effort is needed on behalf of the user. Illusion Button is another shoulder surfing denial Button-based authentication system. The authentication is based on the virtual keyboard principle the author has used the technique of hybrid picture to merge the pictures of two keypads with a consumer keyboard and a shoulder surfer's keyboard with multiple digits to create a single virtual keyboard hybrid picture. The author has taken the opinion that the target is still closer than the shoulder surfer to his phone. If the consumer searches from a shorter distance for the prototype keys, he can see the app keypad.While the surfer on the shoulder looks at the keyboard from a distance away and sees another keyboard, the shoulder surfer keypad. In addition, every authentication attempt changes the digits of the user keypad, so that the shoulder surfer is not able to track the user keypad's spatial arrangement. The author assumed that a shoulder navigator stands at a distance from the user display, which is not always true, with this authentication scheme.

3.1 HOLDER ACCOUNT APPLICATION MODULE

In this module the holder is going to create an account with some bank mandatory field, these fields are used in further upcoming process. This module is like a privilege form to get an action in bank service.

3.2 ATM CARD AND ACCOUNT FORMULATION MODULE

In this module is used to do formalities to get an ATM card like an ATM card Request. The holder’s Account Number and pin number are sending to our E-mail, through the save our time because now a days the account holders are wasting the time to complete their initial process.

3.3. ACCOUNT HOLDER INFO UPDATING MODULE

In this module Update the user’s detail when he needs, the ATM card are supposed to lose in that time the going to give new ATM card Request and we update the Pin detail in that particular Holders.

3.4 ATM TRANSACTION BY SHUFFLING KEY PAD MODULE

In this module get the input like a pin number through the ATM keypad, Actually our Application Provide the keypad number are changing in dynamically so the hacker cant able to hack the pin Number.

3.5 VIEW HOLDER LAST LITTLE TRANSACTION

In this module is used to provide the last few transactions are made in those particular domain users. This transaction detail consists of transaction amount, Area of ATM, Transaction Time and Date Details

4. PROPOSED SYSTEM

Shouldering involves eavesdropping confidential details by inspection such as an alphanumeric password or a Lock. A typical example is an enemy who stands behind an ATM machine in a line and looks over the shoulder or 'surf' to gain information about his PIN. In this scenario, while in their vicinity, the attacker observes a person. However, by using recorded information gathered purposely or even accidentally, the intruder can track others remotely. For

Example: Accidental recording of shoulder surf equipment may result from a surveillance camera that caught an individual in order to open their phones in a shop or on the workplace when entering their authentication credentials. Systems of authentication that are not observationally robust are susceptible to shoulder surfing. Any sensory details, like the button flickering when pushed, or even the sticky mark left from the fingertips on the touch screen can be noticed. The shoulder surf is especially a great threat to PIN authentication since an outsider can track the PIN authentication cycle fairly quickly.

In these cases, it becomes safer for an intruder to stand next to the victim while avoiding detection. Shoulder-surfing becomes simpler.

5. IMPLEMENTATION

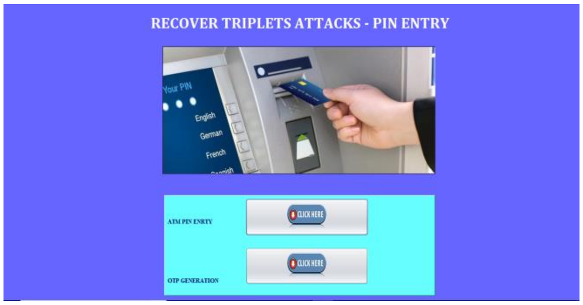
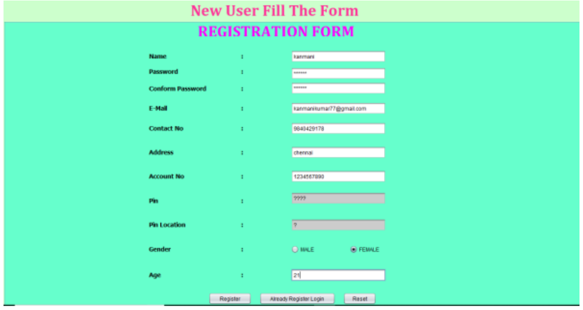


Fig 2. A graphical pin entry home page to login and registration

User to register and login the account page.



