International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7676
***Article Received**: 22 April 2023 **Revised:** 24 June 2023 **Accepted:** 12 July 2023*

An Advanced Knowledge Based Graphical Authentication Framework with Guaranteed Confidentiality and Integrity

[1]Priti C. Golar, [2]Dr. Rika Sharma
[1]Research scholar
Department of Computer Science & Engineering
Amity University
Raipur, (Chhattisgarh), India
priticgolar@gmail.com

[2]Associate Professor
Department of Computer Science & Engineering
Amity University
Raipur, (Chhattisgarh), India
rsharma1@rpr.amity.edu

Abstract: The information and security systems largely rely on passwords,which remain the fundamental part of any authentication process. The conventional authentication method based on alphanumerical username and password suffer from significant disadvantages. The graphical password-based authentication system has recently been introduced as an effective alternative. Although the graphical schemes effectively generate the passwords with better flexibility and enhanced security, the most common problem with this is the shoulder surfing attack. This paper proposes an effective 3D graphical password authentication system to overcome such drawbacks. The system is based on the selection of click points for generating passwords. The proposed work involved a training phase for evaluating the model in terms of the success rate. The overall evaluations of the model in terms of password entropy, password space, login success rates, and prediction probability in the shoulder surfing and guessing attacks proved that the model is more confidential and maintains a higher range of integrity than the other existing models.

Keywords: Graphical authentication system, shoulder surfing attack, guessing attack, knowledge base, click points, confidentiality, integrity.

I. Introduction

Websites traditionally rely on the username and text password for user authentication. Later, text password-based authentication is unsafe since the users find it difficult to remember the strength and length of text passwords [1]. As a result, the users are liable to select weak passwords for better recall. Moreover, it is easy for the hackers to obtain the passwords via shoulder surfing attacks, guessing attacks, dictionary cracking attacks or others [2]. Certain websites use dynamic codes through e-mails or phone messages to provide authentication. It is one of the most successful two-factor authentication schemes, but the identified problem is that it mainly relies on other devices [3, 4]. Some of the earlier studies found that the users can better recall images than text passwords. With this finding, graphical passwords are introduced as an alternative to textual passwords, where the users are allowed to create their credentials over images [5]. Common examples of graphical authentication schemes involve PassPoints, DAS, and cued click points (CCP) [6].

The graphical passwords provided more flexibility to the users associated with the system as the images are much more user-friendly than the textual passwords [7]. The DAS scheme employed a 2D grid, and users were allowed to draw the passwords over the 2D grid. The users can click at any point in the image for password generation in the PassPoints scheme [8]. In CCP, the next image is varied from the previous click-point and the users are allowed to choose a total of five points from a sequence of images [9]. Overall, graphical passwords are more flexible and are also highly user-friendly. Though the graphical authentication scheme is useful in later times, it is unable to complete the password due to the memory burden [10]. If the authentication system is followed on multiple websites, the memory burden is again increased.A new type of graphical authentication system is being developed to resolve this issue, where users are asked to remember the images in place of text or alphanumeric letters [11].

Several studies revealed that the human brain works more efficiently when recalling images than texts. The graphical passwords are developed solely to reduce memory burden and enhance the overall security [13].A huge full password space is provided to the users based on images to produce more secured passwords and enhance the system's security. As an

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7676
***Article Received**: 22 April 2023 **Revised:** 24 June 2023 **Accepted:** 12 July 2023*

effective solution for different attacks in the authentication systems, click points are introduced. Aselecting points technique in the images and the locations selected by the users are stored in the database for password generation [14]. It is done by extracting the selection pattern of click points in the image for password generation. Different techniques are introduced based on the selection of click points in the images to offer a higher security perimeter to the users connected to the web systems[15].

1.1 Motivation

Several methodologies are introduced in the literature to provide security for web-based applications. Most of the founded techniques are text-based or alphanumeric, which suffer from serious shortcomings. The textual based passwords are a memory burden for the users who cannot recall the password after a long time. A survey based on psychological studies found that passwords based on images are easier to recall than text-based passwords. With this understanding, graphical password authentication systems have been developed in recent times to enhance security and offer more flexibility for users. The existing solutions based on graphical passwords cannot completely resolve the shoulder surfing attack issue as the click points that the users select are sometimes visible to the attackers. Motivated by this fact, this paper introduces a novel 3D graphical password authentication system based on selecting click points for password generation. In the registration phase, the proposed method selects the click points from 2D images and compares them with the click points selected from the 3D cubic structure for verification. The proposed system avoids highlighting the selected click points in the cubic structure to prevent the shoulder surfing attack.

1.2 Contribution

The main contributions of the proposed work are as follows:

- A novel and secure graphical password authentication system is proposed in this paper to protect the user information from various attacks such as shoulder surfing, brute force and guessing attacks.
- One of the main novelty of the proposed authentication system is the construction of a graphical cubic structure for password verification. The click points selected by the users in the registration and login phases are matched for verifications.
- Training a total of 250 users from different genders and age groups belonging to different professions to prove the model's reliabilityand determine the overall success rates.
- The proposed system is evaluated to ensure that it provides security against shoulder surfing and guessing attacks and evaluates various parameters.

1.3 Paper organization

The remainder of the paper is structured as follows: Section 2 covers the literature review of the recently published papers relevant to the graphical password authentication system. Section 3 presents the proposed methodology with sequential steps followed in the work. Section 4 presents the evaluation and comparison of the proposed work, and section 5 concludes the paper.

