International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-1, October, 2019

Gaze Touch Cross PIN: Secure Multimodal Authentication using Gaze and Touch PIN

Dina M. Ibrahim, Sadaf Ambreen

Abstract*: The basic goal of information security is, to protect the privacy, reliability, and availability of information on devices that manipulate and store the information. To protect this information, the fundamental step is user authentication. The most common method for authentication on devices is the personal identification number (PIN) method, which is vulnerable to shoulder surfing attack. Shoulder surfing attack used by attacker especially in the crowded public places. For shoulder surfing attack prevention several methods had been proposed. This paper proposed a *GazeTouchCrossPIN* authentication method that overcome the limitations found in the earlier work. we propose a multimodal authentication system that combines between the gaze gesture and touch PIN authentication systems. The results illustrate that the proposed *GazeTouchCrossPIN* method is more secure hence it decreases the shoulder surfing rate in both side attacks and iterative attacks.

***Keywords* : Shoulder surfing, Gaze base method, Information security, *PIN*.**

I. INTRODUCTION

Shoulder surfing attack is a non-technical social engineering attack used by an attacker to obtain sensitive information like password, personal identification number, and other confidential data, while the victim is oblivious. Shoulder surfing could be used especially in the crowded places (when the victim uses ATM, smartphone or computer) either by direct observation, close range or by vision-enhancing devices, long range, depends upon the location and situation [1].

To prevent the shoulder surfing attacks many other methods were developed like textual passwords, graphical passwords, and augmented reality technique for passwords, but the limitation of all are well-known. The domain of our study is GAZE Based techniques to prevent the shoulder surfing attacks and to perform the analysis of these different techniques.

The paper organization is in six sections where section II describes various Gazed based methods for shoulder surfing attack as a prior work, section III presents the proposed GazeTouchCrossPIN method. In Section IV, an evaluation and analyses of the proposed method is presented. Section V analyzes all these methods on the behalf of authentication accuracy, time, security, and usability factor. Finally, section VI is about the conclusion and future work.

Revised Manuscript Received on October 30, 2019.

* Correspondence Author

Dina M. Ibrahim, Information Technology Dept., College of Computer, Qassim University, Buraidah, KSA. Email: d.hussein@qu.edu.sa

Sadaf Ambreen, Information Technology Dept., College of Computer, Qassim University, Buraidah, KSA. Email: abasy@qu.edu.sa

II. PRIOR WORK

A. GazeTouchPass: Multimodal authentication using gaze and touch on mobile devices

An approach to resisting the shoulder surfing attack is GazeTouchPass, for user authentication on mobile devices for user authentication attacker needs to observe the eye movement and device screen frequently [2]. The contribution of this work is divided into two folds, first is the introduction of GazeTouchPass and second, evaluation of system usability and security. The results of different experiments show that GazeTouch Pass approach is more secure than single – model authentication against shoulder surfing attacks. The proposed system addresses Side Attack Threat model, the attacker observes the user while authenticating once, and Iterative Attack threat model, where an attacker can observe the user much time (e.g. a colleague at work). GazeTouchPass Scheme depends upon these threat models. User select four symbols for a password, either selected by touch or via gaze movements (left or right).

- *Advantages:*

No significant main effects were found for the number of modality switches on authentication time. No significant effect of the number of modality switches on the error rate. Moreover, this model is more secure than the single-model ones especially for side attack due to having quick switch focus between phone and eyes.

- *Limitation:*

Iterative attacks are still possible. Video-based eye tracking has its own limitations, like light effects, eyeglasses reflection and heavy makeup can affect the quality of eye tracking.

- *Future work*

More focus on iterative attack resistance. The future system can use more eye movements instead of just left and right.

B. GazeTouchPin: Protecting Sensitive Data on Mobile Devices using Secure Multimodal Authentication

Although mobile devices provide access to a plethora of sensitive data, most users still only protect them with PIN or patterns, which are vulnerable to side channel attacks (e.g., shoulder surfing) [3]. GazeTouchPin is a well-known approach for secure authentication of mobile devices. It is a multimodal scheme, specially designed to confound the shoulder surfing attacks by its interface requirements.

