



A Comparison Between Position-Based and Image-Based Multi-Layer Graphical user Authentication System

AUDU LOVINGKINDNESS EDWARD*, HASSAN SURU
and MUSTAPHA ABUBAKAR GIRO

Department of Computer Science, Kebbi State University of Science & Technology Aliero, Nigeria.

Abstract

System security is very important, especially in the age that we live in. One of the ways to secure data is by creating a password that makes it difficult for unauthorized user to gain access to the system. However, what makes it difficult for the system to be attacked is directly dependent on approach used to create it, and how secured it is. Text based approach is the oldest authentication approach. It requires that the user supplies textual password in order to gain access to the system. However, this approach has shown a significant drawback and several vulnerabilities, one of which is the difficulty in recalling or remembering textual passwords. Several other attacks that textual passwords are vulnerable to include brute force attacks, shoulder spying, dictionary attacks etc. The introduction of graphical schemes made things a lot better. Graphical passwords make use of images. However, most graphical schemes are vulnerable to shoulder surfing attacks. In this research work, we developed two systems; A position-based multi-layer graphical user authentication system and an Image-based multi-layer graphical user authentication system. The reason behind this research work is to compare the two systems, and evaluate them based on three major performance metrics: (1) Security, (2) Reliability (3) Individual preference.



Article History

Received: 30 December 2022

Accepted: 01 March 2023

Keywords

Graphical User Authentication;
Image-Based Security;
Multi-Layer;
Position-Based;
Randomization;
Shoulder Surfing Attack.

Introduction


The heart of security system is user authentication. When it comes to computer system security, Human factors are often considered the weakest link. There are three major areas where human computer interaction is important: authentication, security operations, and developing secure systems

(Patrick, *et al*). Here we focus on the authentication problem. The most common computer authentication method is for a user to submit a user name and a text password. The challenge with this approach is that it is difficult to remember long passwords, and so users prefer to use short passwords, which can be easily guessed or stolen.

CONTACT Audu Lovingkindness Edward ✉ lkaudu@gmail.com 📍 Department of Computer Science, Kebbi State University of Science & Technology Aliero, Nigeria.



© 2023 The Author(s). Published by Oriental Scientific Publishing Company.

This is an  Open Access article licensed under a Creative Commons license: Attribution 4.0 International (CC-BY).

Doi: <http://dx.doi.org/10.13005/ojst16.01.03>

Graphical user authentication scheme was introduced as an alternative to text-based schemes, which was somehow motivated by the fact that humans can easily remember pictures better than text; psychological studies supports this assumption as well. Pictures are generally easier to be remembered or recognized than text (R. N. Shepard).

Seeing that, most graphical Passwords schemes are prone to shoulder surfing and malware attacks (Vimal *et al.*, 2017). We embarked on this reaserch work to develop two graphical user authentication schemes, and compare both of them, order to test against shoulder surfing attack. The first scheme is image-based, in which the images selected during registration becomes the user password, while the second scheme is position-based, where the user only pays attention to the position of the images at the point of registration, keeps the positions to heart, as those positions will become user password.

Related Work

So many related projects which captures the minds and thoughts of scholars and researchers that have worked on areas relating to this subject matter were reviewed. Intelligent and useful scientific techniques was used to develop schemes in a bid to help provide security to personal information of users and prevent attacks. Some of these research works are given below

Tunga (2015), presented a survey of comparative study between different techniques of Graphical User Authentication (GVA). GUA has been considered to be a better alternative to text-based authentication, because psychologists have been able to prove, that humans remember images better than text. The strengths of each Graphical User Authentication technique were listed out, and their unique features, alongside the weaknesses. kaka *et.al* (2021) reviewed 10 recognition based graphical passwords algorithms, and evaluated them which respect to their individual strength and weaknesses and also analyzed them on the basis of their common usability and security threats. A comparison table was shown which showed that shoulder surfing attack remains a challenge for graphical password authentication. Even though, researchers have been able to develop algorithms to solve this problem, users still find it hard to easily create and understand recognition based graphical passwords. In a research work

carried out by Katsini *et al*, (2019), an eye tracking study was done in a bid to investigate the effects of users' cognitive styles towards the strength of the password that the user created and also explain whether and how the visual strategy during the graphical password composition, directly influences the passwords' strength. Witkin's Field Dependence-Independence Theory was adopted, and the analysis showed that users with different cognitive processing Characteristics, followed different patterns of visual behavior when they were creating their password, and this affected the strength of the password they created. Ndako *et al.*, (2021) took a closer look at Pure Recall-based GUAs with emphasis on the contextual parameter used for user authentication. It also opens up all the Pure Recall-based graphical user authentication schemes that were developed in the first 20 years (1996-2016) that Graphical passwords were introduced and the recently developed schemes. These studies were carried out in a bid to come up with a better positioned Pure Recall-Based Graphical User Authentication schemes, as alternatives to text password. Istyaq *et al*, (2021) proposed a security system which Combines both textual and graphical password, and uses the generation of Unique Grid Code (UGC), which is been selected by a user during registration, and then becomes the user's password. The significant feature that makes the security level of the proposed system quiet potent is that the system assigns a unique code for each image that is been selected, will varies from one image to another. Users are to select not more than 10 images and make not more than 5 clicks on each image. Atish, (2016) used persuasive Cued Click Points to influence the choice of users in click-based graphical passwords, in a bid to encourage users to select more images, so that it would be very difficult for hackers to guess the clicked-points. The main focus of the work, was on the evaluation of the Persuasive Cued points (PCP) graphical authentication system which incorporates usability and system security in three different levels. Furthermore, Suru and Murano, (2019), gave a detailed review of the current state of research in graphical authentication system. It also gives concise description of some of the mechanisms used in graphical authentication along with the strength and flaws of each. Some of the flaws include predictability, difficulty involved in using the system, its vulnerability to attacks, and the inability of systems to combine security

