International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 1 Jan. 2023, pp: 1082-1088 www.ijaem.net ISSN: 2395-5252

Usability Comparison of Alternative Keyboard Based Interactions For Grid Based Graphical Authentication Systems

Surajo Yusuf[1], Hassan Umar Suru[2], Ibrahim Suleiman[3], Danjuma Mairo [4,]

[1,2,3] *Computer Science Department, Kebbi State University of Science And Technology, Aliero, Kebbi State, Nigeria*

[4] *Sociology Education Department, Kebbi State University of Science And Technology, Aliero, Kebbi State, Nigeria*

Date of Submission: 17-01-2023 Date of Acceptance: 31-01-2023

ABSTRACT: Alphanumeric text and numeric's continue to be the dominant authentication methods in spite of the numerous concerns by security researchers of their inability to properly address usability and security flaws and to effectively combine usability and security. These flaws have, however, contributed to the growing research interest in the development and use of graphical authentication systems as alternatives to text based systems. Graphical passwords or graphical authentication systems are password systems that use images rather than characters or numbers in user authentication. In spite of the growing acceptance of graphical passwords, empirical studies have shown that graphical authentication systems have also inherited some of the flaws of text-based passwords. These flaws include predictability, vulnerability to observational attacks and the inability of systems to efficiently combine security with usability. Hence, there is a continued quest to find a system that has both strong usability and strong security. This paper compares the usability of click base, numeric base and alphanumeric base passwords in three research models namely; passface, passpoint and object base models. A significant result for total login time was established between numeric and click base passwords for all the three model designs.

KEYWORDS: passfaces, passpoints, clickbase, authentication, password**.**

I. INTRODUCTION

Authentication is the primary gatekeeper for computer systems. It both verifies authorized users of a system and distinguishes between different users. Halting and detecting intruders is only possible with a strong authentication mechanism and efficient access control. However, users dislike inconvenient authorization methods and may compromise them to make their lives easier [12]. The traditional and most common authentication method employs usernames and passwords composed of alphanumeric text. This method has proven to be insecure in practice [4]. For example, users may choose easily guessed passwords or, if a password is hard to guess, users may find it too difficult to remember leading to increased support issues, users writing down their passwords where they can be easily found [3] or users using the same password for multiple sites. The human factor is the weakest link in security [5]. and authentication is one of the critical points where humans play an active role in security. Therefore, we need substitutes or supplements for traditional authentication methods to have a more secure and reliable authentication. Recently, several new methods for authentication such as token-based authentication, biometric-based and graphical authentication have been developed [11]. All of these can be used together with conventional usernames and passwords. The most commonly used approaches to authentication are knowledge-based techniques which include text and picture-based passwords [5]. Since it is easier for humans to remember pictures than text, graphical authentication schemes have been proposed as an alternative to text-based schemes [1]. With graphical authentication there is no need to remember long sequences of characters. Instead, a user can pass the authentication step by recognizing or recreating the graphical password. When the number of pictures is large enough graphical

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 1 Jan. 2023, pp: 1082-1088 www.ijaem.net ISSN: 2395-5252

authentications may be superior to text-based methods [13].

II. LITERATURE REVIEW

The recognition-based system studied most extensively to date is Pass faces [6]. Users pre-select a set of human faces. During login, a panel of candidate faces is presented. Users must select the face belonging to their set from among decoys. Several such rounds are repeated with different panels. For successful login, each round must be executed correctly. The set of images in a panel remains constant between logins, but images are permuted within a panel, incurring some usability cost. The original test systems had n = 4 rounds of M = 9 images per panel, with one image per panel from the user portfolio. The user portfolio contains exactly 4 faces, so all portfolio images are used during each login. The theoretical password space for Passfaces has cardinality Mn, with M = 9, n = 4 yielding 6561 _ 213 passwords.

Figure 1: Pass faces scheme

Security Analysis

No single mechanism or scheme has completely solved the threats of attacks on computer systems. Even though graphical password schemes promise to provide better security (e.g. larger password space) than text-based passwords, they still face potential attacks [10]. Possible attacks on graphical password schemes include shoulder surfing, brute force attacks, dictionary attacks, guessing attacks, spyware and social engineering attacks.