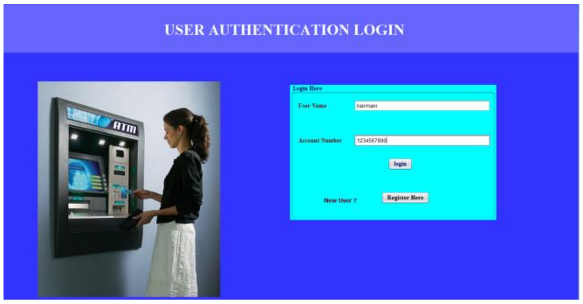
New User Fill The Form

REGISTRATION FORM

Name	:	kanmani
Password	:	******
Conform Password	:	******
E-Mail	:	kanmanikumar77@gmail.com
Contact No	:	9840429178
Address	:	chennai
Account No	:	1234567890
Pin	:	????
Pin Location	:	?
Gender	:	○ MALE ● FEMALE
Age	:	21

Fig 3. Registration form

The new user to register our basic details.



USER AUTHENTICATION LOGIN

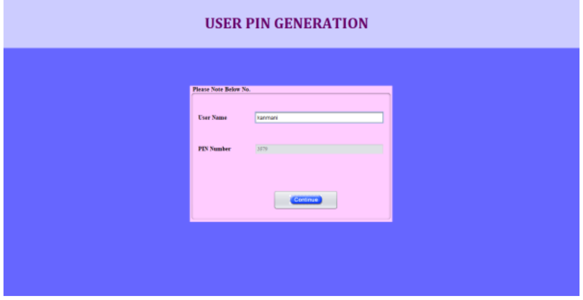
Login Here

User Name: kanmani

Account Number: 1234567890

Fig 4. User authentication login page

The user already registers the form then the user directly to login the page.



USER PIN GENERATION

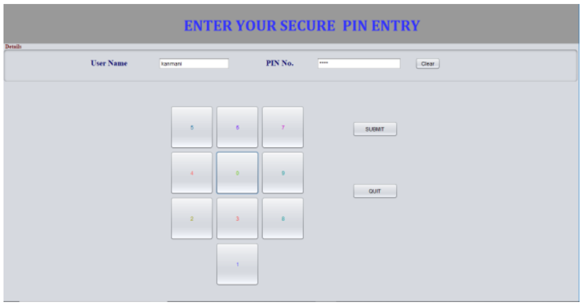
Please Note Below No.

User Name: kanmani

PIN Number: 3579

Fig 5. User pin generation page

The admin to generate the 4-digit pin for user.



ENTER YOUR SECURE PIN ENTRY

Details

User Name: kanmani PIN No.: ****

Fig 6. Enter your secure pin entry screen

The user to enter the 4-digit pin for sufflekeybad.

6. CONCLUSION

The key goal of our research was to build a PIN authentication device immune to shoulder surfing assaults. To this end we generated Illusion Ring. By adding the concept of protection space, which we calculated using a visibility algorithm, we quantified the degree of resistance. We required a simple description of the functioning of the human visual system in the sense of the visibility algorithm. The user made a number of simplifying assumptions in this phase which restrict the accuracy of our calculations. The clearest example is the pinhole camera model we used to illustrate the phase in which the picture was created. The visual algorithm forms the core of our research and we want to explore how the exposure of pictures other than hybrid keyboards can be evaluated. The visibility algorithm is used to calculate distortion between the 2 artifacts by using the MSSIM table.