II. Related work

Several works are published in the literature to guarantee confidentiality for user login. Some of the recent and effective ones are reviewed in this section.

Several websites still rely on usernames and text passwordsfor basic authentication. However, text passwords are considered insecure, and to enlighten security in user login, graphical password authentication schemes have been recently introduced. Inspired by this concept, Chu et al. [16] introduced a two-factor graphical password authentication scheme called PassPagewith higher security. The system included 4 main modules: sign-up, browsing history recording, decoy web page maintenance, and log in. After the user login, the browsing history recording module recorded the user's browsing history. While login, 9 pages were made visible to the user consisting of browsed and decoy pages. If the user has correctly selected all the visited pages from the 9 pages, then login is made successful for the user. Experimentations of the approach with 12 volunteers resulted in a login success rate of 80%.

An application to offer personal storage for children was introduced by Yang et al. [17] to provide security for the personals of children for primary school syllabus. The application was named graphical password authentication for child personal storage application, and it offered personal storage for the notes in softcopy forms. The application was developed on the android mobile application platform, and based on the user requirements, the system's functional requirements were implemented. The main significance of the project was that it maintained awareness among the children about secure file keeping. The experimentations of the method proved better security for the notes of the primary school syllabus.

Numerous applications are based on graphical or image password-based authentication systems. The problem with such systems is that the management of pictorial data is difficult and results in a slower authentication process. An approach to improve the overall effectiveness of graphical

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7676
***Article Received**: 22 April 2023 **Revised:** 24 June 2023 **Accepted:** 12 July 2023*

password authentication was introduced by Juneja [18]. The approach followed the XML based schema to indicate the graphical image. The server processed the password image with the graphical pattern loaded by the user and verified if the pattern was valid using stroke length and drift. The XML pattern database stored the pixel values extracted from the graphical input pattern. The pattern bits of the image were also updated by the server using the LSB steganography, and for every user input, pattern extraction and mapping were carried out. Implementations of the work as desktop and mobile applicationsproved the approach's effectiveness over the other methods.

It is required a password to provide security against diverse forms of attacks. The conventional textual password-based authentication scheme is found to have several drawbacks and is prone to attacks such as shoulder spying, brute force attacks, dictionary attacks, etc. A new position-based multi-layer graphical user authentication scheme was developed by Edward et al. [19] to resolve the shoulder surfing attack. Three main phases were compiled to ensure maximum security for the users. The positions in the image selected by the user were set up as a password during the registration phase. The system was evaluated using three parameters such as reliability, usability and security and provided better results.

Faraji and Manochehri [20] developed another secure graphical password authentication systemto provide security against smudge, shoulder surfing and brute force attacks. The method was formulated by combining two major recognition and cued recall techniques. Initially, the registration phase was carried out where the users' personal details were acquired,and then a set of random images were made visible from which the users were allowed to select three images. The password was created using the selected images, and then the login phase was entered, which was recognition-based. After verification, the graphical password was created, and the login phase was completed. The system was evaluated and provided better security compared to other methods.

The literature review indicates that efforts are being made to improve the use of graphical password authentication systems. In recent years, several attempts have been made to use image-based passwords to enhance the overall security of user login. Most of the techniques obtained the patterns of the images selected from the domain and stored them in the database. While clicking on the images, the attacker can steal the point information leading to shoulder surfing attacks. The proposed method is introduced to overcome such a drawback by introducing a graphical cubic structure from which the click points can be selected for password verification. The highlights for the selection are removed to preserve the click point information, and the shoulder surfing attack is resisted.

III. Proposed methodology

A new knowledge-based graphical authentication framework is introduced in this paper to provide integrity and confidentiality to users. The proposed model builds a web-based application to achieve higher security in user login and provide guaranteed security against certain attacks such as shoulder surfing. There are three main phases in the proposed work: the user registration phase, the training phase,and the user loginphase.

Figure 1: The developed authentication system

Initially, the user registers in the registration form provided by the website by filling in their demographic information. After this step, the password will be created and stored in the database for verification. Then, a set of images are provided to the users, and they are allowed to select 6 images. The click points of the images are stored in the database for password generation. In the next training phase, the users are allowed to get trained with the authentication system to increase the login success rates. Later, the completed users can enter the login phase to generate the graphical password. At this step, a geometric shape or a 3d-cube is made visible to the users. Some random images are displayed over the cube and the selected images in the registration phase. The users are allowed to click on the images, and the click points of the users are again collected and evaluated with the password generated. If the click points stored in the database match the new click points selected over the cube, the login is made successful. The developed authentication system is displayed in Figure 1.

3.1 User registration phase

The user registration phase is the beginning of the proposed methodology,where the user is provided with a registration form to obtain their demographic information. The registration form developed in the proposed work includes the entities such as name, gender, age, occupation, contact number, e-mail id and a space to enter the OTP (One Time Password). The registration form generated in the proposed work is displayed in Figure 2.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7676
***Article Received**: 22 April 2023 **Revised:** 24 June 2023 **Accepted:** 12 July 2023*

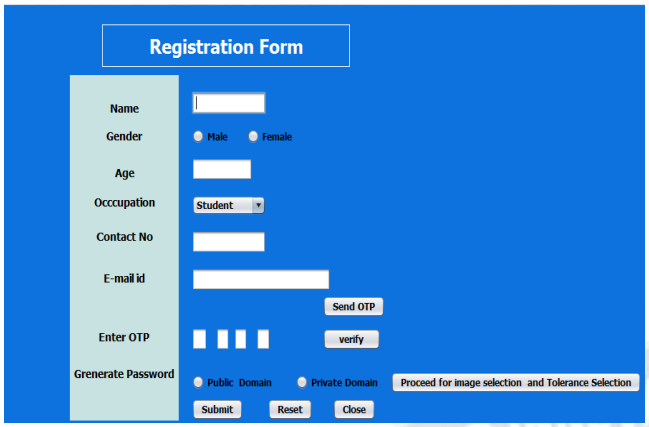

Figure 2: Registration form generated in the proposed work

After obtaining the above-mentioned demographic information, the system will send a 4-digit OTP to the registered mobile number. The user is then asked to enter the OTP, and the system verifies it. After sending the OTP to the registered mobile number, the system displays a dialog box displaying 'OTP sent successfully' shown in Figure 3.

