Shuffled Illusion PIN Framework to Prevent Shoulder – Surfing

M. Kavitha, D. Hari Haran, P. Meenan, J. Likhitha Priya

Abstract*: Shoulder surfing is a kind of technique applied to sneak the personal data like passwords and some confidential data of the user. For this type of attacks there is no need of any kind of technical knowledge but just a keen observation towards the user performance is necessary. However, secret gadgets made these shoulder surfing easy for the attackers like cc cams. To overcome these attacks some authentication schemes are proposed- Illusion pin that works on digital display. It applies the method of hybrid pictures with 2 keypads blended one keypad with another, it is designed by using the human visibility and quotes the least distance at which an attacker is incapable to understand the buttons. We developed an innovative shuffling algorithm for shuffling the keys for every single pin entry. Using this Shuffling algorithm, we create a new pattern of the keypad for every exclusive entry of the pin. Through this technique the attacker is unable to track the pin even if he remembers the spatial arrangement of the digits in a keypad. To provide more security we are adding one-time password generating (OTP) technique.

***Keywords:* Hybrid Images, Illusion Pin, OTP, Shuffling Algorithm, Shoulder Surfing.**

I. INTRODUCTION

The internet is yet creating and online undertaking is on its encouraging. The noteworthy advancement of Internet has included various wonderful things like computerized business, email, straightforward access to gigantic stores of reference material, etc. PC hacking is the demonstration of adjusting pc devices and programming to obtain an objective outside of the producer's one of a kind reason [3], [21].

At present we are observing ATM misrepresentation Malevolent cash exchange and robbery are occurs by methods for absence of security assurance in current plan. Shoulder surfing is the usage of direct observation techniques, to get records barring the commentary of the user. Shoulder surfing should likewise be possible protracted separation with the asset of binoculars or other vision-improving gadgets.

Shoulder surfing is a kind of social building technique used to get information, for example, non-open recognizable number as password and other private facts through searching over the victim's shoulder. This attack can be performed at close range by at once searching over the victim's shoulder. To enforce this approach attackers, do no longer require any technical abilities and eager commentary of victim's surroundings.

Crowded locations are the more likely areas for an attacker fascinated to shoulder surfing the victim. However, the creation of modern-days technologies like hidden cameras and secret microphones makes shoulder surfing less complicated and offers greater scope for the attacker to operate shoulder surfing. A hidden digital camera permits the attacker to seize total login system and other personal data of the victim, which subsequently ought to lead to monetary loss or identity theft [1].

Authentication factors which are not flexible to observation are inclined to shoulder-surfing. It consists of mainly three types i.e., first type which consists of passwords, personal identification numbers, code words, puzzle handshakes and the subsequent sort incorporates something we have like physical things, for instance, keys, propelled cell phones, crafty cards, USB drives, and token devices and the third kind involves something we look like any bit of the human body that can be shown for check, for instance, fingerprints, palm analyzing, facial affirmation, retina channels, iris breadths, and voice affirmation.

Stick verification is regularly performed in jam-pressed spots, e.g., when any individual is opening client cell phone on the road or in the metro. Shoulder-surfing is supported in such conditions as it is simpler for an aggressor to be shut down while avoiding the scrutiny of the user. IPIN's digital keypad consists of two one-of- a-kind digit ordering keypads, combined in a mixture image. The authors in [16], [17], [22] discusses how to enhance visibility of images by using deep learning techniques

The person on the screen can see an actual Using keypad, but a potential attacker scanning the screen from a wider distance can only see the other keypad. Advantages include remote control, time saving, space saving, user-friendly and touch screen phones [2], [15].

The shuffling keypad technique is implemented for providing more security during the pin entry. With this we provide a new ordering of the digits in the keypad after every respective digit entered.

