Volume: Issue: Pages: (2017) ISSN: 0975-0290

# Pin Shuffling Authentication Scheme for Preventing Shoulder Surfing Attack

**P. Latchoumy**
Department of IT, B.S.Abdur Rahman Crescent Institute of Science and Technology, Chennai-48, India
Email: latchoumy@crescent.education
**G. Kavitha**
Department of IT, B.S.Abdur Rahman Crescent Institute of Science and Technology, Chennai-48, India
Email: gkavitha@crescent.education

----------**ABSTRACT**----------

**In the current ATM process, a significant number of ATM frauds and thefts are occurring, particularly shoulder-surfing attacks. To prevent such attacks, the Shuffling PIN Authentication Scheme is proposed, which operates on touch display screen devices. This scheme employs the technique of displaying two keypads with different digit arrangements: one keypad is closer to the user in which the user can enter their PIN value comfortably and another keypad can be kept far away for the attacker, where an attacker observing the PIN value from a distance making it hard to predict the pressed digits. Whenever the user can enter their PIN value, the keypad is shuffled with new generated PIN. Additionally, the scheme implements a color keypad mechanism for OTP authentication, further enhancing user security. Thus, the Shuffling PIN authentication scheme and color keypad for OTP authentication are proposed to prevent shoulder-surfing attacks in ATM transactions.**

Keywords – **ATM Transactions, Color Keypad, OTP Authentication, PIN Shuffling, Shoulder Surfing Attack**

Date of Submission: Date of Acceptance:

## I. INTRODUCTION

ATM frauds have become increasingly common in today's world, necessitating the development of robust authentication schemes [1, 3, 9-11]. User authentication can be performed in various ways, and this paper focuses on PIN authentication due to its simplicity and maturity. A PIN (Personal Identification Number) is a 4 to 6 digits' number and it is easily guessed by the attacker by shoulder surfing.

Shoulder-surfing is process of overhearing the personal information of the user. For example, someone waiting in line behind a person at an ATM might look over their shoulder to see their PIN. In such cases, the attacker observes the individual directly. Alternatively, the attacker can get the user's personal information remotely by using some recording devices [5-7].

There is a necessity for the PIN authentication mechanism can meet user needs if it increases its resistance to shoulder-surfing without significantly impacting usability. The proposed work, the Shuffling PIN Authentication Scheme aims to prevent shoulder-surfing attacks, which operates on touch display screen devices. This scheme employs the technique of displaying two keypads with different digit arrangements: one keypad is closer to the user in which the user can enter their PIN value comfortably and another keypad can be kept far away for the attacker, where an attacker observing the PIN value from a distance. Whenever the user can enter their PIN value, the keypad is shuffled with new generated PIN, making it hard to predict the pressed digits.

The scope of the proposed scheme includes:

- The Shuffling PIN process is intended for individuals requiring higher security to prevent shoulder-surfing attacks (e.g., ATM machines).
- OTP generation in this scheme is more secure and protects users from attackers.

The remaining of the paper is structured as follows: In Section 2, a brief review of the challenges and PIN shuffling authentication methods has been discussed to motivate the proposed scheme. Section 3 explains the proposed PIN Shuffling Authentication System to resist the Shoulder-Surfing attack and in Section 4 the implementation of the proposed scheme and the experimental results are elaborated. Finally, Section 5 summarizes the findings and outlines future work.

## II. RELATED WORK

Volker Roth, Kai Richter, and Rene Freidinger have discussed the vulnerabilities of magnetic stripe cards used in electronic payment systems [13]. Magnetic cards are commonly used for money withdrawals in ATM. The attacker can be pickpocketing these cards easily. PINs are

often obtained through shoulder-surfing or hidden cameras [8]. In this paper, cognitive trapdoor games PIN entry methods are introduced. These methods complicate the process significantly to obtain PINs by the attackers, even if the attackers fully observe all the process of the PIN entry and PIN value using cameras.

