Journal of
Computer Science and Software Development

JScholar
Fostering Scholarly Communication

Research Article Open Access

A Comparison between Position-Based and Image-Based Multi-Layer Graphical User Authentication System

Audu Lovingkindness Edward*, Dr. Hassan Suru and Mustapha Abubakar Giro

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

***Corresponding author:** Audu Lovingkindness Edward, Department of Computer Science, Kebbi State University of Science & Technology Aliero, Nigeria, Tel: +2348148964291, E-mail: lkaudu@gmail.com

Received Date: September 27, 2023 **Accepted Date:** October 27, 2023 **Published Date:** October 30, 2023

Citation: Audu Lovingkindness Edward, Dr. Hassan Suru, Mustapha Abubakar Giro (2023) A Comparison between Position-Based and Image-Based Multi-Layer Graphical User Authentication System. J Comput Sci Software Dev 2: 1-11.

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 calls for that the user provides textual password as a way to benefit get right of entry to the system. But, this technique has shown a considerable disadvantage and several vulnerabilities, certainly one of which is the difficulty in recalling or remembering textual passwords. Numerous different attacks that textual passwords are susceptible to encompass brute force attack, dictionary attack, and shoulder spying and so on. 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. For the purpose of this research work, two systems were developed; An Image-based multi-layer graphical user authentication system and a Position-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.

Keywords: Graphical User; Human Computer Interaction; Multi-Layer; Image-Based; Password; Shoulder Surfing Attack; Randomization; System Security; Position-Based; Authentication

Introduction

The heart of security system is user authentication. In terms of computer system security, Human factors are frequ ntly taken into consideration as the weakest hyperlink. There are three major areas where human computer interaction is important: authentication, security operations, and developing secure systems [13]. Here we focus on the authentication problem. The most commonplace computer authentication approach is for a user to submit his or her username 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.

Graphical user authentication password scheme came into the scene as an alternative to textual content-primarily based schemes, which was one way or the other prompted through the fact that people can effortlessly don't forget pictures higher than text; psychological studies supports this assumption as well. Pictures are typically less difficult to be remembered or recognized than textual content [9].

Seeing that, most graphical Passwords schemes are prone to shoulder surfing and malware attacks [1]. We embarked on this research work in order to build two graphical authentication schemes, and compare both of them, order to check towards shoulder surfing attack. The first scheme is image-based, in which the images selected during registration becomes the user passward, 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: [2] supplied a survey of comparative look at between specific strategies of Graphical User Password Authentication. The model has been taken into consideration to be a higher opportunity to text-primarily based authentication, due to the fact psychologists were capable of prove, that humans don't forget pictures higher than textual content. The strengths of each Graphical User Authentication approach have been listed out, and their particular functions, alongside the weaknesses. [3] reviewed 10 popularity based graphical passwords algorithms, and evaluated them which respect to their individual power and weaknesses and additionally analysed them on the idea of their commonplace usability and protection threats. A comparison desk become proven which showed that shoulder browsing attack remains a threat for graphical password authentication. Even though, researchers were capable of expanding algorithms to clear up this problem, users nevertheless discover it difficult to create and apprehend recognition based totally graphical passwords. In a research work accomplished by [4], an eye tracking examination was done in a bid to find out 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 subject Dependence-Independence principle was adopted, and the evaluation confirmed that users with distinctive cognitive processing characteristics, accompanied special styles of visible behaviour once they have been growing their password, and this affected the power of the password they created. [5] took a closer study on Pure Recall-based Graphical User Authentication, with emphasis on the contextual parameter used for person's authentication. It also opens up all of the Pure Recall-based Graphical User Authentication schemes that have been developed within the first twenty years (1996-2016) that Graphical passwords have been added and the currently evolved schemes. These studies were accomplished in a bid to provide you with a better placed pure keep in mind-primarily based Graphical User Authentication schemes, as alternatives to textual content password. [6] proposed a security model which combines both textual and graphical password, and uses the generation of unique Grid Code (UGC), that is been selected by a person in the course of registration, after which will become the person's password. The good sized feature that makes the security stage of the proposed machine quiet robust is that the system assigns a completely unique code for each picture this is been selected, will varies from one image to every other. Users are to choose not extra than 10 snap shots and make not more than 5 clicks on every image. [7] used persuasive Cued click on points to persuade the choice of users in click-based totally graphical passwords, in a bid to inspire users to select more snap shots, in order that it'd be very hard for hackers to wager the clicked-points. the main awareness of the paintings, turned into on the evaluation of the Persuasive Cued points (PCP) graphical authentication gadget which incorporates usability and device safety in 3 unique degrees. furthermore, [8], gave a detailed assessment of the current