The attacker needs to perceive the movement of user's eyes as well the status of the screen also to hack the password. The author recommends using this method insensitive context rather than on regular basis. This method is highly secure against Side attack threat and Iterative attack threat [3]. Viola-Jones detector is used to detect the eyes and face of the user.

The proposed system designed three layouts: Touch-only: uses a PIN keypad, Touch+random: uses touch to select the desired digit from one of two randomly shuffling layouts, and GazeTouchPin: uses touch input to select a pair of horizontally aligned PIN digits and then a gaze gesture to the left/right to select the desired PIN [3].

- *Advantages:*

The proposed system is implemented on an Android Platform and does not require any additional hardware. Gaze gestures are spotted using a front-facing camera. In addition to high usability, when feeling observed or when accessing sensitive data.

- *Limitation:*

Phone postion or user posture: the user does not always hold the phone in a way that shows the eyes. The system might not detect both eyes if the phone is too close to the face.

- *Future work*

Evaluate this approach against other threat models such as video attack, insider, and multiple observers. Future work can guide the user into an optimal posture.

C. A Gaze Gesture-Based user Authentication System to Counter Shoulder Surfing Attacks

Authors in [4] presented a smart system based on gaze gesture. Users apply their unique gaze manners onto movable geometric shapes on a screen for authentication. Each shape has a fixed starting and ending points and traverses along a predefined path. The system consists of 36 movable shapes; the user can select only three shapes as a password and follow their path as they move. Moreover, not all the 36 shapes can be selected to conduct a password; only 12 are used for password and the other 24 shapes are fake. The system validates the user by matching their scan path with each shape path in order to identify the closest path.

- *Advantages:*

Users are free from remembering complex gestures or strokes order. The system authentication achieves high accuracy.

- *Limitation:*

The system is time-consuming to video analysis attack. It uses fake shapes, which causes an unacceptable time delay.

- *Future work*

Adding extra solutions like randomizing shape paths. Providing each user with the ability to choose the true and fake shapes.

D. DyGazePass: A Gaze Gesture-Based Dynamic Authentication System to Counter Shoulder Surfing and Video Analysis Attack

Dynamic Gaze Password is a secure approach which uses dynamic gaze gestures for authentication purpose on devices [5]. To counter Shoulder Surfing Attacks, dynamic and static-dynamic interfaces are introduced. The system consists of 10 unique color circles which move concurrently along some random paths for a specific period of time. For password selection, the user must select any four colors for the PIN. After password selection the next step is authentication, the user must select a path of a circle, colored with his/her password, during an animation. As there are four digits for a password so the animation will be repeated for four times allowing the user to enter his/her password.

System architecture consists of two core modules, Gaze Tracking Module, which uses “The Eye Tribe” tracker to provide the user gaze coordinates on the screen, and the Authentication Engine which is responsible for generating the random path for each circle on the interface [5]. To authenticate the user, Scan-path matching also implemented.

- *Advantages:*

From the participant feedback, the static-dynamic interface approach is very easy and required less attention time to follow the moving circles. The static-dynamic approach has high accuracy compared to a dynamic approach. The proposed system is not susceptible to single video iterative attacks.

- *Limitation:*

Colorblind people will have a limited set of colors to choose. Authentication phase takes more time that would not be appropriate where frequent authentication is required. The system has a low success rate for dual video iterative attacks.

- *Future work*

Enhanced interface for password memorability. Reduce authentication time.

E. Gaze-Assisted user Authentication to Counter Shoulder Surfing Attacks

One of the prospective solutions against shoulder surfing attacks is a gaze assisted authentication system proposed in [6]. In this work, the system consists of an authentication interface and an eye tracker parts. The authentication interface has a specific number of pre-defined twelve shapes, which are moving concurrently on the monitor, only three of them are consisting the password. The user authenticating himself by following the three shapes selected as a password. Template machines or decision tree algorithms used to match the scan-path of the route navigated by the shape with user’s gaze.