Manuscript published on November 30, 2019.
* Correspondence Author

M. Kavitha*, Assistant Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India.

D. Hari Haran, Student, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India.

P. Meenan, Student, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India.

J. Likhitha Priya, Student, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India.

So, by using this kind of approach we can avoid the attack which is performed by remembering the spatial course of action of the keypad digits. Some existed security mechanisms and frameworks of various applications we studied in [11]-[14]. The sentiment analysis, data management and processing algorithms are discussed by several authors are studied from [18]-[20] papers.

We are discussing the remaining part of this article as section 2 for existing work, section 3 for proposed work, section 4 for implementation, section 5 for result analysis and concludes the article work in section 6 along with future work specification.

II. EXISTING WORK

Shoulder Surfing is the common attack at public places specially and these attacks are increasing day to day. So many researchers gone through this problem and proposes solutions by using diversity of technologies.

In [4], the authors proposed a novel confirmation framework as Pass Matrix dependent on graphical passwords. It has one-time login and circulates a kind of vertical and horizontal bars which makes the pass-images invisible. So, the attackers are unable to capture the credentials even by using multiple cameras during the attack.

In [5], the author's uses tictoc stick passage technique with a Scheme 'Turning flywheel PIN Entry'. In this the customer will utilize the digits as stick. While entering pin, four color buttons will be used instead of digits. While using this method in mobile apps or in ATM transactions no need of analytical or logical burden over the users.

In [6], the authors discuss an integrated shoulder surfing authentication scheme to avoid the risk of password stealing by attackers at public places like ATM machines by using shoulder surfing defense feature of click point graphical password approach.

In [7], the authors discuss an authentication scheme to support two distinguishable modes as learning and recognition mode. Here the attached touch screen device is used to enter the pin, and this is not visible to the attacker who is observing the screen at user end.

In [8], the author discusses a confirmation conspire where VpointsPES, can be embraced in different client frameworks, including cloud verification frameworks. Here VpointsPES utilizes 8-digit PINs, it very well may be stretched out to utilizing PINs with discretionary length. By using Localized Tactile Feedback, the usability has been suggestively improved. VpointsPES provides enough protection and usability.

In [9], the author talks about an adaptable shoulder surfing safe literary equation based secret key confirmation framework which flawlessly joins the printed secret key and recipe to create an irregular secret key.

In [10], the author proposed a new authentication scheme by using an augmented misinformation and key-based existing techniques for both mobile and personal computers. By using camera recorder, it improves the security against attacks.

Problem Statement:

In current ATM process there is part of ATM extortion Malicious cash exchange and burglary are occurred by methods for absence of security assurance in current plan. Not only ATM machines even in offices while entering passwords or even in homes also. So many researchers are currently addressing this issue by proposing various authentication schemes. So, providing security to the personal information while doing transactions is a one of the current research problems. Due to advanced sensing gadgets in the market hacking PIN at ATM machine is very easy now a day. In this connection, we focus on the challenge of shoulder-surfing incidents with an innovative verification scheme by using two keypads visibility and shuffling methodology. Here we proposed the idea of ATM security incorporating rearranging console with OTP validation.

III. PROPOSED SYSTEM

Shoulder surfing is one of the most common attack which is more likely to occur in crowded places because of uncovering private content and may leads to leakage of sensitive information of the user. For such type of attacks there is no need of any technical knowledge, just a keen observation towards the user performance is necessary to attack. Many researchers are working on this issue.

In this connection we come up with some sort of solution for this type of attacks. We developed an innovative shuffling algorithm which is used to shuffle the keypad for every exclusive entry of the pin. When the pin is entered on the keypad, then the keys are shuffled for the next entry of the pin. The keys are shuffled in such a way that the attacker is unable to track the credentials of the user depending upon the spatial arrangement of the keys or the usual digit orderings. By this approach we can provide security for the user to some extent.

Shuffling algorithm receives an input as 0 to 9 digits in an array. A random method has been called to generate a random number every time and swapping of elements is done in this process. Random digit creation algorithm is utilized to produce the one-time passwords while doing transaction. By using shuffling algorithms, the digits positions in the pads are changes randomly.