nation of studies in graphical authentication gadget. It also gives concise description of some of the mechanisms used in graphical authentication, alongside the energy and flaws of each. some of the failings include predictability, issue involved in the usage of the machine, its vulnerability to assaults, and the incapability of systems to mix protection and usefulness efficaciously. The paper concluded with suggestions for feasible enhancements of each authentication model. [9] came up with a scheme that might be easy to use, supply better security so that it might be very hard for attackers to benefit get entry to the machine. in this papers, cued click on factor (CCP) being the high-quality and more reliable alternative for textual content password and the old graphical password system, was mixed with new technologies like cellular phones and E-mail. The model was examined the usage of 500 pictures of the equal format. The result confirmed that the developed model isn't always at risk of Brute pressure attack and is secured, as an alert message whilst an attacker tries to log-in with incorrect info after the 1/3 attempt. A few researchers designed and applied a polynomial based totally Google Map Graphical Password (P-GMGP) machine. this is an improvement of the existing Google Map Graphical Password system in which a selected area serves as password for authentication, so and that location can be captured by means of an attacker. The proposed system is immune to shoulder surfing assault and is faster than the existing model. It additionally allows efficient and powerful person authentication in cloud environment. [10] took an observe and reviewed the prevailing structures and noticed a gross problem of computational resources for cellular nodes. as a result, an extraordinary need for the improvement of a mild weight anonymous scheme for authentication, so that mobile nodes can roam securely on more than one service area. a new scheme was developed, which when as compared with the prevailing scheme confirmed first-rate improvement in terms of performance, gadget protection and resistance to quantum assault.

Methodology

The methodology adopted for this research work is the Design Research methodology (DRM). This technique became carefully decided on as it helps a greater rigorous studies approach by way of helping to devise and enforce design studies. Research Methodology also indicates how the studies final results on the stop may be obtained in line with meeting the goal of the have a look at [12].

One of the advantageous objectives of design research methodology is that it does not only aims at understanding, but also at improving designs. It requires a model or theory of the existing system, model of the proposed system, and the vision of the support that is likely to change the existing model into the desired system, and maintain this. That means, design research methodology itself involves design, namely the creation and evaluation of a model or theory of the proposed system.

