DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING,
SHARDA SCHOOL OF ENGINEERING AND TECHNOLOGY,
SHARDA UNIVERSITY, GREATER NOIDA

IMAGE-BASED OBJECT-SEQUENCED GRAPHICAL PASSWORD AUTHENTICATION SYSTEM

A project submitted
in partial fulfilment of the requirements for the degree of
Bachelor of Technology in Computer Science and Engineering

by

U. P. PRASHASTHI SAGAR (2019006396)

U. P. PRAVARDHA SAGAR (2019006399)

Supervised by:

MS. PREETI DUBEY, ASST. PROFESSOR (CSE)

May 2023

CERTIFICATE

This is to certify that the report entitled **"IMAGE-BASED OBJECT-SEQUENCED GRAPHICAL PASSWORD AUTHENTICATION SYSTEM"** submitted by MS U.P.PRASHASTHI SAGAR (2019006396) and MR U.P.PRAVARDHA SAGAR (2019006399) to Sharda University, towards the fulfilment of requirements of the degree of Bachelor of Technology is the record of bonafide final year Project work carried out by him/her in the Department of Computer Science and Engineering, School of Engineering and Technology, Sharda University.

The results/findings contained in this Project have not been submitted in part or whole to any other University/Institute for the award of any other Degree/Diploma.

Signature of Supervisor

Name: Ms Preeti Dubey

Designation: Asst. Professor, CSE Dept.

Signature of Head of Department

Name: Prof. (Dr.) Nitin Rakesh

(Office seal)

Place: Sharda University

Date:

Signature of External Examiner

Date:

ACKNOWLEDGEMENT

A major project is a golden opportunity for learning and self-development. We consider ourselves very lucky and honoured to have so many wonderful people lead us through completing this project.

First and foremost we would like to thank Dr. Nitin Rakesh, HOD, CSE who gave us an opportunity to undertake this project.

My grateful thanks to Ms. Preeti Dubey for her guidance in our project work. Ms. Preeti Dubey, who in spite of being extraordinarily busy with academics, took time out to hear, guide and keep us on the correct path. We do not know where we would have been without his help.

The CSE department monitored our progress and arranged all facilities to make life easier. We choose this moment to acknowledge their contribution gratefully.

Name and signature of Students

U.P.PRASHASTHI SAGAR (2019006396)

U.P.PRAVARDHA SAGAR (2019006399)

ABSTRACT

In the current scenario, everyone is highly reliant on technology in numerous ways, such that their everyday chores are not complete without technological intervention, logically so due to modernization and advancements in technology. There are software systems available for every venture that the users require and utilise, which needs a proper mechanism to validate the users' identity for security purposes. The key terms associated with 'security' are confidentiality, integrity and authentication. And in the present age of cyber security, due to great developments in the field of computer science, authentication plays a key role in data security. Authentication is a process to validate the user's credentials in order to provide access to the system only with use of passwords, which preferably must be unique or distinct and confidential to the user only. There are several kinds of authentication systems categorised on the basis of the type of passwords used.

Graphical passwords are cognition dependent, these employ the images of objects, people, sceneries, etc. These are image based authentication means that are not as burdensome on the users' memorability as the text-based passwords. Not as rigid as the biometric-based passwords, since an individual's physical features can hardly be duplicated. Graphical passwords can improve ease-of -use (usability), reduce password space as well, but only with much research and development of improved GPA systems. Our review for this project provides a detailed study of graphical passwords, existing GPA techniques and relevant advancements in the domain of authentication systems pertaining to improved security of the system, also the users' convenience.

In this project, we have reviewed several systems and 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. Our objective for inventing a new authentication scheme is, to provide a reliable Graphical password authentication alternative with an easy-to-use, easy-to-memorise 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.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

Security is one of the most significant necessities in the current progressing society. Security implies reliability, safety, protection of privacy and business of any kind. Authentication is the process of asserting one's identity to access the user's information, accounts, and business (of any kind); medium to procure efficient security to the user's accounts, hence providing the user with privacy. Password authentication also known as Knowledge-based authentication is the most frequently used Authentication method. The most commonly used passwords are text-based. Graphical-based passwords along with Text-based passwords come under the category of Knowledge-based authentication as the password needs to be created/chosen and remembered by the user. Strong security requires lengthy and complicated passwords, but such alpha-numeric (text) are extremely hard to remember and inconvenient. Graphical passwords mainly require icons/ objects to prepare a password.

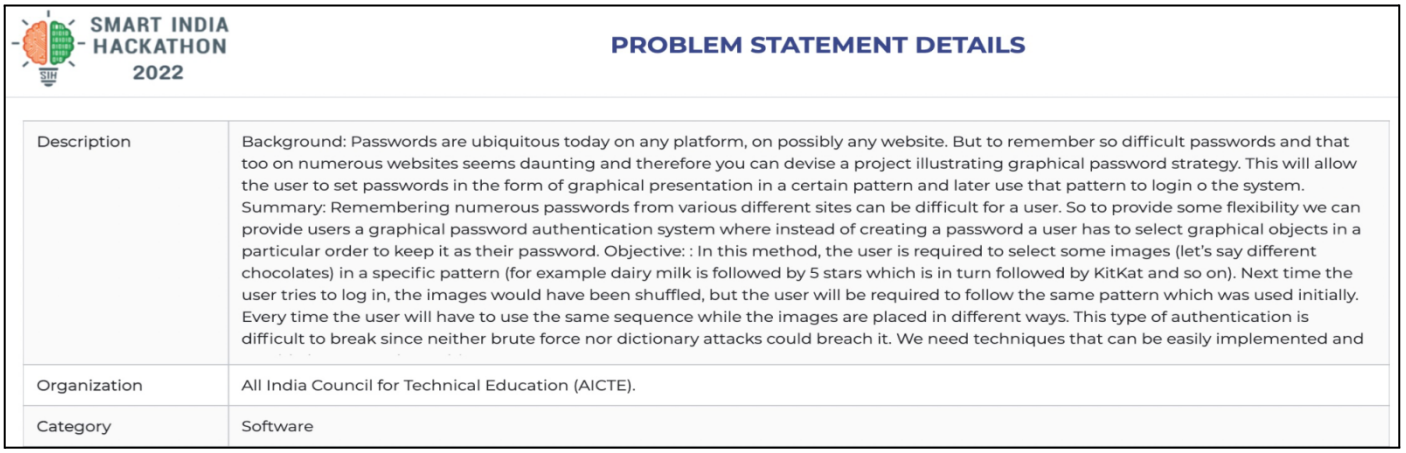
This mode of authentication is also prone to security attacks such as shoulder-surfing, etc,. Nevertheless, the graphical passwords are difficult to hack, easy to memorise and improve one's cognitive abilities unlike the text-based passwords.

Our proposed system shall be a combination of both graphical and text-based passwords but it is predominantly a Graphical Authentication System. Proposed GPA scheme is a hybrid comprising both Recognition and Cued-recall based schemes.

The aim of the research is to propose a Graphical Password Authentication System with a better password entropy, security from various kinds of attacks and most importantly improve the ease of usability.

1.1. Problem Statement

Passwords are ubiquitous today on any platform, on possibly any website. But to remember so difficult passwords and that too on numerous websites seems daunting and therefore you can devise a project illustrating graphical password strategy. This will allow the user to set passwords in the form of graphical presentation in a certain pattern and later use that pattern to login to the system. This type of authentication is difficult to break since neither brute force nor dictionary attacks could breach it. We need techniques that can be easily implemented and provide better results to this process.



SMART INDIA HACKATHON 2022

PROBLEM STATEMENT DETAILS

Description	Background: Passwords are ubiquitous today on any platform, on possibly any website. But to remember so difficult passwords and that too on numerous websites seems daunting and therefore you can devise a project illustrating graphical password strategy. This will allow the user to set passwords in the form of graphical presentation in a certain pattern and later use that pattern to login o the system. Summary: Remembering numerous passwords from various different sites can be difficult for a user. So to provide some flexibility we can provide users a graphical password authentication system where instead of creating a password a user has to select graphical objects in a particular order to keep it as their password. Objective: : In this method, the user is required to select some images (let's say different chocolates) in a specific pattern (for example dairy milk is followed by 5 stars which is in turn followed by KitKat and so on). Next time the user tries to log in, the images would have been shuffled, but the user will be required to follow the same pattern which was used initially. Every time the user will have to use the same sequence while the images are placed in different ways. This type of authentication is difficult to break since neither brute force nor dictionary attacks could breach it. We need techniques that can be easily implemented and
Organization	All India Council for Technical Education (AICTE).
Category	Software

1.2. Motivation

Cyber security has been a modern day necessity for a safe and secure interaction and Authentication through alphanumeric passwords, restrict our ability to easily access. But to remember so difficult passwords and that too on numerous websites seems daunting and therefore you can devise a project illustrating graphical password strategy. We need techniques that can be easily implemented and provide better results to this process. Further, we found the idea for Graphical Password Authentication from SIH.gov.in, it was listed in the problem statement for the Hackathon.