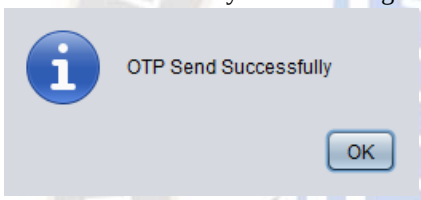

Figure 3:Dialog box for sending OTP

If the user enters the correct OTP sent to the mobile number, then the system verifies it and generates the ID for the user. After generating the ID, the system again displays a dialog box as'Your id is: ID' as shown in Figure 4.

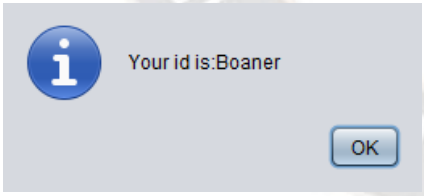

Figure 4: Dialog box for displaying id after a successful registration

If the registration is successful, the password is generated based on the image selected by the user. The user is provided with 2 options such as private and public domain. When the user clicks on the private domain, the images stored in the system can be selected for password generation according to the user's preference. If the user selects the public domain, then the system provides a total of 15 images randomly for click point selection. Once the user selects the domain of the images for password generation, the system provides a screen to select the tolerance area for the click points. This screen provides 2 options for tolerance area selection,25*25 and 50*50 and the click points are selected based on this area. The images are provided for the user's view after selecting the tolerance area for the click points, as shown in Figure 5.

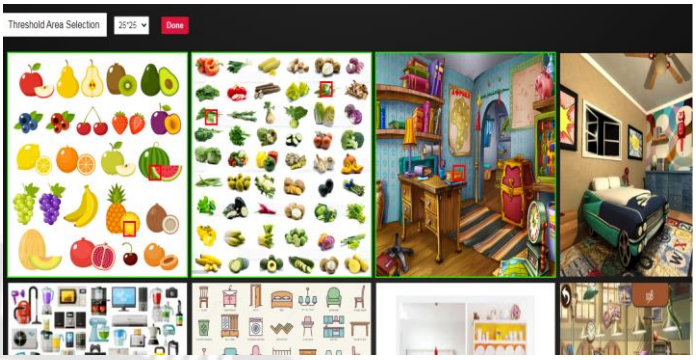

Figure 5: Images for click point selection [Public domain images]

The images displayed in Figure 5 are from the public domain and are provided randomly. The user selects the click points based on their choices for password generation. In the figure, the tolerance selected for click point generation is 25*25,and the click points are made visible by highlighting the region with red squares. The users can select any number of click points in the images based on their recalling capability. After selecting the click points,the password is generated based on the x and y-coordinates of the click points.The image ID and the generated password are stored in the database. Finally, the registration phase is completed,and a dialog box displays'Your registration completed'to the user, as shown in Figure 6.If the username already exists in the database, a dialog box displaying 'Your id is already registered. Please use the different usernames displayed on the screen, asshown in Figure 7.

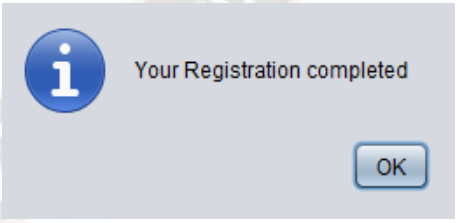

Figure 6: Dialog box to confirm successful registration

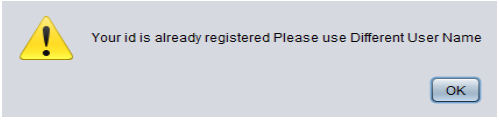

Figure 7:Dialog box to show that the username is already registered

3.1.1 Private domain registration

In the case of private domain registration, the users are allowed to select images as per their choice. The users can upload the images stored in the system, and the tolerance area can be selected, similar to public domain registration. After

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7676
***Article Received**: 22 April 2023 **Revised:** 24 June 2023 **Accepted:** 12 July 2023*

this, a similar login process for the public domain is followed here. An example of the registration phase based on private domain images is shown in Figure 8.

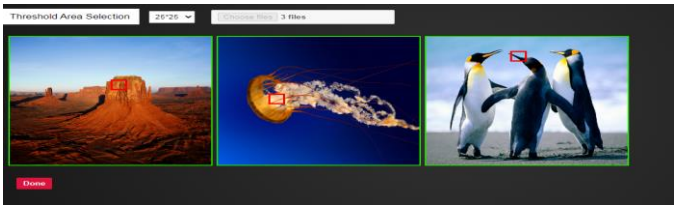

Figure 8:Registration phase based on private domain images

3.2 Training phase

In the training phase, users from different parts of the place are trained with the registration and login phases to determine the login success rates. A total of 250 users are selected for the training, and these users belong to different age groups from different professions. Both male and female candidates are involved in equal proportion in the registration and login phases. The demographic information is collected from every user by making them fill out the registration form. All the details obtained are stored in a separate database for verification purposes.