and usability efficiently. The paper concluded with suggestions for possible improvements of each authentication system. Bhand *et al.*, (2015) came up with a scheme that would be easy to use, give higher security so that it would be very difficult for attackers to gain access to the system. In this papers, cued click point (CCP) being the best and more reliable alternative for text password and the old graphical password system, was combined with new technologies like mobile phones and E-mail. The system was examined using 500 images of the same format. The result showed that the system is not prone to Brute force attack and is secured, as an alert message when an attacker tries to login with incorrect details after the third attempt. A few researchers designed and implemented a polynomial based Google Map Graphical Password (P-GMGP) system. This is an improvement of the existing Google Map Graphical Password system in which a specific location serves as password for authentication, so and that location can be captured by an attacker. The proposed system is resistant to shoulder Surfing attack and is faster than the existing system. It also allows efficient and

effective user authentication in cloud environment (Zhou *et al* 2019). Wang, (2020) took a study and reviewed the existing systems and saw a gross limitation of computational resources for mobile nodes. Hence, a great need for the development of a light weight anonymous and anti-quantum scheme for authentication, so that mobile nodes can roam securely on multiple service domain. A new scheme was developed, which when compared with the existing scheme showed great improvement in terms of efficiency, system security and resistance to quantum attack.

Methodology

The methodology adopted for this research work is the Design Research methodology (DRM). This method was carefully selected because it supports a more rigorous research approach by helping to plan and implement design research. Research methodology also shows how the research outcome at the end will be obtained in line with meeting the objective of the study (Sileyew, 2019). The dataflow diagram of the developed systems

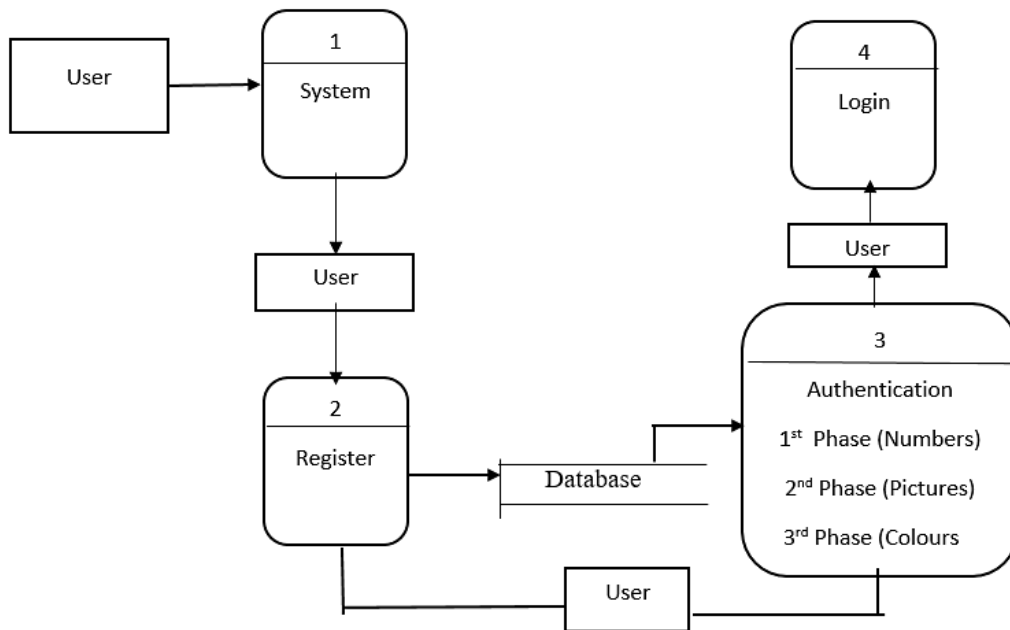


Fig. 1: Dataflow Diagram

Program Module Specification

In this system, several modules are integrated and combined to interact with themselves to provide the

functionalities of the system. The basic modules of the system are

Registration Module

This module allows new users to create an account with the system by registering in the registration page.

Login Module

This module allows users and admin to access the system by entering their login details. It also creates a session for each login by the user.

Home Module

This module presents all the activities carried out by the system.

Logout Module

This module terminates a user's session and allows them to exit the system.

based Multi-Layer Graphical User Authentication System) were implemented using the following tools.

- Laptop
- Django Server
- PostgreSQL
- PG Admin4
- Brackets & Visual Studio Code
- HTML5, CSS3, JavaScript
- Google Chrome

Activity Diagram

This is a model of processes in the system. It offers control flow and data flow mechanisms that coordinate the processes in the system. The activity diagram is illustrated below.