1.3. Hardware and Software Requirements

1.3.1. Hardware Requirements

- Desktop or Mobile device with a minimum of 2 GB of RAM
- Internet Connection with 900 Kbps - broadband speed.

1.3.2. Software Requirements:

- Latest version of Web browser with HTML 3.0 & JavaScript support.
- Visual Studio Code, MongoDB, Node.js as IDE and runtime environments.

1.4. Non-Functional Requirements

1.4.1. Performance:

Even though faster operational speeds depend on Internet speeds, the application design will also be responsible for the performance of the application.

- It has to load within Industry Standard time (3-4) seconds.
- It has to support Multiple concurrent Users.
- It has to verify the database in a short period of time.

1.4.2. Security:

- The storage of the password should be stored in an encrypted format.
- The Request and response should be encrypted.

1.4.3. Usability:

- Easy Navigations with intuitive steps.
- Images Visible and sharp to detect objects, with the object as a clear foreground without any ambiguities.

1.5. Compatibility Requirements

As it is an Internet Application, it has to support various Hardware configurations, Softwares and Network Communications. It should support all types of Hardware versions, Operating Systems and Browsers.

i. *Operating Systems* -

1. Windows 98 and upper Versions (EX: Win98, windows 2000 prof, XP Vista and win NT Server,windows 2000 server, 2003 server and windows 2008 server)
2. Unix and all Unix flavors like LINUX, Solaris etc..
3. Novell netware

ii. *Browsers* - Google Chrome, Mozilla Firefox, AOL, Netscape Navigator.

iii. *Hardware* - All smart devices and computers.

2. LITERATURE SURVEY

2.1. AUTHENTICATION AND ITS TYPES

As mentioned above, Authentication is a security procedure to verify the identity of the user in order 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.

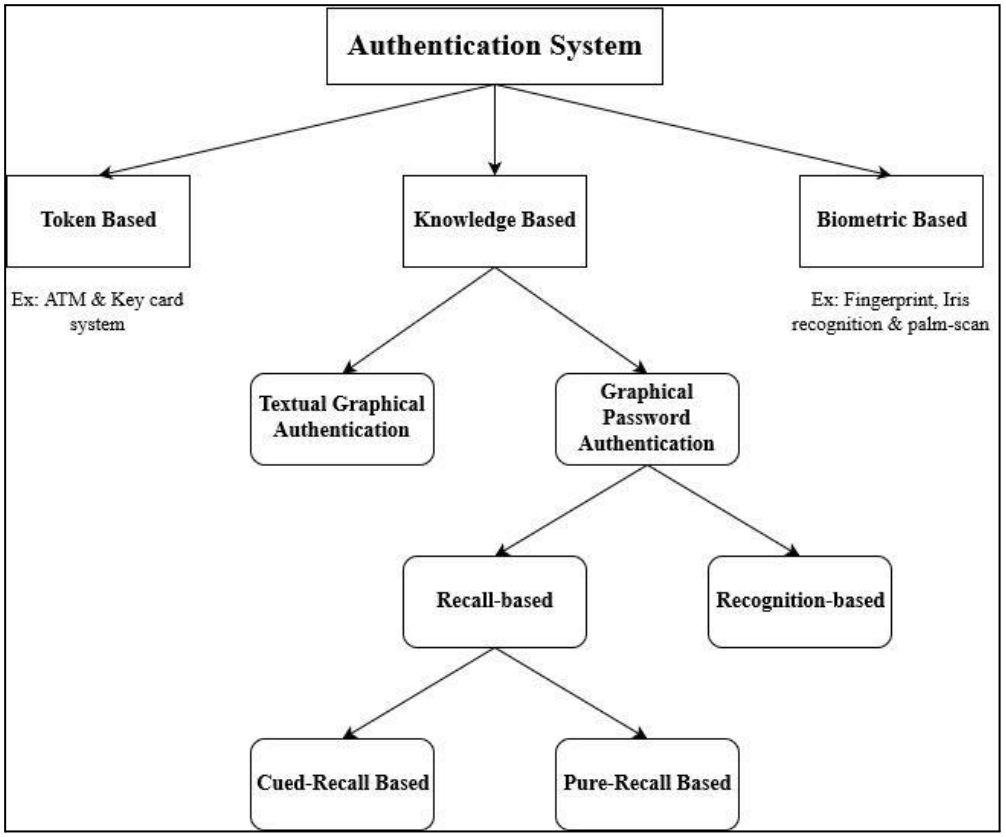


Fig 1. Authentication and its types

Three basic categories of Authentication systems have been recognised :

A. TOKEN-BASED AUTHENTICATION SYSTEM (TBAS)

It requires a physical token/entity to act as a password, like a student ID card or a resident registration card- these contain an unique identification for every user.. The drawback of a token-based authentication system is that a key-like object needs to be

carried about. For example, ATM cards, SIM cards, RFID tags, Bar code, etc [1],[2],[3],[4].

B. Biometric-Based Authentication System (BBAS)

It conducts the authentication after identifying the user's physical features, such as a fingerprint, an iris, or a face. Because a biometric authentication system uses a physical attribute of the user's body as a password, it is challenging to steal such a password, since these attributes cannot be possessed by any two individuals (even in the case of identical twins). The user cannot alter their password and cannot access the system if it is stolen, and it requires separate, expensive equipment for biometrics recognition. These systems must be sensitively handled during construction, operation and maintenance, since inefficient, or faulty systems provide unreliable results. The BBAS system can be classified into two types based on physical contact [1],[4].

1) Requiring physical contact: such as the finger-print scan, palm-scan, etc.,

2) Lacking physical contact: such as iris recognition, facial recognition, etc.,

C. Knowledge-Based Authentication System (KBAS):

This system is dependent on the user's memorability and cognitive abilities. Oftentimes, the password is rather chosen by the user and not assigned by the system [4]. These passwords need to be simple for the user to remember and challenging for the attackers to decipher. There are two kinds of KBAS systems-

***1) Textual Password Authentication System*:** Uses 'alpha-numeric' sequences as passwords. The lengthier the password ensures higher security, but it is often difficult for the user to memorise. But if it is to the users' convenience, then they are short enough to guess.

2) Graphical password Authentication System: It requires the user to choose from shown images in a certain order via a graphical user interface (GUI), hence the use of images of shapes, objects, sceneries, etc.. This system is based on the observation that images are easier to recall than words or numbers [5].

2.2. GRAPHICAL PASSWORD AUTHENTICATION

Both the text-based (alpha-numeric) passwords and graphical passwords come under the category of Knowledge-based password schemes in Authentication. The text-based passwords usually have a low password entropy i.e. the measure of the security of a selected password, require 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.

There are three distinct categories that can be used to categorize graphical password systems:

A. RECOGNITION BASED PASSWORDS

It is a cogno-metric system. A mechanism for enumerating various pieces of information and allowing the user to select the correct password information, in order to be authenticated. For example, PassFaces will display a variety of faces [6]. Users are authenticated only after selecting the correct predetermined face within the allotted number of attempts. With this method, it takes time to enter the password, and various problems may arise, such as communication costs of photo data required for system construction and operation [7],[8]. For example, Jensen's method, Passfaces, Sobrado & Birget method, Hong's method, Deja vu, etc.,

B. RECALL BASED PASSWORDS

It handles validation by comparing input patterns with a stored pattern. This process is comparable to a text-based password system. However, the user has to remember the password without any hint. As a result, long passwords cannot be easily used by users against a callback-based graphical password system. The callback-based graphical password system is therefore very weak against dictionary attacks. For example, Draw-a-secret, Blonder's scheme, v-Go, visKey, Cued Click Points, Passpoints [8].

1) PURE RECALL BASED GPA:

In this system, the user has to reproduce the password without any hints provided by the system. It is a draw metric system. For example, DAS, Grid selection, etc. are pure-recall based techniques.

2) CUED-RECALL BASED GPA:

It is a loco-metric system. It receives a password pattern that uses a background image or other useful information. The burden of remembering on the user is less than with a simple prompt-based password system. For example, [9] refers to a system that grants authentication after the user clicks on predefined points in a certain image in a specified order. Such a system has advantages, such as fast password entry and less load on the user's memory. However, the downside is the hotspot issue and the requirement to click the correct dots [10]. For example, Cued Click Points.

C. HYBRID GPA SYSTEM

A system that uses several types of graphical password techniques together. When creating a new hybrid graphical password system, it is important to think about the interaction and to maximize the effectiveness of the final system [11],[27].

Basically, there are three categories of Authentication: Recognition-based, Recall-based, and Cued-Recall authentication. There are several GPA schemes under these categories. 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.

Graphical passwords have already been proven to have better password entropy and larger password size than text-based passwords. Graphical Passwords can be created using a picture of the user's choice, a drawing, pass points, cued-click, blonder'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, increase usability via reducing login time and at most privacy.

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 the forgotten passwords etc., that determine the ease in usability and performance are the implementation problems of Graphical Password Authentication system.

