ISSN: 2584-0495 Vol. 2, Issue 4, pp. 730-744

International Journal of Microsystems and IoT

ISSN: (Online) Journal homepage: https://www.ijmit.org

Image-based Object-sequenced Graphical Password Authentication System

U.P. Prashasthi Sagar, U.P. Pravardha Sagar, and Preeti Dubey

Cite as Sagar, U. P. P., Sagar, U. P. P., & Dubey, P. (2024). Image-based Object-sequenced Graphical Password Authentication System. International Journal of Microsystems and IoT, 2(4), 730-744. https://doi.org/10.5281/zenodo.11651505

Published online: 22 April 2024

DOI: https://doi.org/10.5281/zenodo.11651505

International Journal of Microsystems and IoT
Vol. 2, Issue 4, pp. 730-744; DOI: https://doi.org/10.5281/zenodo.11651505

Image-based Object-sequenced Graphical Password Authentication System

U.P. Prashasthi Sagar, U.P. Pravardha Sagar, and Preeti Dubey

Department of Computer Science and Engineering, Sharda University, Greater Noida, Uttar Pradesh, India

ABSTRACT
Textual passwords (one of the knowledge-based passwords) have been predictable and have long sustained security breaches due to their predictability (password dictionary attacks) and the possibility of shoulder-surfing and other such attacks. Biometric passwords are too rigid and can't be duplicated but are expensive and cannot be applied to smaller, cost-effective systems. Whereas Graphical Passwords are reliable, memorable and are known to improve one's cognition, hence very convenient to the user. Hybrid Authentication methods are proven to be far more secure than any other authentication methods. This paper provides a detailed study of graphical passwords, existing GPA techniques; and proposes an approach i.e., a combination of Graphical password and Textual authentication, a system with a better password entropy and ease of usability. It is well encrypted enough, to be able to defend against shoulder-surfing, dictionary attacks and many other security attacks. This authentication scheme contradicts the weak/strong password policy, browser cache and default credentials issues.

KEYWORDS
Authentication; Graphical password authentication (GPA); Hybrid Authentication; Memorability; Shoulder Surfing; Security; Mobility; Textual passwords; Sequence of Objects (SOO); Usability

1. INTRODUCTION

In the current world, *security* is a fundamental need to ensure the safety, seclusion and unjust use of sensitive data. Authentication is a security procedure to verify the identity of the individual to access any entity requiring security, such as personal and business information, bank accounts, etc. Every authentication system is a lock that requires a specific, and its very own key i.e., password. The kind of password determines the type of authentication system to be used. Security systems are meant to withstand several security breaches and attacks. Be it social, engineering, shoulder surfing, brute force, sniffing, dictionary and spyware attacks. This can also be ensured when the sensitive data is transmitted through secure channels while providing the utmost privacy to the user's information.

Password memorability and human remembrance are key factors that influence password strength, whether the set password is secure from being discovered or guessed by unauthorized personnel including the administrator of the system. Lengthy combinations of different characters i.e. symbols, numbers and letters, may seem to be the way to ensure a strong password that is impenetrable. But it is observed that most people want to simplify their passwords within these restrictions, hence tend to use personal information such as date of birth, names and nicknames, most often their own or of their loved ones; making combinations of these and using brute force attack will provide access to unauthorized personnel.

A. Token-based authentication - requires a physical entity to act as a key such as ATM cards, RFID cards and tags. It requires that the entity be physically carried, i.e., it must be mobile. [1,2,3,4]

B. Biometric-based authentication - it utilizes rigid, unchangeable physical features of the user such as fingerprints, retina scans, facial recognition, voice recognition, etc., Since no individual shares any similarity with another regarding the biometric features (including identical twins). But these features may get damaged due to extensive construction work. Also, biometric systems are expensive. Two types of systems are observed, one requiring physical contact, and the other lacking it. [1,4]

C. Knowledge-based authentication - It depends on the users' memorability and cognition. Usually, users set their own passwords, and these are required to be simple enough to remember and tough for attackers to crack [4]. As depicted in Fig.1, it is of two types:

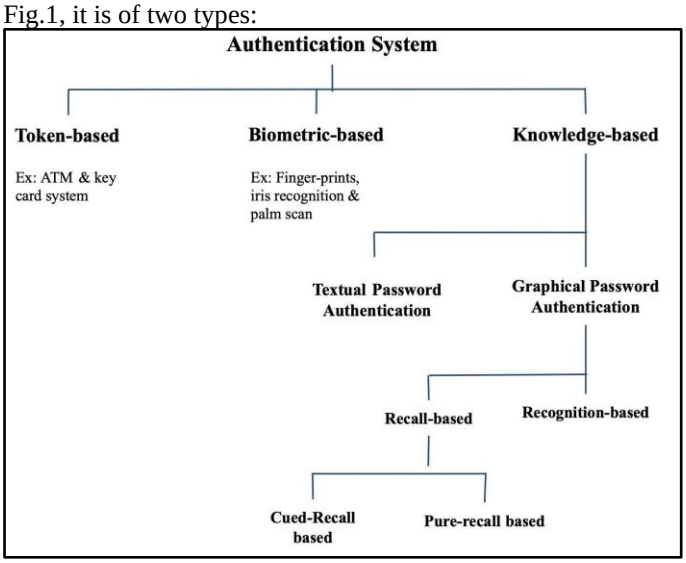

Fig. 1 Authentication and Its Types

The authentication systems can be categorized as follows (See Fig (1).

(a) Textual Passwords use 'alpha-numeric' sequences as passwords. The lengthier the password ensures higher
(b) security, but it is often difficult for the user to memorize. But
(c) if it is to the user's convenience, then they are short enough to guess; and
(b) Graphical Passwords require the user to determine a password via a Graphical user interface, hence any image can be a password. It is proven to be easier to recall compared to words or numbers [5] (Refer to Section 2).

Our objective for inventing a new authentication scheme is, to provide a reliable Graphical password authentication alternative with an easy-to-use, easy-to-memorize authentication experience, which is a reliable and working *content delivery* system with *improved security*. It is within the purview, to develop a unique *Graphical Password Authentication* that is an amalgamation of GPA and other *Knowledge Cognitive* based techniques. To research the advantages and disadvantages of our authentication technique on *human retention* and *accessing efficiency* parameters. Also to develop an *Operational Web Application* using in-house authentication API.

In this study, we have proposed a new GPA system with textual input authentication for websites on all smart devices. It is the fusion of Recognition-based authentication, and Cued-recall-based authentication, all the while incorporating randomization to prevent shoulder-surfing and sniffing attacks. This study is constructed in the following fashion. Section 2 provides classification and reviews the related work in the field of GPA, including important existing systems and methodologies. Section 3 provides the outline of the proposed system, and the study conducted. Section 4 specifies the system architecture and implementation. Section 5 provides the results of the study conducted as well as the analysis of the proposed system. Section 6 puts forth the limitations of the system. Finally, section 7 lays out the future scope and concludes the study.

2. RELATED WORK

Graphical passwords are already proven to have better password entropy and larger password size than text-based passwords. Graphical passwords are constructed using any picture of either the user's choice or a drawing, pass points, cued-click points, blunder's scheme, etc. These passwords have various schemes themselves and different security mechanisms as well, in turn strengthening the authentication GPA is mainly an effort to overcome security issues/attacks, easily remember passwords, and increase usability via reducing login time and at most privacy.
The distinct categories within graphical password systems and existing authentication methodologies as reviewed are described as follows:

I. Recognition-Based Passwords

It is a cog-no-metric system. a mechanism of authenticating users by listing multiple pieces of information and letting them choose the proper password information. For instance, Pass Faces will show several faces, only after choosing the right preset face within the specified number of tries are users authorized. With this approach, entering the password takes time, and a number of issues could occur, such as the transmission costs associated with photo data needed for system development and operation [6, 7, 8]. For example, Jensen's method, Pass faces, Sobrado & Bridget's method, Hong's method, Deja vu, etc.,

Pass faces - Face identification is the foundation of Pass faces, the password will be provided by the system, and you are required to learn and practice them, to be able to login. [18] conducted research on Pass faces by creating their own version of it. It found that user-chosen passwords are predictable and weak making the system insecure and prone to breaches.

[7] proposes a Secure-Pass face algorithm to choose a password at the login phase, introducing the concept of an 'alternative password', while omitting the use of the mouse. Offers comparison of the Pass face and S-Pass face algorithms based on usability, and security (social engineering, shoulder-surfing, brute force, spyware attack and guessing). The benefits of S-Pass face are easier memorization, recognition, understanding and ease of use, on par with the client. It also increases security by creating resistance to shoulder-surfing, but this action reduces the usability of the S-Pass face. According to [7], choosing a password is more difficult than creating one. But attackers will be able to guess the S-Pass face password more precisely over the original Pass face algorithm.