Peipei Shi, Bo Zhu, and Amr Youssef proposed a spin wheel-like PIN authentication scheme to prevent the shoulder-surfing attacks [14]**.** In general, magnetic cards and PINs are mainly used for authentication in ATMs. Cards are easily pickpocketing and PINs are easily captured by the hidden cameras by the criminals. Once both authentication factors are acquired, criminals can easily access user accounts, posing a high security risk. To prevent such attacks, the authors proposed PIN entry scheme using spin wheel. This scheme is resist the shoulder surfing even the attacker gets the information from the recorded device. The two performance metrics such as security and usability have been achieved considerably.

Muhammad Salman, Yang Li, and Jian Wang proposed a new scheme with the graphical method to prevent the shoulder-surfing attacks [15]. The new scheme, indirect PIN entry method is introduced which involves a sliding mechanism to prevent attackers from easily obtaining the PIN value.

Athanasios Papadopoulos, Toan Nguyen, EmreDurmus, and Nasir Memon introduced a new authentication scheme using Illusion PIN to prevent shoulder-surfing attacks [16]. The Illusion PIN method has two keypads with different digit arrangements: one keypad is closer to the user in which the user can enter their PIN value comfortably and another keypad can be kept far away for the attacker, where an attacker observing the PIN value from a distance making it hard to predict the pressed digits. Additionally, the study evaluated the method that cannot capture the information form the keypad.

Divyapriya and Prabhu proposed the strategy for Digital Validation of touch screen devices [17]. This strategy is used for Digital Validation of touch screen devices. The utilizations of touch screen devices incorporate ATM machines, Smart telephones [2,4]. Shoulder Surfing attack experiences different issues, Challenges and constraints like security and protection. This proposed technique using Illusion-pin (I-pin) mixes of two keypads with various requesting digits using hybrid images. This technique is used to limit the shoulder Surfing attack by actualizing this perceivability algorithm. Thus, attackers can't find or predict the user pin which gives greater security and validation.

Farid Binbeshr a c, M.L. Mat Kiah a, Lip Yee Por a, A.A. Zaidan have reviewed different PIN-entry methods with its pros and cons [18]. Generally, the PIN-entry time is considered as an important quality metric for preventing shoulder surfing attacks. In this paper the authors argued that PIN-entry time is considered as an important criterion for usability w.r.t. shoulder-surfing attack.

Yogesh Mali, MahendraEknath Pawar, Abhijeet More, et al., have introduced the a novel method for preventing shoulder surfing attacks [19].In order to prevent the shoulder surfing attacks, the authors presented some guidelines for new method, that is framework based validation method for safety pin entry.

There are different algorithms and strategies have been proposed in the writing to defeat these challenges and still needs improvement. Hence, the proposed method implements a Shuffling PIN authentication scheme to prevent Shoulder surfing attacks during ATM transactions.

## III. PROPOSED WORK

Shoulder-surfing refers to the act of eavesdropping on private information of the user. Someone waiting in line behind a person at an ATM might look over their shoulder to get their private information such as PIN value (digits) and the attacker is physically close to the user. Alternatively, the attacker may get the PIN value from hidden cameras, to capture the user's PIN details. In general, some authentications schemes are attacked by some attacks such as brute force attack w.r.t. Shoulder- surfing. Generally, the PIN value has entered using fingerprints and visual data might be found easily by an attacker. Also, the PIN values are very short (minimum number of digits) compared to password, which is required, a full alphanumeric keyboard. Hence, Shoulder-surfing poses a significant threat or risk to PIN authentication specifically

### 3.1. Proposed Design

Whenever the user can enter their PIN value, the keypad is shuffled with new generated PIN, making it hard to guess the entered PIN value. The primary objective of our proposed system is to implement a PIN Shuffling scheme for preventing shoulder-surfing attacks. To achieve this, the new Shuffling PIN scheme using Fisher-Yates Shuffling Method is proposed and developed.

The overall architecture of the proposed system, PIN Shuffling Authentication Scheme for Shoulder Surfing Resistance is presented in the Fig 1.