Shoulder Surfing

Shoulder surfing refers to looking over someone's shoulder, possibly using binoculars or close-circuit television, in order to obtain information such as password, PIN and other sensitive information. It is effective if the attacker can observe what the user keys in, clicks or touches [10]. Graphical authentication is generally more vulnerable to shoulder surfing attacks than text-based passwords [14]. For this reason, a few graphical authentication methods are specifically designed to resist shoulder surfing attack. None of the search metric or locimetric schemes are considered resistant to shoulder surfing. Previous research has found that the use of mouse clicks, touch screens or stylus pens is vulnerable to shoulder surfing attacks [14]. Little work has been done in the field to improve the evaluation of these attacks, specifically. As a result, shoulder surfing attacks are still poorly understood [15]. All of the previous SLRs answered research questions related to graphical pass- words but did not examine specifically how their susceptibility to SSA is evaluated empirically. Furthermore, no SLRs have been conducted in the field of graphical passwords in the past five years, despite the growing number of publications. [2]

III. MATERIALS AND METHODS

This section provide details on experimentation and analysis of the research. The section will cover about the data collection, approaches to be used, tools and implementation languages.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 1 Jan. 2023, pp: 1082-1088 www.ijaem.net ISSN: 2395-5252

Data collection

System Usability Scale (SUS) model was used to develop the Research questionnaire administered to all the participants at the end of each section of the experiment to state their view, opinion and experience on the interfaces. Participants also ranked the menus according to their preference. few questions were carefully selected from the SUS 10 items questionnaire with one of five responses ranging from strongly disagree, disagree, neutral, agree and strongly agree are as follows:

1) I thought the system was easy to use.
2) I found the various functions in this system were well integrated.
3) I found the system very cumbersome to use.
4) I felt very confident using the system.
5) The application is user friendly.

Tools

The following materials were used in the research:

- Two laptop computers both running Windows 10, 4GB RAM, 500GB HDD, a dual core 2.4330GHz processor, a 64 bit operating system and a 24 inch monitor,
- Firefox internet browser.
- Two Stop watches

Participants

56 participants were selected for the three prototype design. The participants chosen for this experiment were selected from the undergraduate students of kebbi State University of Science and Technology Aliero by means of politely asking for the participants to show interest in the experiment after explaining the aim of the experiment. We decided not to select users with certain characteristics because we believe they have undergone several practical and assignments on high computer usage experience, high confidence in using computers and experience of using the internet. Linked to these, we specifically asked and confirm from the participants if there is anyone without internet browsing and computer usage experience of which no one affirmed to that. Also the subjects recruited had a mixture of male and female participants of at least 16 years and above.

Statistical Analysis

The data was compiled using Microsoft excel 2016 and analyzed by statistical package for social sciences (SPSS) version 26.0. All the collected data was firstly explored with summary statistics and Descriptive statistics such as percentages, frequency, mean, standard deviation, standard error of mean, minimum, maximum distributions mean plots. To be able to analyze the data generated, each of the variables was transformed to find the mean. One-way ANOVA was used to compare the means of the distributions using an alpha level of 0.05.

IV. RESULTS AND DISCUSSION

Result

A total valid number of participants that took part in the experiment were 56 (100%), this implies that there is no invalid data from the experiment. The major descriptive statistics are discussed accordingly.

Personal Information of the participants

The major descriptive statistics are discussed accordingly. Table 1 shows that most of the participants were male (71.4%) and female (28.6%). 44.6% of the participants were between the age group of (16-25), 28.6% were between the age group of (26-35), while 21.4% were between (36-45) and lastly 5.45 of the participants were between the age group of 46 and above. All the participants (100%) were students of tertiary institution.

Table 1: Personal Data of the Respondents

Variables Categories		frequency	Percentage
Gender	Female	16	28.6
	Male	40	71.4
Age Range	(16 -25)	25	44.6
	(26 -35)	16	28.6
	(36 -45)	12	21.4
	46 and above	3	5.4

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 1 Jan. 2023, pp: 1082-1088 www.ijaem.net ISSN: 2395-5252

Education	Primary	0	0
	Secondary	0	0
	Tertiary	56	100

Mean of Total Login Time

The figure below is the mean of total login time by the participants for each of the prototypes passfaces (PF), passpoint (PP) and object base (OB). These prototypes are further classified in to three (3) user authentication type namely; click base, numeric base and alphanumeric. These are then coined as PFC, PFN, PFAN, PPC, PPN, PPAN, OBC, OBN and OBAN which stand for passface click, passface numeric, pass face alphanumeric, passpoint click, passpoint numeric, passpoint aphanumeric, object base click, object base numeric and object base alphanumeric respectively.