The dataflow diagram of the developed systems

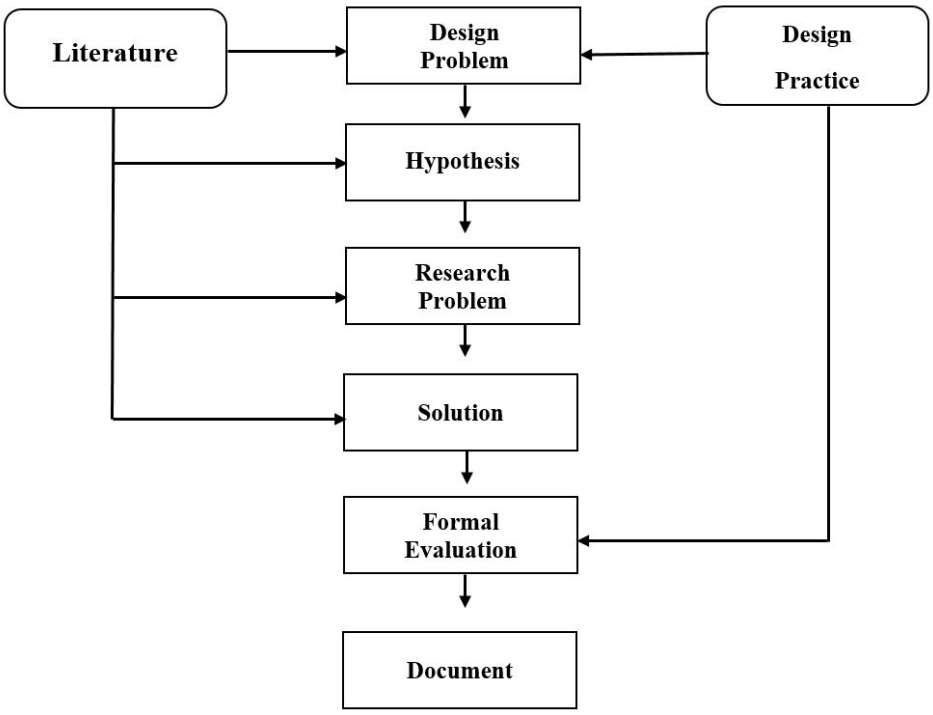

Figure 1: Design Research Methodology (DRM)

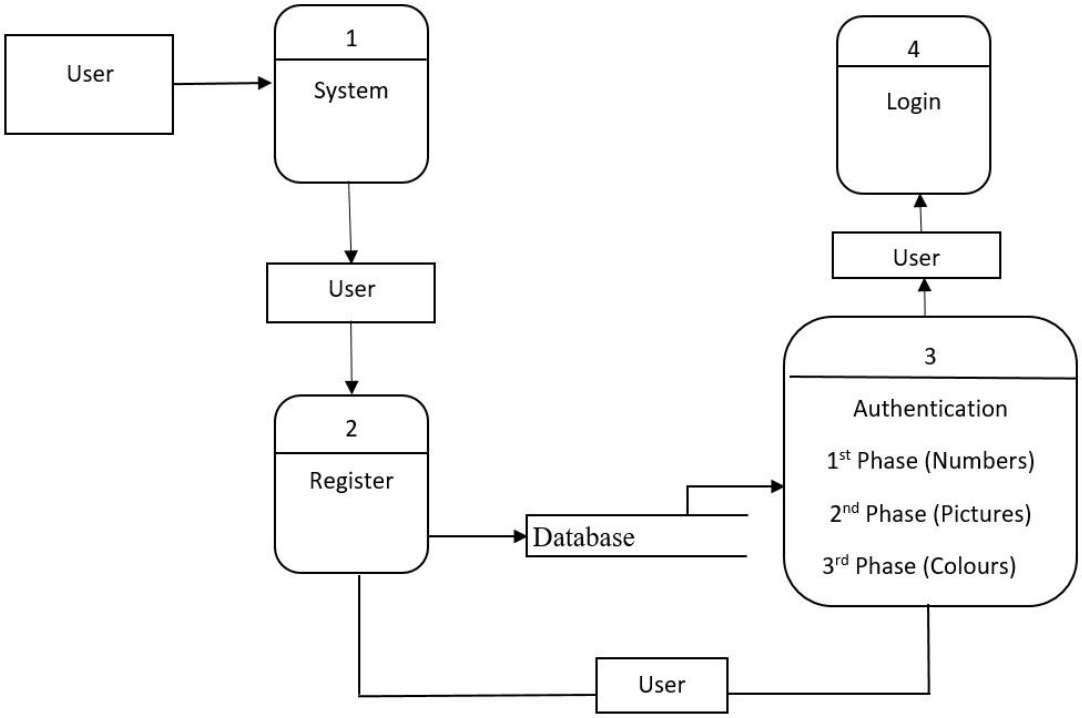

Figure 2: Dataflow Diagram

Program Module Specification

Numerous modules are included and combined to have interaction with themselves to offer the functionalities of the system. The primary modules of the are:

i) **Registration Module:** New users use this module to create an account with the system by clicking on the registration button to register.

ii) **Home Module:** All the activities carried out by the system is represented in this model.

iii) **Login module:** this is the module through which users and admin access the system by simply providing their login details.

It then creates a unique session for each user.

iv) Logout module: Users exit the system using this model

The two software (Position-based multi-layer GUAS and Image-based multi-layer GUAS) were implemented using the following tools.

