American Journal of Software Engineering and Applications
2022; 11(1): 1-11
http://www.sciencepublishinggroup.com/j/ajsea
doi: 10.11648/j.ajsea.20221101.11
ISSN: 2327-2473 (Print); ISSN: 2327-249X (Online)

Position-Based Multi-Layer Graphical User Authentication System

Audu Lovingkindness Edward[1, *], Hassan Umar Suru[1], Jasmyne Okudo[2]

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

[2]GitStart Community, San Francisco, USA

Email address:

lkaudu@gmail.com (A. L. Edward), suruhassan@yahoo.com (H. U. Suru), jasmyneokudo@gmail.com (J. Okudo)

[*]Corresponding author

To cite this article:

Audu Lovingkindness Edward, Hassan Umar Suru, Jasmyne Okudo. Position-Based Multi-Layer Graphical User Authentication System. *American Journal of Software Engineering and Applications*. Vol. 11, No. 1, 2022, pp. 1-11. doi: 10.11648/j.ajsea.20221101.11

Received: March 30, 2022; **Accepted**: April 13, 2022; **Published**: April 20, 2022

Abstract: A password is said to be secure, if it is resistant to various forms of attack. The oldest authentication approach used in computer systems is the text-based approach, which requires that the user supplies textual password in order to gain access to the system. Overtime, this approach has been shown to have a significant drawback and several vulnerabilities, one of which is the difficulty involved in remembering textual passwords. Textual passwords are vulnerable to several attacks like brute force attacks, shoulder spying, dictionary attacks etc. Graphical Password was introduced which involves the use of images for user authentication. In this research work, we developed a position-based multi-layer graphical user authentication system, in order to solve shoulder surfing attacks that most graphical password authentication schemes are faced with. The system authenticates users in three different phases so as to ensure maximum system security. The exact position of the images that the user selects during the registration phase will make up the user's password. However, the images will be randomized during the login phase in order to confuse attackers. The newly develop system was evaluated using three performance metrics: (1) Security, (2) Usability, (3) Reliability, and the result showed that the newly developed methodology is suitable for use, very reliable and provides maximum system security.

Keywords: Graphical User Authentication, Multi-layer, Randomization, Position-Based, Security, Shoulder Surfing

1. Introduction

User Authentication is a bridge between Human Computer Interaction (HCI) and Computer Systems Security. In the early years of computing and Information technology, Computer Applications had little or no security. It continued like that for a number of years until the importance of system security was truly realized. Prior to that time, data was considered to be useful, but not something to be protected. As data continued to increase and started becoming voluminous, the need to compartmentalize data and ensure its security become necessary and important.

There are several authentication techniques. They include: Token based techniques, where a token (unique Pin) is used e.g. ATM Systems; Biometric based authentication techniques, where identification is done based on unique biological characteristics such as fingerprints, face and Iris Scan. We also have the Knowledge based technique, where is based on information supplied via text or images. The knowledge based techniques are the most widely used techniques for authentication. It makes use of both text-based and also picture based passwords. However, alphanumerical usernames and passwords are currently the most common and widely used computer authentication method [14].

Graphical passwords were introduced in order to tackle the limitation that textual passwords were faced with, such as vulnerability to brute force attack, shoulder spying and dictionary attacks [1]. In graphical authentication systems, images form the user's password, and texts, since psychologists have proven that humans can easily recall images much faster than he can recall text or numbers. However, several Graphical Passwords schemes are prone to

shoulder surfing and malware attacks [15].

To solve this problem, we embarked on this research, in a bid to come up with a Position-based multi-layer graphical user authentication system, where user authentication will be carried out in three different stages (Numbers, pictures and Colours). This will help to improve on the level of security of user's information.

2. Related Work

Several related projects have been worked on, which captures the minds and thoughts of experienced individuals on the subject matter. Most of them are an application of scientific and intelligent techniques, in a bid to help secure the personal information of users against attackers. Some of these research works are given below:

Por [10], proposed a method for preventing shoulder-surfing attacks, in which diagraph substitution rules are used together with an output feedback method in order to determine a pass-image. The proposed method was evaluated based on usability and security. The result showed that Digraph Substitution Rules and Pass-Images Output feedback was robust and reliable against both direct observation and video-recorded shoulder-surfing attacks.

Tunga [8], 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.

Katsini et al, [6] carried out an eye tracking study 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.

Kannadasan [11] proposed a novel authentication system that works based on Pass matrix and helps to create resistance against shoulder surfing attacks. The pass matrix doesn't give any hint for attackers to narrow down or figure out the password. A real user experiment was also carried out to evaluate the memorability and usability of the system. The result of the experiment, showed that the proposed system achieves better resistance against shoulder surfing attacks while maintaining its usability, except for the fact that users need to have deep understanding of the system, before they can use it.

Belk et al, [5] analyzed the interplay between, technology and user authentication. It evaluates efficiency and effectiveness towards the completion of tasks, between human cognitive factors (field dependent and field independent users), alternative interaction device types (desktop vs touch screen) and user authentication scheme (textual vs graphical). After a 4-month user study was carried out under the light of the field dependence-independence theory which encompasses human cognitive differences and differences in handling contextual information. The result showed that Field dependent users had a challenge with memorability and also difficulty in interaction with textual passwords. Field independent users had no issues using during authentication and interaction device types.

Alsaiari et al [4] proposed a scheme that seeks to combine the usability of recognition-based and draw-based graphical passwords. It runs on the same principle of OTP security. This scheme was evaluated for five weeks during three different sessions to measure the efficiency, memorability, effectiveness and user satisfaction of the scheme. From the result, it was proven that the scheme is easy to use, and that users can easily create, enter and remember their login details over time.

Istyaq et al, [12] 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.