The mean of the login time of PFC is 32.28, PFN is 31.79, PFAN is 34.78, PPC is 34.95, PPN is 32.25, PPAN is 36.66, OBC is 33.56, OBN is 34.61 and OBAN is 35.51

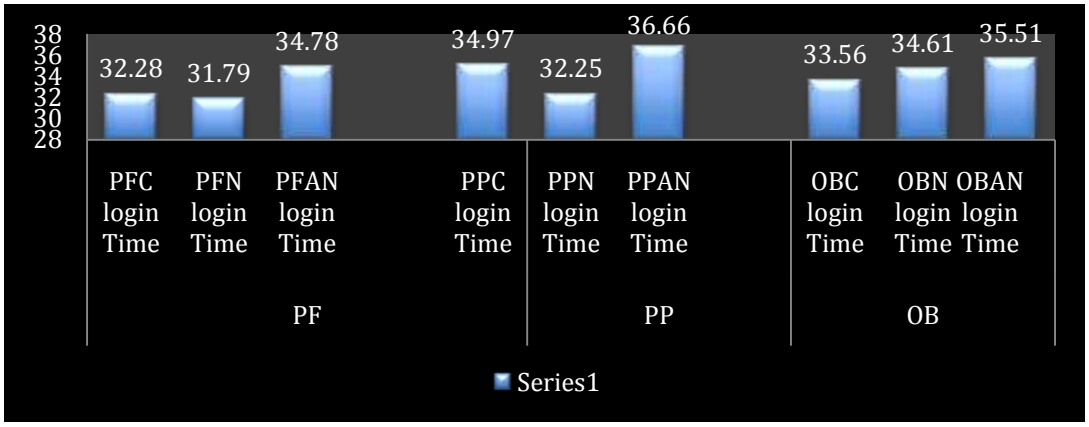

Figure 2: Mean of Total Login Time

User Evaluation in terms of Preference

Figure below displays the mean rank scores of the three models by the participants. In the passface nodel, it shows that the participants prefer passface click (3.85) to passface numeric (2.5) and passface alphanumeric (2.78). in the passpoint model, it shows that participants also prefer passpoint click (4.11) to passpoint numeric (3.66) and passpoint alphanumeric (2.41) while in the last model participants prefer object base click (3.54) to the object base numeric (3.52) and object base alphanumeric (2.32) although the difference between OBC and OBN is not significant.

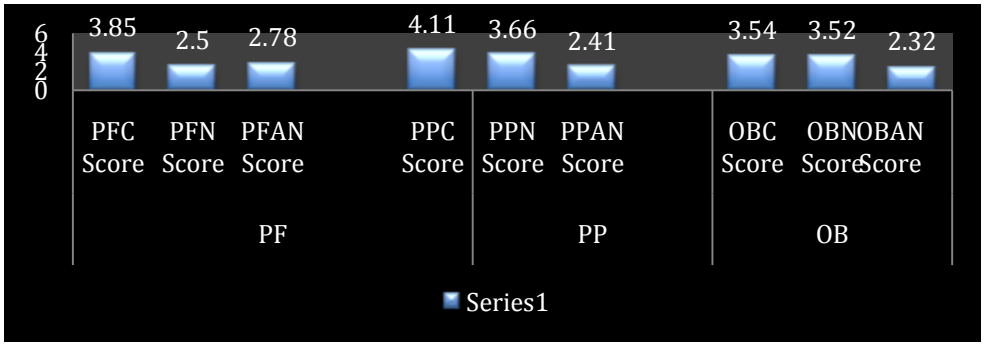

Figure 3: User Preference

User Evaluation in Terms of Ease of Use

Figure 4.4 below displays the mean scores of the three models by the participants in terms of ease of use. In the passface nodel, it shows that the participants find it more easier to use the passface click (3.85) to passface numeric (3.55) and passface alphanumeric (2.55). in the passpoint model, it shows that participants also prefer passpoint click (4.11) to passpoint numeric (3.66) and passpoint alphanumeric (2.41) while in the last

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 1 Jan. 2023, pp: 1082-1088 www.ijaem.net ISSN: 2395-5252

model participants prefer object base click (3.55) to the object base numeric (3.23) and object base alphanumeric (2.12).