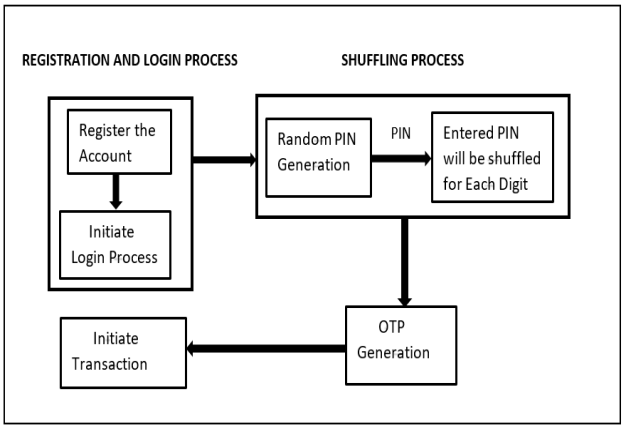


**Fig 1. PIN Shuffling Authentication Scheme for Shoulder Surfing Resistance**

Volume: Issue: Pages: (2017) ISSN: 0975-0290

### 3.2. Modules

There are four modules designed in this system. They are:

a) Account Registration and Login
b) Random PIN Generation using PRNG Algorithm
c) Shoulder Surfing Resistance using Fisher-Yates Shuffling Algorithm
d) OTP Generation and Secured Transaction Initiation

**a) Account Registration and Login**

- The user should register the account with some bank mandatory field. After the registration process is completed, the registered user account details will be stored securely.
- Then the user can able to login into the account.

**b) Random PIN Generation using PRNG Algorithm**

- After the user login process is done, the random PIN number will be generated for the respective user by using PRNG (Pseudo Random Number Generator) algorithm.
- The PIN number will be stored securely and the details such as username and PIN number will be displayed on the screen.

The PRNG algorithm is a strong algorithm due its strong and secured design. Hence, the attacker cannot able to predict the output because he cannot able to get the idea about the seed or the internal state value for getting the information about the future bits.

**c) Shoulder Surfing Resistance using Fisher-Yates Shuffling Algorithm**

- Fisher-Yates shuffling algorithm is used for shuffling process, when the user enter their respective generated PIN number in the shuffling keypad the keypad will be shuffled for every user attempts. After the PIN is entered it will verify the PIN number with the database that the entered PIN number is correct or wrong.

***Fisher-Yates Shuffling Method:***

The pseudo code for the Fisher-Yates Shuffling Method is shown in the Fig 2.

```
void shuffle_Array(String[] Ar)
 {
      // random number generation
  using random method
    Random Ran_No = new Random();

 for (int j = Ar_size-1; j > 0; j--)
  {
  Int Ar_index = Next_Ran_No(j + 1);

 // Swapping
  String A = Ar[Ar_index];
  Ar[Ar_index] = Ar[j];
  Ar[j] = A;
   }
  // shuffling method ends
```

**Fig 2. Fisher-Yates Shuffling Method**

- In this Fisher-Yates shuffling method, the last item is chosen from the given array elements for every single time. After choosing the last item it will pick random item from the remaining array elements.
- After picking the random item from the array it will be swapped with the selected last item in the array.

The proposed shuffling method is a strong authentication scheme, that is the generated and shuffled random number for PIN value making it difficult to predict the pressed PIN value by the attacker.

The running time of the Fisher-Yates Shuffling algorithm is O (n). Even though the pin entry time is increased due to shuffling, the security of the system is not compromised due randomized PIN value generation. Also security is strengthened by using color keypad. Hence, it is very difficult to get the pin entry value by the attacker and it makes the brute force attack is also difficult in this model.

***d) OTP Generation and Secured Transaction Initiaton***

- After the PIN verification process is done it will proceed to OTP generation.
- OTP will be generated and then it will be sent to the user's email.
- The generated OTP will be having 4 alphabets which refers the colors and also having location for the numbers that need to be entered in that particular specified location.
- Then the generated OTP has to be entered in color based keypad. After the OTP is entered correctly and it will be verified. And finally, the user can do the transaction after verification.