We address the issue of shoulder-surfing ambushes at ATM machines on verification conspires by proposing an inventive PIN-based validation strategy that works with respect to touch screen gadgets. This plan utilizes 2 keypads with various digit arrangements in such a manner, that the client who is near the gadget can see two keypads however the attacker the assailant who is staring at the device from faraway is able to see only front keypad. The client's touch screen is rearranged in each verification endeavor. So, the attacker is incapable to track the pin even he may remember the spatial game plan of the squeezed digits.

The virtual keypad of PIN is made from 2 keypads with various digit collections, mixed in a solitary cross breed picture. The client who is near the screen can see and utilize one keypad, yet a potential aggressor who is taking a gander at the screen from a greater separation, can see just the other keypad.

We built up a calculation to appraise whether the client's keypad is noticeable to an eyewitness at a given survey position. We tried the evaluated perceivability of Illusion PIN through a client investigation of reproduced shoulder-surfing assaults on cell phone gadgets. We assessed the base good ways from which a camera can't catch the visual data from the client's keypad.

The outcomes show that it is for all intents and purposes practically incomprehensible for an observation camera to catch the PIN of a cell phone client when proposed PIN conspire is being used. Random generation algorithm is used to generate one-time password (OTP) which is send to our email or phone number, we can use this OTP for amount transaction in ATM, petrol bank, shopping mall and so on in public place. This technique will enhance the protection mechanism while withdrawal of money from ATM and other process. The proposed system architecture is shown in figure 1.

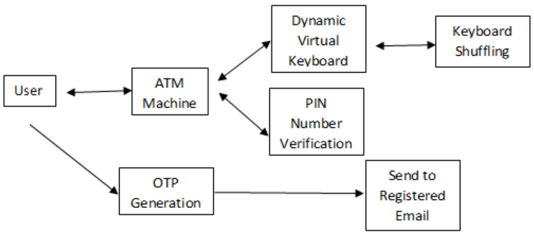

Fig.1. Architecture of proposed method

- Ease to use- the proposed method will be usable anyplace and whenever with a low blunder rate just as a quicker confirmation result.
- Less training- the framework will give clients a straightforward and takes less time to learn.
- The best utilization of human memory- the proposed plan will profit by the contention that individuals are better in perceiving pictures. Along these lines, pass pictures ought to be anything but difficult to recollect.
- Secure- the framework will give a solid line of barrier against shoulder surfing beast power, crossing point and taught surmise attacks.

IV. IMPLEMENTATION

While doing the transactions the users' needs to enter personal identification number (PIN). Generally, PINs are short and require only a little numeric keypad rather than the usual alphanumeric keyboard. While entering the PIN the attackers who are with us or back side are trying to track the PIN to do fraud malicious money transactions. That means shoulder-surfing attacks are common now a day. To prevent this type of common attacks we are implementing an innovative pin-based authentication scheme.

The perceivability calculation gets as information sources a half and half keypad I and a survey position N in the 3D space. It returns a double forecast on whether the client's keypad of I is obvious to an onlooker who is in position N. We utilize this forecast either to gauge the base security separation that compares to a given crossover keypad, or to make a half breed keypad that regards a given wellbeing separation.

we figure the visibility index which evaluates how obvious the client's keypad of I from the audit position N is. Limit Value of the Visibility Index: Let's acknowledge that we are given a combined keypad I and a spectator who first perspectives I from position N1 and afterward from position N2. If the comparing perceivability file esteems are v1 and v2 and holds v2 > v1, we anticipate that the client's keypad should be more subtle from position N2 than from N1. On the off chance that v1 ' v2, we foresee that the customer's keypad ought to be comparably recognizable in the two cases.

It is an immediate outcome of the path, we characterized perceivability file. Presently we should accept that two diverse half and half keypads I1 and I2 are seen by a similar spectator from positions N1 and N2, separately. If v2 > v1, we expect the client's keypads of I1 to be more obviously unmistakable than that of I2. This is the primary supposition that we make about the conduct of the perceivability list and we hope to hold in its turn around structure as well.