REFERENCES

1. M. Harbach, A. De Luca, and S. Egelman, “The anatomy of smartphone unlocking: A field study of android lock screens,” in Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, ser. CHI ’16. New York, NY, USA: ACM, 2016, pp. 4806–4817.
2. T. Kwon, S. Shin, and S. Na, “Covert attentional shoulder surfing: Human adversaries are more powerful than expected,” IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 44, no. 6, pp. 716–727, June 2014.
3. M. Harbach, E. Von Zezschwitz, A. Fichtner, A. De Luca, and M. Smith, “It’s a hard lock life: A field study of smartphone (un)locking behavior and risk perception,” in Proceedings of the Tenth USENIX Conference on Usable Privacy and Security, ser. SOUPS’14. Berkeley, CA, USA: USENIX Association, 2014, pp. 213–230.
4. M. Lee, “Security notions and advanced method for human shouldersurfing resistant pin-entry,” IEEE Transactions on Information Forensics and Security, vol. 9, no. 4, pp. 695–708, April 2014.
5. J. Bonneau, C. Herley, P. C. v. Oorschot, and F. Stajano, “The quest to replace passwords: A framework for comparative evaluation of web authentication schemes,” in 2012 IEEE Symposium on Security and Privacy, May 2012, pp. 553–567.
6. J. Bonneau, S. Preibusch, and R. Anderson, “A birthday present every eleven wallets? the security of customer-chosen banking pins,” in Financial Cryptography and Data Security, A. D. Keromytis, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 25–40.
7. 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, Sep. 2012.
8. 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 Proceedings of the Fifth International Conference on Tangible, Embedded, and Embodied Interaction, ser. TEI ’11. New York, NY, USA: ACM, 2011, pp. 197–200.
9. R. Kuber and W. Yu, “Tactile vs graphical authentication,” in Haptics: Generating and Perceiving Tangible Sensations, A. M. L. Kappers, J. B. F. van Erp, W. M. Bergmann Tiest, and F. C. T. van der Helm, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 314–319.
10. H. Sasamoto, N. Christin, and E. Hayashi, “Undercover: Authentication usable in front of prying eyes,” in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ser. CHI ’08. New York, NY, USA: ACM, 2008, pp. 183–192.
11. S. Shekhar, D. K. Sharma, and M. M. Sufyan Beg, “Language identification framework in code-mixed social media text based on quantum LSTM—the word belongs to which language?” Modern Physics Letters B, Vol. 34, No. 06, 2050086 (2020). [SCI, Impact Factor: 0.731].
12. J. Kumar, D. Saxena, A. K. Singh, and A. Mohan, “Bi-Phase adaptive learning-based neural network model for cloud datacenter workload forecasting”, Soft Computing (2020): pp. 1-18, 14 March 2020 [SCI, Impact Factor: 3.050].
13. J. Kumar, A. Singh, and R. K. Buyya, “Ensemble learning based predictive framework for virtual machine resource request prediction”, Neuro computing (2020). Vol. 397, pp. 20-30, 15 July 2020 [SCI, Impact Factor: 4.072].

14. H. Sharma and A. S. Jalal, "Incorporating external knowledge for image captioning using CNN and LSTM", World Scientific Publishing, Vol x, No. x, pp. x, July 2020, [SCI, Impact Factor: .687], DOI: 10.1142/S0217984920503157
15. D. P. Yadav, A. S. Jalal and G. Pant, "Deep learning-based ResNeXt model in phycological studies for future", Algal Research, Elsevier, Vol. 50, pp. 1-6, 2020, [SCI, Impact Factor 4.008], https://doi.org/10.1016/j.algal.2020.102018
16. S. Agrawal, A. Sharma, C. Bhatnagar and D.S. Chauhan, "Modelling and Analysis of Emitter Geolocation using Satellite Tool Kit", Defence Science Journal, Vol. 70, No.4, pp.440-447, July 2020. SCI https://doi.org/10.14429/dsj.70.15162
17. Varun K L Srivastava, N. Chandra Sekhar Reddy, Dr. Anubha Shrivastava, "An Effective Code Metrics for Evaluation of Protected Parameters in Database Applications", International Journal of Advanced Trends in Computer Science and Engineering, Volume 8, No.1.3, 2019. doi.org/10.30534/ijatcse/2019/1681.32019
18. Bhardwaj, D., Jain, S.K., Singh, M.P. 2009. Estimation of network reliability for a fully connected network with unreliable nodes and unreliable edges using neuro optimization International Journal of Engineering, Transactions A: Basics 22(4), pp. 317-332.
19. Verma U., Bhardwaj D., 2020 "Design of Lightweight Authentication Protocol for Fog enabled Internet of Things - A Centralized Authentication Framework", International Journal of Communication Network and Information Security Vol 12, No 2 (2020) pp. 162-167