- *Advantages:*

The system authentication achieves more accuracy if the template-matching algorithm is used. The system authentication reaches medium accuracy by using the decision tree algorithm but it reduces the time. The gaze-assisted approach realizes a highly secure method against the shoulder surfing attacks

- *Limitation:*

The system is time-consuming when the template-matching algorithm used. Choosing only three shapes from twelve, as a password is very small and being hard to the user tracking.

- *Future work*

The future system can use more eye movements instead of just left and right.

F. Real-time Eye Tracking for Password Authentication

In this work, using the smart camera, gaze-based PIN entry is proposed through real-time eye detection and tracking.

NI Vision Builder is used for eye tracking, while for eye center location on-board data processing and collection LabView is used [7]. The user can enter the password from a digital keypad. Dual processor Camera, which is mounted right above the keyboard, where the camera lens captures the user's eye movements. Eye detection algorithms are implemented using LabVIEW 8.5f.1 and Vision Builder AI 3.6.

- *Advantages:*

The vulnerability of authentication is reduced by non-contact-based authentication. The smart camera provides onboard data capturing, processing and storage.

- *Limitation:*

High-resolution grey scale images are always required for the real-time eye tracking algorithm. Smart camera requirement. Screen size to select a specific digit affects the precision within the clusters. Accuracy of PIN will also be effected by user stability.

- *Future work*

Nine digit keypad, can be extended to character and digit combination password entry. PIN identification algorithms incorporate for all-in-one password identification system. The proposed system can be extended to handheld and other camera-based devices.

III. PROPOSED GAZETOUCHCROSSPIN METHOD

The purpose of this work is to propose an authentication method that overcome the limitations found in the earlier work. we propose a multimodal authentication system that combines between the gaze gesture and touch PIN authentication systems which we called GazeTouchCrossPIN. The implementation of the proposed system is based on Android application without any extra hardware devices. Instead, detecting the gaze gesture using the front-facing camera. Here the attackers must observe both the touch screen and the user's eyes.

The GazeTouchCrossPIN proposed system works on two steps; the first step is the touch input to select a cross of digits by pressing into the middle of that cross, as shown in Fig. 1. For example, if the user press on number 2 this resulting a cross layout has number 2 in the middle, number 1 on the left, number 3 in the right, number 5 in the bottom, and no number above because number 2 is in the first row of the board.

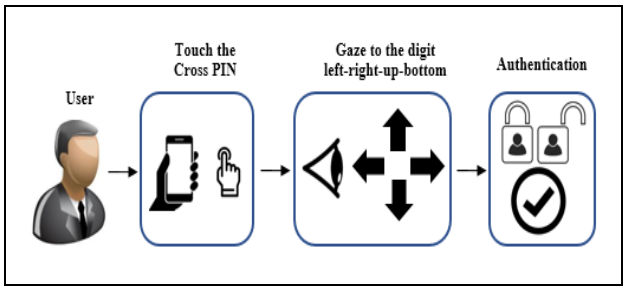

Fig. 1.The proposed GazeTouchCrossPIN architecture.

The second step is the gaze gesture to the up/down/left/right to select the desired digit of the PIN. For example, in choosing number 2, if the user wants to enter number 1 s/he must gaze to the left and if he wants to enter number 3 s/he must gaze to the right, and so on. Taking into consideration that number 2 itself must not be in the desired PIN.

Figure 2 illustrates the layout appearance of pressing the 10 digits from 1 to 9 and number 0. From the figure, it is noticed that, the number of the highlighted resulting squares is not equal for all the cases. Sometimes two, three, four, and five squares.

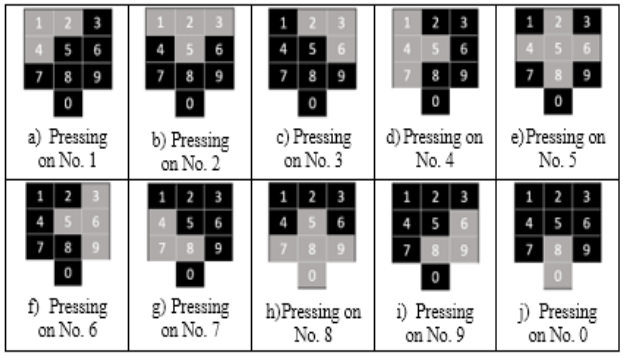

Fig. 2.Layout appearance of the 10 digits.

