PathGazePIN: Gaze and Path-based Authentication Entry Method

Bayan M. AlBaradi[1], Amani M. AlTowayan[2], Maram M. AlAnazi[3], Sadaf Ambreen[4], Dina M. Ibrahim[5]
Information Technology Department, College of Computer, Qassim University, Qassim, Saudi Arabia[1, 2, 3, 4, 5]
Computers and Control Engineering Dept., Faculty of Engineering, Tanta University, Egypt[5]

***Abstract*—In these days, smartphones are being widely used, people use them to store sensitive and private information. The password authentication is the most used authentication method, however, the password can be disclosure through shoulder surfing attack, since the users write their password in public places and they tend to make the password easy to remember which increase the vulnerability to attacks. Many authentications schemes were proposed to prevent shoulder surfing attack, but they still vulnerable to shoulder surfing attack or have accuracy problems or lack in usability. In this paper, we proposed a gaze-text based PIN entry method, which we called PathGazePIN. It will utilize the user's eye movement to enter the password. The main idea is allowing the user to authenticate by following numbers that move along fixed paths on the screen by using two authentication interfaces: random interface and sorted interface. The results represented that the proposed system will increase the security against shoulder surfing attack as well as usability and accuracy.**

***Keywords*—User authentication; shoulder surfing attacks; PIN; gaze-based; security; accuracy**

I. Introduction

The smartphone has become in large-scale utilization because it can be carried anywhere easily and a lot of people have sensitive information stored on their devices, however, the smartphone may be vulnerable to many attacks, especially in crowded places. Accordingly, the password authentication came to ensure security for the user smartphone. Shoulder surfing attack is one of the dangerous attacks [1]. It constitutes a growing danger of device security. The attacker can obtain sensitive information by two ways, first at close range by directly looking over the person's shoulder either by side attack; when the user near to the attacker or even can see the device screen of a user or iterative attack; the attacker monitors the user when he/she enters the password and notes the repeated movements at several times to detect [2], second from long range by using a camera, a pair of binoculars or other vision magnifiers [3].

Shoulder surfing attack is kind of the nontechnical attacks on social engineering used by an attacker to obtain sensitive and private information such as password, personal identification number, and other confidential information, while the user is unaware [4]. The attacker can easily infiltrate to the victim when they are using devices such as Automated Teller Machine (ATM), smartphones or any other devices in crowded places to steal the password without user perception. This project will use gaze-based authentication that allows a user to enter the passwords using his eyes instead of touch to prevent shoulder surfing.

The rest of this paper is organized as follows; Section II presents background on the authentication mechanisms used to prevent shoulder surfing attacks. Our proposed PathGazePIN system is illustrated in Section III followed by the methodology and the implementation of the proposed PathGazePIN system in Sections IV and V, respectively. In Section VI, testing of the proposed system is presented while in Section VII we evaluate our results. Analysis and discussion for our system is given in Section VIII. Finally, we draw our conclusions and present issues for future work in Section IX.

II. Background

There are many authentications schemes were proposed to develop the authentication mechanisms and to prevent shoulder surfing attack, like textual password, graphical password, and biometrics password.

In the graphical password, three schemes were proposed to prevent shoulder surfing attack [5], which are triangle scheme, movable frame scheme, and intersection scheme. The main idea of these schemes is making the screen so crowded to confuse attackers, the main drawback of these schemes are they require long login time since the user needs to find the pass object on the screen, and if a small number of objects is shown on the screen the system will be vulnerable to attacks. To overcome of triangle scheme drawback Convex Hull Click Scheme [6] has been proposed to improve security and usability, this scheme was proved to be effective against Shoulder Surfing attacks, but it also requires long login time. To decrease login time ColorLogin scheme was proposed in [7], in this scheme they use a color background, which will decrease login time and multiple colors are used to confuse the attacker, while not burdening the users.