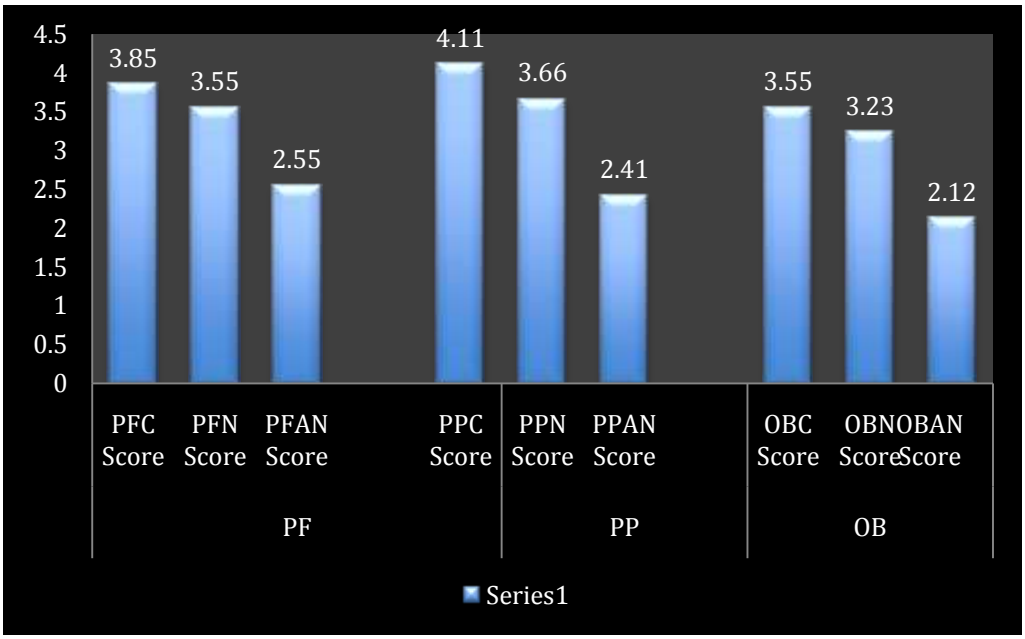

Figure 4: Ease of Use

V. DISCUSSION

This study compared the usability of alternative keyboard based interactions for grid based graphical authentication systems using passface, passpoint and object base as the three model designs. The data was initially explored by looking at the distributions and overall pattern. The study results showed that the users can easily create the password during registration process [9]. The authentication process was also fast as users could easily remember the password. Having developed the needed prototypes, it was paramount that the necessary experiments are performed to evaluate the extent to which these systems meet the research objectives.

In doing this, four usability experiments were performed, four of the experiments were conducted to determine the variation in total time, ease of use, security and user preference among the various implementations of the property based graphical authentication paradigm. In order to capture and understand these metrics, researchers have to obtain data for total login time from the systems, as well as data pertaining to registration and authentication times, that is, data that shows the amount of time it takes for an average user to register onto the systems and to login to it. In both the quantification of effectiveness and efficiency also, subjective data on ease of use and preference must be collected and analysed through well designed survey questionnaires.

It is in this regard that the three experiments are designed to compare the relative total login time, user preference and ease of use. The experiment examined the variation in registration and authentication times between three implementations of property based systems. Passface model, passpoint model and object base model were designed. The results suggest statistically significant variation in both the registration and login times between the factors: click, numeric and alphanumeric. The numeric based factor recorded lowest times in both registration and authentication in all the three models.

For passfaces model, a one way ANOVA of total completion time indicates that there is statistically significance difference in the registration time $F(2, 42) = 8.217$, $P = 0.001$. The post-hoc test revealed that the total time to complete the login is statistically significant for numeric base password ($M = 23014.05$) as compared to click base password ($M = 25871.93$).

For passpoint model, a one way ANOVA of total completion time indicates that there is statistically significance difference in the registration time $F(2, 27) = 14.55$, $P < 0.001$. The post-hoc test revealed that the total time to complete the login is statistically significant for

numeric base password (M = 17867.70) as compared to click base password (M = 20586.50).