Omolara et al, [2] addressed the problem of traditional password based authentication. A FingerEye was introduced, which was integrated with Iris-scan authentication. The pattern of a user's iris is analyzed and converted into binary code during registration. These binary code and stored and then required for verification before any transaction can be made. This model is reliable, secure and efficient and is also resistance to various forms of attacks.

Most of these implemented techniques are very expensive to implement and difficult to use when implemented, hence not many people can use adopt them [3]. In this research work, developed and implemented a position-based multi-level graphical authentication system that would be resistant to shoulder surfing attacks and easy to use.

3. Methodology

Research methodology also shows how the research outcome at the end will be obtained in line with meeting the objective of the study [13]. 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.

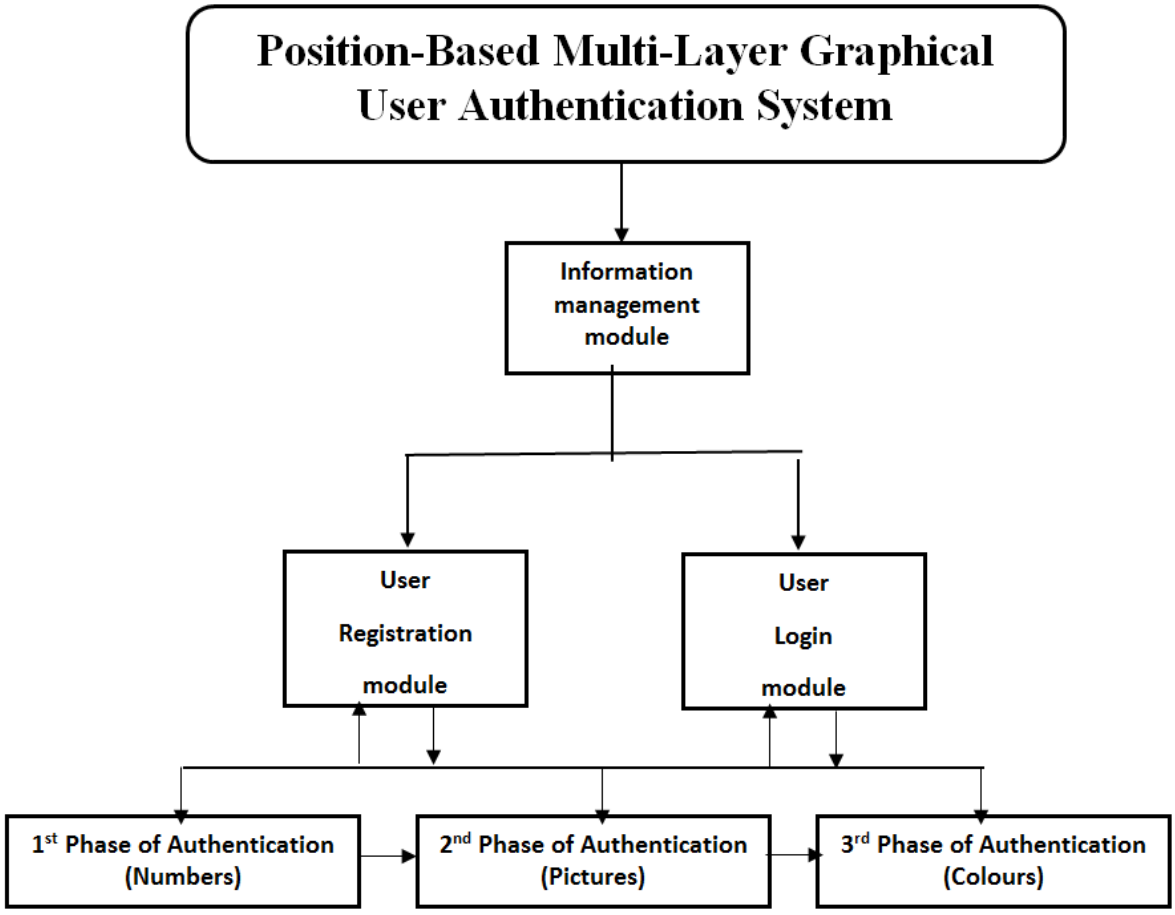

Figure 1. *High Level Model of the System.*

The dataflow diagram of the proposed system is shown below.