In textual password, in [8], they proposed a text-based authentication scheme that prevents Shoulder Surfing attacks using Randomized Square Matrix Virtual Keyboard. This scheme designed to be used in websites that require authentication, this scheme is required long login time due to, the two clicks for each character and the randomization. In this study [9], the scheme has proposed to preventing Shoulder Surfing attack by use of augmented reality. In this system, the user sees a keyboard layout that differs from the actual keyboard QWERTY through augmented reality device. Because the adversary does not have a knowledge of Strategies used consequently, the system will be more secure [10] [11].

On the other hand, typing on a randomized augmented reality keyboard requires more time and it produces errors during writing, which affects usability [12].

In Gaze-based authentication systems, The EyeDent authentication scheme was proposed in [13]. It uses an on-screen keyboard and users use gaze to enter the password, this scheme uses a numeric keypad and also used a QWERTY layout. A novel gaze-based authentication scheme was presented in [14], which is depends on a graphical password by using cued-recall on a single image, this scheme uses a computational model of visual attention to mask the area of images that most user select and it most likely to attract visual attention as called silence map. The study has shown that is images with saliency mask is significantly was more helpful to increase password security [15]. A secure multimodal authentication using gaze and touch PIN called Gaze Touch Cross PIN is presented on [16]. They proved that Gaze Gesture based system provides the most accuracy for authentication.

Smooth pursuit oculomotor control kit (SPOCK) was proposed in [17] it is based on smooth eye movement, selection, and activation to limits the Midas touch problem. Midas touch problem is excessive inadvertent clicking that place intended content outside the clickable area. In this study [3], Gaze-touch pin technology has proposed to cover two models of threats, first is side attack model and second is the iterative attack model. It uses touch and gazes' gestures as an input method. It is also used randomization of the digit to make the system more secure, this system was highly secure against Iterative attack. The authors in [18] has proposed a gaze-based authentication system. The system uses movable shapes and the user should tracks this shapes in the screen for authentication, the shapes have a minimal number to achieve complexity but do not clutter the interface, their study showed that there is no user have an issue with following moving shapes, due to the natural ability of the humans. Moreover, it does not add any cognitive load in human memory. The system has a limitation such that the user should adjust his position to let the Eye Tracker work efficiently and it also requires additional hardware. In [19], they proposed a gaze gesture-based authentication scheme. In this scheme, the interface consists of ten colored circles and each circle is moving in a random path and the user selects four colors as his password. This scheme was secure against video iterative attacks and has less security against dual video iterative attacks. The scheme has few limitations, it is not usable for colorblind users and also it requires long login time.

III. The Proposed PathGazePIN System

This research will provide a new idea for mobile authentication that is the combination of two previous studies [17][19]. By applying textual method and gaze-based technique that enable users to enter their password using their gaze and using SPOCK novel gaze interaction method which will avoid the Midas touch problem and increase accuracy. The system consists of three certain circular paths and ten numbers from 0-9 placed across these paths, the numbers on inner and on outer circular paths are moving, while the numbers on middle circular paths are static. These numbers are randomized across the circular paths but in increasing order for each authentication. The user selects 4 numbers as his/her password and on the authentication, the user either dwells in the static number or follow the moving number to enter each number, as illustrated in Fig. 1.

The static and dynamic approach is used instead of pure dynamic to avoid overwhelmed by the visual cluttering and to avoid more attention requires from the user which affects the usability, also certain circular paths are used to avoid the problem of two numbers with a similar path that may be wrongly recognized by the system which affects the accuracy of the system. Because of the gaze-based entering authentication, the system will be secure against side attack, furthermore, the randomizing of the number is used to completely prevent iterative attack and video analysis attacks. Ordered numbers technique is used to since it reduces the time of finding numbers so it will reduce login time. Also, the nature of human ability to follow moving objects and static and dynamic approach leads to more usability. Moreover, using certain circular paths and Gaze Pursuit-based Authentication will increase the accuracy.

Fig. 1. Application Interface of the Proposed PathGazePIN System.