For implementation, we used Net Beans IDE 8.2 a java based integrated development environment. We created our modules using HTML to design front end pages like home page, login page, registration page, JSP for server programing and MySQL to create database for client data storage.

For every new user the registration is required so we created a home page by using HTML in proposed application. Here the user needs to enter his/her personal information like first name, last name, mail address, username and password. After filling all the fields in page, the client must click on submit button for successful registration. If the user is already having an account, no need of registration. After the successful registration the data is sent and stored to the database.

The user has to login to the application by entering the credentials like username and password which are generated in registration step. If the username and password of the user is valid the server opens a new interface which is an authentication step for the user to enter the pin. The interface looks like a digital keypad with 9 digits.

The keypad follows same mechanism as hybrid image. In hybrid image technique the user can identify the shaded digit that appears in the backside of each digit in a foreground keypad. If we press the digit on front keypad it will show the other digit which is exactly backside of pressed digit for the conformation of user. That means another keypad is present at the backside of original keypad which is called as blended keypad. Likewise, the user can enter the pin.

If the user wants to do another transaction, he has to login to the application again. No user gets another keypad. That means the user gets shuffled keypad. The shuffled keypad is generated automatically by using randomized programming technique for each new transaction. That means this technique changes the positions of digits in keypad randomly.

Due to this shuffled technique we are possible to avoid utmost shoulder surfing attacks because the impact of the continuous blended keypad shuffling the attacker is unable to track the pin positions. That means the proposed framework provides more security for the user's credentials. By adding the existing OTP generating techniques the proposed framework will generate OTP for more security purpose.

V. RESULT AND DISCUSSION

To demonstrate the proposed framework, we are designing a prototype. If we see the insights of the home page module which contains registration and login options. The new user must create an account to use the application by entering all the mandatory fields in registration page as shown in figure 1. This page consists of personal information like name, email and password.

The user credentials are stored at server after successful registration. If the user has necessary credentials, he can login into the application by login page. The outline of the login page is shown in figure 2.

After validating the credentials, the server opens an interface of the required keypad to enter the pin by the user.

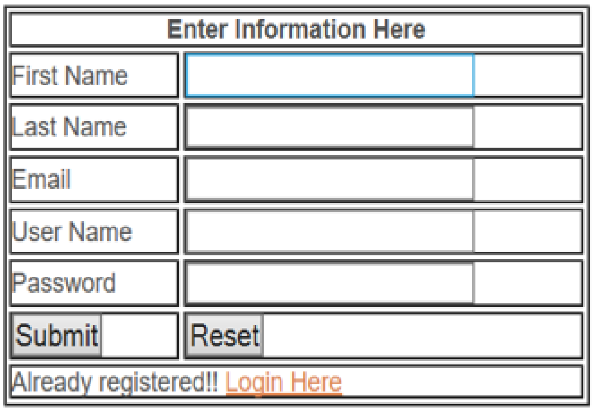

Fig.2. Registration Module

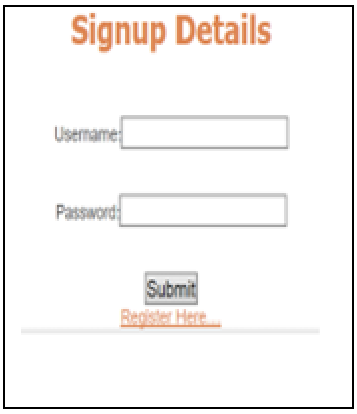

Fig.3. Login Page

The pin entry environment has a combination of two keypads. The client can see both the keypads present backside of one another. The front keypad has the digits in bold format and the background keypad has the digits in the shaded format. The client can enter the pin as per background keypad that means by looking at shaded digits of the keypad, he/her can enter the required pin.