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

Results and Discussion

Activity diagram

This is a model of processes in the system. It shows data and control flow mechanisms that helps to coordinate the various processes in the system. Shown below, is the activity diagram

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

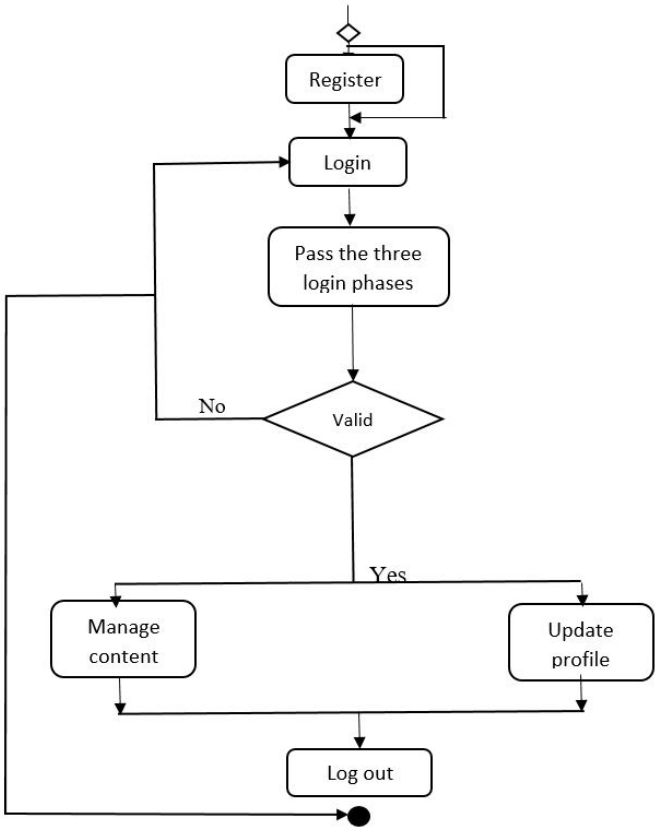

Figure 3: Class Activity Diagram

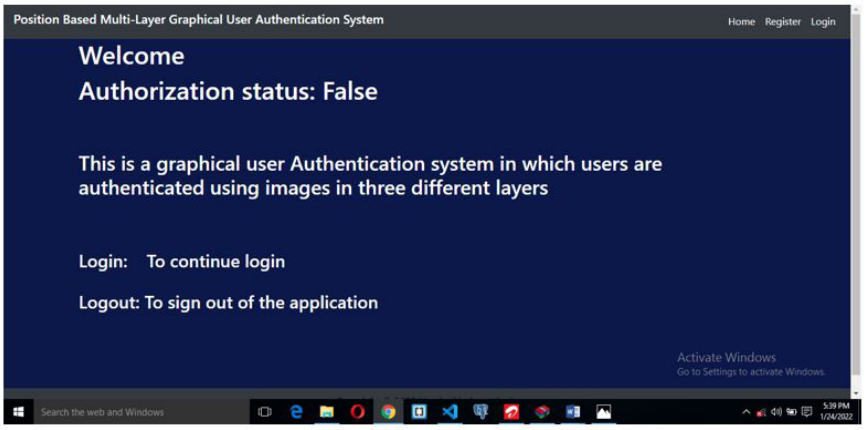

Figure 4: screenshot Home page (Position-Based Multilayer GUAS)

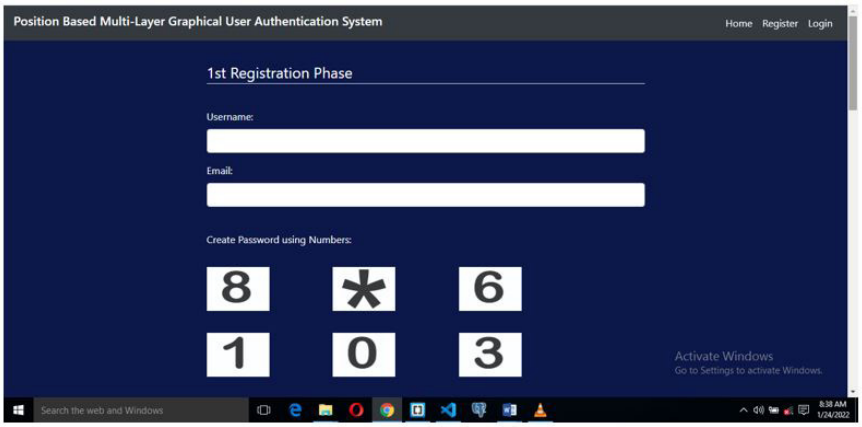

Figure 5: Screenshot of Registration Page-Phase (Position-Based Multilayer GUAS)