TABLE I
LITERATURE REVIEW OF RESEARCH AND REVIEW OF BASE PAPERS

S. No.	***Title***	***Author***	***Year***	***Approach***	***Parameter***	***Merit***	***Demerit***
01.	A Graphical Password Authentication System	*Almulhem et al.*	2011	Intends to: Obtain a picture of user's choice; Selects POIs (Point of Interest) regions from it; Provide corresponding words to each POI, Record the order of POI selection.	Picture of choice; The number & order of POIs in a picture; & the corresponding word for POI.	1. Combination of Graphical & Text-based authentication. 2. Multi-factor authentication(POI order, POI number, graphical & text)	1. Shoulder - surfing is possible; 2. These passwords would usually be pictures of loved & familiar ones, hence, user's kin & acquaintances can easily discover the potential password
02.	An Exploration of Graphical Password Authentication for Children	*Assal et al.*	2018	Uses three PassTiles schemes: Objects, images & words PassTiles to build a child oriented authentication system.	For the comparative study between children & adults memorization time, login times & successes (first & second attempt), degree of correctness, interview results	1. It is a Child-oriented system; 2. Comparative study of child & adult cognitive & memorization abilities; 3. Claims fairy tales as an effective password memorisation method	1. It doesn't take Shoulder surfing into account; 2. Doesn't explain adult responsibility in a child-oriented system.
03.	Enhancement of Password Authentication System Using Graphical Images	*Bhand et al.*	2015	Cued Click Point system with enhanced mobile alert systems on possible security threats	CCP registration, elected image, storage of the CCP order, authentication.	1. This kind of GPA is harder to hack; 2. Uses a single picture, hence, requires limited storage.	1. Harder to memorise; 2. Shoulder-Surfing is possible;
04.	Comparison of Graphical Password Authentic-ation Techniqu-es	*Bhanushali et al.*	2015	Distinguishes all the GPA Techniques	Here, Security & usability are the parameters	1. It considers all GPA techniques; 2. It considers all Security attacks; 3. Tests all usability parameters	-

S. No.	*Title*	*Author*	*Year*	*Approach*	*Parameter*	*Merit*	*Demerit*
05.	Graphical Password Authentication Using Cued Click Points	*Chiasson et al.*	2007	Proposes Cued Click Point system, as a combination of PassPoints, Passfaces & Story	Security, usability, speed, accuracy & no. of errors.	1. Shows comparison between CCP & PassPoints based on users preference & mentioned parameters; 2. CCP is highly preferred as it provides improved security & usability	1. Hotspot identification is a problem
06.	The Shoulder Surfing Resistant Graphical Password Authentication Technique	*Gokhale et al.*	2016	Proposes a system with a combination of recall & recognition based approach	Security against brute force & shoulder surfing, usability, & accuracy	1. Claims Shoulder-surfing resistance; 2. Easily usable & secure than the usual GPA; 3. Passwords are easily created & memorised; 4. Uses Randomisation during authentication	1. Not easily accessible; 2. Difficult to change password when forgotten.
07.	Graphical Password Authentication	*Gurav et al.*	2014	Proposes Cloud with GPA security. Username with selection of images as password.	Security, speed & memorisation ability.	1. Very strong authentication process; 2. Easy remembrance of username & password;	1. Can be accessed by anyone when the sequence of username is known; 2. Shoulder-surfing is possible
08.	Token based graphical password authentication	*Gyorffy et al.*	2011	GPA system with image hashing & input from a crypto-system; Graphical password deployed from Trojan & Virus resistant embedded device	Image data size, hash storage, security, & usability	1. Shows GPA also have low entropy causes, but seem easy to memorise unlike text passwords; 2. Prevents brute force, replay & implementation attacks;	1. Uses Token & graphical based authentication while having a 2 step authentication process with AES encryption key; 2. Requires large memory space; 3. Requises external USB device to store hash values.
09.	Shoulder Surfing attack in graphical password authentic-ation	*Lashkari et al.*	2009	Survey on papers proposing GPA with shoulder-surfing resistance from 2005-2009	Security mainly from shoulder-surfi ng attack & integration of different types of authentication.	Provides comparison on various Shoulder-surfing resistant methods.	1. Only focused on Shoulder-surfing attacks as a security threat; 2. It does not help solve GPA problems.

S. No.	*Title*	*Author*	*Year*	*Approach*	*Parameter*	*Merit*	*Demerit*
10.	Cued Click Point Technique for Graphical Password...	*Moraskar et al.*	2014	Proposes a CCP GPA system supporting better password selection & expanding effective password space.	Click points, hotspot, security, usability & memorization.	1. CCP has better security than other GPA methods; 2. Security using hotspot technique; 3. Hacking is tougher in this mechanism; 4. Memorable authentication mechanism;	1. Shoulder- surfing is still possible; 2. Hotspots are still a problem;
11.	Network Security-Overcome Password Hacking Through Graphical Password Authentic-ation	*Prakash et al.*	2011	Comprehensive survey on several GPA schemes & proposes a new system by distorting the image with grey level concentration.	image quality, image encryption, security & memorisation.	1. Difficult to hack; 2. Offers solutions for shoulder-surfing attacks;	1. Though the original image is unavailable, it can be restored by the hacker through ultimate efforts; 2. Requires large storage space; 3. Does not offer a fool-proof solution to shoulder surfing;
12.	Graphical Password Authentication Schemes: Current Status & Key Issues	*Sarohi et al.*	2013	Comparative study of GPA techniques & various security parameters.	Usability & Security(Social engineering, shoulder-surfing, brute force, spyware attack & guessing)	Offers comparison of various GPA techniques based on said parameters.	Does not offer solutions to security issues.
13.	An Enhancement on Passface Graphical Password Authentic-ation	*Towhidi et al.*	2010	Proposes Secure-Passface algorithm to choose password at login phase. Concept of Alternative password is introduced; Compares Passface & new S-Passface algorithms;	Usability & Security(Social engineering, shoulder-surfing, brute force, spyware attack & guessing)	1. Easy to use, memorise, recognise & understand; 2. Increases security by creating resistance to shoulder-surfing. 3. Easier to create a password rather than selecting one.	1. Increase in security of S-Passface reduces its usability; 2. Attackers can guess the S-Passface password more precisely compared to the original Passface algorithm; 3. Omits the use of mouse;
14.	Shoulder-surfing proof graphical password authentic-ation scheme	*Wu et al.*	2014	Introduces Convex hull algorithm for Shoulder-Surfing-Prevention(SSP) of Graphical Password Authentication(GPA) using dynamic colour balls	Security, password space, usability, process time & memorability.	1. Improves shoulder-surfing resistance by adding dynamic colour ball movement; 2. Applies "DC" Double-Confusion technique to confuses the attacker's sight;	1. The proposed is inconvenient in terms of user acceptability & usability;

S. No.	*Title*	*Author*	*Year*	*Approach*	*Parameter*	*Merit*	*Demerit*
15.	Development Status & Prospects of Graphical Password Authentic-ation System in Korea	*Yang et al.*	2019	Surveys research & development of GPA systems in Korea; Benefits & drawbacks of several known GPA methods along with their characteristics;	Based on type of security provision & type of GPA(Recognition-based, cue-based, cued-recall & hybrid); Memorability, Login time & Usability.	Provides extensive comparison on the basis of the mentioned parameters.	Hybrid GPA system is not considered for comparison here; No new ideas are proposed to increase security & usability.
16.	S3PAS:A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme	*Zhao et al.*	2007	S3PAS is basically a system built to offer highest resistance from shoulder surfing; it integrates both the text-based & GPA schemes while also proposing three enhancement schemes (namely: Three-set, Rule-Based & Enhanced Graphical Scheme).	Security, usability, password space, enhancement of S3PAS (to improve its capability & security)	1. Almost perfect level of security; 2. Can help replace or coexist with conventional textual password systems without changing existing user password profiles.	1. More complicated & longer login process; 2. Ease of usability & adoption is quite low; 3. Hence, the above reason would require the new version of S3PAS to compromise a little on security.