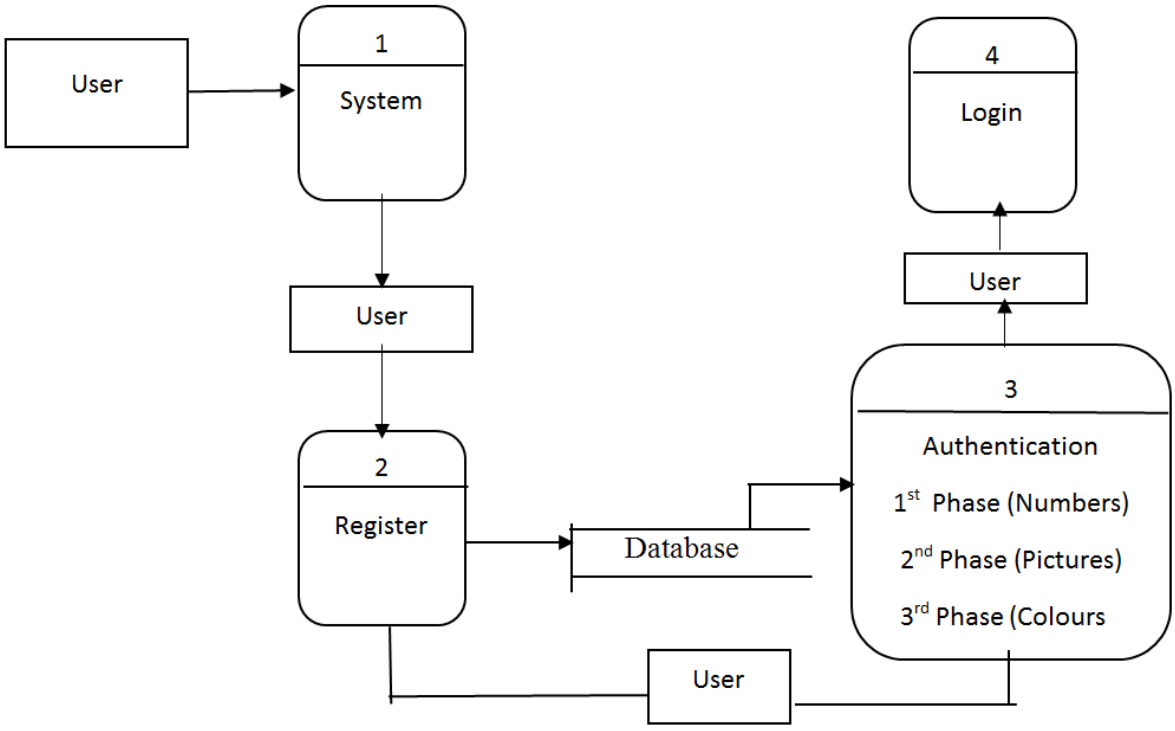

Figure 2. *Dataflow Diagram.*

3.1. Application's Algorithm

Before the system can be assessed, a user must be registered, after which they can access the system with their login details. The details entered by the users are compared with the details in the database for verification [7]. If the login details are authentic, the user can access the system, and logout to exit the system. The pseudo-code of the system is described below.

3.2. Pseudocode of the System

For users
Step 1: Start
Step 2: Register
Step 2.1: Create Password (Phase 1)
Step 2.2: Create Password (Phase 2)
Step 2.2: Create Password (Phase 3)
Step 3: Login
Step 3.1: Login phase 1
Step 3.1: Login phase 2
Step 3.1: Login phase 3
Step 4: Update Profile
Step 5: End.

3.3. 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.

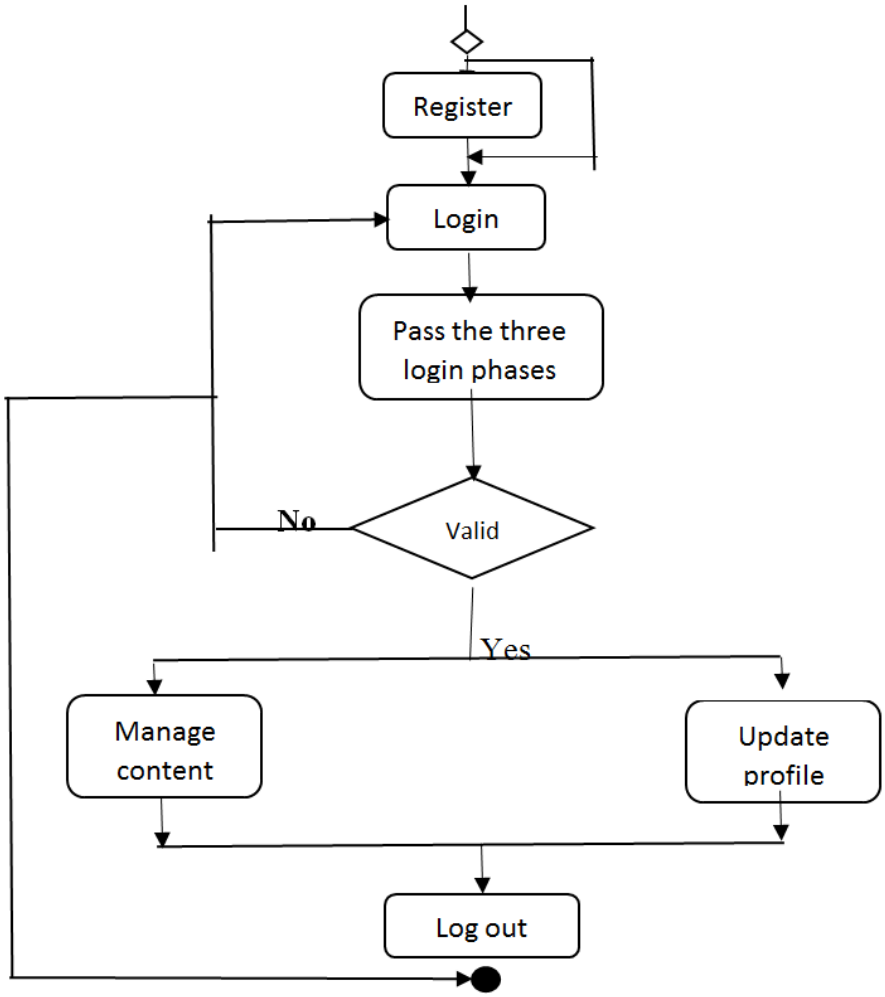

Figure 3. *Class Activity Diagram.*

3.4. Sequence Diagram

The sequence diagram shows the interaction between actors, the system and the system's components. It shows the explicit sequence of messages that are passed between the objects in a defined interaction. It is useful for understanding real-time specifications, and complex use cases, and in understanding the flow of control of a scenario by time. Figures 4 presents the sequence diagram of the system. It is a dynamic model of the system that describes the process a user passes through in accessing and using the system by depicting the objects and messages in the system. The objects are the user, registration page, login and authentication pages. This is illustrated below.