Table I represents the possibilities for each digit in the PIN board. For each pressed digit there is a number of digits appears in the layout, not all of them can be used because we have to except the pressed digit itself.

Table- I: Probabilities of the digits

Pressed digits	*Appeared Layout*	*Digit probability*	*Usable probability*
0	2 digits	2/10	1/10
1, 3, 7, and 9	3 digits	3/10	2/10
2, 4, and 6	4 digits	4/10	3/10
5 and 8	5 digits	5/10	4/10

If we need to get number 0 in the PIN, we can get it only if we press number 8. While if we need number 2 in the PIN, we can get it if we press numbers 1 or 3 or 5. As shown in Table II.

Table- II: Layout possibilities and cases

Number	Appeared Numbers	possibilities	Case
0	8	One possibility	Case1
1	2,4	Two possibilities	Case2
2	1,3,5	Three possibilities	Case3
3	2,6	Two possibilities	Case2
4	1,5,7	Three possibilities	Case3
5	2,4,6,8	Four possibilities	Case4
6	3,5,9	Three possibilities	Case3
7	4,8	Two possibilities	Case2
8	5,7,9,0	Four possibilities	Case4
9	6,8	Two possibilities	Case2

From Tables I and II, we can classify the appeared layouts based on the possibility of the appeared numbers into four cases; Case1, Case2, Case3, and Case4. In the next Section, we will analyze the efficiency of the layout choice.

In order to get higher accuracy, it is better to choose the layout with highest probability. This will increase the complexity of recognize the digit and leads to decrease the side attack possibilities.

IV. EVALUATION AND ANALYSIS

In this Section, performance evaluation of the proposed GazeTouchCrossPIN method in comparison with other two authentication methods are conducted and analyzed. The other two methods are: GazeTouchPIN and GazeTouchPass.

A. Usability-based study

For studying and analyzing the usability of the proposed GazeTouchCrossPIN and the other two earlier methods, we use realistic entries for passwords entered by participants as a repeated measures experiment. We enrolled 20 participants each perform 8 predefined PIN using all the three authentication methods. The participants entries were recorded using three video cameras.

The evaluation of the usability is conducted based on input speed and error rate metrics. Figure 3 illustrates the average time needed to authenticate the PIN user for each method. The figure shows that the average time of the proposed GazeTouchCrossPIN is similar to the average time of the GazeTouchPIN method. While the GazeTouchPass method gives lowest average time. Untrained participants need more time for use our proposed GazeTouchCrossPIN than when using the other two methods.

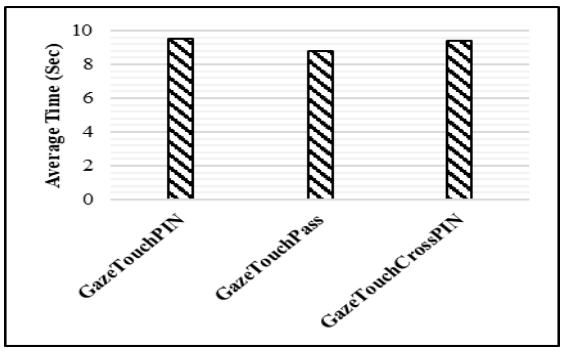

Fig. 3.Average time vs. the three methods

B. Security-based study

Security-based study can be done by following a repeated measures experiment. The participants asked to attack passwords entered by all the three methods and monitored using the recorded videos. GazeTouchCrossPIN proposed method addresses two threat models that attackers can use; side attack and iterative attack models.

In the side attack model, the attackers monitor the participants from one angle of view during the authentication process (e.g. train or subway). The attackers noticed the user's touched input as well as the user's eyes. While in the iterative attacks model the attackers can monitor the user from different view angles several time (e.g. colleague at work). The attacker can observe user's eye movement and the user's touch input on the mobile or vice versa.