2.3. Pre-existing Approaches and Techniques

This project determines these two main questions based on a previous extensive literature survey and suggests an all-inclusive solution supporting cross-examination. The survey also focuses on the several approaches (on GPA system) of the researchers, that mainly include the following:

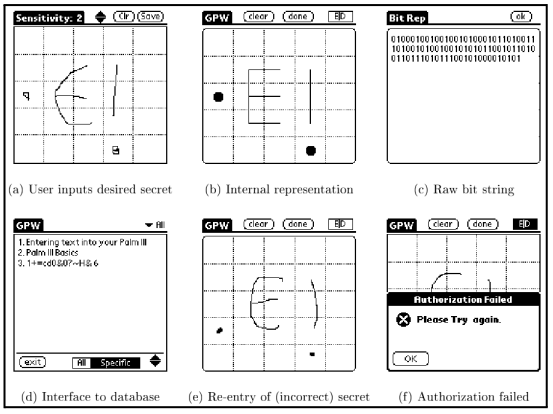


Fig. 2.1 Draw-A-Secret [16]

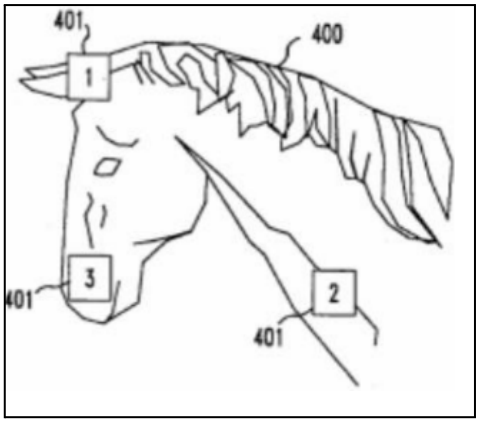


Fig. 2.2 Blonder's Scheme [20]

Fig. 2.3 PassPoint

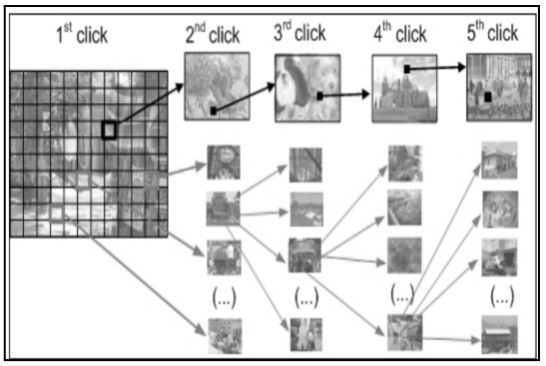


Fig. 2.4 Cued-click Points

Fig. 2.5 Passfaces

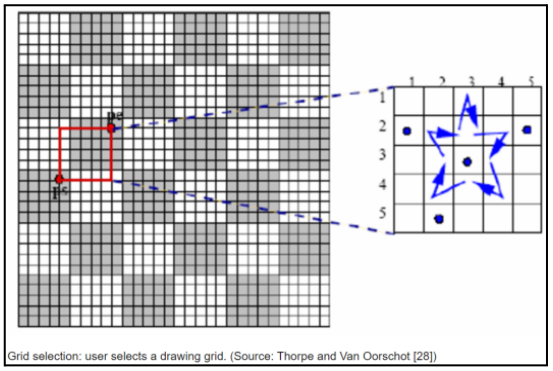


Fig. 2.6 Selection of drawing grid [21].

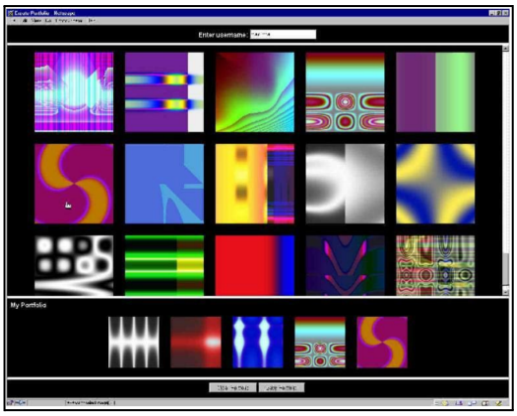


Fig. 2.7 Random images used in [22]

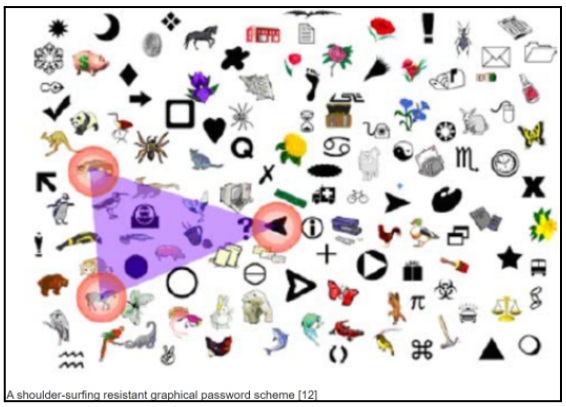


Fig. 2.10 Convex Hull algorithm [23]

Fig. 2.8 Jansen's method

Fig. 2.9 visKey sample image

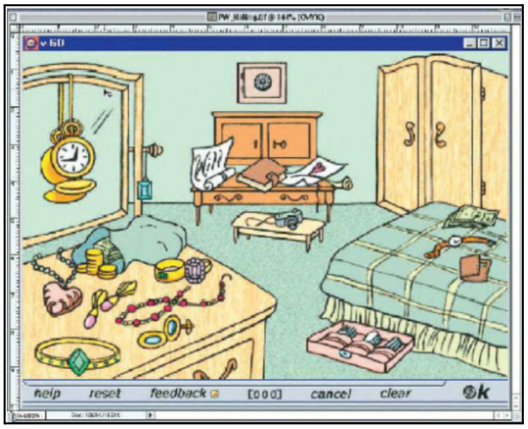


Fig. 2.11 v-Go [8]

TABLE II

PRE-EXISTING METHODOLOGIES WITH RESPECT TO GRAPHICAL PASSWORD AUTHENTICATION

S. No.	Approach	Working	Demerits
01.	Draw - A - Secret (DAS) [16], [19].	Reproducing a drawing in a specific set of grids, exactly in the same coordinates as when the password was set. Proposed by Jemryn et.al .	● 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 GregBlonder 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.	PassPoint [11], [16]	● It overcomes the shortcomings of the Blonder's Scheme. 1. Selection of an image and, 2. Click on the ROI (Regions - of -interest) in a specific sequence to set a password. Step 2 for login.	● Extremely difficult to memorise 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.

S. No.	Approach	Working	Demerits
04.	Cued-click Points [6]	● Several images are chosen in a sequence and regions-of-interests 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 PassPoints	● Regions of interest / the hotspot are inflexible and an issue. ● Password space requires expansion.
05.	Passfaces [7],[18]	● Selects 4 faces from the grid of faces. ● During the registration, the user must confirm it twice.	● Passwords are 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.

S. No.	Approach	Working	Demerits
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 modelled 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 can not 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 recognise 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 memorise but hardly secure. ● Non-resistant to shoulder-surfing.

TABLE III
VARIOUS SECURITY ATTACKS FACED BY PRE-EXISTING APPROACHES

Approach	Resistant	Non-resistant
Draw-a-Secret	Brute-force, dictionary attacks.	Shoulder-surfing, & spyware attacks.
Blonder's Scheme	Brute-force, dictionary and Social engineering attacks.	Shoulder-surfing, & spyware attacks.
PassPoints	Brute-force, dictionary, & Social Engineering attacks.	Shoulder-surfing, spyware & social engineering attacks.
Cued-Click Points	Brute-force, Dictionary & Social Engineering attacks.	Shoulder-surfing, & spyware attacks.
Passfaces	Brute-force, Dictionary & Social Engineering attacks.	Shoulder-surfing, & spyware attacks.
Grid Selection	Brute-force, Dictionary, Social Engineering, & Shoulder-surfing attacks.	Spyware attacks
Deja Vu	Spyware attacks & shoulder-surfing to an extent.	Brute-force, Dictionary & Social Engineering attacks
Jansen's method	Brute-force, Dictionary & Social Engineering attacks.	Shoulder-surfing, & spyware attacks.
visKey	Dictionary & Social Engineering attacks.	Brute force, Shoulder-surfing, & spyware attacks.
Sobrado & Birget's method	Brute-force, Dictionary & Social Engineering attacks.	Shoulder-surfing, & spyware attacks.
v-Go	Brute-force, Dictionary, spyware & Social Engineering attacks.	Shoulder-surfing attacks.

2.4. EXISTING WORK

[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 order of POI selection.

[13] proposes a *Cued Click Point system* to secure *Cloud* with enhanced mobile alert systems on possible security threats. The system stores sets of images corresponding to only the first 9 alphabets respectively (such as *Set A, Set B, ... , Set H, Set I),* since the first digit of any two digit number falls between 1-9 . According to which,

(a) users are allowed to create usernames for themselves;

(b) Calculations are made by adding each and every letter's numerical position in the Alphabetical order.

Suppose, Username = SAGE, whose positions are 19, 1, 7, 5, respectively;

Their sum is *19 + 1 + 7 + 5 = 32.*

(c) The first digit is '3', so *Set C* images will be displayed.

(d) Out of which, two images are to be selected, alongwith two other server side images, which would act as a password.

Problem with this method is that it can be accessed by anyone when the sequence of username is known and shoulder-surfing is possible.

TABLE IV

NUMBERS BETWEEN 1-9 AND THEIR CORRESPONDING ALPHABETS

A	B	C	D	E	F	G	H	I
1	2	3	4	5	6	7	8	9

[14] proposes S3PAS i.e. Scalable Shoulder-Surfing resistant (textual-graphical) Password Authentication Scheme. It is basically built to offer highest resistance from shoulder-surfing, also integrates both the ext-based and GPA schemes while proposing three enhancement schemes, which are: Three-set, Rule-Based, and Enhanced Graphical Schemes. [14] employs parameters like that of most password systems, which are security, usability, and password space; all the while working on

enhancement of the S3PAS, to improve its performance and security. Though, the current version provides an almost perfect level of security; it can help replace or coexist with conventional textual password systems without changing existing user password profiles. Yet, It has a complicated and time-taking process, ease of usability and adoption is quite low, hence, it would require the newer version of S3PAS to compromise on security.