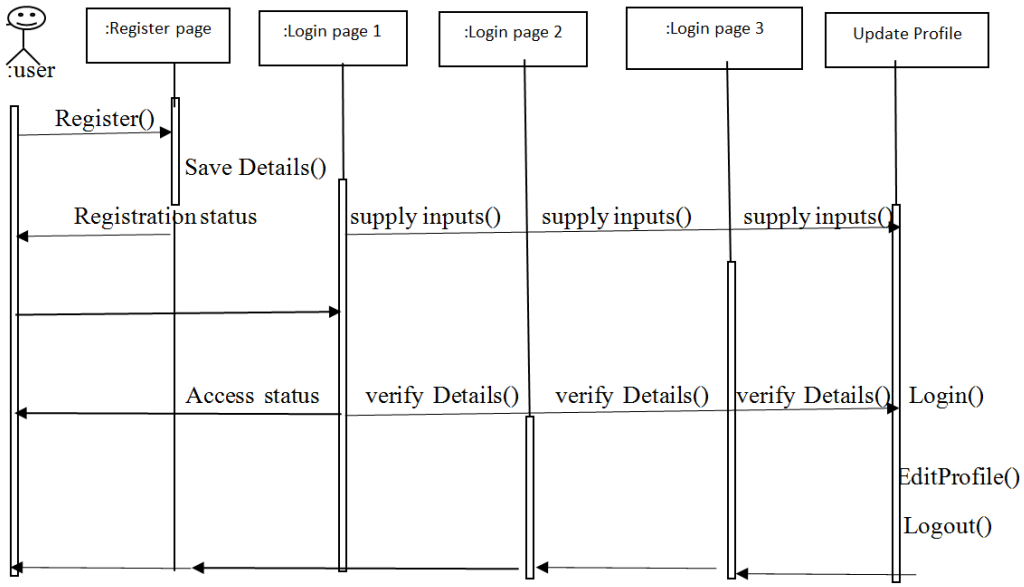

Figure 4. *Sequence Diagram for the System.*

3.5. 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:

3.5.1. Registration Module

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

3.5.2. 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.

3.5.3. Home Module

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

3.5.4. Logout Module

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

4. Results and Discussion

Prior to this time, Image based Graphical User Authentication System is being used to authenticate users [9]. The existing system or approach does not involve the randomization of images. Hence the approach is vulnerable to shoulder surfing attack, as anyone can watch closely and take note of the images that are been selected when a user is trying to login. However, our newly implemented system is not vulnerable to shoulder surfing attack. The software (Position based Multi-Layer Graphical User Authentication System) was implementation using the following tools.

1) Laptop;
2) Django Server;
3) PostgreSQL;
4) PG Admin4;
5) Brackets & Visual Studio Code;
6) HTML5, CSS3, JavaScript;
7) Google Chrome.

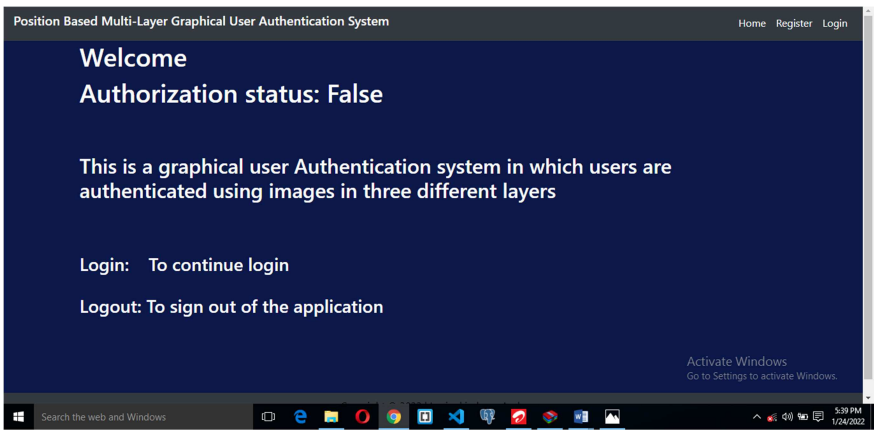

Figure 5. *Screenshot Home page.*

To switch to the user registration page, click on the *Signup* button.