Results and Discussion

The two software (Position-based Multi-Layer Graphical User Authentication System and Image-

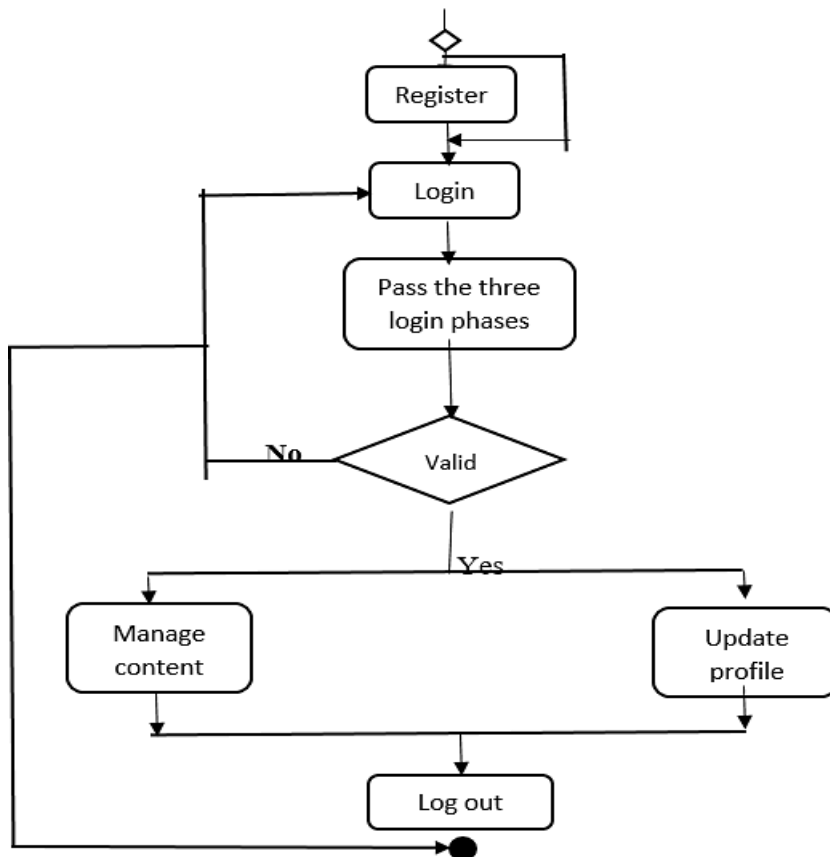


Fig. 3: Class Activity Diagram

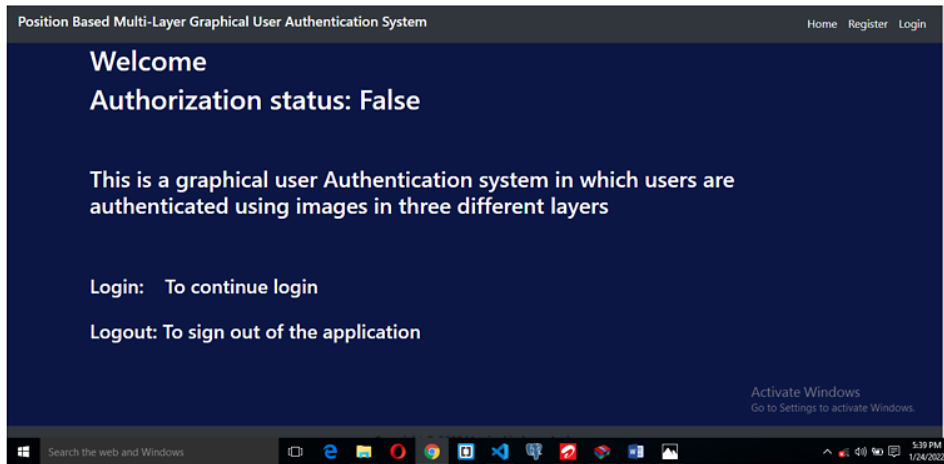


Fig. 3: screenshot Home page (Position-Based Multilayer GUAS)

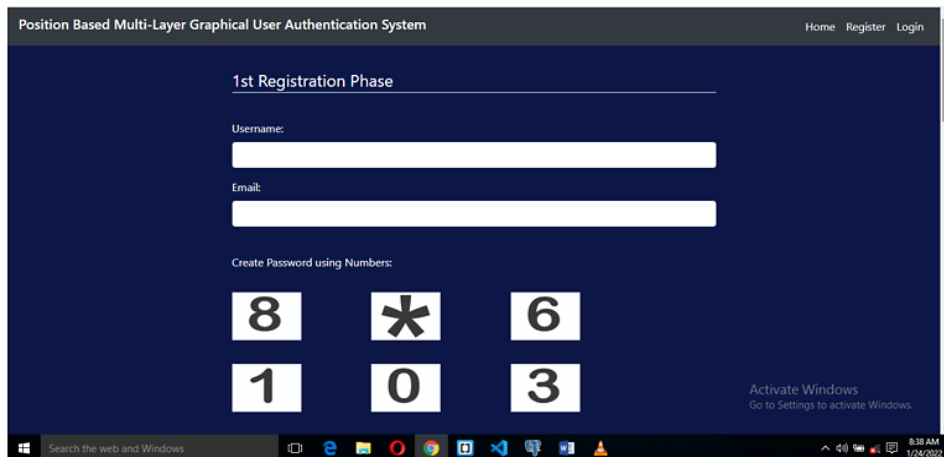


Fig. 4: Screenshot of Registration page-Phase 1 (Position-Based Multilayer GUAS)