3.3 Login phase

After successful registration, the login phase is entered where the user is initially asked to fill a form asking the details such as userID and registered contact number. The form developed for the login phase is displayed in Figure 9.

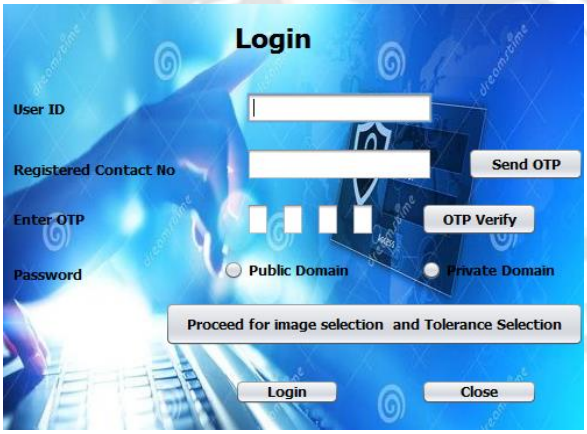

Figure 9: Form for login phase

After filling in those details, the user is asked to enter the OTP sent to the registered mobile number. The system verifies the entered OTP with the OTP sent to the mobile number and displays the command as per the verification. If the entered OTP is wrong, the system displays ‘Wrong OTP’as shown in Figure 10.

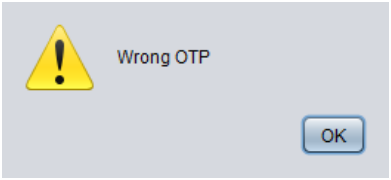

Figure 10:Command for wrong entry of OTP

Once the verification process is completed, the system asks the user to generate the password by providing private and public domain image options. The user selects the tolerance areafor the click point selection, and the system displays the images for password generation. The system displays some random images along with the images that the user chooses for the click point selection in the previous registration phase. It ensures that the user selects the accurate click points as in the registration phase. Also, the images provided to the user are randomly shuffled to ensure security for the users. The randomly shuffled images provided to the user for password generation are displayed in Figure 11.

Figure 11:Randomly shuffled images for password generation

In the above randomly shuffled images, the users can select a maximum of 6 images, allowing each image to appear on one side of the password verification cube. After the selection step, the proposed method enters the 3D environment where a cube is made visible to the users with embedded images on every face of the cube. While displaying the images in the cube, the user selects images provided on the cube’s each face. If the user selects less than 6 images, the system will automatically display some random images on the faces. The generated 3D cubic structure in the proposed work is displayed in Figure 12.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7676
***Article Received**: 22 April 2023 **Revised:** 24 June 2023 **Accepted:** 12 July 2023*

Figure 12:Generated 3D cubic structure of the proposed work

From the cubic structure, the users are allowed to select the exact click points as selected in the registration phase. Based on the tolerance area chosen by the user, the click points are selected from the images in the cube. If the click points selected in the login phase match the click points stored in the database, the login is termed to be successful and displays the command' login successfully'as in Figure 13.

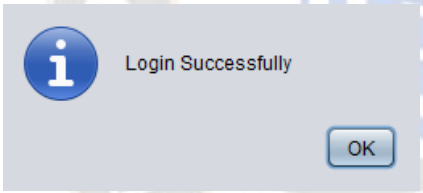

Figure 13:Command for a successful login

After selecting the click points from the cube, thesystem will display the login page again to confirm the login. When the login is successful, the above command is displayed. The appropriate command is displayed when the login is unsuccessful due to a wrong entry or password mismatch. For incorrect user ID or password entry in the given blank, the system returns the command 'Your ID or password incorrect'as in Figure 14.

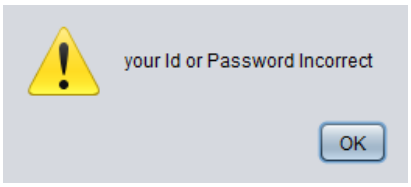

Figure 14:Command for entering incorrect id or password

The proposed system also provides a forgotten password option to the users to make the system user-friendly and maintain flexibility. The users are allowed to enter their username and password 3 times, and if the users are unable to recall their username or password, the system displays a message, as shown in Figure 15.

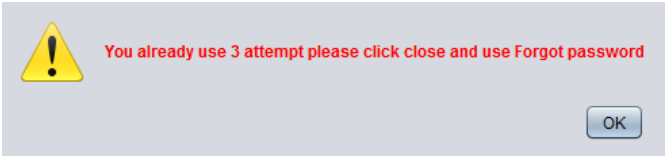

Figure 15:Command for wrong entry of username or password

Once the login phase becomes successful, the process gets terminated, and the password information is preserved in the database. For wrong entries, and in any case, if the user forgets either their username or password, the 'forgot password' option is provided to the users. The users are given three chances, and the 'forgot password'option is invoked after the third time entry of the wrong username or password. After clicking the 'forgot password' option, a dialog box is displayed in Figure 16.

Figure 16:Forgot password option in the login phase

In the 'forgot password' dialog box, the system asks for a new user ID and sends an OTP to the registered contact number. After verifying the OTP, the password is generated as per the image selection done by the users.