## IV. IMPLEMENTATION AND DISCUSSION OF THE RESULT

The proposed PIN shuffling authentication scheme is developed for preventing the shoulder surfing attack using shuffling algorithm. The proposed scheme suggests that it is very difficult to capture the PIN of the user when shuffling PIN and is used. Even though, the pin entry time is increased little bit for shuffling PIN value compared to Illusion PIN method [16], the proposed scheme provides more security using shuffled PIN and color keypad.

The various processes of the proposed system, "PIN Shuffling Authentication System for Shoulder Surfing Resistance scheme" are implemented using JAVA/J2EE language, MYSQL database and Netbeans IDE.

The description of each process is explained below.

**a) Account Registration and Login**

The Account registration process is presented in the Fig 3.

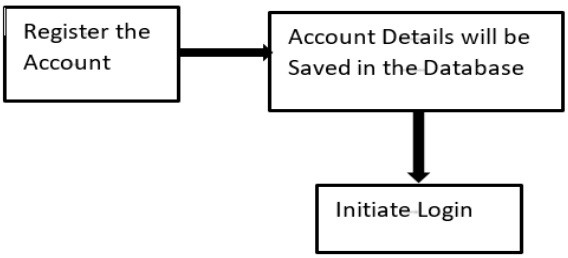


**Fig 3. Account Registration**

- In this process, the user has been created an account by filling few necessary fields in the given form required by the bank. These fields will be used in subsequent processes.
- This form acts as a privilege form, enabling the account holder to access various bank services.
- The user after registering their account information it will be updated and stored in the database securely.
- Account Details can be retrieved from Database for later use.

### b) Random PIN Generation using PRNG Algorithm

The process of Random Pin Generation Using PRNG Algorithm is shown in Fig 4.

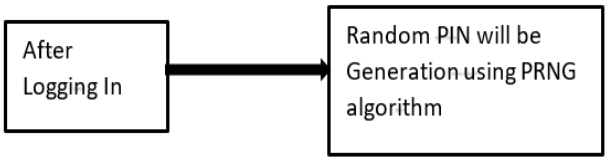


**Fig 4. Random PIN generation using PRNG algorithm**

In this module, a random PIN will be generated for the user after completing the registration process, and it will be sent to the user's email.

- A new random PIN will be generated for each login using PRNG algorithm.
- The random generation of PINs will enhance the security level of this project.
- PRNG algorithm generates a series of many random numbers with minimum time and it will generate the number if the beginning point in the series is well-known.
- This process begins with an n-digit seed number x0.
- And obtain a 2n-digit number by squaring the number
- Find the next random number by taking the middle n digits and repeat the process.
- Numbers generated can be scaled to any interval through multiplication or addition. The working of PRNG algorithm is shown in Fig 5.

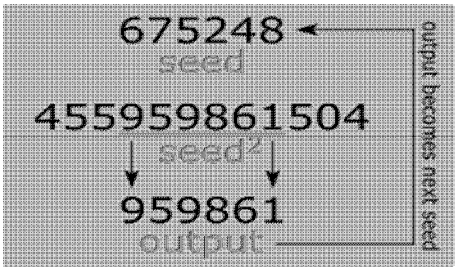


**Fig 5. Working of PRNG**

The interface for secured PIN entries and User PIN generation are developed using Java Applet and are shown in Fig 6 and Fig 7.