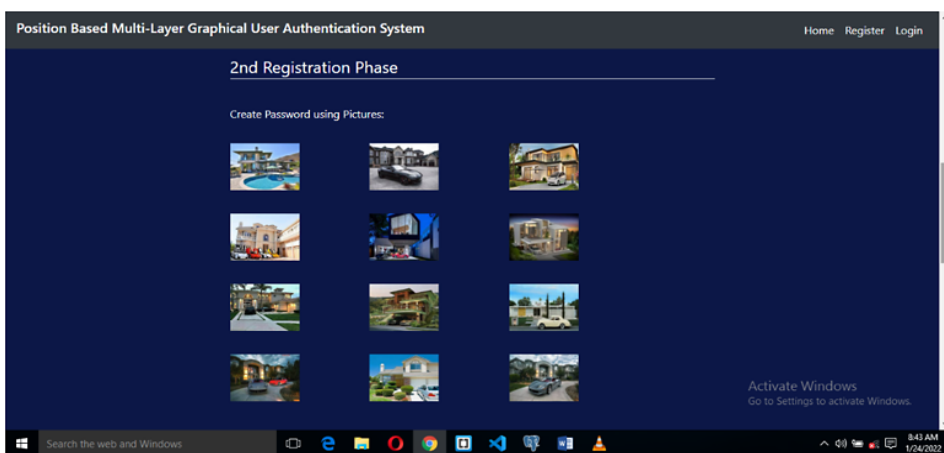


Fig. 5: Screenshot of Registration page -Phase 2 (Position-Based Multilayer GUAS)

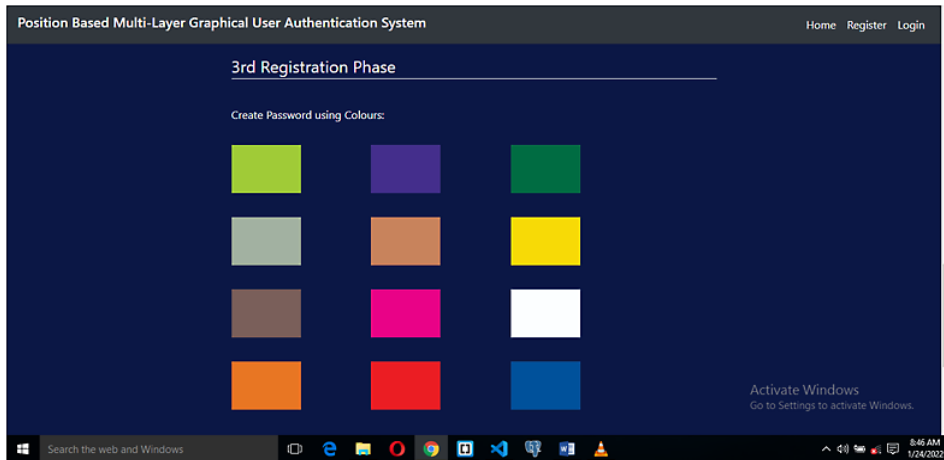


Fig. 6: Screenshot of Registration page -Phase 3 (Position-Based Multilayer GUAS)

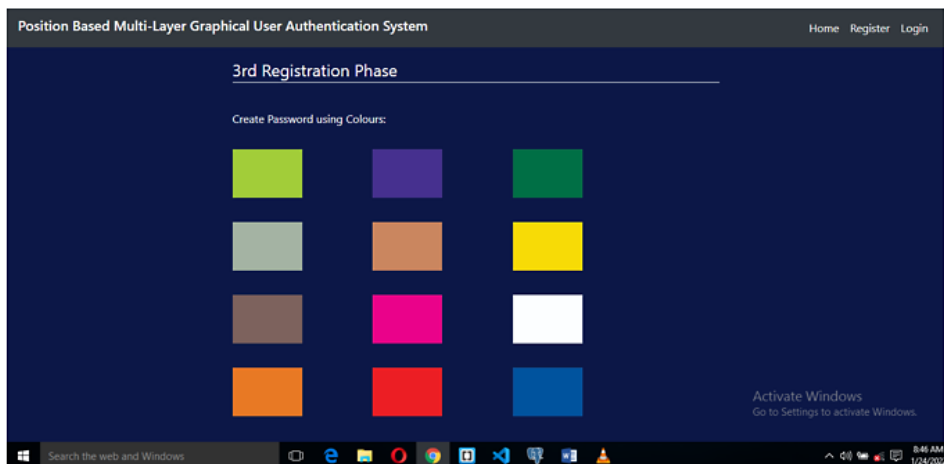


Fig. 7: Screenshot of Registration page -Phase 3 (Position-Based Multilayer GUAS)

To register, enter your proposed 'username', 'Email', 'Password1', 'Password2, and 'password3' for verification, then click on Signup.