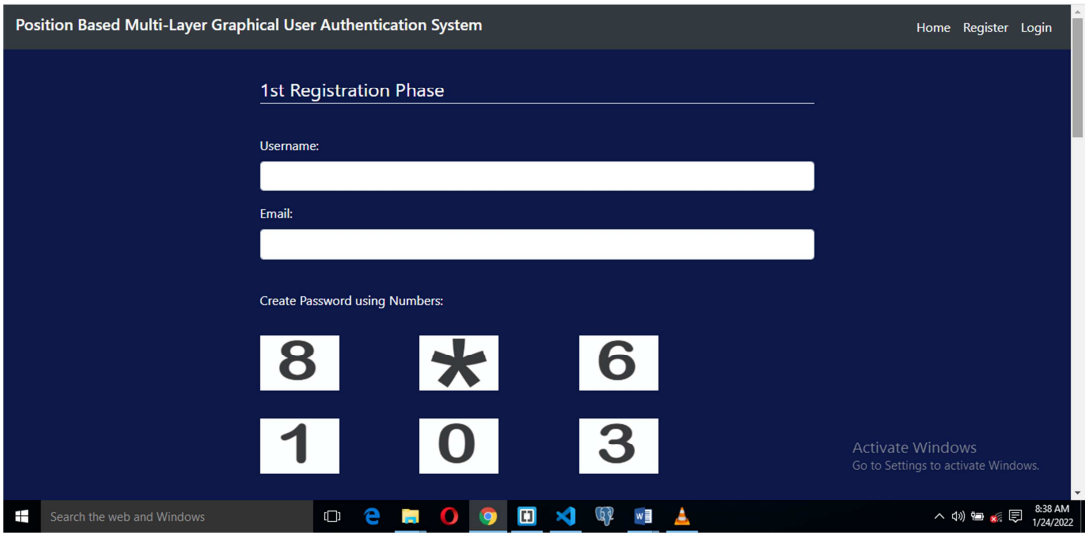

Figure 6. *Screenshot of Registration page (Phase 1).*

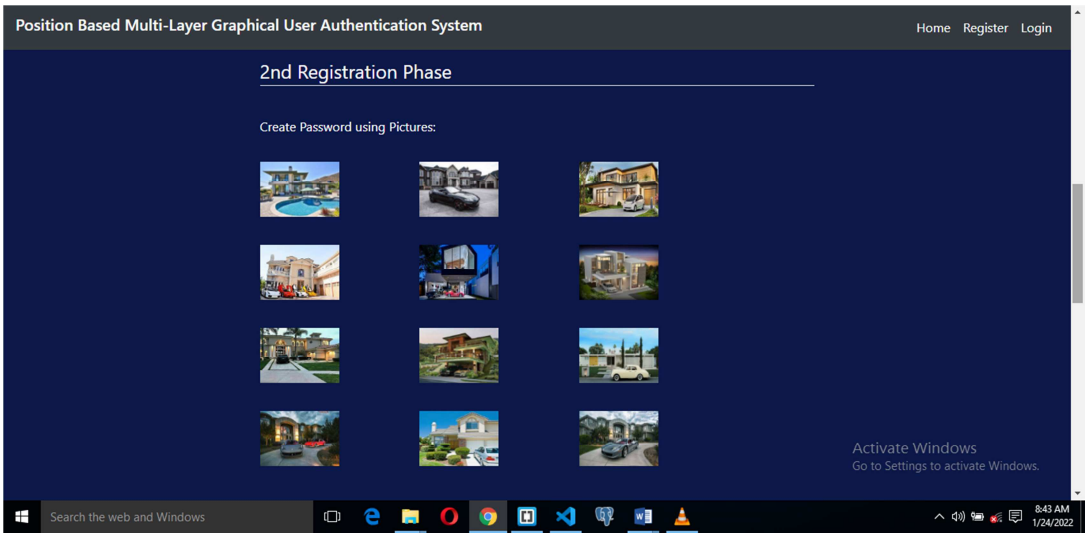

Figure 7. *Screenshot of Registration page (Phase 2).*

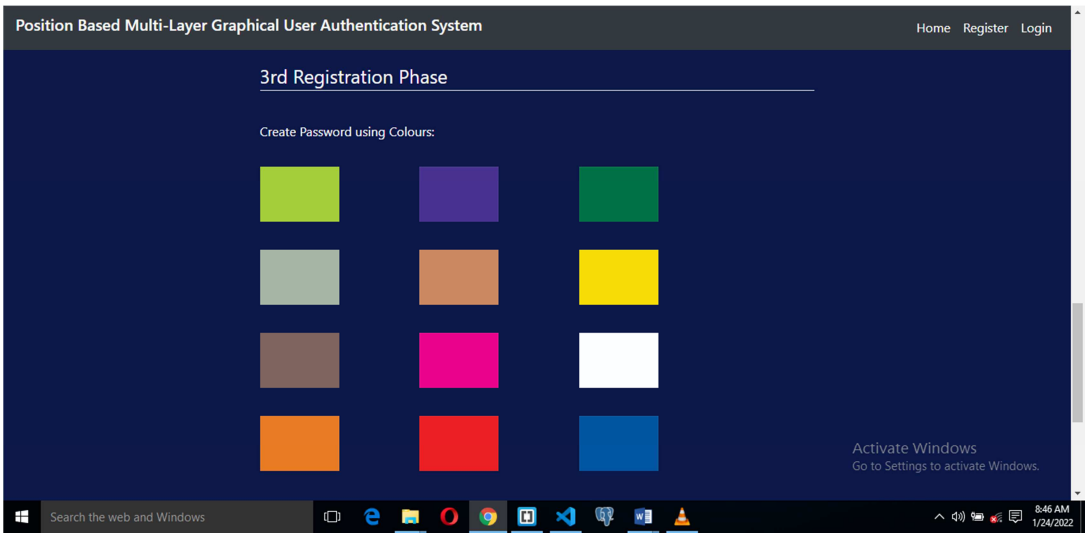

Figure 8. *Screenshot of Registration page (Phase 3).*

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

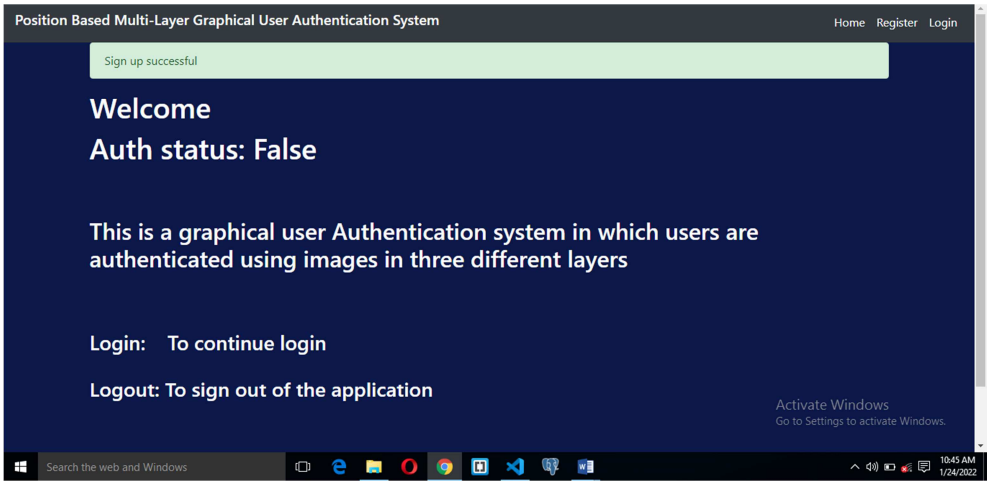

Figure 9. *Screenshot Showing Signup Successful.*

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.

When a user successfully login, his/her user name would be displayed on the screen, and the authorization status would change to true.

5. Performance Evaluation

In order to properly carry out performance evaluation on the system, we got an image based graphical user authentication system and compared it with our newly developed position based Multi-layer graphical user authentication system. The performance metrics we used are:

1) Security;
2) Usability;
3) Reliability.