For the comfort of old persons, we are displaying the digit he/her entered then the user can easily validate the pin by confirming. Due to shaded format of digits the keypad is not visible to the attacker is and he can only observe or watch the front keypad and the keypads are shuffled for every new transaction randomly. The keypad shuffling mechanism uses simple randomization technique to generate new keypad. By observing the results shown in the figure 3 we can identify how the proposed system works. The figure 3 shows two images of the keypad used for two different transactions done by the client. If we observe the keypads, we came to know that the digits in the keypad are shuffled randomly.

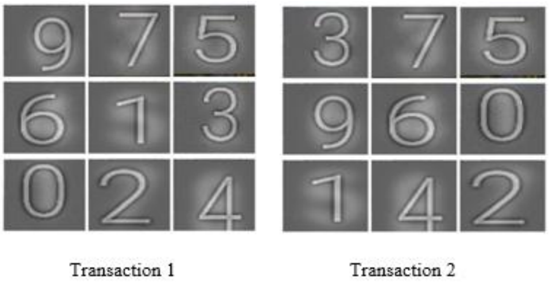

Fig. 3 Keypads of two different transactions

For shuffling the shuffling algorithm work by calling simple random position generation code. The positions of digits in a keypad are changed randomly. After entering the valid pin, the OTP mechanism is used to confirm the transaction from client end. The OTP mechanism will support the proposed work to show better result.

VI. CONCLUSION

The shuffling keypad approach is an alternative authentication system, which can be based on the rearrangement of the keys in the keypad. It has been developed to make the user comfortable and secure during the pin entry and save from attacks. This technique can enhance the security of the system since the keypad randomizes every single time when the user enters the pin to the system. Moreover, shuffled image can be beneficial in order to make more complex for the attacker.

FUTURE WORK

We can develop Progressive Authentication Systems to improve Security for the Module. Adding one-time password via phone call for more secure processing and reliable support can enhance the system.

REFERENCES

1. Prabhu, K. D. D. P. "Image based authentication using illusion pin for shoulder surfing attack." Int. J. Pure Appl. Math 119.7 (2018): 835-840.
2. Papadopoulos, Athanasios, et al. "Illusion pin: Shoulder-surfing resistant authentication using hybrid images." IEEE Transactions on Information Forensics and Security 12.12 (2017): 2875-2889.
3. Kumar.et.al., "Hacking attacks, methods, techniques and their protection measures." International Journal of Advance Research in Computer Science and Management, 4 (4) (2018).
4. Sun, Hung-Min, et al. "A shoulder surfing resistant graphical authentication system." IEEE Transactions on Dependable and Secure Computing 15.2 (2016): 180-193.
5. Kasat, Ojaswi K., and Umesh S. Bhadade. "Revolving flywheel PIN entry method to prevent shoulder surfing attacks." 2018 3rd International Conference for Convergence in Technology (I2CT). IEEE, 2018.
6. Sruthi, P. V. "CRASH—Cued recall authentication resistant to shoulder surfing attack." 2015 Online International Conference on Green Engineering and Technologies (IC-GET). IEEE, 2015.
7. Vaidya, Siddhesh Ashok, and Varsha Bhosale. "Invisible touch screen-based pin authentication to prevent shoulder surfing." 2016 International Conference on Inventive Computation Technologies (ICICT). Vol. 2. IEEE, 2016.
8. Ku, Wei-Chi, and Hao-Jun Xu. "Efficient Shoulder Surfing Resistant PIN Authentication Scheme Based on Localized Tactile Feedback." 2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom). IEEE, 2019.
9. Shakir, Muhammad, and Abdul Ayaz Khan. "S3TFPAS: Scalable shoulder surfing resistant textual-formula base password authentication system." 2010 3rd International Conference on Computer Science and Information Technology. Vol. 8. IEEE, 2010.
10. Dib, Ahmed, and Sabri Ghazi. "Anti-Shoulder Surfing Login Based on Multi-Entry Models on Onscreen Keyboard." 2019 International Conference on Networking and Advanced Systems (ICNAS). IEEE, 2019.
11. Kavitha, M., Manideep, Y., Vamsi Krishna, M., & Prabhuram, P. (2018). Speech controlled home mechanization framework using android gadgets. International Journal of Engineering and Technology (UAE), 7(1.1), 655-659.
12. K Sai Prasanthi et.al.," Hybrid approach for securing the IoT devices." 2019 International Journal of Innovative Technology and Exploring Engineering. Vol. 8(4), 2019.