IV. PathGazePIN Methodology

This system will implement for mobile devices by using gaze-based technique in Android platforms. By apply empirical study to collecting and analyzing data, we check the result whether it is achieving high accuracy, usability, and security from the result of user's experiment. The selected method is an empirical study about the effectiveness of gaze-based technique against shoulder surfing attacks which will focus on the security, usability, and accuracy. We are following the waterfall model, in planning phase we sought about anti-shoulder surfing technique, then analyzed the collected data from the previous research paper to define an appropriate solution, after that, we designed the proposed idea and conduct system implementation, testing procedures and result analyzing.

For testing, we collected a group of participants to measure the system accuracy and effectiveness. The requirements of this study are participants requirement, hardware and software requirements. The participants are a group of victims and

attackers. They must have a background of using smartphones and none of them should be blind. The hardware requirement is a smartphone with an Android operating system to implement the application on Android platform and it does not need for any additional hardware. The application is based on gaze gesture that will detect it by using front camera of the mobile, and software requirement is will analyze the user's eyes movements by using the MATLAB tool. Also, the application will be implemented on Android Studio Development Environment. The data will be collected by participants who will use the application after implementation, a database will be used to store authentication information; login time, the number of wrongs PIN to determine the accuracy and PIN. And other information will be collected manually; the usability and effectiveness against shoulder surfing attack. For analyzing collected data, the Microsoft Excel application will use.

V. PathGazePIN Implementation

A. Application Interface

In this application, Java Android studio is used to design the interface, which consists of animated numbers moving in a circular path and video capture to take a video of user's face while he tracks the numbers. The animated numbers are created by using Canvas and Paint class, and video capture is created by using MediaRecorder class.

Similarly, two types of interface are created which are random interface and sorted interface, as in Fig. 2. In the random interface, the application will randomly generate different arrange of numbers for every start. In the sorted interface, the numbers will appear same arrange for every start.

B. Eye Tracking System

For eye tracking system the MATLAB environment is used, eye Tracking system is consisting of three phases, first is eye extraction, in this phase a video of one eye will be created from recorded video. This video will be used in eye tracking phase to detect and track the pupil and save its X, Y and Z data, then these data are used in the PIN identification phase to determine desired number, for that a different calculations are used for each path, based on the feature of the data on each path.

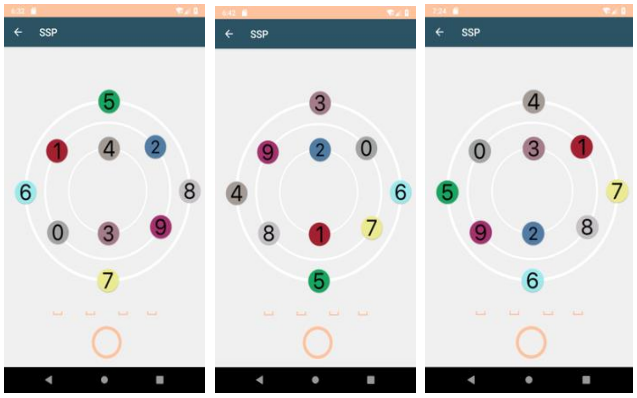

Fig. 2. Random Interfaces for different Login Times.

Outer path, this path consists of four numbers that are moving clockwise, to determine the desired number, first this path has been divided into two halves and then these halves are further divided into two quarters which results as four quarters, namely Right up, Right bottom, Left up and Left bottom. To determine if the gaze moves right or left the values that on y-axes and z-axes are used. The basic idea on this step is to get the highest and lowest y-axes value, and it correspond z-axes value (frame number), after that, we can determine if Y value goes from high to low or from low to high. On 'Left' case, the lowest Y value will have corresponding Z value bigger than the highest Y value, which is mean the plot goes from up to bottom. On 'Right' case, the lowest Y value will have corresponding z value less than the highest Y value which means the plot goes from bottom to up.

To determine if the gaze goes up or bottom the values that on x-axes and z-axes are used. The same idea of determining left and right are used, first get the highest and lowest x-axes value, and it correspond z-axes value (frame number), after that, we can determine if x value goes from high to low or from low to high. On 'Up' case, the lowest X value will have corresponding Z value bigger than the highest X value, which is mean the plot goes from right to left. On 'Bottom' case, the lowest X value will have corresponding z value less than the highest X value. Which is mean the plot goes from left to right. Finally, by combining these two steps we can determine if the gaze goes Right up, Right bottom, Left up or Left bottom.