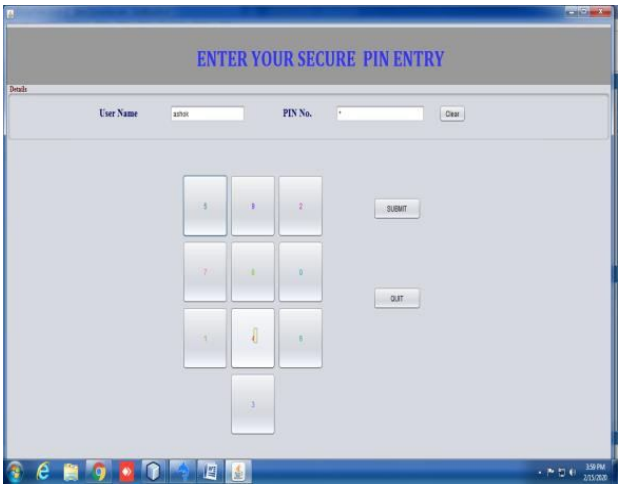


**Fig 6. Secured PIN Entries**

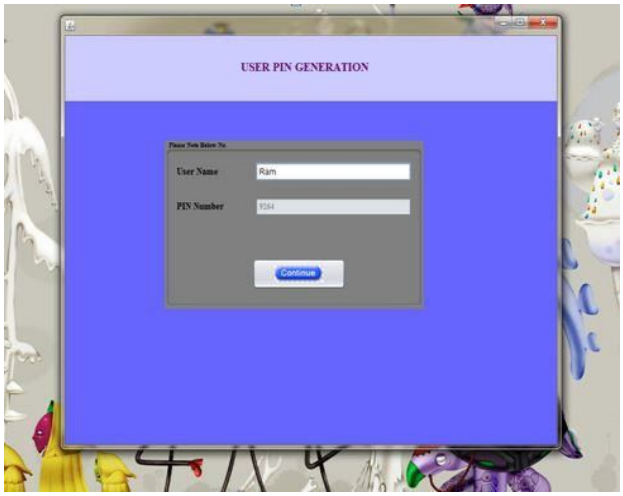


**Fig 7. User PIN Generation**

### *c) Shoulder Surfing Resistance using Fisher–Yates Shuffling Algorithm*

The process of Shoulder Surfing Resistance Using Fisher–Yates Shuffling Algorithm is shown in the Fig 8.

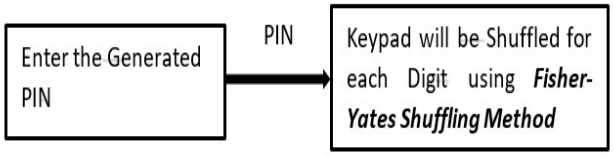


**Fig 8. Fisher-Yates Shuffling Process**

- In this module, the user will enter their PIN number in shuffling keypad, and this scheme provides the dynamically changed PIN so that the hacker can't guess the number easily.
- For every user attempt keypad will be shuffled by using Fisher-Yates shuffling algorithm.
- This process will be on loop until all the array elements have been successfully swapped with the other remaining given array.

The sample Input (Fig 9) and sample output (Fig 10) are shown below.

| 10 | 20 | 30 | 40 | 50 | 60 | 70 | 80 | 90 |
|---|---|---|---|---|---|---|---|---|

**Fig 9. PIN values before Fisher-Yates Shuffling Process**

| 20 | 80 | 40 | 70 | 50 | 10 | 30 | 90 | 60 |
|---|---|---|---|---|---|---|---|---|

**Fig 10. PIN values after Fisher-Yates Shuffling Process**

### *d) OTP Generation & Secured Transaction Initiation*

The process of OTP Generation & Secured Transaction Initiation is shown in Fig 11.

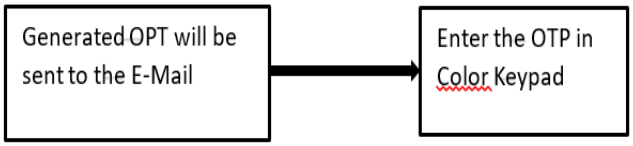


**Fig 11. OTP Generation and Secured Transaction Initiation**

- One Time Password will be generated randomly and the generated number will be forwarded to the user's mail id.
- We are also proposing color keypad; the generated OTP will be in Alphabets which refers the color.
- OTP will be sent to mail with random alphabets with Location (L- Left, M- Middle, R-Right).
- Color pad has three numbers.
- Random generated Alphabets first letter refers to the color pad of the virtual keyboard.
- Numbers in color pad can be located using Location which is sent in mail.
- After the OTP verification process is done, the secured transaction has been initiated.