II. Recall-Based Passwords

It handles validation by comparing input patterns with a pattern that was previously stored. This procedure is identical to a text-based password system. However, no hint is offered, so the user must recall the password. As a result, users of a recall-based graphical password system cannot readily exploit long passwords. Therefore, against dictionary attacks, the recall-based graphical password scheme is particularly vulnerable. For example, Draw-a-secret, Blonder's scheme, v-Go, Vis Key, Cued Click Points, and Pass points [8].

2.1. Pure Recall-Based GPA: It is a draw metric system. Here, without employing any of the system's hints, the user must recreate the password. For example, DAS, Grid selection, etc. are pure-recall-based techniques. Jermyn et al.'s creation, Draw-A-Secret (DAS), is a recall-based system that needs the user to recreate the picture or pattern that is configured as the password sans the system offering any hints. [16]. Here, the drawing area/space is a grid of size s*s, and the pattern is recorded as a sequential set of coordinates. The pattern must be completed in a single stroke (multiple joining or overlapping strokes are not accepted). Hence, the drawing/ password must be reproduced exactly in the same fashion as it was set i.e., during the registration and change password procedures. Only then it is authenticated. The tolerable distance is 0, therefore, the password must be exact [13]. For example, the pattern lock on smartphones and devices. But here instead of a grid of blank squares, it has an s*s node grid that makes node-to-node connection specific, clean and easy, while reducing errors significantly. The tolerable distance is not a question here. But in any case, it is the user's burden to

remember the exact stroke sequence. Also, it is text independent as well as easier to implement [3].

2.2. Cued-Recall Based GPA: It is a loco-metric system. It provides a password pattern that uses an appropriate background image or other data. The burden of remembering is less on the user than with a straightforward prompt-based password system. with a straightforward prompt-based password system. According to [9], for instance, a system that allows authentication only when a user clicks on designated locations on a certain image in a predetermined order. It has the following benefits: fast password entry and reduced strain on the user's memory. The drawbacks are the hotspot issue and the need to click on the right points [10]. For instance, pass points and cued click points (CCP).

Pass Points -

It is a Cued-recall based system; Created by Wiedenbeck et al. and inspired by Blonder's scheme that uses a system-assigned image and click-points in specific regions only [11]. But Pass Point requires a user-fed image and click-points for a password. Here, the order of selection of click-points matters the most, hence the password must be the same as the registered/ set password. But the tolerable distance here is approximately 0.25cm from the original click-point. There can be numerous click-points as determined by the user, in turn reducing the risk of a security breach [11, 16, 17].

The picture must contain objects of identification, which would make the user successfully identify and select them in consecutive order. Hence, it is necessary for the user to be very familiar with the image i.e., set as the password, so that the memorability of the password is high and convenient to the user [14]. But password input from the user's end is a time-consuming process, also several trials are required to authenticate the password depending on the length, memorability of the password and the memory retrieval capacity of the user [3, 13].

Pass faces -

Face recognition is the foundation of Pass face, except it recognizes a warped version of your face rather than your actual one. If it relied just on facial recognition, anyone might impersonate you by flashing a snapshot of yourself.

[18] conducted research on Pass faces by creating their own version of it. It found that user-chosen passwords are predictable and weak making the system insecure and prone to breaches.

[7] proposes Secure-Pass face algorithm to choose password at login phase, introducing the concept of 'alternative password', while omitting the use of mouse. Offers comparison of the Pass face and S-Pass face algorithms based on usability, security (social-engineering, shoulder-surfing, brute force, spyware attack and guessing). The benefits of S-Pass face being easier memorization, recognition, understanding and ease of use, on the part of the client. It also increases security by creating resistance to shoulder-surfing, but this action reduces the usability of S-Pass face. [7] identifies that it is easier to create a password than to select one. But attackers will be able to guess the S-pass face password more precisely over the original pass face algorithm.

Cued Click Point -

CCP is based on cued recall cognition. It was proposed by Chiasson et al as an alternative to Pass Points. It is an integration of Pass Points, Pass faces and Story. There is one click-point per image, where the single selection of a click-point on an image leads to another image with its very own click-point [6]; Applying the Story and Pass faces concept in terms of the progression of images, only if the password is correct otherwise the image does not change, indicating the correctness of the password to the user. Also uses the concept of Pass Points and Pass faces in terms of click-point or select an image strategy. Pass Points' discretization method is implemented in CCP, which initially functions like the former system [25]. From Pass Points, CCP also inherits the grid-like structure on the image and tolerable distance (concept) from the original click-points. The tolerable distance can be set as per convenience and accuracy by the system using the corresponding grid to act as a boundary within which the tolerance of the original point lies.

The user must click each of the five images once, not five times on a single image. A 'path' is predefined for each consecutive click-point, completing authentication. But selecting a wrong click-point on any image might lead the user down an "incorrect path", hence, the login attempt is bound to fail. "*An explicit indication due to the selection of incorrect click-points is only provided after the final selection."- (Chiasson et al)* [6]. To avoid hinting the imposters/hackers i.e. the unauthorized users where they went wrong and make them unable to guess the correct sequence. Therefore, making the password highly unpredictable than Pass faces, in turn, increases the security of the system. Hence, CCP can also be known as choice-dependent path images.

As shown in Fig. 2, the change in visuals/images does not hint at whether the password is correct or not, but it is evident that the legitimate user has the knowledge to distinguish between "correct and incorrect paths". Legitimate users get immediate indications in case of any errors during login. The users identify their mistake when an incorrect image appears and they can spontaneously cancel their login attempt and begin again [6, 9, 10, 25].

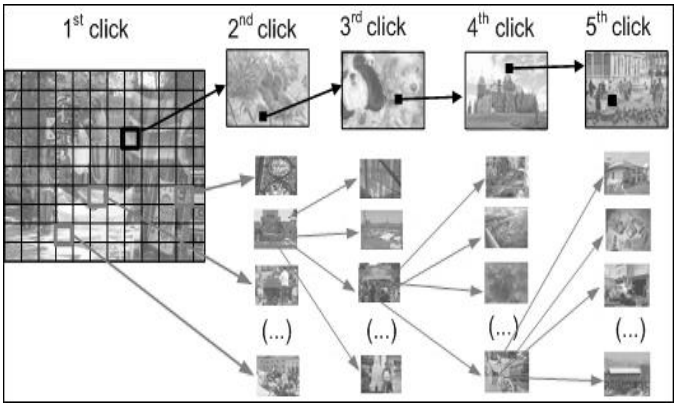

Fig. 2 CCP - sequence of clicks on different progressive images of a path. [6]

[6] also conducted a proper survey, according to which 9 out of 10 users preferred CCP over Pass Points, 2 of them found Pass Points easier than CCP, and all of them agreed that CCP would be tougher to get past i.e., when there is an attack/ breach, therefore more secure. [9] has employed the Cued Click Point system with enhanced mobile alert systems on possible security threats. This CCP system is harder to hack and has tougher security. However, the traditional CCP system does not safeguard against *shoulder-surfing*, the password is difficult to memorize. Hotspot identification is a problem [6]. [18] suggests a system that combines a recall-based method with a recognition-based approach. This system offers security from brute force, shoulder-surfing, and dictionary attacks. Also, it shows the comparison between CCP and Pass Points based on users' preferences and mentioned parameters i.e. security, usability, speed, accuracy and error probability. CCP is highly preferred as its virtue lies in improved security, better usability and accuracy. Whereas, It also states that hotspot identification is an unresolved issue.

2.3 Hybrid Graphical Passwords

A system that combines many graphical password approaches. It's crucial to consider interactivity and maximize the effectiveness of the completed system while developing a new hybrid graphical password system [11, 27]. Basically, there are three types of authentications: cued-recall, recognition-based, and recall-based. Under these categories, there are many GPA schemes, as seen in Fig.1. These GPAs mostly define the serviceability/usability of the authentication systems (ease of use). And each GPA tackles a different security issue but cannot always cover them all. Security and usability are the major design and implementation issues in several GPA schemes.

[12] did propose a system combining both textual and graphical password authentication, while also taking advantage of *multi-factor authentication.* Greater emphasis was laid on Point-of-interest (POIs) regions in the picture. This system fundamentally intends to obtain a picture of the user's choice. Users have to select POI regions in the picture, provide corresponding words to each POI respectively, and create an order of POI selection. [13] proposes a *Cued Click Point system* to secure *Cloud* with enhanced mobile alert systems on possible security threats.

Pastilles-

In [7] to conduct research on the memorability of different types of passwords, emphasizing graphical passwords ("Memory retrieval and Graphical Passwords"). For that purpose, they created Pass Tiles. A five-tile password is used in the Pass Tiles graphical password system, which consists of a matrix of squares or tiles. The proper password tiles must be clicked on by the user in the correct sequence to log in.

It is a perfect integration of DAS (Draw-a-secret), Pass Points and Pass faces. Passwords here can be either chosen by the user or assigned by the system.