We calculate the successful attacks or the success rate for the three methods. The results show that the proposed GazeTouchCrossPIN is more secure against iterative attacks with success rate 3% than the other two methods hence the iterative success rate for the GazeTouchPass and GazeTouchPIN is 34.5% and 4.2%, respectively. Moreover, the proposed method is also more secure against the side attack with success rate 11.2% while in the GazeTouchPass and GazeTouchPIN is 18% and 16.67%, respectively, as illustrated in Fig. 5. Total shoulder surfing rate drops 52.5% and 20.1% for GazeTouchPass and GazeTouchPIN, respectively to 14.2% using the proposed GazeTouchCrossPIN approach.

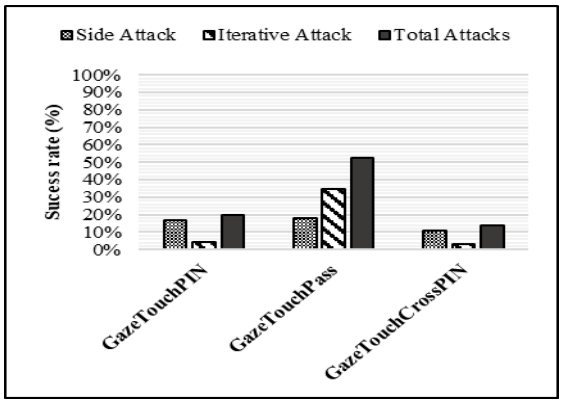

Fig. 4.Success rate percentage vs. the three methods.

V. COMPARISON BETWEEN THE EARLIER METHODS

Table III illustrates the analysis of the methods based on common features, like authentication accuracy, time, security, and usability. Starting with the authentication accuracy feature, the second method, A Gaze Gesture-Based user Authentication System, achieves the highest accuracy with comparison with the other methods by value of 99%. The next feature is security, the first method, Gaze Assisted user Authentication, accomplishes the highest level of security.

The proposed GazeTouchCrossPIN method gives better performance with respect to the success rate in both side attack and iterative attack models. Total shoulder surfing rate drops from 52.5% GazeTouchPass and 20.1% GazeTouchPIN to 14.2%. Compared with the other GazeTouchPIN and GazeTouchPass the proposed GazeTouchCrossPIN reduces the authentication.

As a usability-based study: choosing 2, 5, and 8 digits to enter any number from the 10 digits is easy to the users because these three number are in the middle of the board that easy and quick to be touched. While in the security-based study: the higher number of possible digits in the layout gives high secure system.

VI. CONCLUSIONS

In this paper, we had studied different gaze-based algorithms to prevent the shoulder surfing attacks. In section V, table III represents the analysis of discussed algorithms with their merits and demerits based on accuracy, time, security, and usability factor of each algorithm. Gaze Gesture based system provides the most accuracy for authentication. Time factor is common among all the algorithms.

Table- III: Methods analysis based on the common features

Method name	Authentication Accuracy	Time	Security	Usability
Gaze Assisted	95% (for template-matching algorithm) 90.2% (for decision tree algorithm) High accuracy, more time consumption and vice versa.	Time consuming for template matching algorithms.	Highly secure without assistance of advanced technology.	Shape movements will not affect the usability.
A Gaze Gesture	99%	Time Consuming (video-analysis)	Fake shapes has an important role in preventing the attacker to get the correct shape. 40% less sussesspectible for video attacks.	From interviews, users consider this solution innovative, secure and simple. However, some users expressed that sneezing; lack of attention during password entry would lead to incorrect gaze input.
GazeTouchPin	Learning effect reduce the error rate of authentication. Training is important for accuracy and time.	Time-Consuming compare to the only touch PIN entry method. Training can make PIN entry faster.	More secure against itterative attacks then GazeTouchPass. (4.2% success rate) Secure for Side attacks (16.67% success rate)	Preferred to use, when feeling observed or when accessing sensitive data.
GazeTouchPass	Fewer errors in the case of the password with 3 switches	Mean authentication time is approximately 3.1 second.	Particularly secure agains side attacks (only 15%-21% success rate) Iterative attacks (23%-46%)	System usability based on the input speed and error rate. Particularly useful as a secondary authentication mechanism.
DyGazePass	98.75% 97.5% 70%	3 seconds 2 seconds 1 second	Not suspectible to single video itterative attack. Dual video itterative attacks has less success rate (16.7%), compare to static PIN interface , which is 79.2%	There is a trade-off between accuracy and time, less time will reduce the accuracy, more time will increase the accuracy rate.
Real-time Eye Tracking	Reduce the authentication vulnerabilities compared to physical PIN.	Not discussed	The non-contact PIN-based method adds a layer of security.	Currently used for ATMs.
Proposed method (GazeTouchCrossPIN)	Compared with the other GazeTouchPIN and GazeTouchPass it reduce the authentication.	Approximately 6 seconds.	Total shoulder surfing rate drops from 52.5% GazeTouchPass and 20.1% GazeTouchPIN to 14.2%	System usability based on the input speed and error rate. Particularly useful as a secondary authentication mechanism.