For object base model, a one way ANOVA of total completion time was also conducted and it indicates that there is statistically significance difference in the registration time F (2, 42) = 8.217, P = 0.001. The post-hoc test revealed that the total time to complete the login is statistically significant for numeric base password (M = 23014.05) as compared to click base password (M = 25871.93).

VI. CONCLUSION

Authentication is a data access point that manages consumer security assurance. It is a process that grants in a particular context requiring the customer to. Validation schemes are categorized as token-based authentication, validation based on biometrics, validation based upon knowledge. Tokens are used as a Hidden Key in token-based authentication. [7]

Taking the loopholes of alphanumeric passwords, graphical authentication is an emerging solution. Presently, graphical password techniques can be classified into three types: recognition-based, pure recall-based and cued recall based. As presented in this paper, the existing graphical passwords systems suffer from usability and security issues. To overcome these problems, many authors have proposed newly developed graphical password systems but those systems either solve security issues or usability issues. None of the systems provides both together. Emphasis should be given in building a system which is both user friendly and is completely secure. Otherwise, users will be reluctant to use graphical authentication systems. Hence, graphical authentication system is still an interesting area of research.

REFERENCES

[1]. Abhijith, S., Soja, S., Sreelekshmi, K. U., Samjeevan, T. T., Sneha M. (2021). Web based Graphical Password Authentication System:, International Journal of Engineering Research and Technology. 2021 Conference Proceedings. special issue, 29-32

[2]. Bošnjak L, Brumen B. (2019). Shoulder surfing: from an experimental study to a comparative framework. International Journal of Human.-Computer interaction. 130: 1–20 https://doi.org/10.1016/j.ijhcs.2019.04.003

[3]. Gao H., Ren Z., Chang X., Liu X. and Aickelin, U. (2010). "A New Graphical Password Scheme Resistant to Shoulder-Surfing", International Conference on Cyberworlds. 2010, IEEE: Singapore pp. 194 – 199,

[4]. Irfan, A., Anas, S., Malik, S. Khazima, A. (2018). Text based Graphical Password System to Obscure Shoulder Surfing: Department of Computer Science COMSATS Institute of Information Technology Islamabad Pakistan, 13th January, 2018

[5]. Ives B., Walsh K. R. and Schneider H. (2004). "The domino effect of password reuse." In Communications of the ACM, 47(4), 75-78.

[6]. Passfaces: Two factor authentication for the enterprise". Available online at www.realuser.com, (Accessed July 2015).

[7]. Pathik , N. and Preeti, S. (2022). Graphical Password Authentication System: International journal For Research in Applied Science and Engineering Technology. 10(4), 1759-1765. April 2022. DOI-:10.22214/ijraset.2022.41621

[8]. Patrick S., A. C. Long and Flinn S. (2003). "HCI and Security Systems," presented at CHI, Extended Abstracts (Workshops). Ft. Lauderdale, Florida, USA.

[9]. Priti, G. and Brijesh, K. (2021). Graphical-Based Authentication System and Its Applications: IGI Global publisher of Timely Knowledge. Page 1-29. DOI: 10.4018/978-1-7998-6721-0.ch004

[10]. Poet R. and Renaud K. (2007). "A Mechanism for Filtering Distractors for Graphical Passwords". In 13th Conference of the International Graphonomics Society Melbourne, Australia, volume 11, pg 14.

[11]. Sobrado L. and Birget J. C., (2002). "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4,.

[12]. Still, J. D., Cain, A. A., and Schuster, D. (2017). Human-centered authentication guidelines. Journal of Information and Computer Security, 25, 437–456. doi: 10.1108/ICS-04-2016-0034

[13]. Suo X., Zhu Y. and Owen G. S. (2005). Graphical passwords: A survey. In 21st annual Computer security applications conference (pp. 10-pp). IEEE,.

[14]. Tari, F. Ozok A. and Holden, S. H. (2006). "A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords".

In Proceedings of the second symposium on Usable privacy and security (pp. 56-66).

[15]. Yasmeen, A., Radiah R., Tarek A., Jonathan L., Alia S., Carina L., Uwe G., Pascal K., Mohamed K., Ville M., Stefan S., and Florian A. (2022). Understanding Shoulder Surfer Behavior and Attack Patterns Using Virtual Reality: Proceedings of the 2022 International Conference on Advanced Visual Interfaces. 5(15), 1–9, https://doi.org/10.1145/3531073.3531106