There are three basic variations of Pass Tiles:

1. **Blank Pass Tiles -** Has a blank background, like DAS, free-recall task.
2. **Image Pass Tiles -** Based on an image divided by a grid, like Pass Points, cued-recall task.
3. **Object Pass Tiles -** Here, each square contains a different Image or object, forming a matrix of several object images, like Pass faces, a Recognition based task. It is a shuffled grid. Object Pass Tiles can have two more variations: (a) containing pictures, and (b) containing words.

But the analysis by [7] involved the following password types i.e., the three variations of Pass Tiles as mentioned above (BPT, IPT, OPT), and the traditional forms of passwords - Assigned Text and Chosen Text. [7] mainly studies three variables i.e. memory time, password resets, & login time, of all the password conditions. Pass Tiles permits users to benefit from both recognition and recall memory, while memorability and login times are quicker.

[15] conducts a thorough study on the memory retention capacity of both children and adults with respect to all three cases of Objects, Images and words Pass Tiles. Intends to create a *Child Oriented Authentication System*. Through a survey study, it was found that both children and adults are receptive to Object Pass Tiles. The parameters concluding the result were as follows:

i) Memorization Time
ii) Login Times
iii) Login Success
iv) Degree of Correctness
v) Interview / Feedback

According to the above experimental study by Assal et al., both children and adult candidates were extremely good with Objects Pass Tiles, and they also preferred it. Assal also claims that *fairy tales* are an effective password memorization method. But it neither explains *adult responsibility* in the *Child Oriented Authentication System* nor does it consider shoulder-surfing as a security breach-cum-attack [15].

Story:

As an alternative to Pass faces, Davis et al. advocated the "Story" Graphical Password Authentication system. Using frequently seen images of objects or random pictures and selecting them in the correct sequence. It was suggested that the user frame a story involving the choices of password, for better remembrance of the password. It was observed that the predictability of the user's password is lesser, but memorability is worse than Pass faces [6, 18].

Text-based passwords usually have a low password entropy i.e. the measure of the security of a selected password, requires high memorability, and the usability is highly dependent on the mentioned factors [2]. Text-based systems have a significant issue when it comes to creating passwords, since, in most cases, the user tends to choose terms that hold some emotional value and admiration i.e. their nicknames, close ones, pets, cars, etc. Such passwords can be easily discovered/ realized by their close ones and attackers.

Shoulder-surfing, brute force (guessing), social engineering and spyware attacks are the major security issues, then hotspot identification etc., comprise the design issues of GPA systems. Whereas the increased registration (sign up) and login time, heavy storage space for images, difficulty in changing forgotten passwords etc., that determine the ease in usability and performance are the implementation problems of the Graphical Password Authentication system.

Table.1 Pre-existing Methodologies with respect to Graphical Password Authentication

S.N.	Approach	Working	Demerits
01.	Draw-A-Secret (DAS) [16], [19].	● Proposed by Jemryn et.al. ● Reproducing a drawing in a specific set of grids, exactly in the same coordinates as when the password was set.	● The drawing must be very accurate to be validated, hence it is quite hard to do so. ● The user can't recall the exact predetermined stroke order. ● Familiarity with input devices is necessary. ● Prone to shoulder-surfing and spyware attacks.
02.	Blonder's Scheme [20]	● Proposed By Greg Blonder in 1995. ● During the registration, the user must provide a pattern of tap region selection i.e. the password. ● Login, Sequential clicking on tap regions in a predetermined pattern, on a predetermined image.	● If it is large, then it is quite easy to crack the password. ● The simple background image.
03.	Pass Point [11], [16]	● It overcomes the shortcomings of the Blonder's Scheme. ● 1. Selection of an image and 2. click on the Regions-of-interest in a specific sequence (to set a password). Step 2 for login	● Extremely difficult to memorize and remember. ● And very time-consuming ● Prone to shoulder-surfing and spyware attacks. ● Less accurate since sample training is necessary. ● Login time is longer than textual passwords.
04.	Cued-click Points [6] (Refer to Fig. 2)	● Several images are chosen in a sequence and regions of interest are determined. Users shall have to click on the tap region of every occurring image and in a proper sequence. ● It is a proposed alternative to Pass Points	● Regions of interest / the hotspot are inflexible and an issue. ● Password space requires expansion.
05.	Pass faces [7],[18]	● Select 4 faces from the grid of faces. ● During the registration, the user must confirm it twice.	● Password is usually predictable ● Affected by race, gender and attraction.
06.	Grid Selection [21]	Select a small region from a large grid, if right the selected region would expand and will require the user to draw the predetermined pattern.	● One can't recall the order of the line/stroke exactly. ● The sequence of grids and drawing may change during authentication ● It is hard to use, when the user is unfamiliar with the input tools & devices. ● Prone to spyware attacks.

07.	Deja Vu [22]	Recognition of images at the time of login, that were set as password during the registration.	• Heavier burden on the server, since the seed values are stored on the server & these values get corrupted only when the server fails. • The authentication and validation is very time consuming. • Prone to Brute force, Dictionary, & Social Engineering attacks.
08.	Jansen's Method [8]	• Several images in a matrix are to be selected in a sequence set during the registration. • Images are based on any particular theme.	• It has a smaller password space compared to text-based passwords. • Hence, to overcome this problem users are to select 2 images at once on a single tap to expand the size of the password space. It will become extremely hard & complex for users. • Can confuse the user when struggling to recall.
09.	visKey [8]	• Same as the Blonder scheme but modeled for mobile devices. • SFR Company has developed it.	• Suppose the input precision is small, then the user might find it hard to tap on the exact regions/points • The tap point/regions are restrictive; hence the user cannot click as per wish.
10.	Sobrado and Birget's Method [23]	• Among the displayed objects, those selected during signup must be pooled in the convex hull.	• Very difficult to recognize the required image from the display of a huge array of several images. • Due to its convex-hull mechanism, assignment takes longer time and many attempts.
11.	v-Go [8]	• Also known as "Repeating the sequence of actions". • Clicking and dragging objects according to background image as per the set password.	• Password space is small, and the passwords are poor. • And predictable. • Easy to memorize but hardly secure. • Non-resistant to shoulder-surfing.

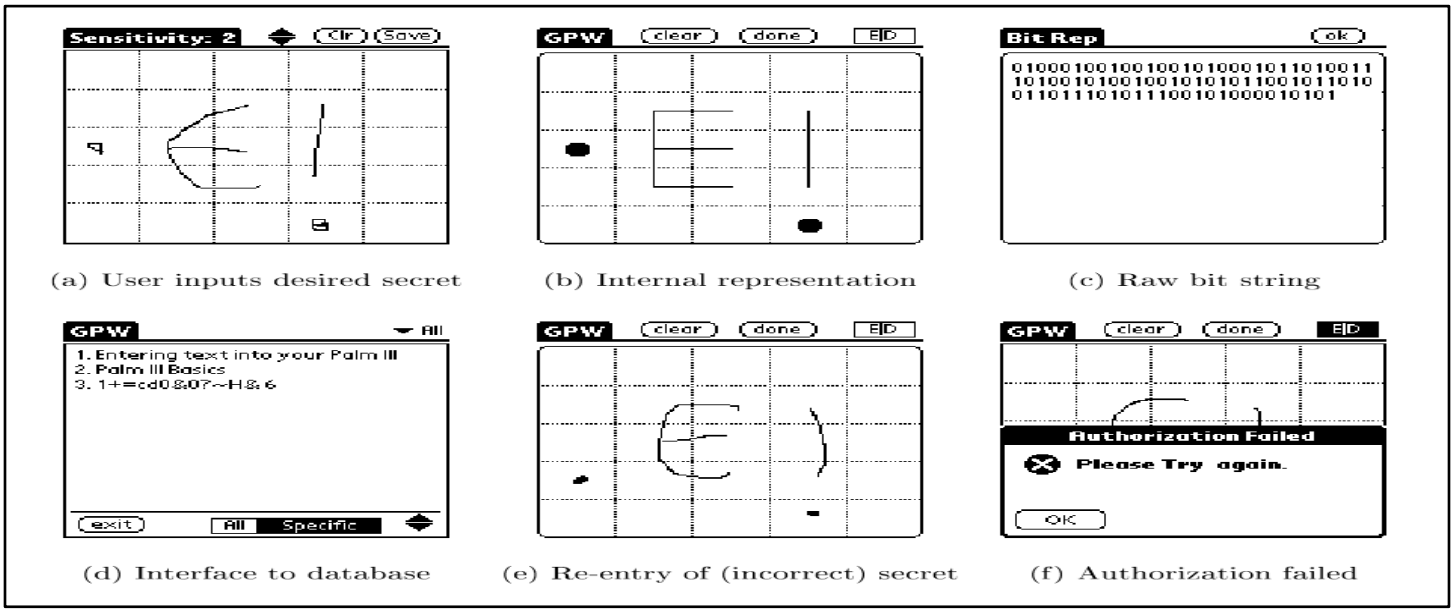

Fig. 3 Draw-A-Secret [16]