The interfaces for secured OTP generation, Color keypad, PIN verification and secured transaction are developed using Java Applet are shown in Fig 12 to Fig 16.


**Fig 12. Secured OTP Generation**

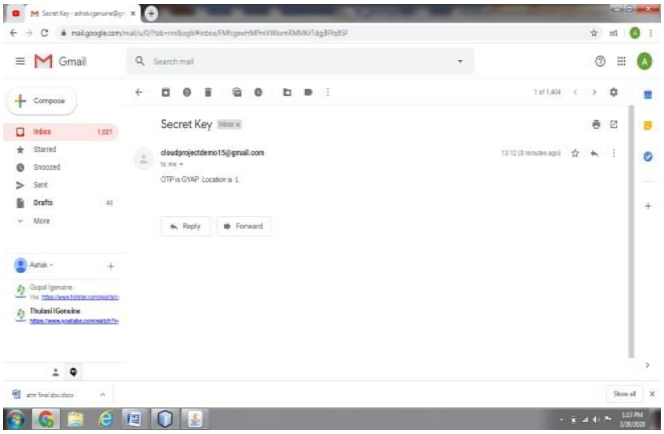


**Fig 13. OTP Sent to e-mail**

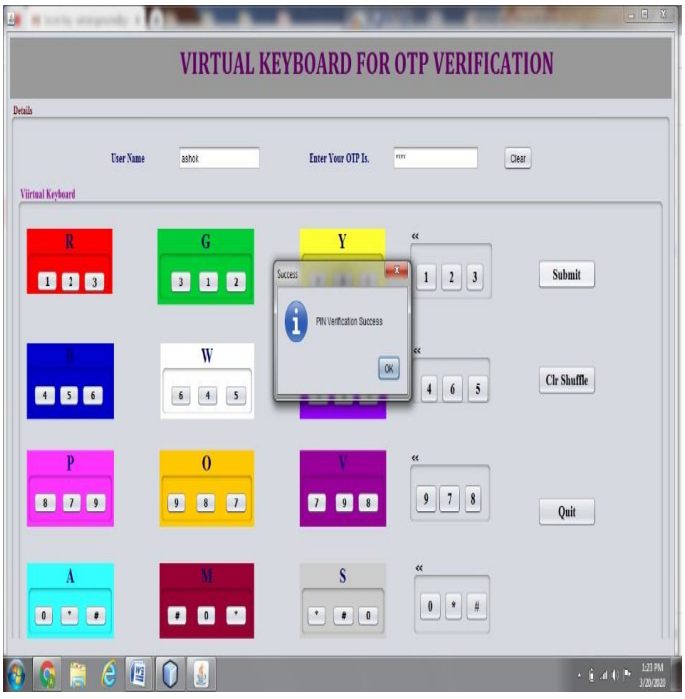


**Fig 14. Color Keypad**

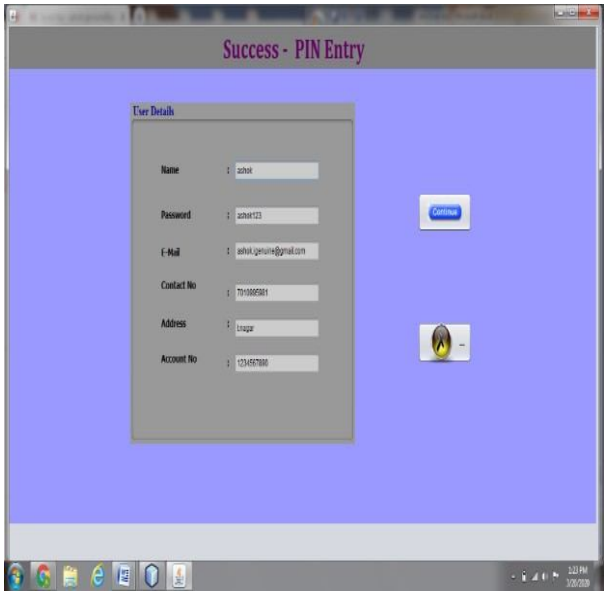


**Fig 15. Verification of PIN Entry**

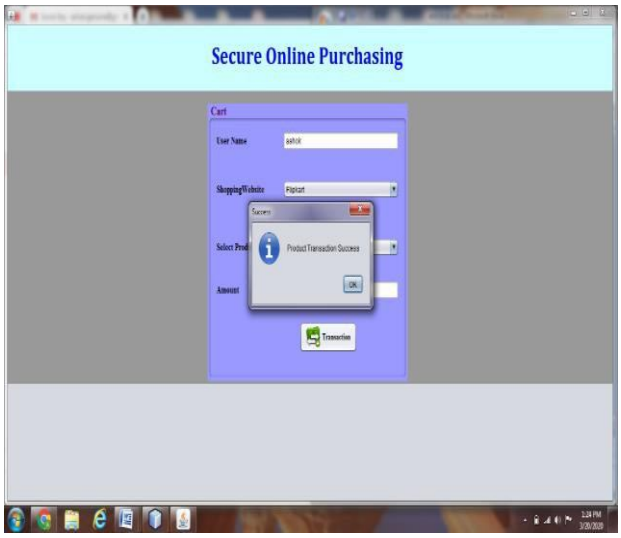


**Fig 16. Secured Online Transaction**

## V. CONCLUSION

This paper introduced and designed an authentication scheme for preventing shoulder-surfing attacks using dynamic PIN shuffling method. The proposed work discussed the vulnerabilities of current authentication schemes to shoulder-surfing and proposed the Shuffling PIN Authentication Scheme as a solution. The proposed method employs the technique of displaying two different keypads with dissimilar digit arrangements. One keypad for user and another keypad for the attacker. The user entering their PIN easily in the keypad which is closer to them and the attacker observing the different keypad from a distance. The configuration of the user's keypad is shuffled each time a PIN is entered, preventing the attacker from predicting the pressed digits. Additionally, the scheme incorporated a color keypad mechanism for OTP authentication, further enhancing security. Hence, the proposed Shuffling PIN authentication scheme, combined with the color keypad for OTP is used to prevent shoulder-surfing attacks in ATM transactions. Future enhancements will focus on other attacks like key logger, skimming and thermal attacks and improving reliability and speed by providing more robust authentication options for users to make it more reliable and faster by providing more authentications for the users.