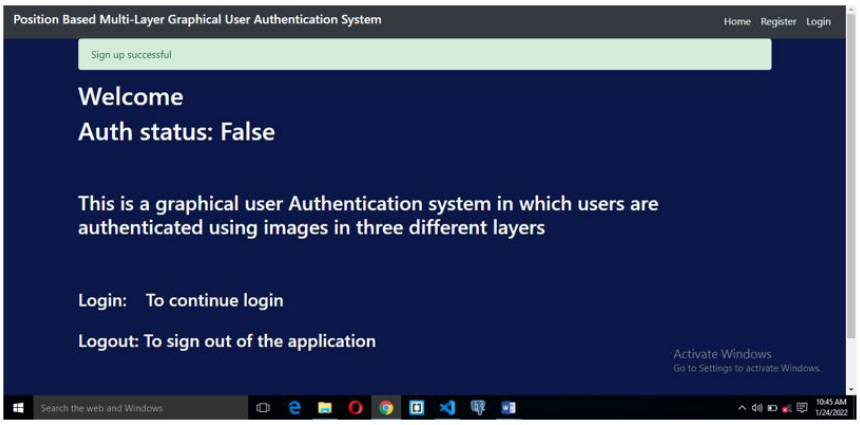

Figure 6: Screenshot Showing Signup Successful (Position-Based Multilayer GUAS)

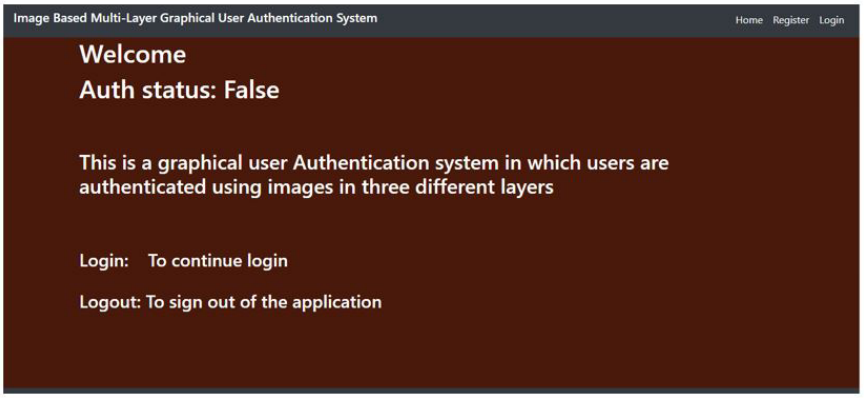

Figure 7: Screenshot Home page (Image-Based Multilayer GUAS)

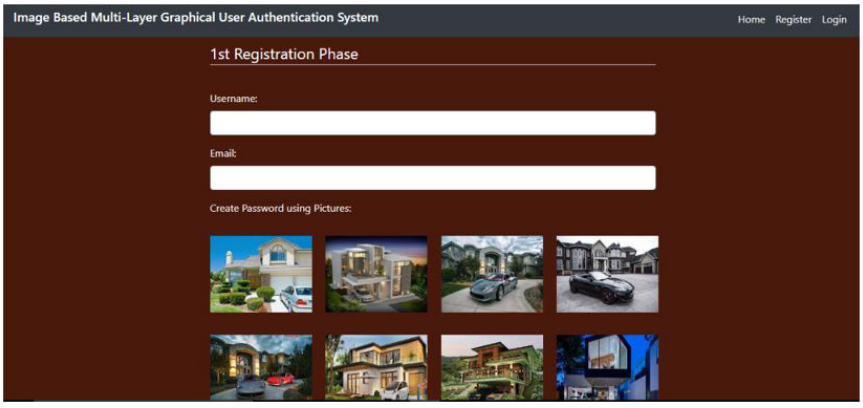

Figure 8: Screenshot of Registration Page-Phases (Image-Based Multilayer GUAS)