3.3.1 Privatedomain login

For private domain login, the images that the users choose are made visible to them, along with some random images for password generation. The users choose the tolerance area, similar to the public domain login, and then the images are provided for the users' view.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7676
***Article Received**: 22 April 2023 **Revised:** 24 June 2023 **Accepted:** 12 July 2023*

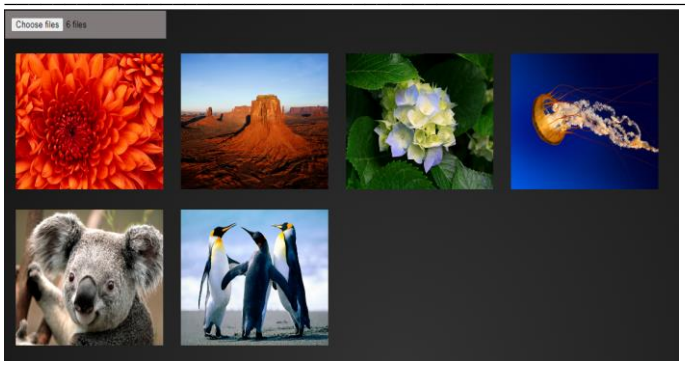

Figure 17: Private domain login

Figure 17 shows the images provided to the users in the private domain login. During private domain registration, the user has chosen a total of 3 images. Along with these images, some randomly chosen images are also provided to the users for image selection. With the selection of a maximum of 6 images from the displayed images, the system creates the 3D graphical cubic structure with the images embedded over its faces. The cubic structure generated after selecting images for the private domain is displayed in Figure 18.

Figure 18:3D cubic structure generated for private domain login

The cubic structure displayed for the private domain images shows the selected images over the faces. If the user selects less than 6 images, some random images taken by the system will be included on the other sides.

IV. Results and discussion

This section presents the performance analysis and evaluation part of the proposed method. The proposed method has been evaluated with several recently published techniques to prove its efficacy over the other works. The methods chosen for comparison are the following: mouse clicking [21], SSP system [22], text-based scheme [23] and 3D graphical user authentication (3D GUA) [24].The detailed analysis, the simulation setup and the performance metrics are presented in the upcoming sections.

4.1 Performance metrics

The major performance metrics considered for the analysis are password entropy, password space and login success rate. The mathematical formulations, along with the descriptions, are as follows:

*Password entropy:*Password entropy is used to measure the password's strength or is a measure to indicate how much unpredictable a password is. The mathematical formulation to compute password entropy is as follows:

$$PE = no\ of\ images * \ln(no\ of\ images * click\ points * no\ of\ run) \quad (1)$$

*Password space:*Password space is the total count of passwords generated from a given alphabet or characters set to achieve the given maximum password length. The mathematical formulation is as follows:

$$PS = \sum_{N=1}^{6} (\Re * o * t * I)^N \quad (2)$$

where, N indicates the total number of images in a user password, $\Re$ is the count of images displayed in the registration phase, o is the total count of objects, t is the time duration taken in the login phase and I is the total count of images displayed in the login phase.

*Login success rate:*The login success rate determines the number of users who correctly complete the login phase within a shorter duration. Achieving a higher percentage of login success rate determines the flexibility and user friendliness of the system and results in higher possibilities of successful implementation.

4.2 Performance analysis

The overall performance analysis of the proposed system is covered in this section. The proposed model is evaluated using different metrics, and the method's excellence is proved based on the results obtained. Detailed evaluations of the proposed scheme are presented below:

4.2.1 Password entropy evaluation

Password entropy can be measured as the probability of correctly guessing the password for random guessing. This metric is expected to be higher to prove that the proposed system is secure against the different attacks in web-based applications. An ideal method can providea higher range of password entropy compared to the other existing techniques. The results obtained through the evaluation of password entropy for the proposed and existing techniques are presented in Table 1. From the table, it is clear that the proposed method obtained higher password entropy compared to the other

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7676
***Article Received**: 22 April 2023 **Revised:** 24 June 2023 **Accepted:** 12 July 2023*

techniques. It proves that the attackers cannot guess the password generated by the proposed scheme. The main reason for the proposed method to obtain the desired results is the usage of a 3D cubic structure and the idea of using images over the cube for click point selection.

Table 1: Password entropy comparison results

Sr. No.	Approaches	Password Entropy (bits)
1	Jumbled PassSteps [13]	14.72
2	Locimetric Scheme [23]	19.69
3	Text-based scheme [23]	39.36
4	Hybrid GUA Scheme [23]	41.28
5	Cognometric Scheme [23]	12.68
6	3-D GUA [24]	36.05
7	SelfiePass [25]	15
8	Association based authentication [27]	35.6
9	**Proposed System**	**45.65**