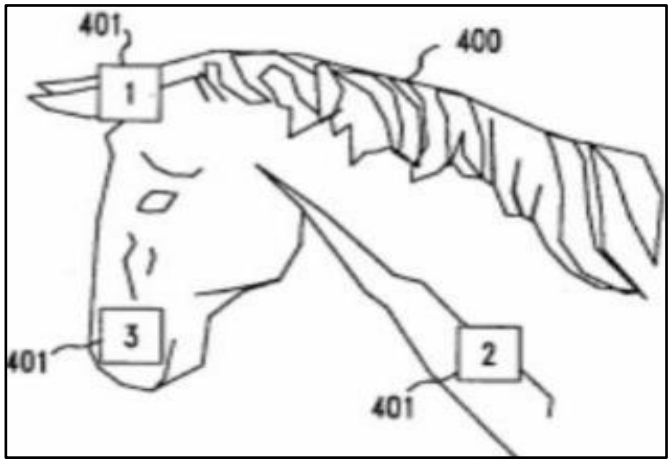

Fig. 4 Blonder's Scheme [20]

Fig. 5 Pass Points [11], [16]

Fig. 6 Pass faces [7],[18]

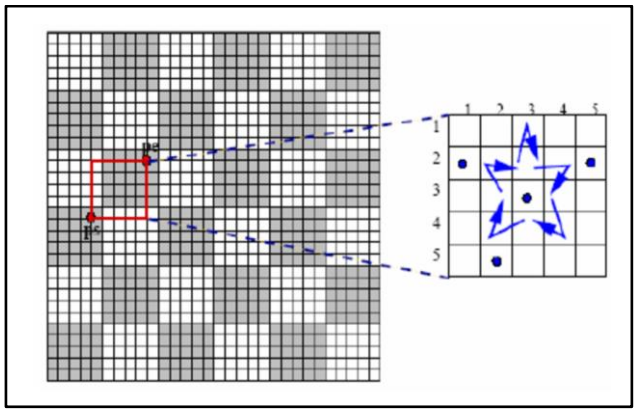

Fig. 7 Grid Selection (Selection of drawing grid) [21].

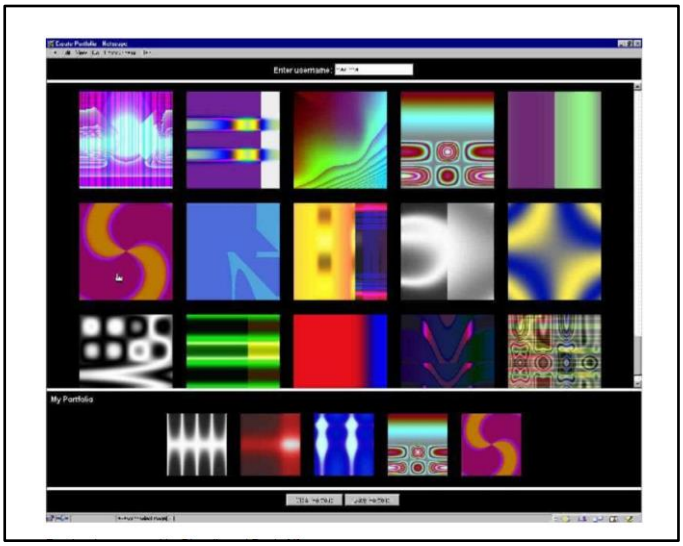

Fig. 8 Random images used in Deja Vu [22]

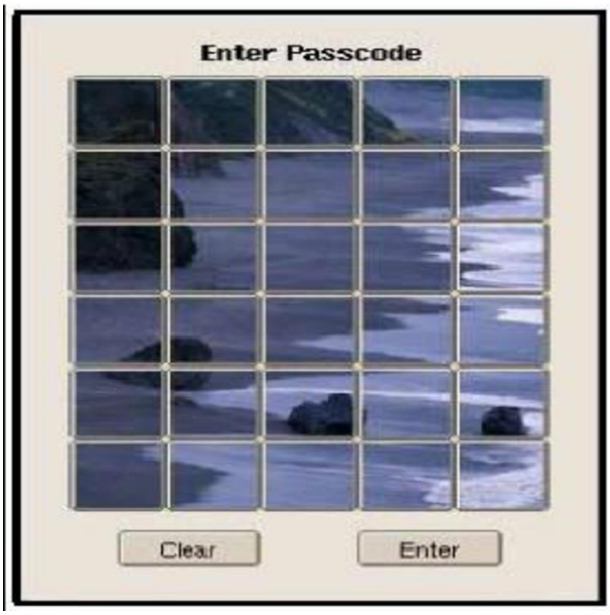

Fig. 9 Jansen's Method [8]

Fig. 10 Vis Key sample image [8]

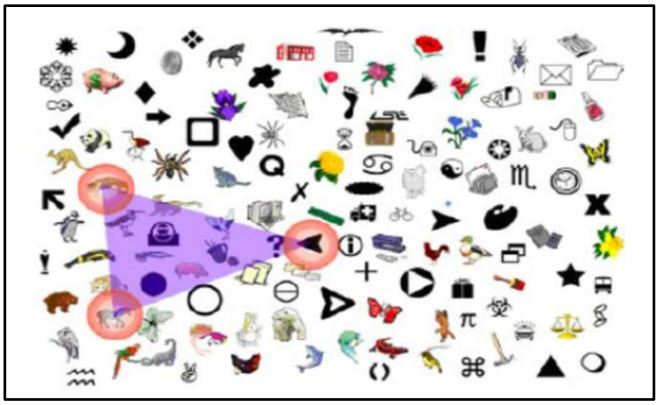

Fig. 11 Sobrado and Birget's Method (Convex Hull algorithm) [23]

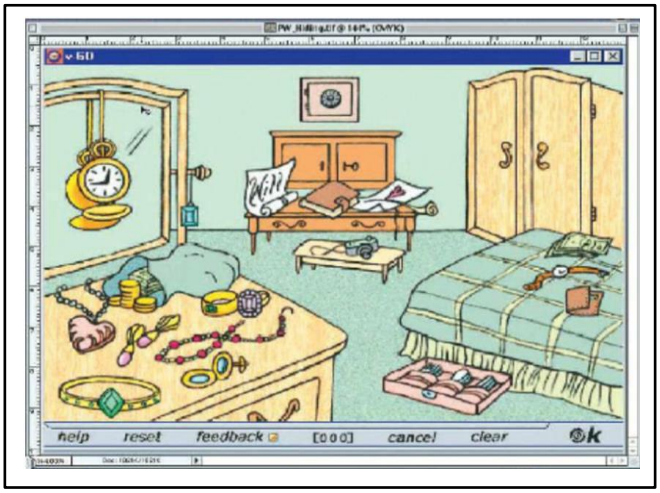

Fig. 12 v-Go [8]

3. METHODOLOGY

The methodology for creating this system involved research on Authentication methods, their merits, human convenience, and exploitation via security breaches. Our research on existing techniques is mentioned in *Related work* (See section II). Whereas, *our* approach, its feasibility, requirements and system Architecture are mentioned below.

A. Proposed Approach

The Proposed System takes in the sequence of objects (SOO) as the password. During the registration, an SOO is taken from the user out of a 3*3 matrix. Repetition of objects is allowed, and the minimum length of the SOO is at least 4. While Login, the user is supplied with a 3*3 matrix consisting of images of different objects, and the user must enter the image positions in numerical order that matches their SOO password.

Every attempt to login to a new matrix with different images of the same objects with shuffled positions is supplied.

Numerical entry encourages accurately stating the position of the SOO invalidating any ambiguity in the GPA procedure. Required cognitive functioning is necessary for every attempt at login.

B. Participation

To investigate the proposed system's usability and memorability. A group of 100 students were gathered to test out the authentication. This process was conducted Online for a 5-week duration, every Sunday.

In the first week, the working of the system was explained, and the Registration procedure was conducted for each participant. This included every participant signing up using the deployed GPA system. Every participant registered using their name as the Username, their Email-ID and their Roll NO as a textual Password. Later they made their SOO with 4 being the minimum Length of the SOO and the maximum Length of the SOO was limited to 10. Repetition of the objects was allowed.

In the Second week, every participant was required to sign in using their Username and SOO Password. For the participants who forgot the SOO password, they used the Forgot Password route to make another SOO and then Sign in. The number of Forgot Password route users was also recorded. The average Login Time was calculated for each participant, this is done using a JWT token consisting of the time of creation and after the successful completion of the login process, the time difference between the creation of JWT and the current time was calculated in the backend server. It was also noted how many attempts it took for a successful login. Feedback after the login process was also taken from the participants.

In the last 3 weeks, the same procedure of login was followed providing us with the data 3 login iterations of 100 users.

C. Complete Registration, Login Example

As mentioned above and shown in Fig.14, The user is required to provide credentials and a textual password in the *Join Us* phase of registration. Next, the *Select Password* phase appears; it consists of a series of object names displayed as buttons, an input box that displays the SOO clicked in a sequence, a backspace button for correction and finally the register button. Here the object set is of 9 animals as seen in Fig.15, out of which a password of length between 4-10 must

be chosen, then clicking the register button would complete the procedure. Suppose the SOO chosen is Elephant, Spider, Hen, and Squirrel, in the same order. The user is then directed to the homepage, at which point they would have to login for the first time.