A. PASSTILES-

In [7] to conduct a research on memorability of different types of passwords, emphasising on graphical passwords ("Memory retrieval and Graphical Passwords"). For that purpose they created PassTiles. PassTiles is a graphical password system consisting of a matrix of squares/tiles and the password consists of five password tiles. In order to login, User must click on the correct password tiles, while the order of clicking does not matter. It is a perfect integration of DAS (Draw-a-secret), PassPoints and Passfaces. Passwords here can be either chosen by the user or assigned by the system.

There are three basic variations of PassTiles:

1) Blank PassTiles : Has a blank backgroundP, similar to DAS, free-recall task.

2) Image PassTiles: Based on an image divided by a grid, similar to PassPoints, cued-recall task.

3) Object PassTiles: each square contains a different Image or object --- forming a matrix of several object images, similar to Passfaces, Recognition based task. It is a shuffled grid. Object PassTiles can have two more variations: (a) containing pictures, and (b) containing words.

But the analysis by [7] involved following password types i.e, the three variations of PassTiles as mentioned above (BPT, IPT, OPT), and also the traditional forms of password- a) Assigned Text (AST), & b) Chosen Text (CHT). Mainly studying three variables i.e. memory time, password resets, & login time, of all the password conditions.PassTiles allows users to take advantage of both recall and recognition memory, whereas memorability and login times were faster.

[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 PassTiles. Intends to create a *Child Oriented Authentication System*. Through survey study, it was found that both children and adults are receptive to Object PassTiles. The parameters concluding the result were as follows:

i) ***Memorisation 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 PassTiles and they also preferred it. Assal also claims that *fairy tales* are an effective password memorisation method. But it neither explains *adult responsibility* in the *Child Oriented Authentication System,* nor does it take into account shoulder-surfing as a security breach-cum-attack [15].

B. DAS -

Draw-A-Secret (DAS), proposed by Jermyn et al. in [16], is a recall based system that requires the user to reproduce the drawing/ pattern i.e, set as the password without any hint provision by the system. Here, 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 is it authenticated. The tolerable distance is 0, therefore, the password has to be exact [13]. For example, the pattern lock on smart phones and devices. But here instead of a grid of blank squares, it has 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].

C. PASSPOINT -

PassPoint is a Cued-recall based system; Created by Wiedenbeck et al. inspired by Blonder's scheme that uses a system-assigned image and click-points in specific regions only [11]. But PassPoint requires an 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 exactly 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 highly reducing the risk of security breach [11], [16], [17].

The picture must contain objects of identification, which would make the user successfully identify and select them in a 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].

Fig. 3 Passfaces procedure during the 1st phase of training

D. PASSFACES

Face recognition is the foundation of Passface, except it recognises 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 Passfaces 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-Passface algorithm to choose password at login phase, introducing the concept of 'alternative password', while omitting the use of mouse. Offers comparison of the Passface and S-Passface algorithms on the basis of usability, security (social-engineering, shoulder-surfing, brute force, spyware attack and guessing). Benefits of S-Passface being easier memorisation, recognition, understanding and ease of use, on the par of the client. It also increases security by creating resistance to shoulder-surfing, but this action reduces the usability of S-Passface. [7] identifies that it is rather easy to create a password than to select one. But attackers will be able to guess the S-Passface password more precisely over the original Passface algorithm.

E. STORY

Davis et al. proposed a Graphical Password Authentication system called "Story" as an alternative to Passfaces . 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 Passfaces [6],[18].

F. CUED-CLICK POINT SYSTEM (CCP)

CCP is based on cued recall cognition. It was proposed by Chiasson et al as an alternative to PassPoints. It is an integration of PassPoints, Passfaces and Story. There one click-point per image, where single selection of a click-point on an image leads to another image with its very own click-point [6]; Applying the Story and Passfaces concept in terms of 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 PassPoints and Passfaces in terms of click-point or select an image strategy. PassPoints' discretization method is implemented in CCP, which initially functions like the former system [25]. From PassPoints, CCP also inherits the grid like structure on the image and tolerable distance (concept) from the original click-points. 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 has to click on 5 images each only once, and not 5 clicks on one 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-point, is only provided after the final selection.*"- *(Chiasson et al)* [6]. So as 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 Passfaces, in turn increasing the security of the system. Hence, CCP can also be known as choice-dependent path images.

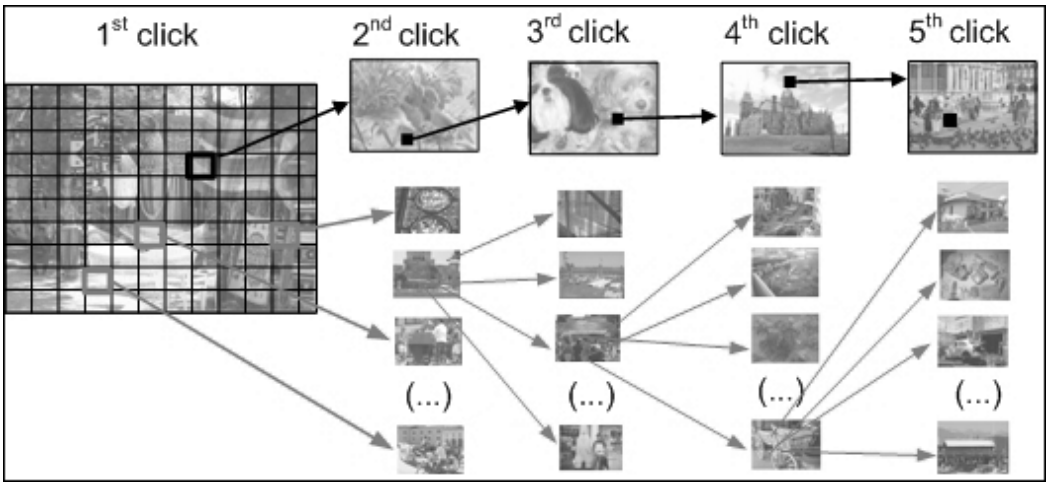


Fig. 4 CCP - sequence of clicks on different progressive images of a path.

The change in visuals/images does not hint at the password being correct or not, but it is evident that the legitimate user has the knowledge to distinguish between "correct and incorrect paths". The 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].

Chiasson et al. also conducted a proper survey, according to which 9 out of 10 users preferred CCP over PassPoints, 2 of them found PassPoints easier than CCP, and all of them agreed that CCP would be tougher to get past i.e., if and 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 as a whole does not safeguard against *shoulder-surfing*, the password is difficult to memorise. Hotspot identification is a problem [6].

[18] proposes a system that is a combination of recall and recognition based approach, it provides security against brute-force, and shoulder-surfing attack. Also, it shows comparison between CCP and PassPoints 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.

2.5. PROPOSED APPROACH

The Proposed System takes in the sequence of objects as the password. During registration a sequence of objects [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 a new matrix with different images of the same objects with shuffled position's is supplied.

Numerical entry encourages to accurately state the position of the SOO invalidated any ambiguity in the GPA procedure. Required cognitive functioning is nessesary for every attempt of the login.

During Registration or Sign up,

1. the user should create a username,
2. And for a password, the user will have several distinct objects to choose from.
   a. Suppose the chosen images are Cat, Rabbit, Dog and Bat.
3. The order selection and re-occurrences of the icons will also be recorded.
   a. Suppose, Rabbit → Cat → Dog → Bat→ Rabbit;
   b. Here, we can observe that 'Rabbit' has been repeated twice.
4. Also a text-based (alpha-numeric) password shall be created as an alternative password for better assurance.

During Sign In or Log In,

1. the user shall enter the username.
2. On the basis of which, 9 different images of distinct objects comprising of the certain set of the user's chosen password icons along with random images in 3*3 matrices shall be displayed .

Fig. 5. Images displayed in a 3*3 matrix

3. Each object/box of the matrix shall have corresponding values like a number-pad as follows:

1	2	3
4	5	6
7	8	9

TABLE V. CORRESPONDING NUMBERS OF EACH PICTURE IN THE MATRIX

4. The user must enter the values of the position or icons, according to the order and occurrence of the icons set by the user as the password during registration.

Password = Rabbit → Cat → Dog → Bat→ Rabbit

Entered Text = 7 2 3 6 7

5. If the password entered is wrong a new set of images with different placements will be shown. If true, there is no specific sequence of characters to crack, and for every try, the sequence/order of values will change. Hence, the Brute force attack will not work. But the probability of opening a 4-sequence

password =1/3024. This is true for every try.

6. Else, the User shall then be logged in to his/her account.

Shoulder surfing is one of the main problems in several other Graphical Password Authentication systems, since the patterns or visual passwords are easy to notice and remember. In our proposed method, as the visual input requires a typed sequence of numbers it is hard to notice it, even if the key strokes are tracked by any malware this is obviously not the password the corresponding visual data is required to crack the password thereby eliminating keylogger hacks.