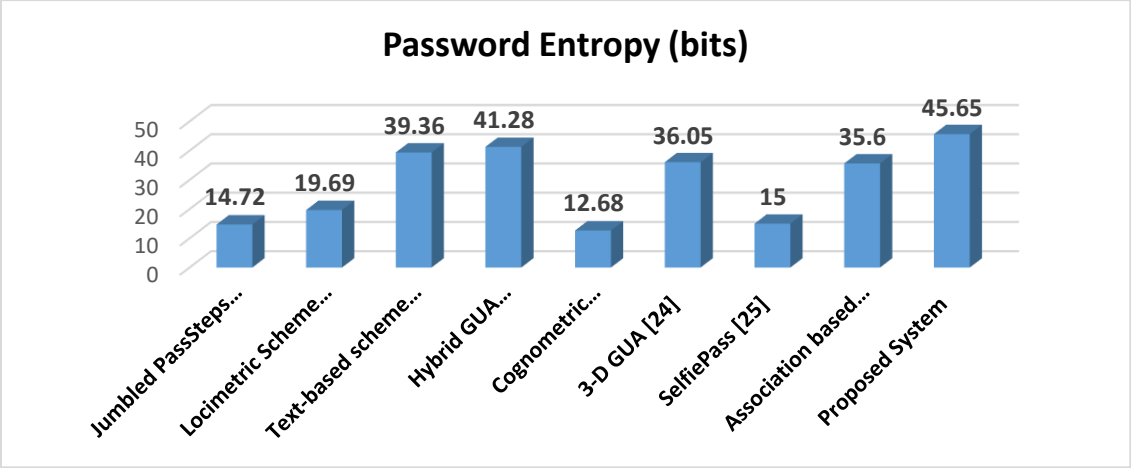

Figure 19:Password entropy comparison of the proposed and existing works

The graphical representation in Figure 19 represents the password entropy comparison of the proposed and existing techniques. The comparison clearly shows that the proposed method achieveda higher password entropy value than the other techniques. Therefore, the password generated by the proposed method is identified to be stronger than the other passwords, proving it to be more secure.

4.2.2 Password space analysis

The Password space has a significant contribution in the password generation phase,and a larger password is more secure than the other text passwords. A comparison between the proposed and existing techniques in terms of password space is presented in Table 2. The values are obtained by varying the password length as 3, 4 and 5. The password length indicates the number of images considered for password generation. From the comparison, it is clear that the proposed technique is more effective than the other techniques.

Figure 20 indicates the password space comparison of the proposed and existing techniques. From the figure, it is clear that the password space of the proposed technique is higher than the other techniques. It proves that the proposed method is more optimal in password generation and can result in better and larger passwords than the other compared techniques. Since the users are provided with the flexibility to select any number of click points from the images, the password length is huge for the proposed method.

Table 2:Password space comparison results

Sr. No.	Approaches	Password length	Password space
1	Graphical scheme [23]	3 4 5	220 222 226
2	Hybrid GUA Scheme [23]	3 4 5	275 2100 2125
3	Text based schemes [23]	3 4 5	220 226 233
4	**Proposed**	**3** **4** **5**	**472.392** **3401.2224** **22958.2512**

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7676
***Article Received**: 22 April 2023 **Revised:** 24 June 2023 **Accepted:** 12 July 2023*

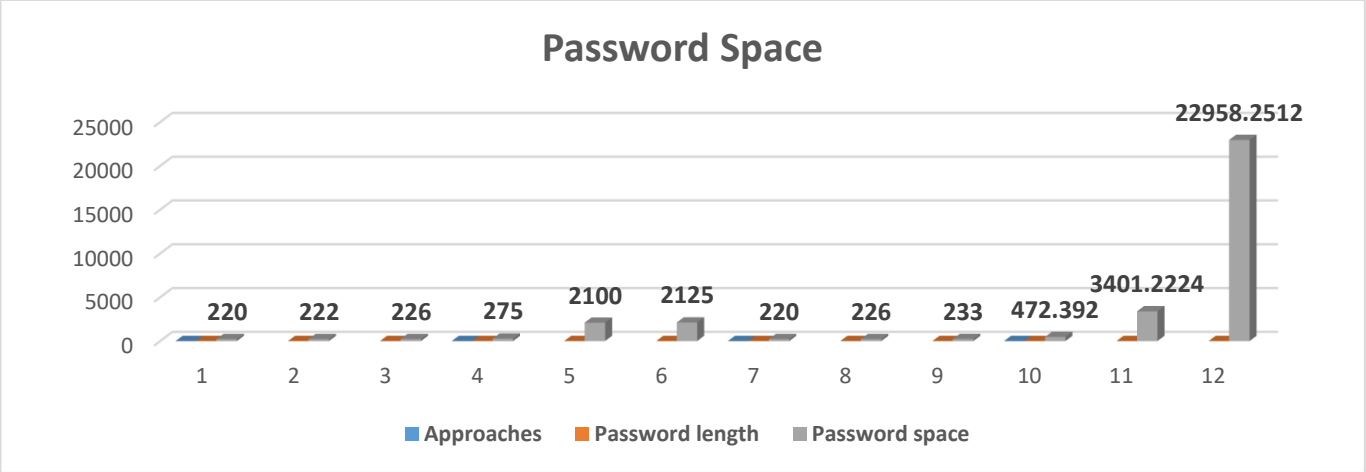

Figure 20: Password space comparison of the proposed and existing works

The overall simulations prove that the proposed scheme is more suitable for password authentication than the existing schemes. The analysis of different security issues indicated that the model is more reliable and suitable for password authentication than the other schemes. The possibility of any number of click point selections over the image improved the flexibility and security of the system. The success rate comparison for both the shoulder surfing and password guessing attacks proved that the proposed model can be applied for real-time simulations and is more optimal. Compared to the existing schemes, the login time taken by the proposed method is also low. It enhanced the overall net performance of the proposed scheme compared to the existing schemes.

4.2.3Shoulder Surfing Attack

The Shoulder Surfing Attack, which requires a slightly different circumstance of the zero-knowledge proof procedure, is the most well-known attack. Zero-knowledge approaches are mathematical techniques used to validate predictions without revealing or sharing the supporting information. The goal of Zero Knowledge Proof is to determine the average number of observations required to find the right password. Based on the data from the Alice-Bob [27] example, the suggested system can be divided down into four categories of security, namely:

• Can the attacker predict the image?

• Can the attacker identify the image's clickable point?