The user must enter their username during the login process as shown in Fig.16, next the system progresses to *Object Identification.* Here, a 3*3 grid of object images is displayed consisting of the password objects (determined by the user during registration), The username is a variable that helps the system procure the respective password of the user. Along with other random object images, all arranged in a random fashion. A textual input box is provided right below the grid to enter the passcode. The passcode is the position of occurrence of the SOO (password objects) in the right sequence. The positions are sequenced from 1 to 9, like in a number pad without a zero, i.e. ascending order from left to right and continue accordingly in the other two rows. According to the set SOO, the passcode for this grid shown in Fig.16 is 2934.

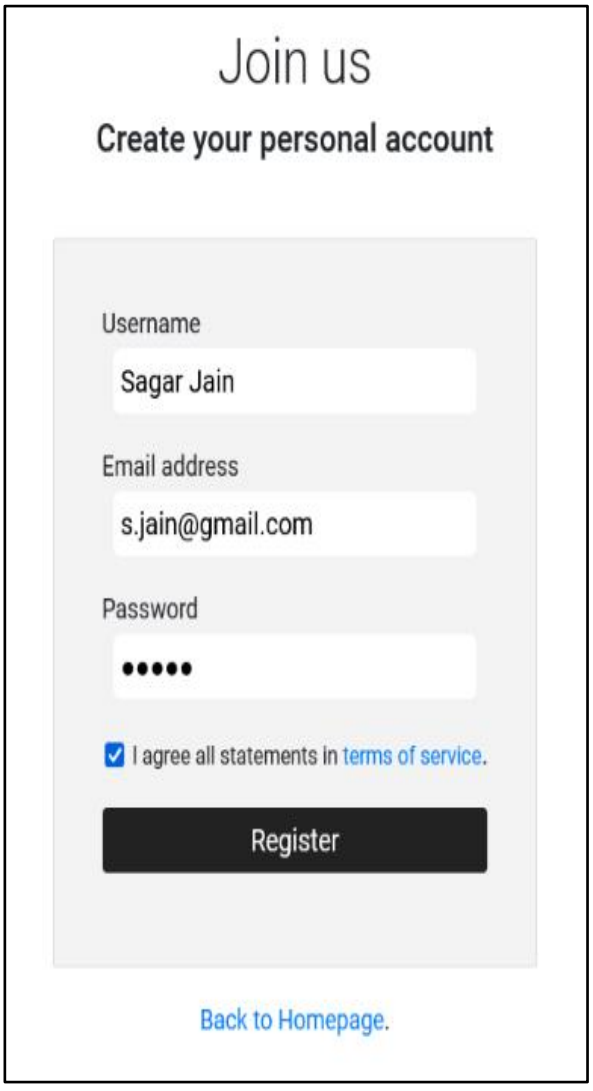

Fig. 13 JOIN US PAGE

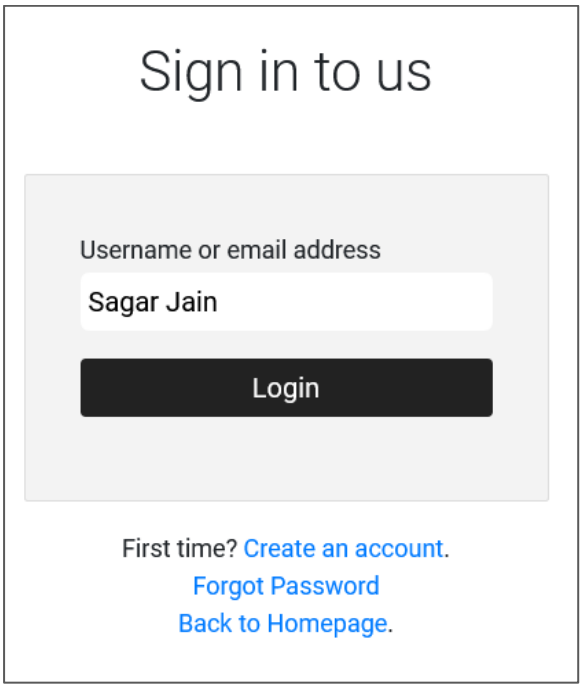

Fig. 14 SIGN IN PAGE

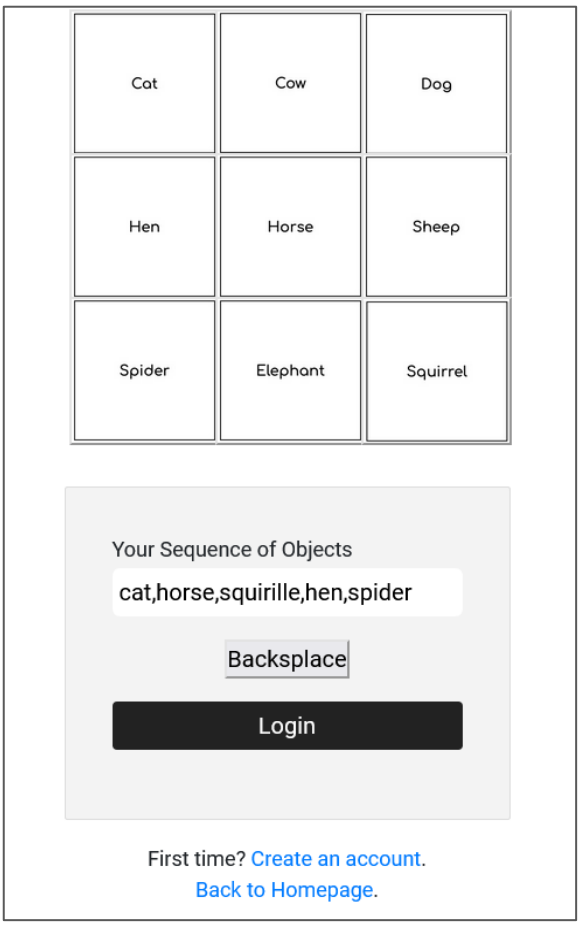

Fig. 15 SELECT PASSWORD PAGE

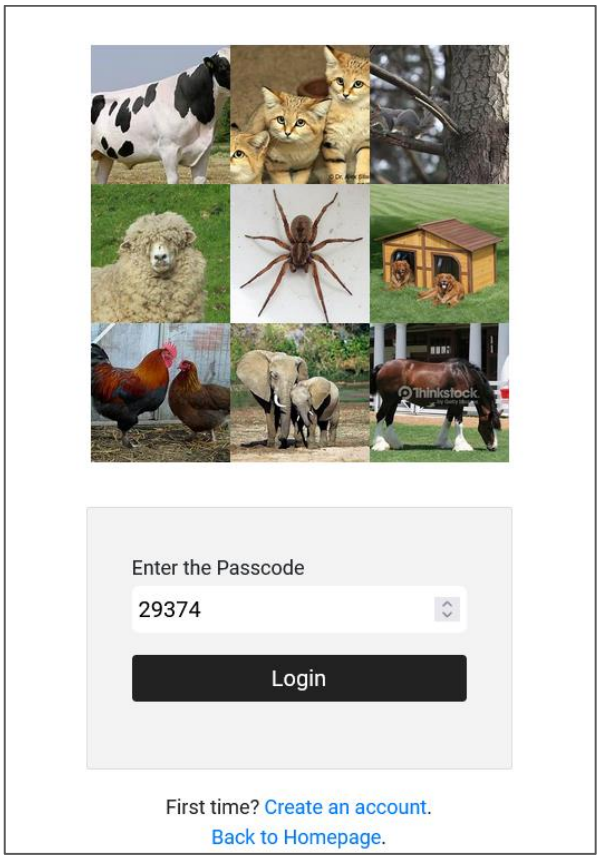

Fig. 16 GPA SIGN-IN PAGE

4. SYSTEM MODULES AND IMPLEMENTATION

Following the review of several GPA techniques, we have learnt their major achievements and failures in terms of security, convenience, and memorability. Most of the research highlights the fact that visuals tend to be more memorable than any other knowledge-based authentication system. The point of having a GPA system is to get rid of long-and-lengthy textual passwords, as well as rigid biometric systems. The user must be able to determine and have full control over their desirable password for the user's accounts in different applications, and they must have guaranteed security for their sensitive information. Our proposed model of system authentication in development functioning is as follows.

This section describes the utility of each element of our model. It consists of the following components as depicted in the front-end of the model, which is: a. Dashboard, b. Homepage, c. Register, d. Select password, e. Login, f. Forgot Password/Reset password. The front-end has been developed using ReactJS, Whereas the back end is made using Node.js server and Express web framework and for database management MongoDB Atlas.

It basically has 4 modules consisting of the Registration phase (See Fig. 13 and 15), Login Phase (See Figures. 14 and 16) and Forgot Password phase (See Figures. 17, and 15), as depicted above.