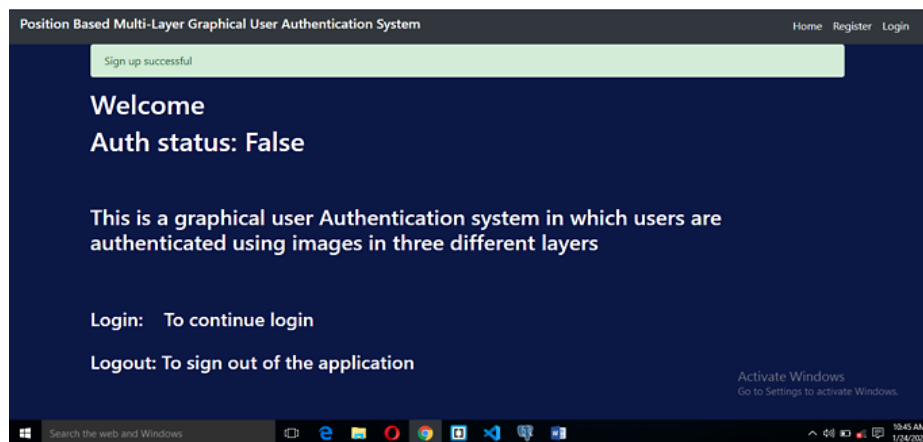


Fig. 8: Screenshot Showing Signup Successful (Position-Based Multilayer GUAS)

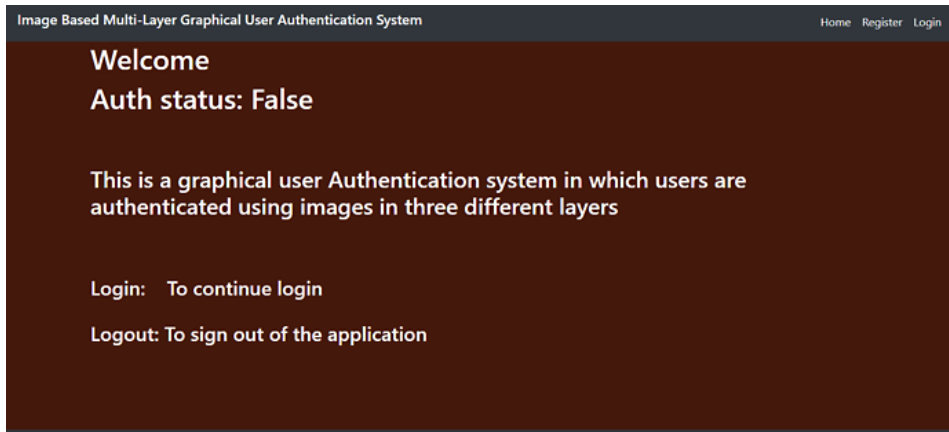


Fig. 9: Screenshot Home page (Image-Based Multilayer GUAS)

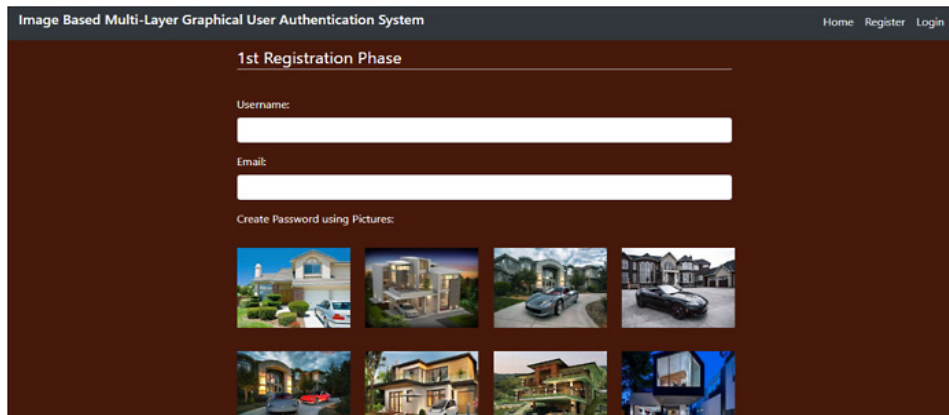


Fig. 10: Screenshot of Registration page-Phase 1 (Image-Based Multilayer GUAS)



Fig. 11: Screenshot of Registration page-Phase 2 (Image-Based Multilayer GUAS)



Fig. 12: Screenshot of Registration page-Phase 3 (Image-Based Multilayer GUAS)

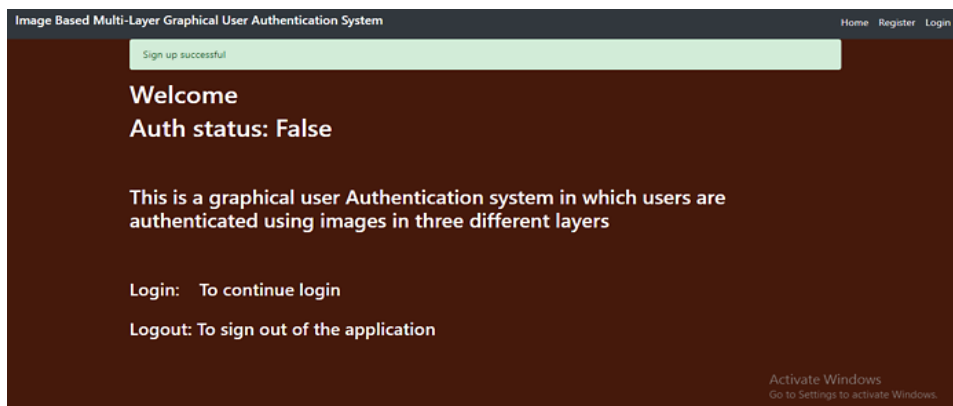


Fig. 13: Screenshot Showing Signup Successful (Position-Based Multilayer GUAS)

After registration, the user will need to go through three different phases to login. Each Login phase is connected to the next. So, if a user supplies a wrong login details in the 1st phase, he would not be able to move to the 2nd phase. The user successfully login to the system after passing through the three authentication phases.