Middle path: This path consists of four numbers that are static. To determine the desired number this path has been divided into four quarters, Right up, Right bottom, Left up and Left bottom. To determine if the path is static or not the y-axes value is used the biggest y-axes value is subtracted from lowest y-axes value to measure the distribution of the plot. After that, the median values of y-axes and x-axes are used with center point values that we get it from the previous phase to determine the desired quarter.

Inner path: This path consists of two numbers that are moving anti clockwise. Therefore, to determine the desired number this path has been divided into two halves Right and Left. The anti-clockwise path is used to increase the accuracy of the system. To determine if the gaze goes right or left the value that is on y- axes and z-axes is used. On 'Right' case, the lowest Y value will have corresponding Z value bigger than the highest Y value, which is mean the plot goes from up to bottom. On 'Left' case the lowest Y value will have corresponding Z value less than the highest Y value, which is mean the plot goes from bottom to up. to distinguish the inner path from the outer path the x-axes value and y-axes value are used. The main idea is in the inner path the lowest or the highest x-axes value will be in the middle, wherein lowest or the highest x-axes value in the outer path is in the end or in the beginning. Examples of outer left up plot and inner right plot are shown in Fig. 3 and Fig. 4, respectively.

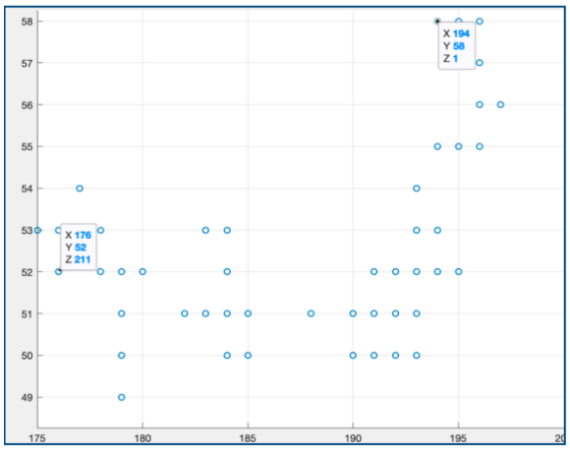

Fig. 3. Outer Left up Plot.

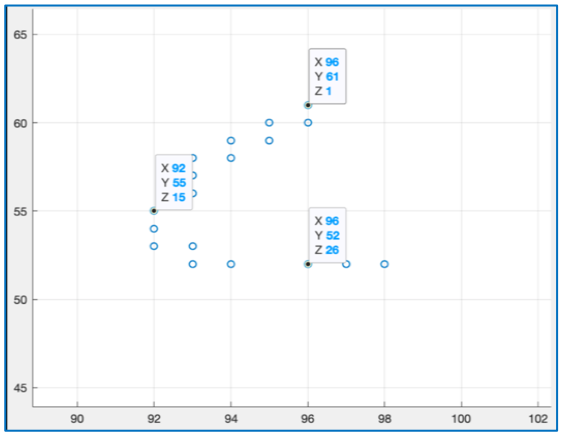

Fig. 4. Inner Right Plot.

VI. PathGazePIN Testing

For connecting the eye tracking system with Android Interface, the MATLAB DRIVE is used; the recorded videos are uploaded to MATLAB drive and then execute them through eye tracking system in the laptop. Before the connection, there are some changes is applied on eye tracking system. First, for each phase it will takes four videos on each run instead of one video, moreover in PIN identification phase the change is applied to save the PIN as a number instead of its place on the circle based on its place and the video number.