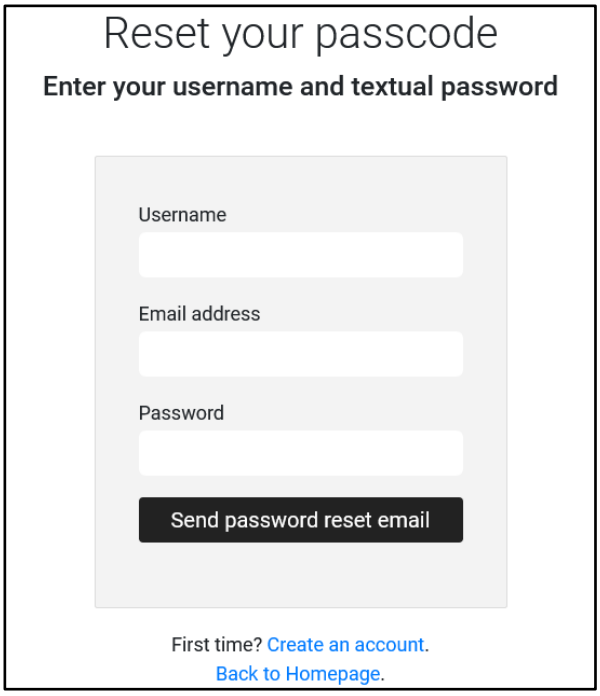

Fig. 17 RESET PASSWORD PAGE

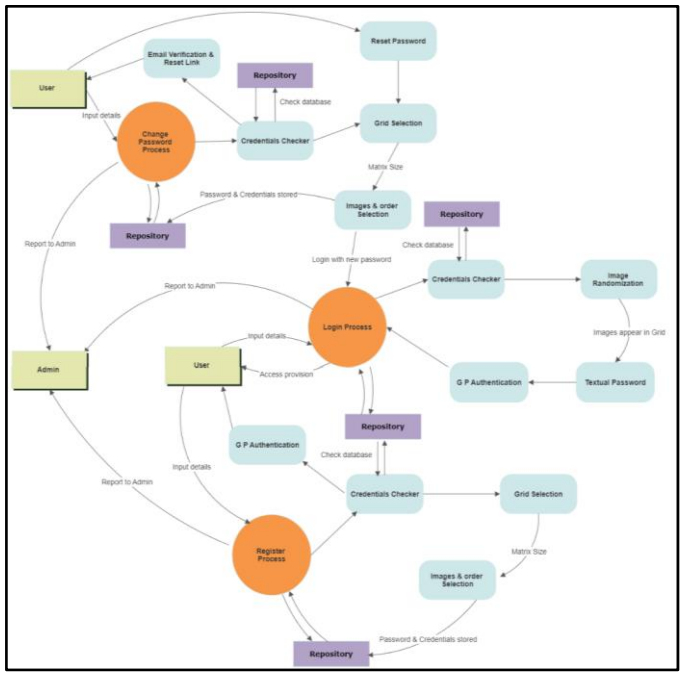

Fig. 18 SYSTEM ARCHITECTURE

On the front end:

a. Dashboard Component:

The above-mentioned component is an element 'used in the testing phase' to showcase whether the account is personal to the user, or if it is a default standard page. Hence, to highlight this difference, the user after login is asked to provide a "QUOTE" to customize their page to identify the difference between one user's account and another.

b. Homepage Component:

The navigation offered by this component allows users to select either the login option for previously registered users or the register option for new users.

c. Registration Component:

The sign-up procedure is inclusive of all the user's details required such as Username, Email-id, and a textual authentication key to verify the user in case the password is yet to be chosen, or, in the case of a forgotten password. Sign-up is Part 1 of the Registration phase, it will lead to the Select Password Phase, the 2nd Part of the phase.

An assortment of photos will be available for the user to choose from during the select-password phase. One must select/click on the desired images to have the system record the set of images and their order of selection to form a specific password. A point to note is that the password (to be entered in the login phase is textual) is not in the format of images, it is actually a passcode or numeric key that signifies the order of image selection (i.e., done in the Select Password Phase). The textual password required here is also encrypted using Salt + Hash to avoid easier discovery of this password as well.

d. Select Password Component:

In this phase, there are clickable buttons consisting of object names and an input text box below it. The string is automatically added into the input box in the sequence of Password Image. This "string" considered password is encrypted using '*Salt*' and '*Hashing*', the password remains privy only to the user even the *Administrator* cannot decrypt it, since no key is maintained to decode the Salt + Hash encryption. Whereas comparison is possible (See login component section).

The password chosen must be of convenience, must have a length between 4-6, and any element in the password can be repetitive, i.e. suppose in an array of images - the password can consist of 'Rabbit ⟶ Squirrel ⟶ Tiger ⟶ Rabbit', or "Rat ⟶ Rat ⟶ Apple ⟶ Rat".

It is advised that the password must be memorable, hence the password can be made with help of a story, such as "Rabbit ⟶ Tunnel ⟶ Cat ⟶ Hat" inspired by 'Alice in the wonderland', or "Glasses ⟶ Broomstick ⟶Dragon ⟶ Egg" suggesting the 'Harry Potter series. Davis et. al. has also asserted that a password containing a story increases the memorability of the password. Therefore, a user can make up a story to remember the password (order of image selection).

e. Grid Image Component:

This component is responsible for the appearance of the grid of images on the login/Sign-in page. At Least 1000 images of different animals each have been used as a dataset, which has been collected from Kaggle. The images are arranged in such a fashion that every time the page has refreshed the placement of those animal images is shuffled, also these images keep changing to different images of those same animals to avoid easier detection when it comes to shoulder-surfing.

These images load within a second even though there is a large quantity of dataset. According to the users' *Password image*, the grid would most definitely include the images in the *password image* while also including other random images within the grid. The passcode is used to verify the locations of the password images and a string consisting of images corresponding to the entered passcode is later used to validate the user against the *Salt + Hash* encrypted password.

f. Login Component:

The user must first input the login or email address used to log in to the specific domain. A text entry box and an image *grid* are both included in this stage. The grid contains additional random photos in addition to the pictures used as passwords. The placement of the images is random in the grid and it changes every time the login page is refreshed.

The MongoDB database retains the location of the password photos in the current grid as a string of matching image names. In continuation to the "Salt + Hash" encryption of the Select Password Component, the string Posted by the Login component is compared with the encrypted user password, which will be used to authenticate the Passcode entered by the user. Only numeric entries are accepted according to the password length determined by the user.

Taking the Harry Potter example, "Glasses ⟶ Broomstick ⟶ Dragon ⟶ Egg" - the respective positions of these images on the grid are 2, 5, 6, and 3. So, the passcode entered in the input field is "2563". Since the password length set by the user is four, only four-character entries are accepted by the entry field.

The Lock-out mechanism - The user is successfully logged in and will not be logged out for the next hour (60 minutes), post which the user must log in again. The URL of the previously used- login page does not enable the user to access the same grid that appeared prior.

g. Forgot Password/ Reset Password Component:

Both these terms signify the 'change of password'. When the user does not remember the password or has had unsuccessful login attempts, then the Forgot Password is the essential option to gain access and change the password. Whereas the Reset Password option is to ensure a frequent and timely change of password to avoid prospective security and sniffing attacks or simply ought to change it. Both these options require *User-Authentication* (Verifying the user), to proceed with the *Password Change (Reset Password).*

Authentication requires the user credentials (confirmed with registration information) and the text password supplied by the user during registration. A reset password link is issued through email to allow the user access to change his or her password after the user has verified his or her identity using the email address and text password provided by the user (at the time of registration). This reset link will direct the user to

the *Select Password component*, which allows the user to reset the password.
The *Reset password* will lead the user to the Select *Password page* where the user can set his/her desired password (as explained in the section Select Password). The user would be required to log in immediately after the reset, to test the change.

5. RESULTS

Every module was tested individually and is expected to function well and in conjunction with other modules as well. The unit testing was conducted on the following elements:

- Grid Image module
- Randomization algorithm
- Select Password Module
- Encryption outcome (Salt +Hash)
- Login module
- Compare Typed-in passcode to Encrypted password
- Forgot Password module
- Email Reset link
- Authentication implementation

The following tests were conducted on the authentication application (after deployment) to examine its security and convenience. Though convenience and memorability are parameters subject to human understanding and interpretation. Testing is necessary for the following: the transmission of credentials over an encrypted channel or medium, the use of default credentials during initial authentication, the avoidance of authentication schema, the remember password functionality, browser cache weaknesses, the security and policy surrounding passwords, the functionality for changing or resetting passwords, the login state (grid) changing upon refreshing the page, and unsuccessful login.

During the 5 sessions held, the 100 participants' data of login time, login, and forgot password attempts was recorded. The participants were asked to attempt login until they have a successful attempt, in every session.

Average Login Times

As conveyed in Fig. 9, in the initial session, the system login takes an average of 56.6 seconds and 21.4 seconds for the last session. The average time for login has reduced drastically by 30 seconds, it is due to practice and improvement in the cognitive ability of the user. Yet there was a good section of people who failed to remember their passwords in one session or another, and they resorted to changing their passwords.