Performance Evaluation

In order to properly carry out performance evaluation on the system, we compared the Image-based graphical user authentication system with the Position-based Multi-layer graphical user authentication system. The performance metrics we used are.

- Security
- Reliability
- Individual Preference

The approach we used for this experiment is the within user, in which the total number of users were been divided into two groups. Some of the users begin by using the first system while others begin by using the second system, after which the users will swap. At the end of the day, all the users we able to use both systems. We used a total of 50 participants for this experiment. Each user registered and logged in using the systems. Their registration and login time was recorded and their comments were received using google form and then interpreted and analyzed using SPSS (Statistical Package for Social Sciences). A summary of their registration and login time is shown in the tables below.

Table 1: Registration time of Users (Position-Based GUAS)

Users	Registration Time	Percentage (%)
18 users	1- 60 seconds	36%
26 users	60-120 seconds	52%
6 users	120-200 seconds	12%

Table 2: Calculation of mean for Registration time of Users (Position-Based GUAS)

Registration Time	Average time (x)	Users (f)	Fx
1- 60 seconds	30 seconds	18 users	540
60-120 seconds	60 seconds	26 users	1560
120-200 seconds	90 seconds	6 users	540
		$\sum f=50$	$\sum fx=2640$

$$\text{Mean} = \frac{\sum fx}{\sum f} = \frac{2640}{50} = 52.8 \text{ seconds}$$

Table 3: Registration time of Users (Image-Based GUAS)

Users	Registration Time	Percentage (%)
12 users	1- 60 seconds	24%
23 users	60-120 seconds	46%
15 users	120-200 seconds	30%

Table 4: Calculation of mean for Registration time of Users (Image -Based GUAS)

Registration Time	Average time (x)	Users (f)	Fx
1- 60 seconds	30 seconds	12 users	360
60-120 seconds	60 seconds	23 users	2070
120-200 seconds	90 seconds	15 users	1350
		$\sum f=50$	$\sum fx=3780$

$$\text{Mean} = \frac{\sum fx}{\sum f} = \frac{3780}{50} = 75.6 \text{ seconds}$$

From the mean gotten from table 4.2, the average registration time of users for the (Position-Based GUAS) is 52.8 seconds. But, from the mean gotten

from table 4.4, the average registration time for (Image-Based GUAS) is 75.6 seconds. Hence, the Position-Based GUAS takes shorter time to register.

Table 5: Login time of Users (Position-Based GUAS)

Users	Login Time	Percentage (%)
36 users	1- 60 seconds	72%
12 users	60-120 seconds	24%
2 users	120-200 seconds	4%

Table 6: Calculation of mean for Login time of Users (Position -Based GUAS)

Login Time	Average time (x)	Users (f)	Fx
1- 60 seconds	30 seconds	36 users	1080
60-120 seconds	60 seconds	12 users	720
120-200 seconds	90 seconds	2 users	180
		$\sum f=50$	$\sum fx=1980$

$$\text{Mean} = \frac{\sum fx}{\sum f} = \frac{1980}{50} = 39.6 \text{ seconds}$$

Table 7: Login time of Users (Image-Based GUAS)

Users	Login Time	Percentage (%)
36 users	1- 60 seconds	72%
10 users	60-120 seconds	20%
4 users	120-200 seconds	8%

Table 8: Calculation of mean for Login time of Users (Image -Based GUAS)

Login Time	Average time (x)	Users (f)	Fx
1- 60 seconds	30 seconds	36 users	1080
60-120 seconds	60 seconds	10 users	600
120-200 seconds	90 seconds	4 users	360
		$\sum f=50$	$\sum fx=2040$

$$\text{Mean} = \frac{\sum fx}{\sum f} = \frac{2040}{50} = 40.8 \text{ seconds}$$

The result of the mean gotten from table 4.6, the average login time of users for the (Position-Based GUAS) is 39.6 seconds. But, from the mean gotten from table 4.8, the average registration time for (Image-Based GUAS) is 40.8 seconds. Hence, the Position-Based GUAS takes shorter time to register.

System Security

The primary objective of this research work is to solve the problem of shoulder surfing attack, hence the development and implementation of the Position-Based Graphical Authentication System. We evaluated the system to see if it is resistant

to shoulder surfing attack, in comparison with the Image-based graphical user authentication system. Our Position-Based GUAS is resistant to both picture capturing and video recording of password (images clicked) during login. Hence it is resistant to shoulder surfing attack, but the Image-Based GUAS is not.

System Reliability

After giving room to 50 participants to test the two systems, they were asked to make recommendation and individually chose the system that they feel is more reliable. Their responses are shown below.