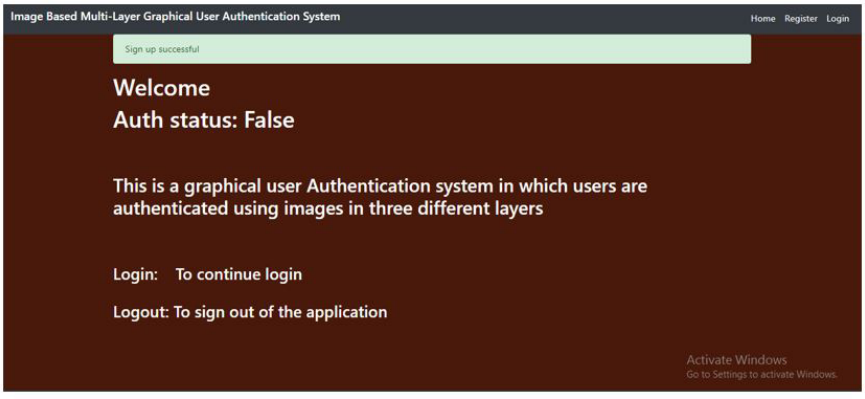

Figure 9: Screenshot Showing Signup Successful (Position-Based Multilayer GUAS)

Once the registration has been completed, the user will need to go through three different phases to login. The three Log-in phases are connected to each other and so they work together. If a user supplies a wrong login details in one phase, he would not be able to move to the next 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 GUAS.

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
		$\sum f = 50$	$\sum fx = 2640$

$Mean = \sum fx = 2640 = 52.8\ seconds\ \sum f = 50$

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
		$\sum f = 50$	$\sum fx = 3780$

$Mean = \sum fx = 3780 = 75.6\ seconds\ \sum f = 50$

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
		$\sum f = 50$	$\sum fx = 1980$

$Mean = \sum fx = 1980 = 39.6 seconds \ \sum f = 50$

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
		$\sum f = 50$	$\sum fx = 2040$

$Mean = \sum fx = 2040 = 40.8 seconds \ \sum f = 50$

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 systems were evaluated in order to find the most secured, against shoulder surfing attack. It was concluded after experiment that the 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. The bar chart below perfectly captures their responses:

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 bar chart below captures their responses in a clear way:

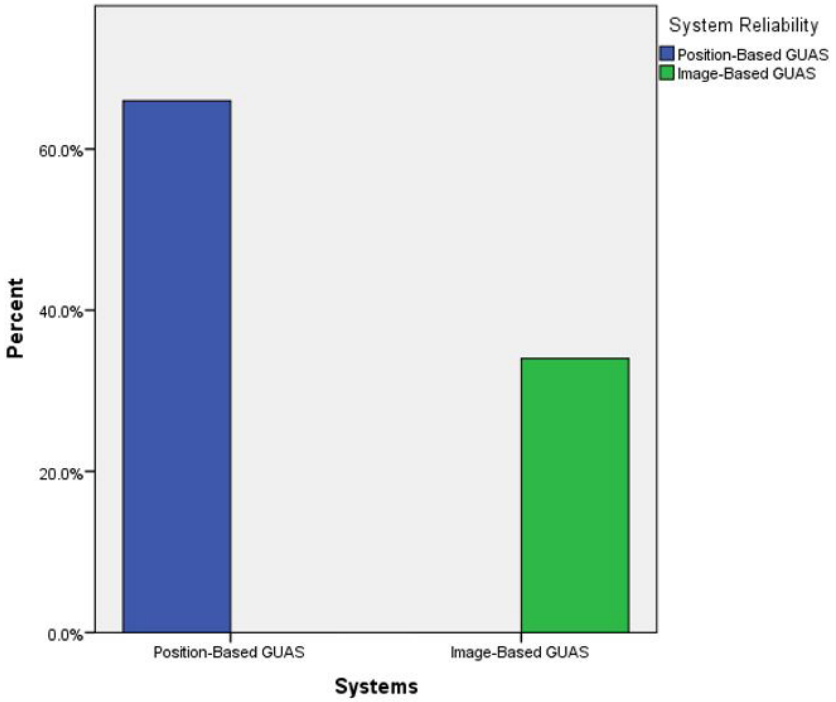

Figure 10: Graphical representation of Performance Evaluation (System Reliability) carried out