It is hard for Network analysers to manoeuver the packets and crack the packets, for developing algorithms of this sort will require having human intelligence to logically reason the why this corresponding images are chosen. To Prevent this we will require to implement an typical HTTPS public key-private key cryptography.

It can also be observed that our approach is critically inspired from Jansen's method. We intend to improve the efficiency of the GPA system, make it secure and provide the user with utmost privacy; while successfully preventing shoulder-surfing and other such attacks

2.6. FEASIBILITY STUDY

a. Technical Feasibility:

- A similar *Graphical Password Authentication system* 'AuthEasy' was developed with the use of server *client interaction* and *images identification* character; it was implemented through mobile application. 'AuthEasy' used a randomization technique but used identical tokens for each try. In contrast we will be using a *large categorised data set* and *numerical input*.
- Delivery of Images will be key, to provide a clear enough set of images for easy identification and also small enough for a faster transmission. Employing Image compression to achieve this objective.

b. Operational Feasibility:

- Our proposed system has an efficient usability, to provide the user with a better operational ease compared to other GPA models.
- It is designed to function largely on web browsers, such as Google Chrome, Mozilla Firefox or any other browser with JavaScript Support.

c. Economic Feasibility:

- Our GPA model will have corresponding costs of a Server, the bandwidth of a minimum of 10 Mbps, and for memory as well. 'Amazon Azure A2' Standard server with 3.5 Gb data will suffice with ample future *scalability* option.
- The Maintenance requirement will be very low except *database administration* work to ensure the data *integrity*, *redundancy* and *maintainability*.

d. Schedule Feasibility:

- Developing the back-end with a stable and reliable *content delivery* system for the images and *proper encryption* will take a substantial amount of time.
- Considering the complexity of the project, it is possible to complete it and arrive at the working model within 8 months.

3. System Design and Analysis

3.1. Project Objectives

a. Provide a reliable Graphical password authentication alternative.

b. Provide an easy to *use,* easy to *memorise* authentication experience

c. Reliable working *content delivery* system and *improved security*.

3.2. Project Requirement Specification

a. Purpose:

To make authentication graphical which is easily memorizable and more secure than purely recall based authentication systems

b. Scope:

- To develop a unique *Graphical Password Authentication* using a combined *Knowledge Cognitive* based Approach.
- To research the advantages and disadvantages of this authentication technique on *human retention* and *accessing efficiency*.
- To develop an *Operational Web Application* using inhouse authentication API.
- Documenting the *human interaction* with the authentication and finding the interactive limitation of *recallability/memorability* and *industry usability* scenario of this application.

3.3. Relevant Constraints

a. Bandwidth:

Bandwidth for the transmission of 9 individual images and their arrangement code will require a minimum of 900 Kbps of bandwidth for the *authentication* to be at minimum operational.

b. Client processing:

Client side encryption of the sequential passcode will require some processing capacity of the user's computer, Hence using minimal computational resources and maximising encryption complexity will be key in providing secure communication.

c. Server availability:

As authentication relies heavily on server side *data provision*, we will need a redundant server setup which also will cater to different users across many geographical locations.

d. Memory constraints:

Server side memory will be a constraint for storing of a large interface *characterised data set* in some encrypted format to fend any data breach attacks

3.4. Functional Requirements Specification.

Table VI. Functional Requirement Specification

Requirement ID	Requirement Statements	Want/ Must	Comment
FR01	The System must require the user length of the Password Object Sequence(POS).	Must	The Length also takes duplicate objects into account.
FR02	The System must require the user during registration to choose the order of the selected objects.	Must	Numerical Input
FR03	The System can require the user to choose the number of objects visible in the grid view.	Want	Number of objects should be restricted to grid size.
FR04	The System must require the user during registration to choose the set of objects out of the given limited options.	Want	None
FR05	The System must require the user during registration to enter some credentials such as {User's Email ID},{User Name}	Must	Email-id is essential
FR06	The System should send a confirmation email to {User's Email ID} for the registration process to be validated.	Want	None
FR07	The System must allow the user to reset the password by clicking the "Forgot Password" button.	Want	None

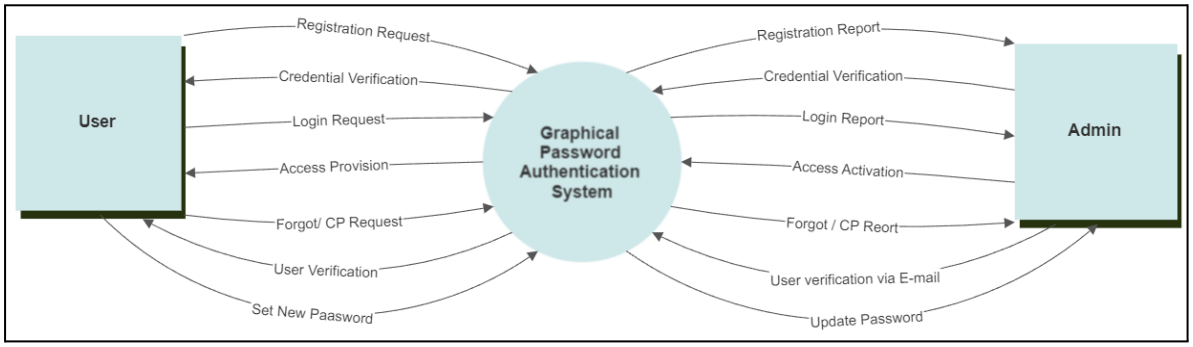
FR08	During Login, the system must input {User's Email ID} as a username.	Must	None
FR09	The System must display objects in random fashion in a grid view.	Must	None
FR10	The System must display different images of the objects in different attempts of Login	Must	None
FR11	The System must display the user's Name after the Login.	Must	To successfully validate the authentication process
FR12	The System must sent the link of re-registration to the {User's Email ID}, when "Forgot Password"	Must	None

TABLE. VI. FUNCTIONAL REQUIREMENT SPECIFICATION

3.5. METHODOLOGY

We have adopted the "Kanban model" for project development and management. The Kanban framework is the simplest form of Agile methodology. It particularly focuses on visualising the entire workload on boards/ records so as to increase efficiency, accountability and project transparency among the team, mainly in collaboration. It allows the project managers to manage methodically and to keep the project on track. It helps in continuous improvement and flexibility in task management, it is also highly compatible with current organisational settings in comparison to other agile frameworks. In place on Kanban boards, we replicated a register structure (i.e. similar to kanban board) using 'NOTION' software, in order to keep a track of our developments.

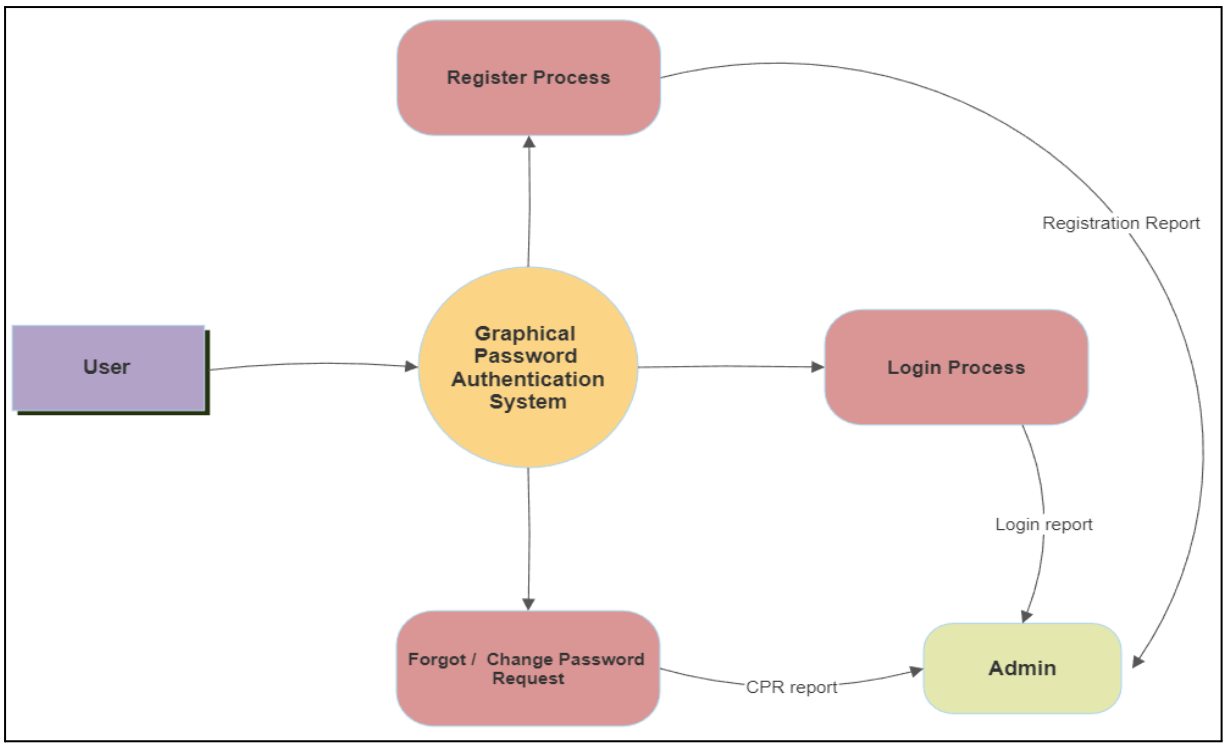
Below are the DFDs (Data-Flow-Diagrams) that define our GPA system's structure and working. These help visualise the expected project outcome as well as help us in future developments, all the while acting as a reminder of the measures to be taken in due period.