• How quickly can an attacker determine how many clickable areas there are in an image?

• Can an attacker predict the order of the images?

The following assumptions are taken into account for the shoulder surfing attack designed for the proposed systems:

1. Assume three factors, including image shuffle, image sequence, and part of the image used to identify an object that can be revealed by the attacker, for a total of three cases.

2. We want to determine the first probability of success, p=2/3, and the chance of failure, q=1-p. We have taken into account a favourable number of cases, m=2, when the attacker knows the image sequence and the objects because the object shuffle is random.

3. N represents the maximum password length, and M represents the number of observations the attacker needs to make.

In order to investigate the worst scenario and determine the number of observation rounds, we have used geometric distribution.

$$P(X) = p\,q^{(x-1)} \qquad where\ x=1,2,3\ldots \qquad (1)$$

So, for M number of observations, we have

$$P(X=M) = p\,q^{(M-1)} \qquad (2)$$

Then the probability of revealing all the click points (2≤N≤6) in less or equal to *M* observations is:

$$P_{all}(m \le M) = \left[\sum_{m=1}^{M} P_{rnd}(m)\right]^{N} \qquad (3)$$

- Therefore, the probability of revealing all the click points in *M* observations is:

$$P_{all}(M) = P_{all}(m \le M) - P_{all}(m \le M-1) \qquad (4)$$

- The average number of observations needed is:

$$\bar{M}_{all} = \sum_{m=1}^{\infty} m P_{all}(m) \qquad (5)$$

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7676
***Article Received**: 22 April 2023 **Revised:** 24 June 2023 **Accepted:** 12 July 2023*

Table 3. Shoulder-Surfing Attack Assumptions

Assumptions		**Parameters**	**Probability**
n = favorable number of cases	2	Image sequence	Success Probability p=2/3 Success Probability q=1-p
		Object	
m = influencing factors	3	Image shuffle (for each login, a different face will be displayed)	
		Sequence of Images	
		A small part of the image to identify the thing that the attacker could reveal	

Table 4. Shoulder-Surfing Attack of Proposed System

Length of Password (N)	2	3	4	5	6
Avg Number of Observations (M)	1.8746	2.1629	2.3906	2.5753	2.7290
Result:	**Observation requires more than twice**				

Interpretation

For passwords longer than two, an attacker often has to observe the password more than twice before understanding its significance. Additionally, the table 4 displaying the average number of observations grow monotonically as password length grows. Actually, the possibilities of the attacker are minimal. An attacker must typically watch the password more than twice to determine its meaning for passwords longer than two. The table also shows that when password length grows, the average number of observations rises monotonically. In actuality, the attacker's chances are low. As a result, we believe that our system is safe from shoulder-surfing attacks.

V. Conclusion

This work proposes a new and effective 3D graphical password authentication system based on the selection of click points. Initially, the users enter the registration phase, where the system obtains the user demographic information and the OTP verification. Then, based on selecting public or private domain images, the images are provided for the user's view. The click points selected over the images are stored in the database for future use. After completingthe registration phase successfully, the user enters the login phase, where the system asks for the username and password. Then, some random images and the images with click points are provided to the users for image selection. The users select a maximum of 6 images, and then the selected images are displayed over the cube for click point selection. The selected click points are then compared with the previously generated click points. The login phase is terminated based on the correct selection of click points. The proposed model can secure the users from different attacks,including shoulder surfing and guessing attacks. The evaluations of the system proved that the system is capable of providing a higher range of confidentiality and integrity to the users with high success rates in the training phase. The overall evaluations proved that the model could be applied in real-time as it is flexible and user-friendly with better security capabilities. In future, it is aimed to consider more 3D objects in the login phase further to enhance the security and flexibility of the authentication system.

Compliance with Ethical Standards

Funding: No funding is provided for the preparation of manuscript.

Conflict of Interest: Authors declare that they have no conflict of interest.

Ethical Approval: This article does not contain any studies with human participants or animals performed by any of the authors.

Consent to participate: All the authors involved have agreed to participate in this submitted article.

Consent to Publish: All the authors involved in this manuscript give full consent for publication of this submitted article.

Authors Contributions: All authors have equal contributions in this work.

Data Availability Statement: Data sharing not applicable to this article.

References

[1] Meng W, Zhu L, Li W, Han J, Li Y (2019) Enhancing the security of FinTech applications with map-based graphical password authentication. Future Generation Computer Systems101:1018-27.

[2] Sepideh F (2019) Providing a Secure Hybrid Method for Graphical Password Authentication to Prevent Shoulder Surfing, Smudge and Brute Force Attack. International Journal of Computer and Information Engineering 13(12):624-8.

[3] Yang GC, Oh H (2018) Implementation of a graphical password authentication system 'PassPositions'. Journal of Image and Graphics 6(2):117-21.

[4] Meng W, Fei F, Jiang L, Liu Z, Su C, Han J (2018) CPMap: design of click-points map-based graphical password authentication. InIFIP International Conference on ICT Systems Security and Privacy Protection 18-32. Springer, Cham.

[5] Najoua T (2018) KASP: a cognitive-affective methodology for designing serious learning games. International Journal of Advanced Computer Science and Applications 9(11).

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7676
***Article Received**: 22 April 2023 **Revised:** 24 June 2023 **Accepted:** 12 July 2023*

[6] Jiya GK, Oyefolahan IO, Ojeniyi JO. Recognition Based Graphical Password Algorithms: A Survey.