We tested three important aspects of authentication systems which are usability, accuracy, and its security of shoulder surfing attacks. We perform three experiments: usability experiments, accuracy experiments and security experiments. We did a usability experiment for two modes interface, one with random numbers and other with sorted numbers. To measure the usability in terms of which of them takes less time and easy to remember, we made a database to measure the time for every run. The test is conducted on a number of people and divided them as attackers and victims. The victims choose the mode of interface either sorted or random, or can use both. A questionnaire was made after the test with some questions to take the users opinion and information. Furthermore, we applied an experiment on two interface modes to analyze the security of the application if it is exposed for shoulder surfing attacks (side, iterative) attacks. We conducted a number of complete logins with different modes, which are random or sorted. In full session, there can be two attackers one of them is side attack and other is iterative attack. To check if this approach is exposed to iterative attack, victim will have to login more than one times with same password. Also, we measure the time if victim takes a long time to enter his/her password that will be easy for attacker to detect the password or not.

VII. Evaluation Results

A. Security

The most important aim of our application is shoulder surfing prevention. The results appear percentage of success login for attackers in both interfaces. In sorted interface, there are 30 logins trying for users that means there are 30 trying from the attackers to guessing the numbers. The success of iterative attackers for sorted interface are 7 times from 30 means 23.3% the attacker was guessed one to two numbers but not in the same order. For side attack there are 4 times from 30 attackers which means 13.3% guess one to two numbers also not in the same order. The success of attackers for the random interface are 2 times for iterative attacks from 15 trying 13.3%, and for side attacks was guess one number 2 times from 15 trying 13.3% also not in the same order as in Fig. 5.

We requested from users to enter their password fourth times, and attackers are different for each user to measure how many numbers attackers can guess in more than one login for user. The first login for 18 users represents 100% for first trying to attackers to guessing. There are four attackers for different users was guess just one number 22.2% and there two attackers were guessing two numbers for each user 11.1%. In the second logging for 12 users, there are four attackers three of them were guess one number which by 33.3% and the other was guess two numbers 8.3%. In the third login, one attacker was guessed one number 12.5% from 8 tries, and for the fourth login, there were 5 users try to log in for the fourth times and just two attackers were guessed two numbers 40% as shown in Fig. 6. At the end, all attackers that guessed the numbers, they did not guess it in the same order that users put at their password. They trying to guess but no one of them was guess it at same order like user chosen.

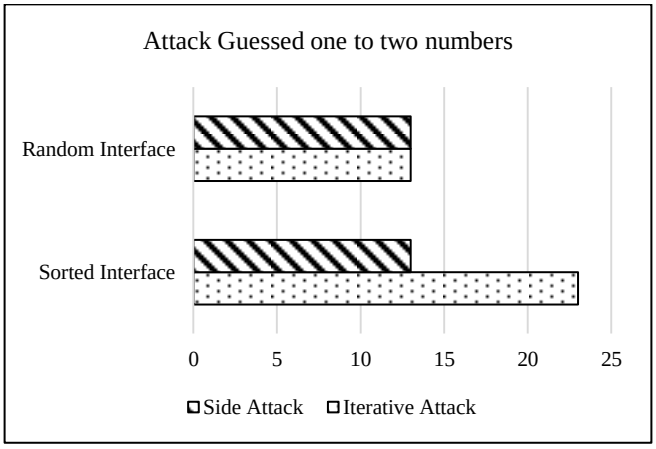

Fig. 5. Attacker Guessed One to Two Numbers.

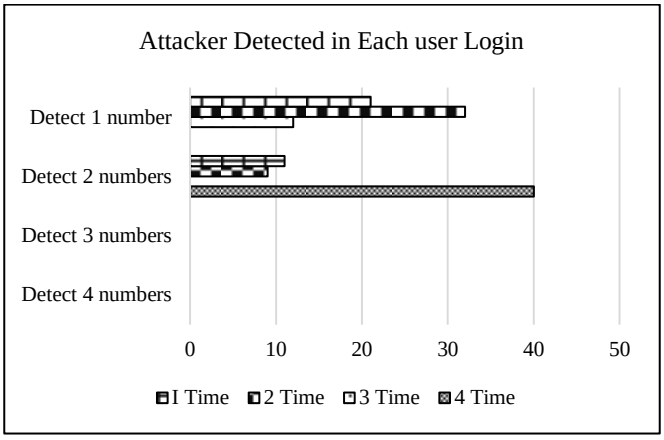

Fig. 6. Attacker Detection on Each user Login.