## ACKNOWLEDGEMENTS

We thank A. Mohamed Afzal Kasim and A. Abdul Haleem, B.Tech.(IT) Students of the Department of Information Technology at B.S. Abdur Rahman Crescent Institute of Science and Technology for their assistance. Currently both are working in the reputed IT industry.

## REFERENCES

[1] 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, pp. 553–567, May 2012, DOI 10.1109/SP.2012.44.

[2] 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, pp. 4806–4817, 2016, https://doi.org/10.1145/2858036.2858267.

[3] J. Bonneau, S. Preibusch, and R. Anderson, "A birthday presents 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, pp. 25–40, 2012.

[4] 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, pp. 213–230, 2014.

[5] 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, DOI: 10.1109/TSMC.2013.2270227

[6] M. Lee, "Security notions and advanced method for human shoulder surfing resistant pin-entry," IEEE Transactions on Information Forensics and Security, vol. 9, no. 4, pp. 695–708, April 2014, DOI: 10.1109/TIFS.2014.2307671

[7] 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 Proceedings of the Fifth International Conference on Tangible, Embedded, and Embodied Interaction, ser. TEI '11. New York, NY, USA: ACM, pp. 197–200, 2011, https://doi.org/10.1145/1935701.1935740

[8] 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, Sep. 2012, https://doi.org/10.1016/j.intcom.2012.06.005

[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, pp. 314–319, 2010, DOI: 10.1007/978-3-642-14064-8_45

[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, pp. 183–192, 2008, https://doi.org/10.1145/1357054.1357085