DFD- LEVEL 1

Fig. 6. Overview of GPA system (User-request and Admin-response)

The above figure depicts the overview of the GPA system, which is to be further carved up into different processes with a much more detailed view.



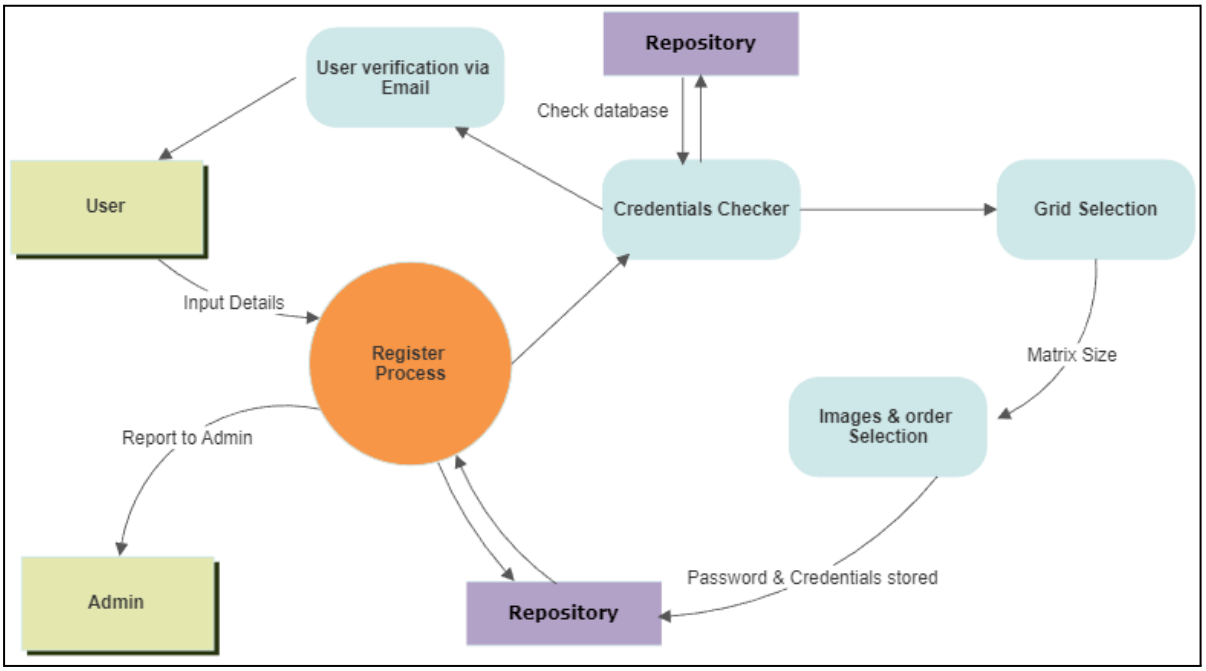
DFD- LEVEL-2

Fig. 7.1 A summarised diagram of GPA.

Above is the simplified depiction of the main processes, which when combined together in a proper and structured manner with the help of the algorithms and framework form our GPA system. These processes are further expanded below to show their working. The registration, login and change password process are depicted below.

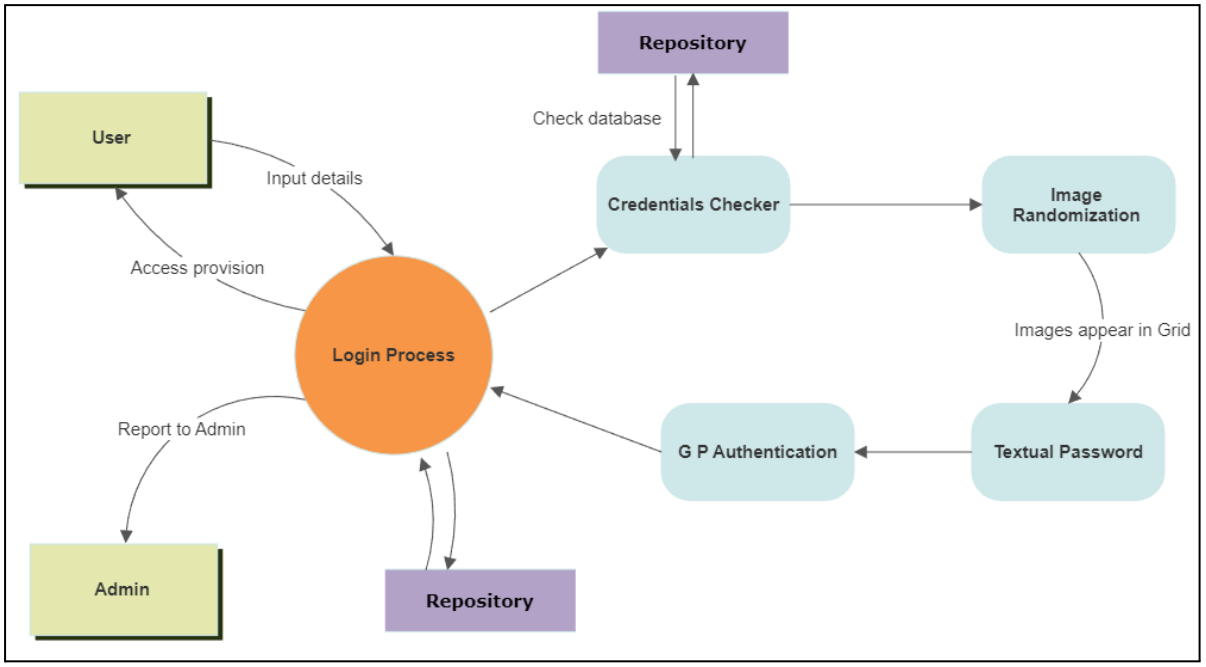
DFD- LEVEL-2 (A)

Fig. 7.2. Registration Process



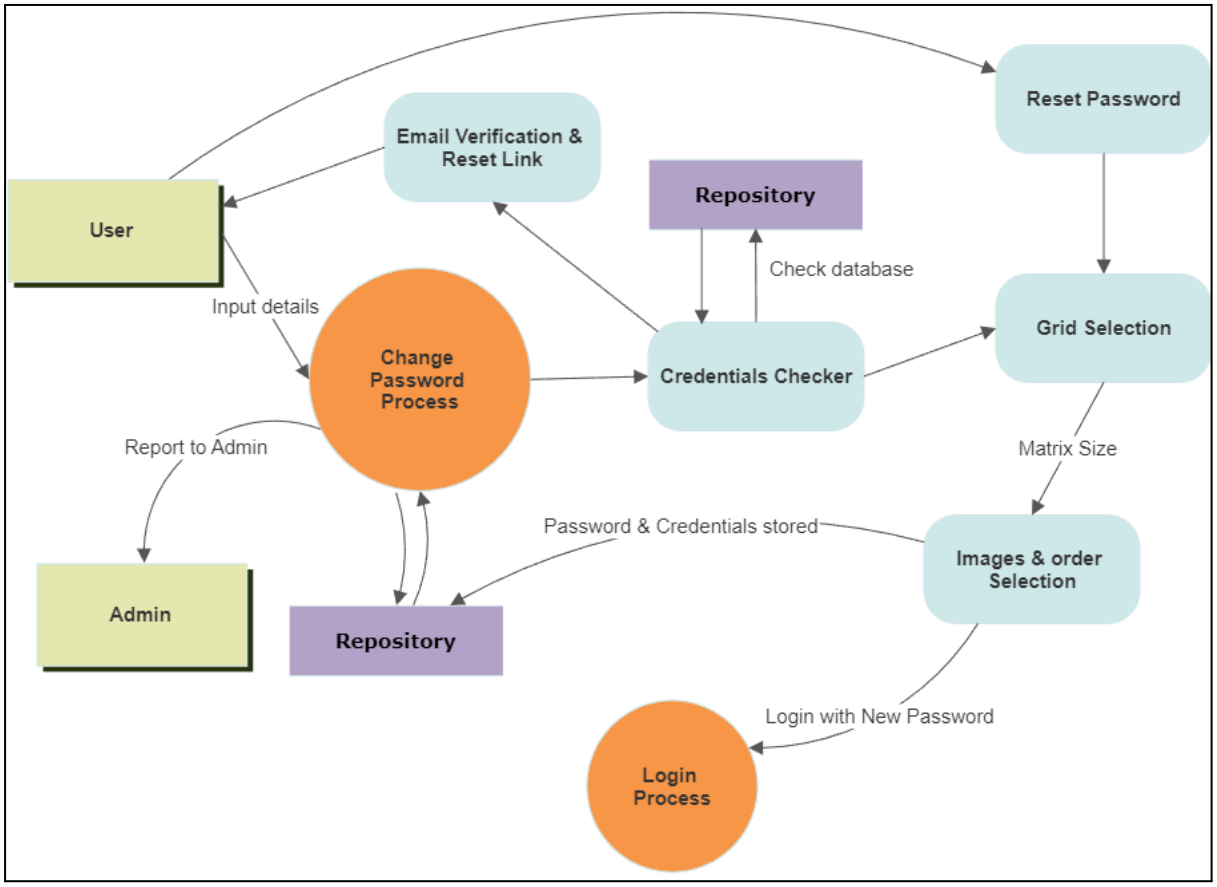
DFD- LEVEL-2 (B)