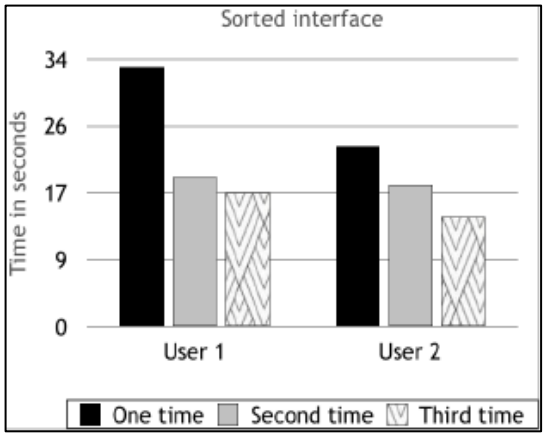

Fig. 9. Maximum, Minimum and Average Login Time on Sorted Interface.

B. Usability

Fig. 7 and 8 show four persons use the same mode with the same password multiple times. In the sorted interface, the time required from the user to complete the login was decreased. While, in the random interface the time required from the user to complete the login did not change.

Fig. 9 and 10 show the average, maximum and minimum login time for all the login in the sorted interface and the random interface. In the sorted interface, the average login time was 23s and the maximum login time was 37s and the minimum login time was 14s, while the average login time in the random interface was 24s and the maximum login time was 39s and the minimum login time was 18s.

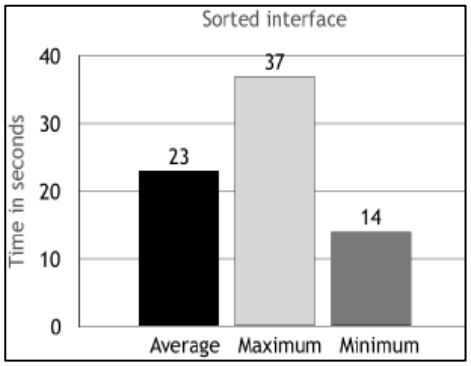

Fig. 7. Login Time for Three users on Sorted Interface.

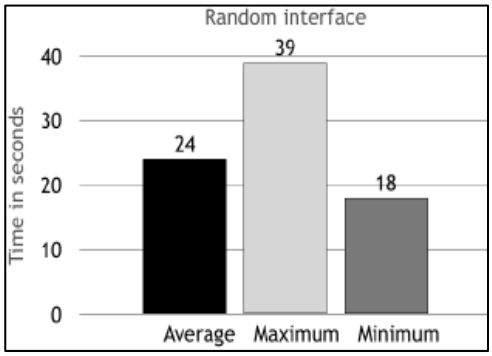

Fig. 8. Login Time for Two users Multiple Time on Random Interface.

C. Accuracy

To measure the accuracy of our eye tracking system the data was collected from users based on different situations to analyze factors that affect the accuracy, also with different numbers to analyze the accuracy of each path. In this experiment, the sorted interface was used and ten logins were performed with seven different passwords, the total entered numbers were 40 number.

In this experiment, the successful login was 40 %, as illustrated in Fig. 11, the means by successful login the eye tracking system detects all four number successfully. On the other hand, the unsuccessful login was 60%, the unsuccessful mean that the eye tracking system does not detect all four number successfully, it may be detected 0, 1, 2, or 3 numbers successfully.

For all the entered numbers, Fig. 12 shows the percentage of true detection of numbers and the percentage of wrong detection of numbers. The percentage of true detection of numbers was 75% which means 30 numbers out of 40 are detected, and the percentage of the wrong detection of numbers was 25% which means 10 numbers out of 40 are not detected truly.