Table 9: Responses from Participants based on System Reliability

Participants	System Reliability
Participant 1	Position-Based GUAS
Participant 2	Position-Based GUAS
Participant 3	Image-Based GUAS
Participant 4	Position-Based GUAS
Participant 5	Position-Based GUAS
Participant 6	Position-Based GUAS
Participant 7	Position-Based GUAS
Participant 8	Position-Based GUAS
Participant 9	Position-Based GUAS
Participant 10	Image-Based GUAS
Participant 11	Image-Based GUAS
Participant 12	Position-Based GUAS
Participant 13	Position-Based GUAS
Participant 14	Position-Based GUAS
Participant 15	Image-Based GUAS
Participant 16	Position-Based GUAS
Participant 17	Position-Based GUAS
Participant 18	Image-Based GUAS
Participant 19	Position-Based GUAS
Participant 20	Position-Based GUAS
Participant 21	Position-Based GUAS
Participant 22	Position-Based GUAS
Participant 23	Position-Based GUAS
Participant 24	Position-Based GUAS
Participant 25	Position-Based GUAS
Participant 26	Position-Based GUAS
Participant 27	Position-Based GUAS
Participant 28	Position-Based GUAS
Participant 29	Position-Based GUAS
Participant 30	Position-Based GUAS
Participant 31	Position-Based GUAS
Participant 32	Position-Based GUAS
Participant 33	Position-Based GUAS
Participant 34	Image-Based GUAS
Participant 35	Position-Based GUAS
Participant 36	Position-Based GUAS
Participant 37	Position-Based GUAS
Participant 38	Image-Based GUAS
Participant 39	Image-Based GUAS

Participant 40	Image-Based GUAS
Participant 41	Image-Based GUAS
Participant 42	Image-Based GUAS
Participant 43	Image-Based GUAS
Participant 44	Image-Based GUAS
Participant 45	Position-Based GUAS
Participant 46	Image-Based GUAS
Participant 47	Image-Based GUAS
Participant 48	Image-Based GUAS
Participant 49	Position-Based GUAS
Participant 50	Image-Based GUAS

Their responses were further represented using a bar chart, as shown below.

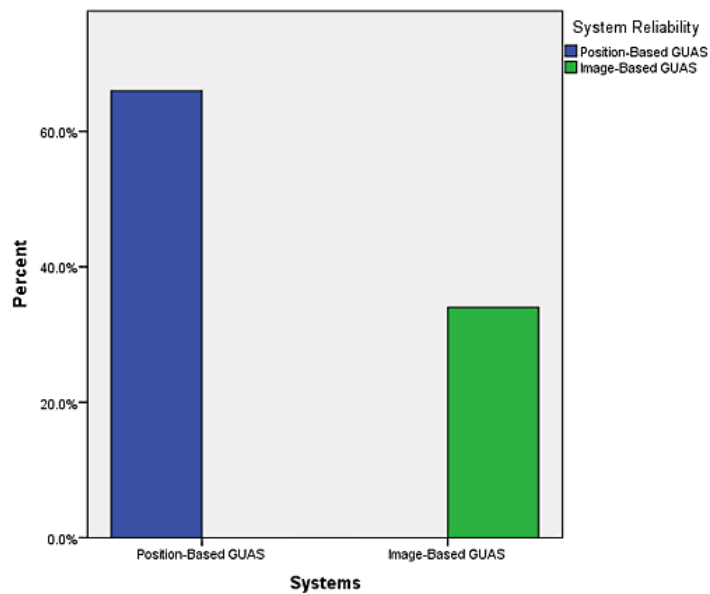


Fig. 14: Graphical representation of Performance Evaluation (System Reliability) carried out

From the graph above, 66.6% which is equivalent to 33 out of the 50 Participants responded that the Position-based Multi-layer Graphical user authentication system is more reliable than the Image-Based Graphical user authentication system.

Individual Preference

Furthermore, the 50 participants were asked to choose the system that is best for them between the two systems, based on personal preference. The choices they made is shown in the table below.

Table 10: Responses from Participants based on Individual Preference

Participants	Personal Preference
Participant 1	Position-Based GUAS
Participant 2	Position-Based GUAS
Participant 3	Image-Based GUAS
Participant 4	Position-Based GUAS
Participant 5	Position-Based GUAS

Participant 6	Position-Based GUAS
Participant 7	Position-Based GUAS
Participant 8	Position-Based GUAS
Participant 9	Position-Based GUAS
Participant 10	Image-Based GUAS
Participant 11	Image-Based GUAS
Participant 12	Position-Based GUAS
Participant 13	Position-Based GUAS
Participant 14	Position-Based GUAS
Participant 15	Image-Based GUAS
Participant 16	Position-Based GUAS
Participant 17	Position-Based GUAS
Participant 18	Image-Based GUAS
Participant 19	Image-Based GUAS
Participant 20	Position-Based GUAS
Participant 21	Position-Based GUAS
Participant 22	Position-Based GUAS
Participant 23	Position-Based GUAS
Participant 24	Position-Based GUAS
Participant 25	Position-Based GUAS
Participant 26	Image-Based GUAS
Participant 27	Position-Based GUAS
Participant 28	Image-Based GUAS
Participant 29	Image-Based GUAS
Participant 30	Position-Based GUAS
Participant 31	Position-Based GUAS
Participant 32	Image-Based GUAS
Participant 33	Position-Based GUAS
Participant 34	Image-Based GUAS
Participant 35	Position-Based GUAS
Participant 36	Position-Based GUAS
Participant 37	Position-Based GUAS
Participant 38	Image-Based GUAS
Participant 39	Image-Based GUAS
Participant 40	Image-Based GUAS
Participant 41	Image-Based GUAS
Participant 42	Image-Based GUAS
Participant 43	Image-Based GUAS
Participant 44	Image-Based GUAS
Participant 45	Position-Based GUAS
Participant 46	Image-Based GUAS
Participant 47	Image-Based GUAS
Participant 48	Image-Based GUAS
Participant 49	Image-Based GUAS
Participant 50	Image-Based GUAS

Their responses were further represented using a bar chart, as shown below.