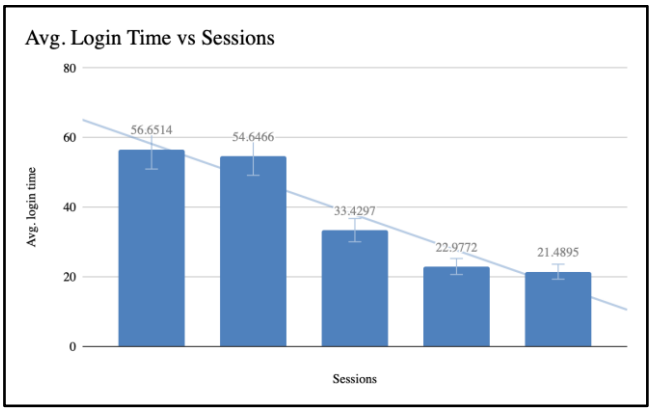

Fig. 19 AVERAGE LOGIN TIME PER SESSION

Number of Attempts for a successful login: It tests the memorability of every participant, as human retention and memory vary from individual to individual. 34 participants never entered the wrong password or chose the forgotten password option, i.e., they did not fail in any of the login attempts. 45 participants took many attempts to successfully login without choosing to change the password. They had 4.6 average unsuccessful login attempts in all the sessions.

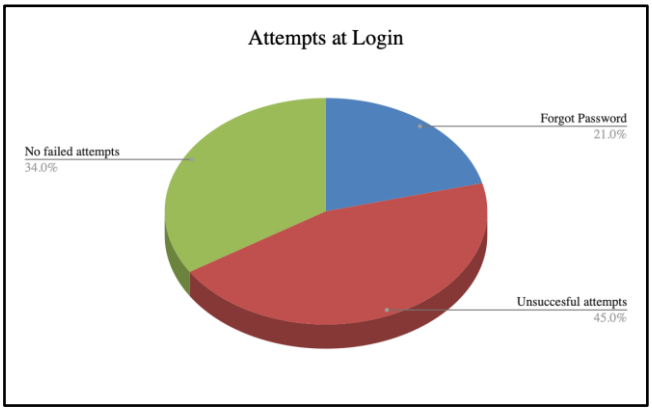

Fig. 20 ATTEMPTS AT LOGIN

Number of Forgot Password Route Users: 21 participants, after several failed attempts, resorted to choosing the forgotten password option and changing their password.

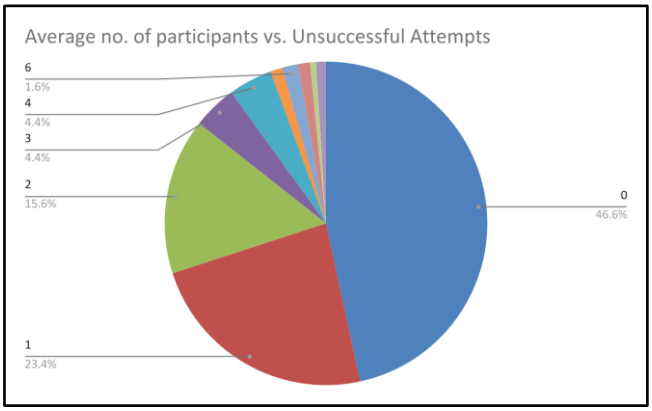

Fig. 21 UNSUCCESSFUL ATTEMPTS - WEEK 5

As depicted in the above figure, 46.6% of participants had zero unsuccessful attempts on average in all five sessions. Participants with 6 and more attempts were negligible, also those with 9 unsuccessful attempts in a session were directed to reset their passwords.

A. Password Space

The proposed system is protected against brute-force and shoulder-surfing attacks. Nine unsuccessful attempts triggered the verification procedure to reset the password. In an attempt with 9 objects on the grid, at random positions, while considering the password length *'L'* with a range of four to twenty (4 - 20), our proposed system has a large password space calculated as follows in (1):

TOTAL NO. OF PASSWORDS =

$$\sum_{L=4}^{20} 9^L = 13677373641439044000 = 13.67 * 10^{18} \quad (1)$$

B. Resistance against accidental logins

The probability of getting a password object correct in an attempt is one-ninth (1/9). The success probability of an accidental login in an attempt is (P_{AL}), having password length '*L*', is calculated as follows in (2):

$$P_{AL(L)} = [1/9]^L \quad (2)$$

C. Resistant against Brute-force and Shoulder-surfing attacks

The proposed GPA system is resistant to several security attacks including brute force and shoulder-surfing. Due to the randomization, the arrangement of the images within the grid changes with every attempt, decreasing the possibility of shoulder surfing and the password length will not be shown, hence misdirecting the attacker to prevent brute-force and dictionary attacks. Hints are absent in this GPA system. These features enhance the security strength, making the password highly unpredictable.

The comparison of password lengths cannot be made between our proposed GPA system and other existing textual authentication systems or GPA systems that use ASCII characters, since the text is their premise for authentication whereas ours is purely dependent on images and their arrangement.

Let the probability of an object being placed in any position of the password SOO (sequence of objects) be denoted by P(o) which can be calculated as follows in equations (3) and (4):

$$P(o) = \frac{1}{Total\ no.of\ Object\ images} \quad (3)$$

$$P(o) = \frac{1}{9} \quad (4)$$

6. LIMITATIONS

6.1 Higher Login Times

This GPA system takes longer to login than any textual authentication system. This is because after using the text password for a long time, it becomes muscle memory as it is easier to login. Whereas in the proposed system, though the password SOO remains the same, recognition of images is necessary and hence it is a time taking task.

6.2 Smaller Object Database

The proposed system utilizes the images of only 9 objects, each having a dataset of 1000 images. It does provide the user with a greater choice; it might be prone to dictionary attacks but offering a larger choice will mitigate this risk.

6.3 Limitation of Grid Size

More than 9 images per grid itself is an extensive job. Whereas a 6*6 or 10*10 grid is not possible as associating it with numbers would become a difficult task and will increase the effort and time required for login. It will also negatively impact the content delivery speed (faster access and more image).

7. CONCLUSION

Many authentication techniques exist that follow the context of GPA, but very few of them satisfy all the criteria/parameters such as security, memorability, password space, and usability, to produce a fool-proof authentication system. Security would entail protection against several kinds of attacks namely social-engineering, guessing, brute-force, dictionary attacks, and most importantly shoulder-surfing [19],[26]. Since, resistance to shoulder-surfing and screen mirroring or capture is crucial in any ideal GPA system, as observed in Section 2. Both Pass faces and CCP have considerably better performance compared to other techniques. We require a GPA system that prevents and resists security breaches, while fulfilling all the parameters mentioned above, which our proposed system meets.

The proposed system provides an intuitive login interface. It minimizes password sharing. It eliminates shoulder surfing since it is a GPA system with a textual input provision. The usage of objects as a medium seems to increase password memorability. It is recommended to login to the system at least four or five times to become comfortable with the procedure and it helps with the memorability of the password. As suggested earlier, creating a *story*, though not essential, boosts the memorability of any password for any system, reduces the possibility of forgetting the password and the need to periodically change passwords. After testing, it was also found to be error-free, efficient, convenient and reliable.

8. FUTURE SCOPE

This authentication scheme can be further developed, an API can be made. The number of objects offered for password creation can be increased for the sake of avoiding dictionary attacks, and also provide the user with greater choice.