In this paper we proposed a GazeTouchCrossPIN authentication method that overcome the limitations found in the earlier work. It combines between the gaze gesture and touch PIN authentication systems. The results illustrate that the proposed GazeTouchCrossPIN method is more secure hence it decreases the shoulder surfing rate in both side attacks and iterative attacks.

REFERENCES

1. A. Maiti, M. Jadliwala and C. Weber, "Preventing shoulder surfing using randomized augmented reality keyboards," *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, Kona, HI, 2017, pp. 630-635.
2. O.Kasat, U.Bhadade, N.Trivedi, "Study and Analysis of Shoulder-Surfing Methods ", I*nternational Journal of Scientific Research in Science, Engineering and Technology (IJSRSET)*, ISSN : 2456-3307, Volume 1 Issue 6, pp. 256-261, November-December 2015.
3. M. Khamis, M. Hassib, E. Zezschwits, A. Bulling, and F. Alt "GazeTouchPIN:Protecting Sensitive Data on Mobile Devices using Secure Multimodal Authentication," In Proceedings of 19th ACM *International Conference on Multimodal Interaction, Glasgow, UK*, 2017, pp. 446-450.
4. V. Rajanna, P. Taele, S. Polsley, and T. Hammond., "A gaze gesture-based user authentication system to counter shoulder surfing attacks," *In Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, CHI EA '17. ACM, 2017, pp. 1978-1986.
5. V. Rajanna, A.H. Malla, R.A. Bhagat, and T. Hammond, "DyGazePass: A Gaze Gesture-Based Dynamic Authentication System to Counter Shoulder Surfing and Video Analysis Attacks," *IEEE 4th International Conference on Identity, Security, and Behaviour Analysis (ISBA)*, 2018.
6. V. Rajanna, and T. Hammond.," Gaze-Assisted User Authentication to Counter Shoulder–surfing Attacks," *In Proceedings of the 2018 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, CHI EA '18. ACM, 2018.
7. M. Mehrubeoglu and V. Nguyem, "Real-time Tracking for Password Authentication" *IEEE International Conference on Consumer Electronics (ICCE)*, 2018.

AUTHORS PROFILE

Dina M. Ibrahim Assistant Professor at Information Technology Dept., College of Computer, Qassim University, KSA from September 2015 till now. In addition to, Dina works as Lecturer at Computers and Control Engineering Department-Faculty of Engineering, Tanta University, Egypt. She was born in United Arab of Emarat at 1980, her B.Sc., M.Sc. and Ph.D. degrees taken from Computers and Control Engineering Department-Faculty of Engineering-Tanta University at 2002, 2008, and 2014, respectively. Dina Works as consultant Engineer, then a Database administrator, and finally acts as a Vice-Manager on Management Information Systems (MIS) Project–Tanta University, Egypt, from August 2008 until November 2014.

Sadaf Ambreen Lecturer at Information Technology Dept. College of Computer, Qassim University KSA from 2008 till 2019. In addition to, Sadaf worked as lecturer at University of Azad Jammu & Kashmir from 2005 till 2008. She was born in Azad Kashmir - Pakistan at 1983.Her MCS and MS degrees taken from COMSAT and Iqra University, Pakistan at 2005 and 2012 respectively.