IJARCCE

ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 9, September 2021

DOI: 10.17148/IJARCCE.2021.10903

An Investigation on the Impact of Age Group and Gender on the Authentication Performance of Keystroke Dynamics

Ademola O. Adesina[1], **Olasupo Oyebola**[2]

Lecturer, Computer Science Department, Olabisi Onabanjo University, Ago-Iwoye, Nigeria[1]

Graduate Student, Computer Science Department, National Open University, Ibadan, Nigeria[2]

Abstract: Keystroke dynamics is a biometric that has been explored as a means of making user authentication more secure. However, studies have indicated that the performance of such a system might be influenced by the demography of the user population. The purpose of this study is to investigate the relationship between the age and gender of the users of a keystroke dynamics-based mobile phone user authentication and the performance of the scheme. Using a mobile keystroke dynamics dataset containing the age and gender information of the participants, an anomaly detector algorithm was used to test whether an impostor user would have been recognised or not. A False Acceptance Rate (FAR) is calculated for the genuine user and impostors' combination. A Two-Way Analysis of Variance (ANOVA) was used to test the hypotheses whether there are significance differences and interaction between the FARs obtained with respect to the age group and gender categories. The result suggests that the age and gender of the users of a keystroke dynamics user authentication system on a mobile phone is not expected to have significant impact on the performance of such a system. Unlike previous studies that were based on keystroke dynamics data from desktop computer users, this investigation focused on keystroke dynamics for mobile phones. The results obtained in this paper has further improved our understanding that demographic bias relating to age and gender may be eliminated from the concerns that may arise from the use of a keystroke dynamics user authentication on a mobile phone.

Keywords: Biometrics, User Authentication, Keystroke Dynamics, Classification, Machine Learning.

I. INTRODUCTION

User authentication involves a person proving a claimed identity on a device such as a mobile phone or on a computer. Traditional authentication can be done by the person supplying the same information such as a password or producing the correct object such as a swipe card which is the same as that earlier stored by the device to represent the genuine user when prompted by the device. The third means of user authentication is by the use of biometrics, in which a person's physiological or behavioural characteristics is used for identification or verification of identity.

Keystroke dynamics is a behavioural biometric that utilises a person's habitual way of typing at a terminal such as a computer keyboard or the keypad of a mobile phone to recognise them as demonstrated in [1] and has been proposed as a biometric authentication medium and has also been explored as a means of strengthening user authentication by enhancing the security of password-based authentication on computers and mobile devices [2]. Demographics is one of the variables that may affect the recognition performance of such a biometric modality [3, 4]. Moreover, some biometrics that have been shown to be biased in their performance with respect to different age categories and gender as observed in [5]

In literature, our understanding of the interactions between personality traits and the performance of keystroke dynamics authentication on mobile phones has not been sufficiently addressed. This study aims to investigate the impact of age and gender on the performance of a keystroke dynamics-based mobile phone user authentication.

The authors in [6] conducted experiments using a desktop computer and keyboard to collect keystroke dynamics data and investigated the uniqueness property of keystroke dynamics.

They concluded that there is a significant difference in the recognition performance depending on whether an attacker is a male or a female. In contrast, [7] also investigated the robustness of keystroke dynamics against synthetic forgery attacks using keystroke dynamics data collected on a desktop computer platform but did not observe any significant difference in the performance of their keystroke dynamics classifier between males and female participants. In his thesis, [8], using keystroke dynamics data collected also on a computer platform did not observe any significant influence of the demographic traits considered, including the volunteers age and gender on the tested classifiers' miss rates.

A review of relevant literature revealed that while the nature of the relationship between the performance of keystroke dynamics on computer platforms and user demographics such as age and gender has been investigated, not much

ISSN (O) 2278-1021, ISSN (P) 2319-5940

Vol. 10, Issue 9, September 2021

DOI: 10.17148/IJARCCE.2021.10903

attention has been placed by authors on similar efforts on mobile devices, especially the ubiquitous smartphones. This point to the fact that more efforts are needed to improve our understanding of the relationships between keystroke dynamics performance on mobile platforms and the duo of the age and gender categories of the user population.

II. MATERIALS AND METHODS

The authentication scenario being considered is that of a mobile phone user that uses a keystroke dynamics-enhanced password authentication to log in to his device while some impostors also attempt to login to the same device using the same password and as discussed in the previous sections, the performance of a keystroke dynamics based authentication system on a mobile phone might be influenced by the age and gender category of both the owner of the mobile phone and impostors attempting to log in to the mobile phone. We will assume that other user factors have negligible effects on the outcome of our investigation.