REFERENCES

1. Bhanushali, A., Mange, B., Vyas, H., Bhanushali, H., & Bhogle, P. (2015). Comparison of graphical password authentication techniques. International Journal of Computer Applications, 116(1). https://doi.org/10.5120/20299-2332
2. Gokhale, M. A. S., & Waghmare, V. S. (2016). The shoulder surfing resistant graphical password authentication technique. Procedia Computer Science, 79, 490-498. https://doi.org/10.1016/j.procs.2016.03.091
3. Gyorffy, J. C., Tappenden, A. F., & Miller, J. (2011). Token-based graphical password authentication. International Journal of Information Security, 10(6), 321-336. https://doi.org/10.1007/s10207-011-0147-0
4. Towhidi, F., Masrom, M., & Manaf, A. A. (2010). An enhancement on Passface graphical password authentication (Doctoral dissertation, Universiti Teknologi Malaysia). http://eprints.utm.my/40517/
5. Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A., & Memon, N. (2005). PassPoints: Design and longitudinal evaluation of a graphical password system. International journal of human-computer studies, 63(1-2), 102-127. https://doi.org/10.1016/j.ijhcs.2005.04.010
6. Chiasson, S., Van Oorschot, P. C., & Biddle, R. (2007, September). Graphical password authentication using cued click points. In European Symposium on Research in Computer Security (pp. 359-374). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-74835-9_24
7. Stobert, E., & Biddle, R. (2013, July). Memory retrieval and graphical passwords. In Proceedings of the ninth symposium on usable privacy and security (pp. 1-14). https://doi.org/10.1145/2501604.2501619
8. Sarohi, H. K., & Khan, F. U. (2013). Graphical password authentication schemes: current status and key issues. International Journal of Computer Science Issues (IJCSI), 10(2 Part 1), 437. https://www.semanticscholar.org/paper/Graphical-Password-Authentication-Schemes%3A-Current-Kumar-Khan/9b0420ee4179c5b64989a9816ae50d0da60974cc
9. Bhand, A., Desale, V., Shirke, S., & Shirke, S. P. (2015, December). Enhancement of password authentication system using graphical images. In 2015 International Conference on Information Processing (ICIP) (pp. 217-219). IEEE. https://doi.org/10.1109/infop.2015.7489381
10. Lashkari, A. H., Farmand, S., Zakaria, D., Bin, O., & Saleh, D. (2009). Shoulder surfing attack in graphical password authentication. arXiv preprint arXiv:0912.0951. https://arxiv.org/pdf/0912.0951#:~:text=An%20attacker%20can%20capture%20a,when%20authenticating%20in%20public%20places.
11. Yang, G. C. (2019). Development status and prospects of graphical password authentication system in Korea. KSII Transactions on Internet and Information Systems (TIIS), 13(11), 5755-5772. https://doi.org/10.3837/tiis.2019.11.026
12. Almulhem, A. (2011, February). A graphical password authentication system. In 2011 world congress on internet security (WorldCIS-2011) (pp. 223-225). IEEE. https://doi.org/10.1109/worldcis17046.2011.5749855
13. Gurav, S. M., Gawade, L. S., Rane, P. K., & Khochare, N. R. (2014, January). Graphical password authentication: Cloud securing scheme. In 2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies (pp. 479-483). IEEE. https://doi.org/10.1109/icesc.2014.90
14. Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A., & Memon, N. (2005, July). Authentication using graphical passwords: Effects of tolerance and image choice. In Proceedings of the 2005 symposium on Usable privacy and security (pp. 1-12). https://doi.org/10.1145/1073001.1073002
15. Assal, H., Imran, A., & Chiasson, S. (2018). An exploration of graphical password authentication for children. International Journal of Child-Computer Interaction, 18, 37-46. https://doi.org/10.1016/j.ijcci.2018.06.003
16. Jermyn, I., Mayer, A., Monrose, F., Reiter, M. K., & Rubin, A. (1999). The design and analysis of graphical passwords. In *8th USENIX Security Symposium (USENIX Security 99)*. https://www.usenix.org/conference/8th-usenix-security-symposium/design-and-analysis-graphical-passwords
17. Zhao, H., & Li, X. (2007, May). S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme. In 21st international conference on advanced information networking and applications workshops (AINAW'07) (Vol. 2, pp. 467-472). IEEE. https://doi.org/10.1109/ainaw.2007.317
18. Davis, D., Monrose, F., & Reiter, M. K. (2004, August). On user choice in graphical password schemes. In USENIX security symposium (Vol. 13, No. 2004, pp. 11-11). https://users.ece.cmu.edu/~reiter/papers/2004/usenix2.pdf
19. Nali, D., & Thorpe, J. (2004). Analyzing user choice in graphical passwords. *School of Computer Science, Carleton University, Tech. Rep. TR-04-01*. https://carleton.ca/scs/wp-content/uploads/TR-04-01.pdf
20. Blonder, G. (1995). *Graphical Password* (U.S. Patent No. US08/520,904). U.S. Patent and Trademark Office. https://rb.gy/ik0fb0
21. Thorpe, J., & Van Oorschot, P. C. (2004, December). Towards secure design choices for implementing graphical passwords. In *20th Annual Computer Security Applications Conference* (pp. 50-60). IEEE. https://doi.org/10.1109/CSAC.2004.44
22. Dhamija, R., & Perrig, A. (2000). Deja {Vu--A} User Study: Using Images for Authentication. In *9th USENIX Security Symposium (USENIX Security 00)*. https://users.ece.cmu.edu/~adrian/projects/usenix2000/usenix.pdf
23. Sobrado, L., & Birget, J. C. (2002). Graphical passwords. *The Rutger Scholar*, *4*. https://rutgersscholar.libraries.rutgers.edu/index.php/scholar/article/view/60
24. ArunPrakash, M., & Gokul, T. R. (2011, February). Network security-overcome password hacking through graphical password authentication. In 2011 National Conference on Innovations in Emerging Technology (pp. 43-48). IEEE. https://doi.org/10.1109/ncoiet.2011.5738831
25. Moraskar, V., Jai Kalyani, S., Saiyyed, M., Gurnani, J., & Pendke, K. (2014). Cued click point technique for graphical password authentication. International Journal of Computer Science and Mobile Computing, 3(1), 166-172. https://ijcsmc.com/docs/papers/January2014/V3I1201431.pdf
26. Wiedenbeck, S., Waters, J., Sobrado, L., & Birget, J. C. (2006, May). Design and evaluation of a shoulder-surfing resistant graphical password scheme. In Proceedings of the working conference on Advanced visual interfaces (pp. 177-184) https://doi.org/10.1145/1133265.1133303
27. Kausar N, Din IU, Khan MA, Almogren A, Kim BS. GRA-PIN: A Graphical and PIN-Based Hybrid Authentication Approach for Smart Devices. Sensors (Basel). 2022 Feb 10;22(4):1349. https://doi.org/10.3390/s22041349
28. Gao, H., Liu, N., Li, K., & Qiu, J. (2013, November). Usability and security of the recall-based graphical password schemes. In *2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing* (pp. 2237-2244). IEEE. https://doi.org/10.1109/hpcc.and.euc.2013.321
29. Lashkari, A. H., Saleh, R., Towhidi, F., & Farmand, S. (2009, December). A complete comparison on pure and cued recall-based graphical user authentication algorithms. In *2009 Second International Conference on Computer and Electrical Engineering* (Vol. 1, pp. 527-532). IEEE. https://doi.org/10.1109/iccee.2009.81
30. Sun, H. M., Chen, S. T., Yeh, J. H., & Cheng, C. Y. (2016). A shoulder surfing resistant graphical authentication system. *IEEE Transactions on Dependable and Secure Computing*, *15*(2), 180-193, https://doi.org/10.1109/TDSC.2016.2539942
31. Y. Zhu, G. Owen and X. Suo, "Graphical Passwords: A Survey," in Computer Security Applications Conference, Annual, Tucson, Arizona, 2005 pp. 463-472. https://doi.org/10.1109/csac.2005.27
32. G. Wei, W. Hu and X. Wu, "The Security Analysis of Graphical Passwords," in Communications and Intelligence Information Security, International Conference on, Nanning, Guangxi Province, China, 2010 pp. 200-203, https://doi.org/10.1109/icciis.2010.35
33. A. Kayem, "Graphical Passwords -- A Discussion," in 2016 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA), Crans-Montana, Switzerland, 2016 pp. 596-600, https://doi.org/10.1109/WAINA.2016.31
34. Wu, T. S., Lee, M. L., Lin, H. Y., & Wang, C. Y. (2014). Shoulder-surfing-proof graphical password authentication scheme. International journal of information security, 13(3), 245-254, https://doi.org/10.1007/s10207-013-0216-7
35. Al-Ameen, M. N., Marne, S. T., Fatema, K., Wright, M., & Scielzo, S. (2022). On improving the memorability of system-assigned recognition-

based passwords. Behaviour & Information Technology, 41(5), 1115-1131. https://doi.org/10.1080/0144929x.2020.1858161

36. Rodriguez, J. J., Zibran, M. F., & Eishita, F. Z. (2022, May). Finding the middle ground: measuring passwords for security and memorability. In 2022 IEEE/ACIS 20th International Conference on Software Engineering Research, Management and Applications (SERA) (pp. 77-82). IEEE. https://doi.org/10.1109/sera54885.2022.9806772
37. Nizamani, S. Z., Hassan, S. R., Shaikh, R. A., Abozinadah, E. A., & Mehmood, R. (2021). A novel hybrid textual-graphical authentication scheme with better security, memorability, and usability. IEEE Access, 9, 51294-51312, https://doi.org/10.1109/access.2021.3069164

AUTHORS

U. P. Prashasthi Sagar received her BTech degree in Computer Science and Engineering from Sharda University, Uttar Pradesh, in 2023.

Corresponding author Email: prashasthisagar@gmail.com

U. P. Pravardha Sagar received his BTech degree in Computer Science and Engineering from Sharda University, Uttar Pradesh, in 2023.

Email: pravardha.u@gmail.com

Preeti Dubey is currently working as an Assistant Professor in Department of Computer Science and Engineering at Sharda University, Greater Noida, U.P. India. She has also worked as Programmer Analyst in Cognizant Technology Solution, Pune. She is currently working in the field of Machine Learning and Cyber Security. She has 9 years of academic experience and 2 years of Industry experience.

Email: preetidubey19dec@gmail.com