[11] A. De Luca, E. von Zezschwitz, and H. Hussmann, "Vibrapass: Secure authentication based on shared lies," in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ser. CHI '09. New York, NY, USA: ACM, pp. 913–916, 2009, https://doi.org/10.1145/1518701.1518840

[12] A. Bianchi, I. Oakley, J. K. Lee, and D. S. Kwon, "The haptic wheel: Design & evaluation of a tactile password system," in CHI '10 Extended Abstracts on Human Factors in Computing Systems, ser. CHI EA '10. New York, NY, USA: ACM, pp. 3625–3630, 2010, https://doi.org/10.1145/1753846.1754029

[13] V. Roth, K. Richter, and R. Freidinger, "A pin-entry method resilient against shoulder surfing," in Proceedings of the 11th ACM Conference on Computer and Communications Security, ser. CCS '04. New York, NY, USA: ACM, pp. 236–245, 2004, https://doi.org/10.1145/1030083.1030116

[14] P. Shi, B. Zhu, and A. M. Youssef, "A rotary pin entry scheme resilient to shoulder-surfing," 2009 International Conference for Internet Technology and Secured Transactions, (ICITST), pp. 1–7, 2009, DOI: 10.1109/ICITST.2009.5402625

[15] Muhammad Salman, Yang Li, and Jian Wang, "A Graphical PIN Entry System with Shoulder Surfing Resistance" IEEE 4th International Conference on Signal and Image Processing, pp. 203-207, 2019, DOI: 10.1109/SIPROCESS.2019.8868388

[16] Athanasios Papadopoulos, Toan Nguyen, EmreDurmus, "Illusion PIN: Shoulder-Surfing Resistant Authentication Using Hybrid Images" IEEE Transaction on Information Forensics and Security, pp. 1-14, 2017, DOI:10.1109/TIFS.2017.2725199

[17] K. Divyapriya, P. Prabhu, "Image Based Authentication Using Illusion Pin for Shoulder Surfing Attack", International Journal of Pure and Applied Mathematics, Volume 119, No. 7, pp. 835-840, 2018, DOI:10.20894/IJCOA.101.007.001.009

[18] Farid Binbeshr a c, M.L. Mat Kiah a, Lip Yee Por a, A.A. Zaidan b, "A systematic review of PIN-entry methods resistant to shoulder-surfing attacks", Computers & Security, Elsevier, Volume 101, 102116, 2021, https://doi.org/10.1016/j.cose.2020.102116

[19] Yogesh Mali, MahendraEknath Pawar, Abhijeet More, "Improved Pin Entry Method to Prevent Shoulder Surfing Attacks", 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), IEEE, 2023. DOI:10.1109/ICCCNT56998.2023.10306875

**Biographies and Photographs**

*Dr. P. Latchoumy* is working as an Associate Professor in the Department of Information Technology at B. S. Abdur Rahman Crescent Institute of Science and Technology, Chennai. With 26 years of teaching experience, she has a profound impact on her students and the academic community. She holds a B.Tech. in Computer Science and Engineering (CSE) from Pondicherry University and an M.Tech. in CSE from Anna University and earned her Ph.D. in "Fault Tolerant Resource Management in Computational Grid". She has published more than 25 research papers in national and international journals and conferences and her areas of interest include Cloud Computing, Networks, Artificial Intelligence & Machine Learning, Data Science, and Deep Learning.

Dr.G. Kavitha is presently working as a Professor in the Department of Information Technology, B.S.A. Crescent Institute of Science & Technology. She obtained her Master's Degree in Computer Science and Engineering from Madras University in 2002 and Doctor of Philosophy in Faculty of Information and communication, Anna University in 2013. She has published more than 26 papers in refereed International Journals, 20 papers in International Conferences and 7 book chapters. She has handled courses on Data Structures and Algorithms, Computer Architecture, Cloud Computing, Wireless Networks, Artificial Intelligence, Machine learning for both UG and PG Programmes. Her research interests focus on Grid and Cloud Computing, Wireless Sensor Networks and Artificial Intelligence.

Volume: Issue: Pages: (2017) ISSN: 0975-0290