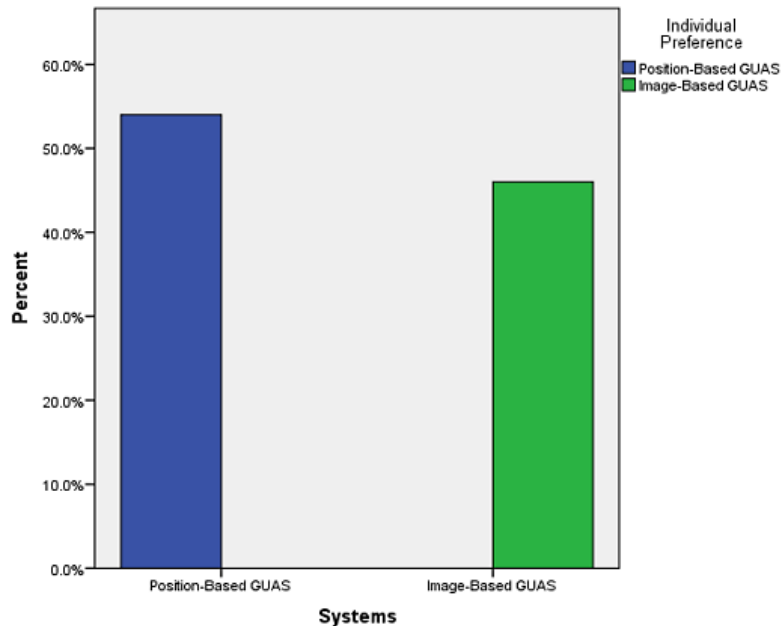


Fig. 15: Graphical representation of Performance Evaluation (Individual preference) carried out

From the graph above, 54% which is equivalent to 27 out of the 50 Participants responded that they prefer the Position-based Multi-layer Graphical user authentication system to the Image-Based Graphical user authentication system.

Conclusion and Future Work

In this research work, we developed two systems, Position-Based graphical user authentication system and an Image-Based graphical user authentication system. We compared both systems based on three performance metrics (Security, reliability, Individual Preference).

The scope of this research work cuts across all sectors. This research will be beneficial to the society in general, and also help different sectors and industries to secure their data against intruders.

At the end of this research and after the comparison, the Position based multi-layer graphical user authentication system performed better, both in terms of security, reliability and Individual preference.

Acknowledgement

The author would like to thank, (Insert university name and Dept. name) for their guidance and support to complete this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

Conflict of Interest

The authors do not have any conflict of interest.

References

1. Vimal Gaur, A. S. (2017). Authentication using a Combination of Color Scheme and Musical Notes. *International Journal of Engineering Research & Technology (IJERT)*, 1-5.
2. Harinandan Tunga, D. S. (2015). Graphical User Authentication Techniques for Security: A Comparative Study. *International Journal of Engineering and Advanced Technology (IJEAT)*, 1-7.
3. Jiya Gloria Kaka, I. O. (2021). Recognition Based Graphical Password Algorithms: A Survey. 1-10.
4. Christina Katsini, Christos Fidas, Marios Belk, George Samaras, Nikolaos Avouris. (2019). A Human Cognitive Perspective of Users' Password Choices in Recognition-based Graphical Authentication. *International Journal of Human-Computer Interaction*, 1-24.
5. Adama Victor Ndako, O. I. (2021). Pure Recall-Based Graphical User Authentication Schemes: Perspectives from a Closer look. *African Human-Computer Interaction Conference*, 1-5.
6. Istyaq, S. (2016). Hybrid Authentication System using QR Code with OTP. *International Journal of Computer and Information Engineering*, 1-4.
7. Atish Nayak, R. B. (2016). Analysis of Knowledge Based Authentication System Using Persuasive Cued Click points. *7th International Conference on Communication, Computing and Virtualization*, 1-8.
8. Murano, H. U. (2019). Security and User Interface Usability of Graphical Authentication Systems – A Review. *International Journal of Computer Trends and Technology (IJCTT)* - Volume 67 Issue 2, 1-21.
9. Amol Bhand, v. d. (2015). Enhancement of Password Authentication system using Graphical Images. *International Conference on Information Processing (ICIP)*, 1-4.
10. Zhili Zhou, C.-N. Y. (2019). Polynomial-Based Google Map Graphical Password System against Shoulder-Surfing Attacks in Cloud Environment. *Hindawi*, 1-9.
11. Wang, Y. Z. (2020). A Lattice-Based Authentication Scheme for Roaming Service in Ubiquitous Networks with Anonymity. *Hindawi Security and Communication Networks*, 1-19.
12. Sileyew, K. J. (2019). Research Design and Methodology. *Intech Open*, 1-14.
13. D. Weinshall and S. Kirk Patrick, Passwords you'll never forget, but can't recall, 2004, doi: 10.1145/985921.986074