Thirteen users made use of the two system, and then gave their comments afterwards. Their comments were received using google form and then interpreted and analyzed using SPSS (Statistical Package for Data Science). The results are shown below. In each graph, 1 stands for “Position Based Multi-Layer Authentication System”, 9 Stands for “Image password Authentication System”.

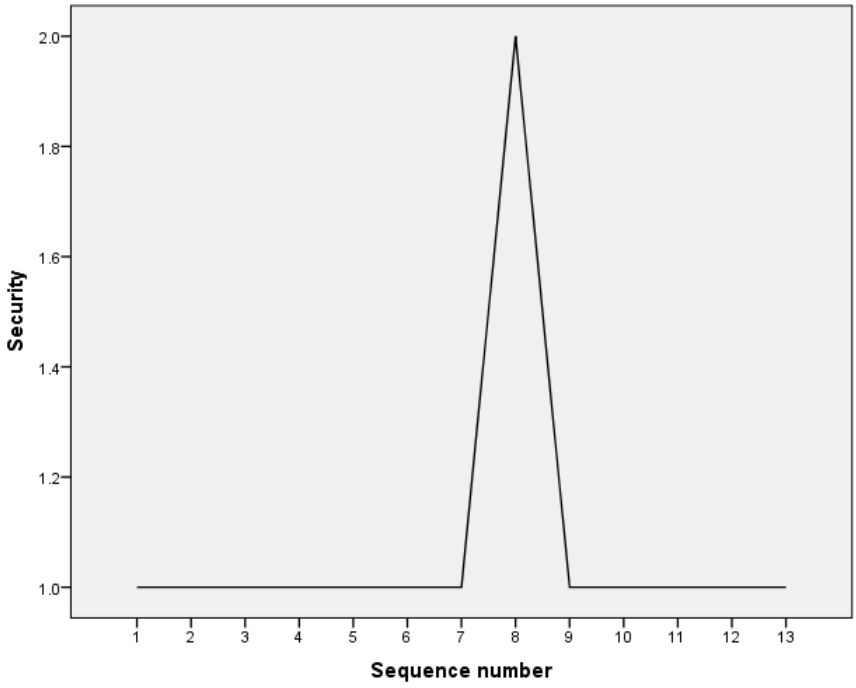

Figure 10. *Graphical representation of Performance Evaluation (security) carried out.*

From the graph above, 12 out of the 13 users responded that the Position based Multi-layer Graphical user authentication system provides more security than the Image Based Graphical user authentication system. A clearer diagrammatic representation is given in figure 13.

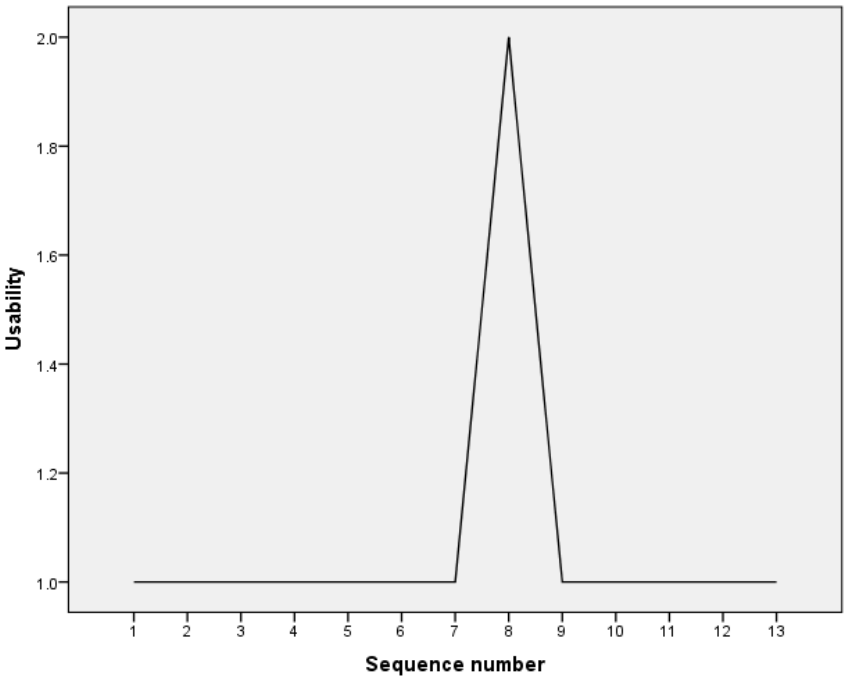

Figure 11. *Graphical representation of Performance Evaluation (Usability) carried out.*

From the graph above, 12 out of the 13 users responded that the Position based Multi-layer Graphical user authentication system is easier to use, compared to the Image Based Graphical user authentication system. A clearer diagrammatic representation is given in figure 14.

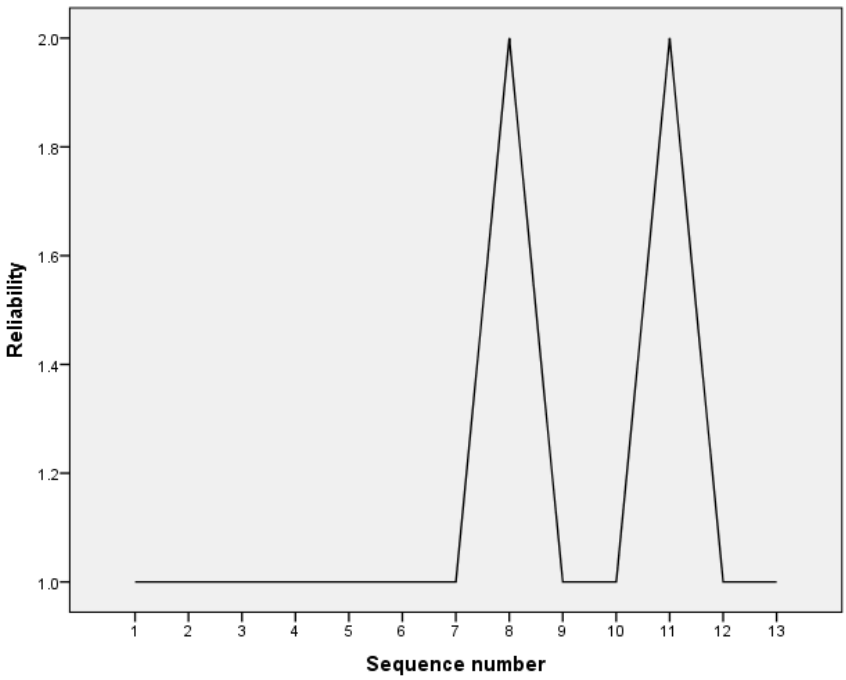

Figure 12. *Graphical representation of Performance Evaluation (Reliable) carried out.*