The performance of a biometric user authentication system can be measured by evaluating its False Acceptance Rate (FAR) and False Rejection Rate (FRR).

$$\text{FAR} = \frac{\textit{Number of Times the System Accepts an Impostor}}{\textit{Number of Impostor Attempts}} \quad (1)$$

$$\text{FRR} = \frac{\textit{Number of Times the System Rejects the Genuine User}}{\textit{Number of Genuine User Attempts}} \quad (2)$$

Of the two performance measures, it is only the FRR that can be predetermined and is set to match the requirements of the genuine user(s) in terms of security, the limiting factor being the usability considerations for the genuine user. Once the FRR has been set, the performance of the authentication system can be measured in terms of the system's FAR. The lower the FAR, the better the authentication system performance is.

Thus, the approach is to observe if there are any significant difference in the average FAR of a keystroke dynamics user authentication with respect to the age and gender category of the genuine user and impostors. To carry out this experiment, we must obtain the keystroke dynamics data of mobile device users alongside their age and gender information.

The dataset used was that made available by [9] and is available for download at *http://www.coolestech.com/rhu-keystroke/*. The keystroke data had 50 participants who have typed the phrase "rhu.university" between 15-20 times in 2 or 3 sessions. The sessions are separated by 3-30 days. For this work, we have used only users that completed 3 sessions in 3 different dates with at least 5 repetitions per session. Thus we have used keystroke data with 5 repetitions of the said phrase per day for three days making a total of 15 repetitions per user. These requirements left us with 45 users out of 50 in the original dataset.

The dataset contains the codified age groupings with 11 participants in the 7-18 years old (*Teens*), 24 participants in the 19-29 years old (*Young Adults*) and 10 participants in the 30-65 years old categories (*Adults*). The gender category of each participant was also included in the dataset with 21 female participants (*Females*) and 24 male participants (*Males*) in our data. The dataset for each user is a vector made up of the concatenation of the four keystroke dynamics features and as shown in figure 1, these are namely the press-press time (PP), press-release time (PR), release-press time (RP) and release-press time (RP).

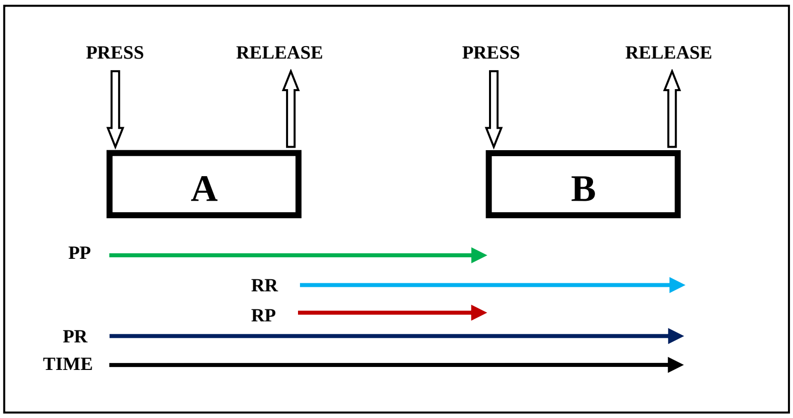

Fig. 1 Keystroke Dynamics Timing Features

DOI: 10.17148/IJARCCE.2021.10903

The approach used for the determination of the authentication performance of keystroke dynamic biometric features is that presented in [8], where the scaled Manhattan anomaly detection algorithms returned the lowest FAR and is used for classification in this work. One of the 45 users in the dataset is designated as the genuine user while the rest are designated as impostors. The anomaly detector is then trained on the first 12 password repetitions of the genuine user data to build a profile of that user. Thereafter, anomaly scores are generated for the remaining 3 password repetition of the genuine user using the trained anomaly detector. The anomaly score indicates how dissimilar the test data is to the genuine user profile. A threshold is chosen such that the genuine user is only accepted if his anomaly score is lower than this pre-determined threshold. The threshold such chosen will dictate the designed FRR with which the authentication system is expected to operate. The classifier was tuned to operate with an FRR of 20%, which means the genuine user is expected to be falsely rejected once out of every five login attempts.

The keystroke dynamics data of each of the remaining 44 users designated as impostors are picked one by one and used together with the trained anomaly detector of the genuine user to generate anomaly scores for the first 3 password repetitions by the impostor users. An impostor user will be falsely accepted if his anomaly score is lower than the chosen threshold. The FAR is calculated for the genuine user and impostors' combination. The procedure is repeated by designating other users as the genuine user and the remainder as impostors in turn.

Based on our experimental design, an appropriate statistical tool to properly interpret the empirical results is the Two-Way Analysis of Variance (ANOVA) which will enable us to determine whether there are indeed significance differences between the FARs obtained for the age group and gender categories. Specifically, we are testing the following null hypotheses;

i. There is no difference in the FAR obtained for the three age categories.

ii. There is no difference in the FAR obtained for the two gender categories.

iii. There is no interaction between age and gender with respect to the FAR.

The statistical test will be taken at 0.05 significance level. The analysis of variance was implemented using the *aov()* function while the statistical test were implemented using the relevant function as made available in the *car* package of the R software environment [10].

.