13. Modepalli Kavitha, Singaraju Srinivasulu, Kancharla Savitri, P. Sameera Afroze, P. Akhil Venkata Sai, S. Asrith l. (2019). "Garbage bin monitoring and management system using GSM." International Journal of Innovative and Exploring Engineering 8(7),pp. 2632-2636.
14. K Sai Prasanthi et.al.,"Survey on secure protocols for data sharing through edge of cloud assisted internet of things." International Journal of Engineering and Technology (UAE)., Vol. 8(2), 2018.
15. M. Kavitha, K Anvesh, P Arun Kumar, P Sravani . (2019). "IoT based home intrusion detection system." International Journal of Recent Technology and Engineering 7(6),pp. 694-698.
16. Praveena, M., Pavan Kumar, V., Asha Deepika, R., Sai Raghavendhar, C.H., Rahul Sai Reddy, J. "Enhancing visibility of low-light images using deep learning techniques", International Journal of Innovative Technology and Exploring Engineering, 8(6), 298-301, 2019.
17. Venubabu Rachapudi and Golagani Lavanya Devi, "Feature selection for histopathological image classification using levy flight salp swarm optimizer", Recent Patents on Computer Science (2019) 12: 329. https://doi.org/10.2174/2213275912666181210165129
18. Anjali Devi, S., Sapkota, P., Obulesh, M.,"Sentiment analysis on products using social media".Journal of Advanced Research in Dynamical and Control Systems,Vol 10, pp. 137-141,2018.
19. Rachapudi, V., Venkata Suryanarayana, S., Subha Mastan Rao, T.," Auto-encoder based K-means clustering algorithm", International Journal of Innovative Technology and Exploring Engineering,8(5), pp. 1223-1226,2019
20. Kompalli V.S., Kuruba U.R. (2017) "Combined effect of soft computing methods in classification. In: Satapathy S., Prasad V., Rani B., Udgata S., Raju K. (eds) Proceedings of the First International Conference on Computational Intelligence and Informatics. Advances in Intelligent Systems and Computing, vol 507. Springer, Singapore
21. Syed.Karimunnisa, Dr.Vijaya Sri Kompalli Cloud Computing: Review on Recent Research Progress and Issues, International journal of advanced trends in computer science and engineering, Vol 8,No.2, March-April-2019, ISSN 2278-3091 Pages 216-223
22. YAMINI SATYA, T. and PRADEEPINI, G., 2016. Harvesting deep web extractions based on hybrid classification procedures. Asian Journal of Information Technology, 15(18), pp.3551-3555.

AUTHORS PROFILE

Mrs. Modepalli Kavitha, Assistant professor in the department of CSE, KL University. She registered for Ph.D. at Sri padnavathi Mahila Vishwavidyalayam in the year of 2015.she has published 11 research articles in Scopus indexed journals. She is having around 8 years of experience in teaching. Her research area is Internet of Things, Machine Learning and Big data analytics.

D Hari Haran, studying fourth year B. Tech in the department of CSE, KL University. His area of interest is Internet of Things. He participated in two IoT conferences and One FDP on Internet of Things.

P. Meenan, studying fourth year B. Tech in the department of CSE, KL University. His area of interest is Internet of Things. He participated in One FDP on Internet of Things.

J. Likhitha Priya, studying fourth year B. Tech in the department of CSE, KL University. Her area of interest is Internet of Things. She participated in two IoT conferences and One FDP on Internet of Things.

.