From the graph above, 11 out of the 13 users responded that the Position based Multi-layer Graphical user authentication system is more reliable and would stand the test of time, compared to the Image Based Graphical user authentication system. A clearer diagrammatic representation is given in figure 15.

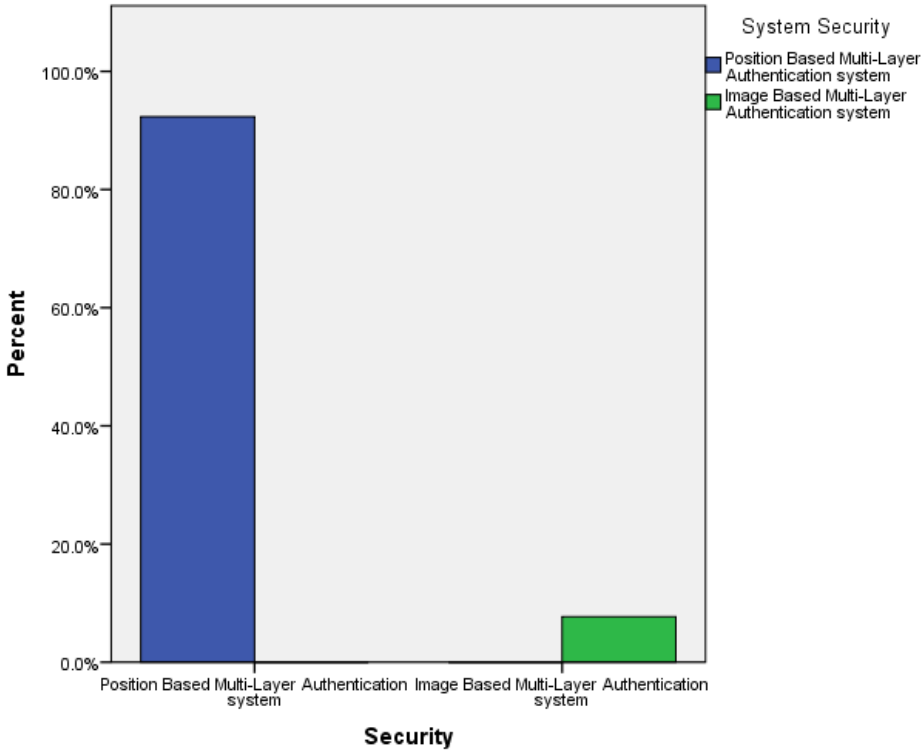

Figure 13. *Bar Chart representation of Performance Evaluation (Security) carried out.*

From the bar chart above, 92.3% out of the users responded that the Position based Multi-layer Graphical user authentication system provides better password security, compared to the Image Based Graphical user authentication system.

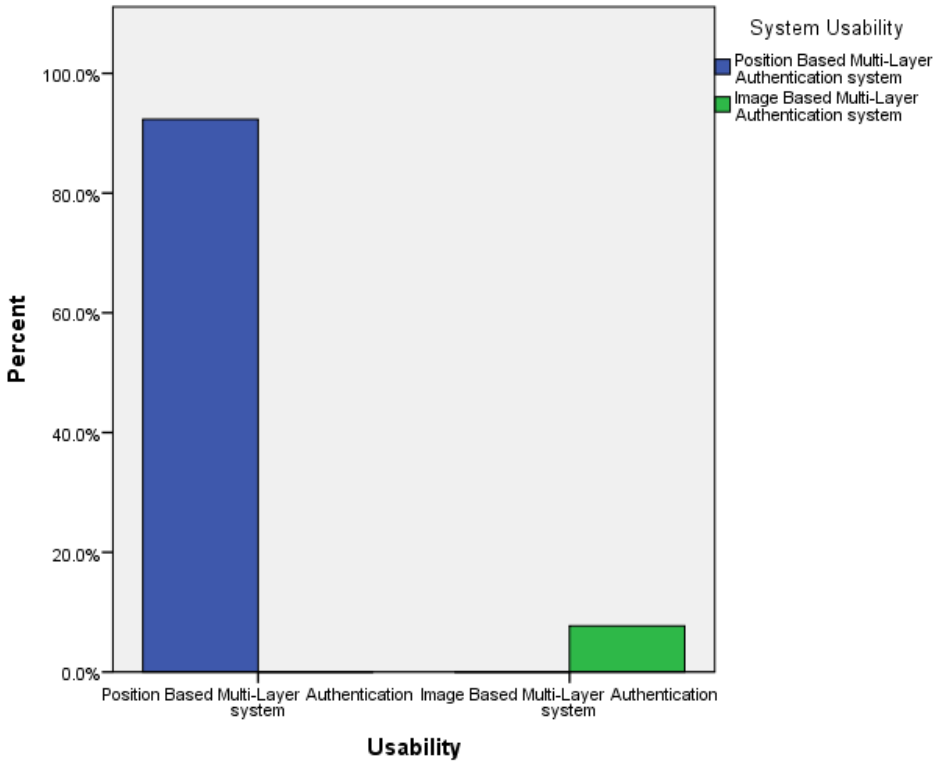

Figure 14. *Bar Chart representation of Performance Evaluation (Usability) carried out.*

From the bar chart above, 92.3% out of the users responded that the Position based Multi-layer Graphical user authentication system is easier to use, compared to the Image Based Graphical user authentication system.