[7] Khodadadi T, Javadianasl Y, Rabiei F, Alizadeh M, Zamani M, Chaeikar SS (2021) A Novel Graphical Password Authentication Scheme with Improved Usability. In2021 4th International Symposium on Advanced Electrical and Communication Technologies (ISAECT) 01-04. IEEE.

[8] Shaik, D. ., & Santhosh Gollapudi, S. K. . (2023). Analogy of Distinct Constructions of FinFET GDI Full Adder. International Journal of Intelligent Systems and Applications in Engineering, 11(1s), 120–135. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2484

[9] Scholar PG (2018)Graphical Password Authentication System Based On Persuasive Cued Click-Points, International Journal of Recent Trends In Engineering And Research 54-60. doi:10.23883/ijrter.conf.02180328.008.d09qi.

[10] Ho YL, Lau SH, Azman A (2019) Comparison Between BlindLogin and Other Graphical Password Authentication Systems. InInternational Conference on Advances in Cyber Security 235-246. Springer, Singapore.

[11] Shaikh A, Pathan R, Patel R, Rukaiya AP (2018) Implementation of authentication using graphical password cloud computing. International Research Journal of Engineering and Technology 5(5):3293-7.

[12] Ms. Elena Rosemaro. (2014). An Experimental Analysis Of Dependency On Automation And Management Skills. International Journal of New Practices in Management and Engineering, 3(01), 01 - 06. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/25

[13] Mackie I, Yıldırım M (2018) A novel hybrid password authentication scheme based on text and image. InIFIP Annual Conference on Data and Applications Security and Privacy 182-197. Springer, Cham.

[14] Chopra A, Gupta M (2020) A bankable pictorial password authentication approach. InProceedings of the International Conference on Innovative Computing & Communications (ICICC).

[15] Songcuan JP, Sison AM (2019) Jumbled passsteps: a hotspot guessing attack resistant graphical password authentication scheme based on the modified passmatrix method. InProceedings of the 3rd International Conference on Cryptography, Security and Privacy. 55-59.

[16] Jóhann, Þorvaldsson, Koskinen, P., Meer, P. van der, Steiner, M., & Keller, T. Improving Graduation Rates in Engineering Programs Using Machine Learning. Kuwait Journal of Machine Learning, 1(1). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/110

[17] Constantinides A, Belk M, Fidas C, Samaras G (2018) On cultural-centered graphical passwords: leveraging on users' cultural experiences for improving password memorability. InProceedings of the 26th Conference on User Modeling, Adaptation and Personalization 245-249.

[18] Jaffar JA, Zeki AM (2020) Evaluation of Graphical Password Schemes in Terms of Attack Resistance and Usability. In2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT) 1-5. IEEE.

[19] Chu X, Sun H, Chen Z (2020) PassPage: Graphical Password Authentication Scheme Based on Web Browsing Records. InInternational Conference on Financial Cryptography and Data Security 166-176. Springer, Cham.

[20] Dhablia, A. (2021). Integrated Sentimental Analysis with Machine Learning Model to Evaluate the Review of Viewers. Machine Learning Applications in Engineering Education and Management, 1(2), 07–12. Retrieved from http://yashikajournals.com/index.php/mlaeem/article/view/12

[21] Yang TY, Shamala P, Chinniah M, Foozy CF (2021) Graphical Password Authentication For Child Personal Storage Application. InJournal of Physics: Conference Series 1793(1): 012065. IOP Publishing.

[22] Juneja K (2020) An XML transformed method to improve effectiveness of graphical password authentication. Journal of King Saud University-Computer and Information Sciences 32(1):11-23.

[23] Elena Petrova, Predictive Analytics for Customer Churn in Telecommunications , Machine Learning Applications Conference Proceedings, Vol 1 2021.

[24] Edward AL, Suru HU, Okudo J (2022) Position-Based Multi-Layer Graphical User Authentication System. American Journal of Software Engineering and Applications 11(1):1-1.

[25] Faraji S, Manochehri K. Attack Resistant Graphical Password Authentication Method Against Shoulder Surfing, Smudge and Brute Force Attacks. Smudge and Brute Force Attacks.

[26] Wiedenbeck S, Waters J, Sobrado L, Birget JC (2006) Design and evaluation of a shoulder-surfing resistant graphical password scheme. InProceedings of the working conference on Advanced visual interfaces 177-184.

[27] Pathak, D. G. ., Angurala, D. M. ., & Bala, D. M. . (2020). Nervous System Based Gliomas Detection Based on Deep Learning Architecture in Segmentation. Research Journal of Computer Systems and Engineering, 1(2), 01:06. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/3

[28] Malek B, Orozco M, El Saddik A (2006) Novel shoulder-surfing resistant haptic-based graphical password. InProc. EuroHaptics 6(1-6).

[29] Saeed S, Umar MS (2015) A hybrid graphical user authentication scheme. In2015 Communication, Control and Intelligent Systems (CCIS) 411-415. IEEE.

[30] Katsini C, Raptis GE, Fidas C, Avouris N (2018) Does image grid visualization affect password strength and creation time in graphical authentication? InProceedings of the 2018 International Conference on Advanced Visual Interfaces 1-5.

[31] Rajarajan S, Priyadarsini (2021) SelfiePass: A shoulder surfing resistant graphical password scheme. Research Gate.

[32] Sun T, Lee M (2013) Shoulder-surfing-proof graphical password authentication scheme. © Springer-Verlag Berlin Heidelberg.

[33] Li Z, Sun Q, Lian Y (2005) An association-based graphical password design resistant to shoulder surfing attack. IEEE.