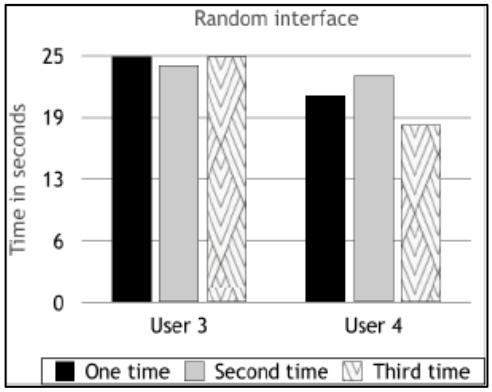

Fig. 10. Maximum, Minimum and Average Login Time on Random Interface.

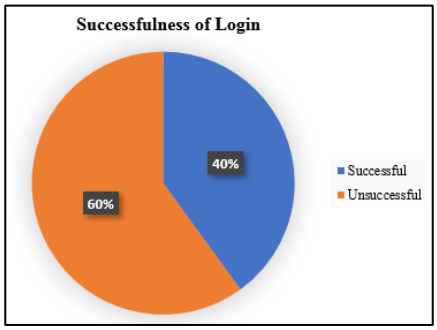

Fig. 11. Successfulness of Login.

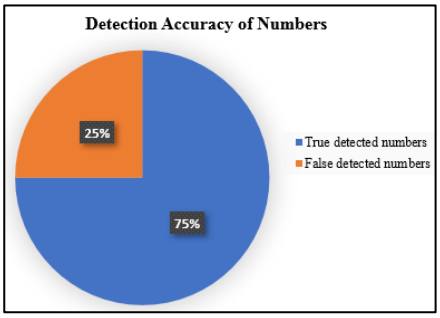

Fig. 12. The Detection Accuracy of Numbers.

VIII. Analysis and Discussion

A. Security-based Analysis

The first and important aim of our project is security. After we measured the security for each interface and how many percent for each trying was success, we found that both interfaces are secure from shoulder surfing attack. There is no successful complete login for attacks which guess the completely four numbers and with same order, and the attacker who guess one number or two numbers did not guess these numbers with same place of the number. For 45 user's login there are attackers by 28% who were guess one or two numbers only and not with the same order.

B. Usability-based Analysis

We have concluded that the difficulty of the password is not affected by login time. Also, if the user used sorted interface more than once it will reduce time login. While, if used random mode it will change at each run. The interface is user friendly and did not faced attenuation but the sorted interface is easier than random interface.

C. Accuracy-based Analysis

The third aim of our project was achieving high accuracy on the login. Unfortunately, this aim was not achieved because of the Eye Tracking System has just 40% successful detection of logins, and the unsuccessful detection was 60% of logins. From the 60% unsuccessful logins, 30% of them detected three number successfully, 20% of them detected two number successfully and 10% of them detected just one number successfully. This is being because a front camera of the smartphone is used, also there was no use special software for analyzing gaze data, in all previous studies that were studied in this project there was use a special tracking camera within its software, except one [3] which was used the device's front camera but it was tracking only the horizontal gaze direction.

IX. Conclusions and Future Work

In this paper, we presented a Shoulder Surfing Attacks Prevention scheme by using Enhanced gaze PIN Entry Method which we called PathGazePIN system, we applied it on Android device and for the tracking, the front camera was used. We implemented two authentication interfaces: Random interface and Sorted interface, and it was evaluated to measure the usability and security for each of them. Through system evaluations, for the usability, we found that the Sorted Interface has less time login if used more than once, while, the time in the Random Interface did not change, for the user perspective, we were found that the interface is user-friendly and did not require more attention from the user. For the security, we found that the sorted interface was less secure compared with the Random interface, however, it is still secure against shoulder surfing attack since there was no successful complete login for attacks in both Interfaces. For the accuracy, we found that our system has low accuracy 40% successful complete login, but with an individual number it detected 75% successfully, and this is being because we were used a front camera of the phone instead of special tracking camera within its software.

As a future work, we will improve this system to be more accurate by using eye-tracking tools that help analyze the results. In addition, we will try to increase accuracy and usability by improving the paths.

References

[1] Y. S, R.Sathishkumar, A. L, and A. V, "Counterfeit Shoulder Surfing Attack Using Random Pin," International Journal of Pure Appl. Math., vol. 118, no. 22, pp. 1757–1761, 2018.