III. RESULTS AND DISCUSSION

Table I shows the average FAR obtained for the various categories considered in this paper. The result from Table1 suggests that keystroke dynamics user authentication scheme works better for the users in the *Young Adults* category than the other age groups. Likewise, using keystroke dynamics based user authentication seems more appropriate for male participants as compared to their female counterparts.

Table I Average FAR (%) for Each Category of the Participants

Category	**FAR (%)**
Males	43.7
Females	50.2
Teens	56.0
Young Adults	37.7

The Two-Way ANOVA statistical test resulted in an F-value of 1.9133 (p=0.1612) for age effect, an F-value of 0.8907 (p=0.3511) for gender effect and an F-value of 0.3 (p=0.7425) for the age and gender interaction effect on the FAR. Hence, we did not have sufficient evidence to reject the three null hypotheses stated earlier.

This statistical test is validated with the Levene's test for homogeneity of variance which returns a test statistic of 0.6732 at a p-value of 0.6462 and confirms the assumption of homogeneity of variance required by the Two-Way ANOVA. Also, the normality assumption is supported by the test statistic of 0.96839 at a p-value of 0.2529 obtained from the Shapiro-Wilk normality test. Thus, both assumptions required for the Two-Way ANOVA are satisfied. These results suggest therefore that the age and gender of the users of a keystroke dynamics user authentication system on a mobile phone is not expected to have significant impact on the performance of such a system. While such results were obtained by Kilourhy (2012), the study was based on keystroke dynamics data from desktop computer users. Proving that algorithms used in keystroke dynamics user authentication are not biased towards certain demographics such as teenagers or females is a move towards a complete understanding of the behavioural biometric. However, a larger keystroke dynamics dataset would have increased our confidence in the results obtained. Also, only timing features were made available in the dataset used, it would be interesting to see if similar results are gotten from a dataset that includes features extracted from the motion and other touchscreen sensor outputs such as accelerometer values in the various axes of the mobile phone, gyroscope readings and touch position of the fingers on the surface of the mobile phone touchscreen.

IV. CONCLUSION

Keystroke dynamics is a cheap and non-obtrusive behavioural biometrics that can be used to overcome some challenges associated with the use of passwords, a popular choice for user authentication on mobile devices. A concern that may militate against the effective utilisation of the biometric, that of whether there is a significant difference in the performance of authentication system based on the biometric with respect to the demography of the user population, has not been sufficiently addressed in the literature, especially on mobile phones. The results obtained in this paper has further improved our understanding that demographic bias relating to age and gender may be eliminated from the concerns that may arise from the use of a keystroke dynamics user authentication on a mobile phone. In further researches, we intend to use of a larger mobile keystroke dynamics datasets with features available from the phone touchscreen and embedded motion sensors to further strengthen the validity of the results obtained in this paper.

REFERENCES

[1] Banerjee, S. P. and Woodard, D. L. (2012). Biometric Authentication and Identification using Keystroke Dynamics: A Survey. *Journal of Pattern Recognition Research*, *7*(1), (pp. 116-139).

[2] Kambourakis, G., Damopoulos, D., Papamartzivanos, D. and Pavlidakis, E. (2016). Introducing Touchstroke: Keystroke-Based Authentication System for Smartphones. *Security and Communication Networks*, *9*(6), (pp. 542-554).

[3] Cook, C. M., Howard, J. J., Sirotin, Y. B., Tipton, J. L. and Vemury, A. R. (2019). Demographic Effects in Facial Recognition and Their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, *1*(1), (pp. 32-41).

[4] Nicholson, J., Coventry, L. and Briggs, P. (2013). Age-related Performance Issues for PIN and Face-based Authentication Systems. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 323-332).

[5] Drozdowski, P., Rathgeb, C., Dantcheva, A., Damer, N. and Busch, C. (2020). Demographic Bias in Biometrics: A Survey on an Emerging Challenge. *IEEE Transactions on Technology and Society*, *1*(2), (pp. 89-103).

[6] Teh, P. S., Zhang, N., Teoh, A. B. J. and Chen, K. (2016). A Survey on Touch Dynamics Authentication in Mobile Devices. *Computers & Security*, *59*, 210-235.

[7] Stefan, D., Shu, X. and Yao, D. D. (2012). Robustness of Keystroke-dynamics based Biometrics against Synthetic Forgeries. *Computers and Security*, *31*(1), (pp. 109-121).

[8] Killourhy, K. S. (2012). *A Scientific Understanding of Keystroke Dynamics*. Ph.D. Thesis. Carnegie Institute of Technology, Dept. of Computer Science. Pittsburgh Pa. USA.

[9] El-Abed, M., Dafer, M. and El Khayat, R. (2014). RHU Keystroke: A Mobile-Based Benchmark for Keystroke Dynamics Systems. In *2014 International Carnahan Conference on Security Technology (ICCST),* (pp. 1-4). IEEE.

[10] The R Foundation (2020). What is R? Available at: https://www.r-project.org/about.html Accessed 5th February, 2020.