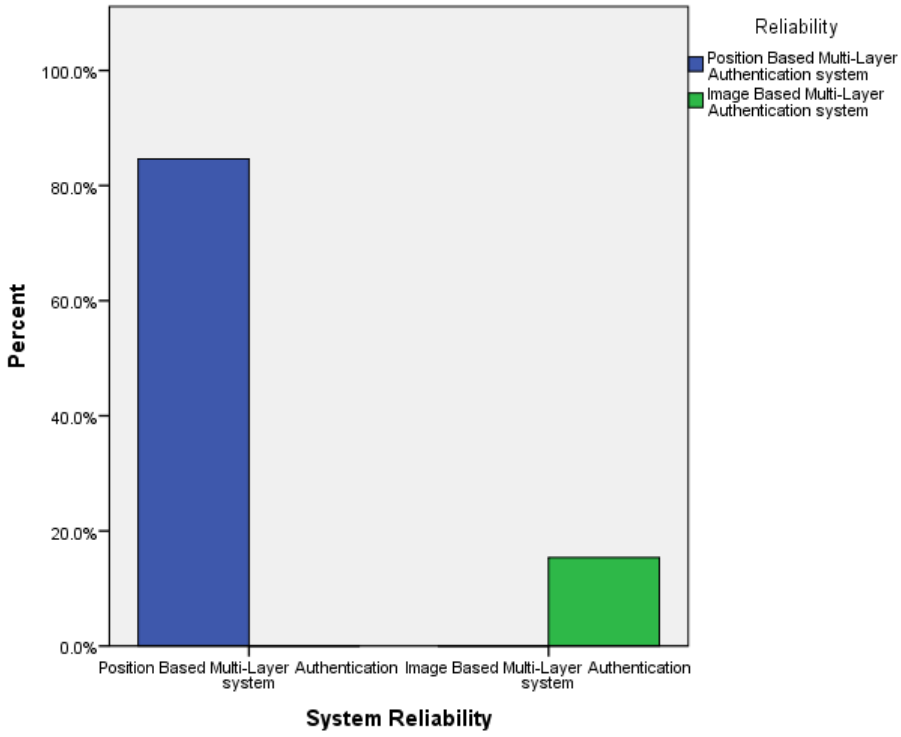

Figure 15. *Bar Chart representation of Performance Evaluation (Reliability) carried out.*

From the bar chart above, 84.6% out of the users responded that the Position based Multi-layer Graphical user authentication system more reliable than the Image Based Graphical user authentication system.

6. Conclusion & Future Work

This research work is concerned with the development of a Position based multi-layer graphical user authentication system that authenticate users in three different layers, using Numbers, picture (car and houses) and colours. The user is expected to provide the correct login details for the 1st stage before he/she would be allowed to proceed to the next phase. The implemented system completely solves the problem of shoulder surfing attacks.

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, a Position based multi-layer graphical user authentication system was developed, which solves the problem of shoulder surfing attack and guarantees the safety of user data.

Research can still be carried out in this area especially with the application of artificial intelligence, in other to come up with a more efficient model that will have a higher level of security and reliability.

References

[1] Abhijith S, S. S. (2021). Web Based Graphical Password Authentication System. *International Journal of Engineering Research & Technology*, 1-4.

[2] Abiodun Esther Omolara, A. J. (2019). FingerEye: Improving Security and optimizing ATM transaction time based on Iris-Scan Authentication. *International Journal of Electrical and Computer Engineering (IJECE)*, 1-9.

[3] Adnan Ali 1, H. R. (2019). A Fractal-Based Authentication Technique Using Sierpinski Triangles in Smart Devices. *Sensors*, 1-19.

[4] Alsaiari H, P. M. (2016). Graphical One-time Password (GOTPass): A Usability Evaluation. *Centre for Security Communication and Network Research, School of Computing Electronics and Mathematics*, 1-31.

[5] Belk, M. F. (2017). An Interplay Between Humans, technology and Users Authentication: A Cognitive Processing Perspective. *Central Lancashire online Knowledge*, 1-32.

[6] 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.

[7] Gouri Sankar Mishra, P. K. (2020). User Authentication: A Three Level Password Authentication Mechanism. *Journal of Physics: Conference Series*, 1-8.

[8] Harinandan Tunga, D. S. (2015). Graphical User Authentication Techniques for Security: A Comparative Study. *International Journal of Engineering and Advanced Technology (IJEAT)*, 1-7.

[9] Jiya Gloria Kaka, I. O. (2021). Recognition Based Graphical Password Algorithms: A Survey. 1-10.

[10] Lip Yee Por, C. S. (2019). Preventing Shoulder-Surfing Attacks using Diagraph Substitution Rules and Pass-Image Output feedback. *Symmetry*, 1-16.

[11] M. Kannadasan, J. r. (2017). Shoulder Surfing Resistant Graphical Authentication System using Pass Matrix. *International Journal of Scientific & Engineering Research Volume 8, Issue 5, May-2017*, 1-5.

[12] Salim Istyaq, A. N. (2021). Hybrid Graphical User Authentication Schemes Using Grid Code. *International Journal of Engineering Trends and Technology*, 1-11.

[13] Sileyew, K. J. (2019). Research Design and Methodology. *Intech Open*, 1-14.

[14] Sreelatha, S. A. (2011). Authentication Schemes for Session Passwords using Color and Images. *International Journal of Network Security & Its Applications (IJNSA), Vol. 3, No. 3,* 9.

[15] Vimal Gaur, A. S. (2017). Authentication using a Combination of Color Scheme and Musical Notes. *International Journal of Engineering Research & Technology (IJERT)*, 1-5.