[2] M. Khamis, M. Hassib, E. von Zezschwitz, and A. Bulling, "GazeTouchPIN: Protecting Sensitive Data on Mobile Devices using Secure Multimodal Authentication," in Proceedings of the 19th ACM International Conference on Multimodal Interaction, 2017, pp. 446–450.

[3] Y. Kita and M. Park, "Proposal and its Evaluation of a Shoulder-Surfing Attack Resistant Authentication Method : Secret Tap with Double Shift," International Journal of Cyber-Security Digit. Forensics, vol. 2, no. 1, pp. 48–55, 2013.

[4] O. Kasat, U. Bhadade, N. Trivedi, "Study and Analysis of Shoulder-Surfing Methods ", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), ISSN: 2456-3307, vol. 1, no. 6, pp. 256-261, November-December 2015.

[5] H. R. Chennamma and X. Yaun, "A Survey on Eye-Gaze Tracking Techniques," Indian Journal of Computer Science an Engineering (IJCSE), vol. 4, no.5, pp. 389-393, 2013.

[6] S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," in Proceedings of the working conference on Advanced visual interfaces - AVI '06, 2006, pp. 177–184.

[7] H. Gao, X. Liu, S. Wang, H. Liu, and R. Dai, "Design and analysis of a graphical password scheme," 2009 4th International Conference Innov. Comput. Inf. Control. ICICIC 2009, pp. 675–678, 2009.

[8] P. Nand, P. K. Singh, J. Aneja, and Y. Dhingra, "Prevention of shoulder surfing attack using randomized square matrix virtual keyboard," 2015 International Conference Adv. Comput. Eng. Appl., pp. 916–920, 2015.

[9] A. Maiti, M. Jadliwala, and C. Weber, "Preventing shoulder surfing using randomized augmented reality keyboards," 2017 IEEE International Conference Pervasive Comput. Commun. Work. PerCom Work. 2017, pp. 630–635, 2017.

[10] A. Jesudoss, N. P. Subramaniam, "A Survey on Authentication attacks and countermeasures in A Distributed Environment," Indian Journal of Computer Science an Engineering (IJCSE), vol. 5, no.2, pp. 71-77, 2014.

[11] A.A. Gawande and G. Nathaney, "A Survey on Gaze Estimation Techniques in Smartphone," International Research Journal of Engineering and Technology (IRJET), vol. 4, no. 4, pp. 2647-2650, 2017.

[12] M. Mehrube and N. Vuong, "Real-Time Eye Tracking for Password Authentication," International Conference on Consumer Electronics (ICCE), pp. 1-4, 2018.

[13] J. Weaver, K. Mock, and B. Hoanca, "Gaze-based password authentication through automatic clustering of gaze points," 2011 IEEE International Conference Syst. Man, Cybern., pp. 2749–2754, 2011.

[14] A. Bulling, F. Alt, and A. Schmidt, "Increasing the Security of Gaze-Based Cued-Recall Graphical Passwords Using Saliency Masks," in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 3011–3020, 2012.

[15] P. Sorate and G. J. Chhajed, "Survey Paper on Eye Gaze Tracking Methods and Techniques," International Research Journal of Engineering and Technology (IRJET), vol. 4, no. 6, pp. 5612-5616, 2017.

[16] D. M. Ibrahim and S. Ambreen, "Gaze Touch Cross PIN: Secure Multimodal Authentication using Gaze and Touch PIN," International Journal of Engineering and Advanced Technology (IJEAT), vol. 9, no. 1, pp. 777-781, 2019. doi: 10.35940/ijeat.A1381.109119.

[17] S. Schenk, P. Tiefenbacher, and G. Rigoll, "SPOCK: A smooth pursuit oculomotor control kit," in Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems, 2016, pp. 2681–2687.

[18] V. Rajanna, S. Polsley, P. Taele, 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, 2017.

[19] 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," 2018 IEEE 4th International Conference Identity, Secur. Behav. Anal. ISBA 2018, vol. 2018, pp. 1–8, 2018.