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

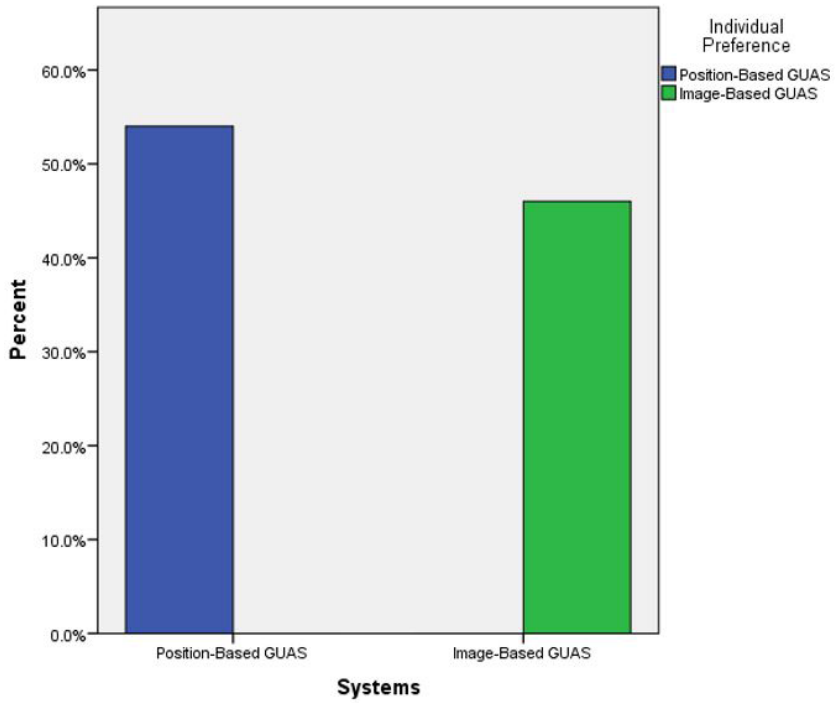

Figure 11: Graphical representation of Performance Evaluation (Individual preference) carried out

From the graph above, 54% which is equivalent to 27 out of the 50 Participants responded that they prefer the Position-based multi-layer GUAS 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 throughout all sectors. This research will be useful to the society in standard, and additionally help different sectors and industries to secure their records in opposition to 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.

References

1. Vimal Gaur AS (2017) Authentication using a Combination of Color Scheme and Musical Notes. International Journal of Engineering Research & Technology (IJERT) 1-5.

2. Harinandan Tunga DS (2015) Graphical User Authentication Techniques for Security: A Comparative Study. International Journal of Engineering and Advanced Technology (IJEAT) 1-7.

3. Jiya Gloria Kaka IO (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 OI (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 RB (2016) Analysis of Knowledge Based Authentication System Using Persuasive Cued Click points. 7th International Conference on Communication, Computing and Virtualization 1-8.

8. Murano HU (2019) Security and User Interface Usability of Graphical Authentication Systems – A Review. International Journal of Computer Trends and Technology (IJCTT) 67: 1-21.

9. Amol Bhand vd (2015) Enhancement of Password Authentication system using Graphical Images. International Conference on Information Processing (ICIP) 1-4.

10. Zhili Zhou CNY (2019) Polynomial-Based Google Map Graphical Password System against Shoulder-Surfing Attacks in Cloud Environment. Hindawi 1-9.

11. Wang YZ (2020) A Lattice-Based Authentication Scheme for Roaming Service in Ubiquitous Networks with Anonymity. Hindawi Security and Communication Networks 1-19.

12. Sileyew KJ (2019) Research Design and Methodology. Intech Open 1-14.

13. D Weinshall, S Kirk Patrick (2004) Passwords you'll never forget, but can't recall.