Fig. 7.3. Login Process



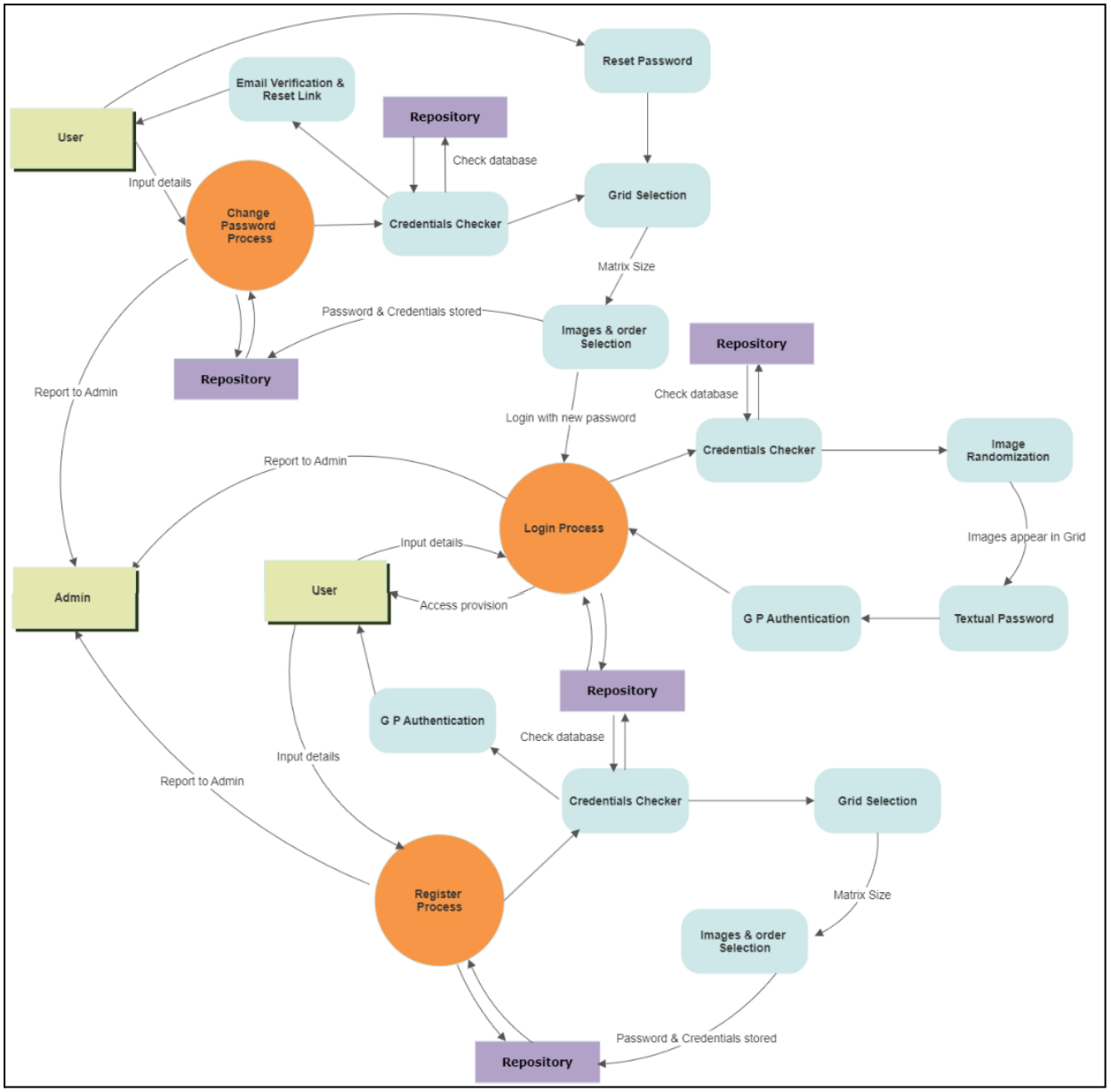
DFD- LEVEL-2 (C)

Fig. 7.4. Change Password Process



DFD- LEVEL-3

Fig. 8. Complete Process including sub-processes



USE CASE DIAGRAM DURING LOGIN

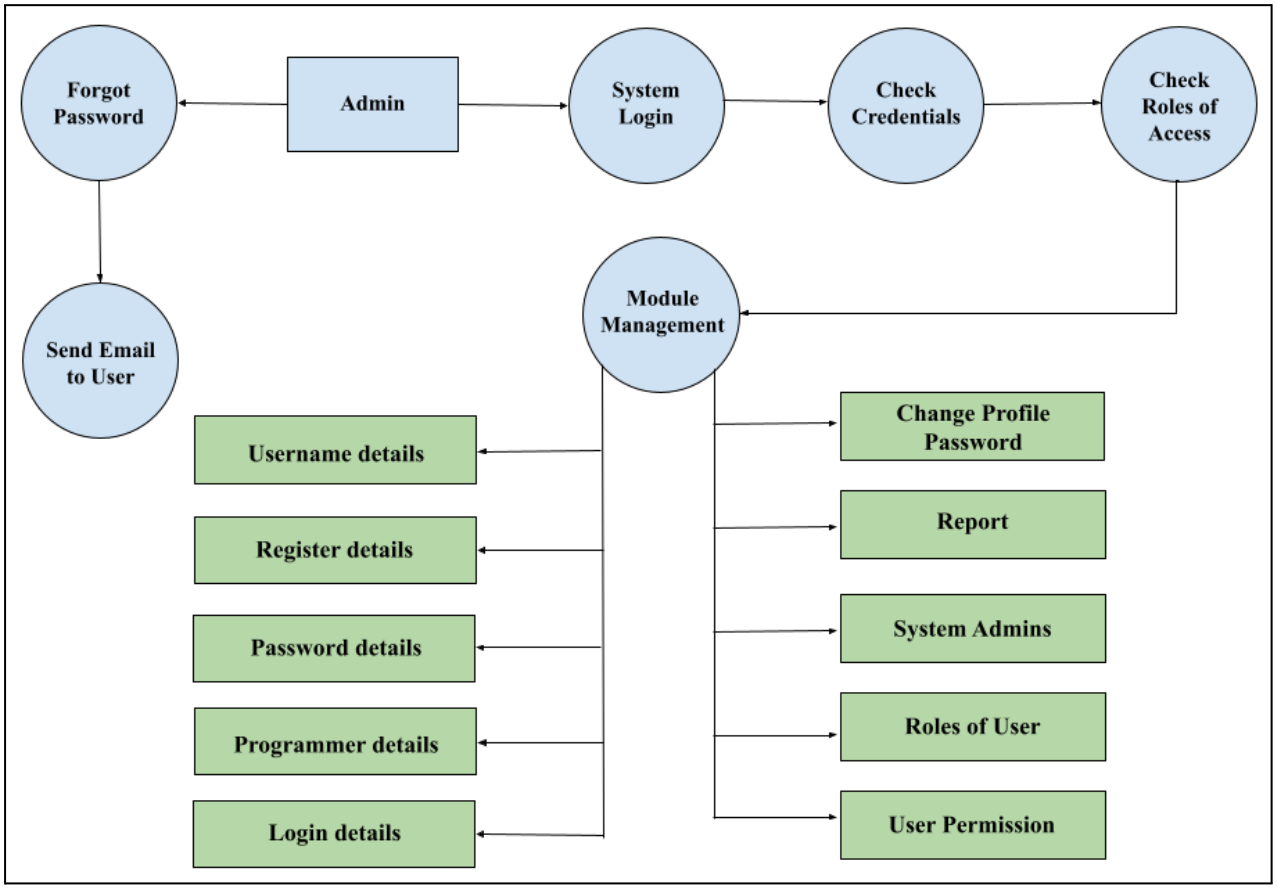


Fig. 9. Use Case diagram for login process

4. IMPLEMENTATION

4.1. SYSTEM MODULES AND IMPLEMENTATION SPECIFICATION

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 has 4 modules consisting of the Registration phase (See Fig. 11.1 and 11.3), Login Phase (See Figures. 11.2 and 11.4), and Forgot Password phase (See Figures. 11.5, and 11.3), as depicted in the system designs.

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 customise their page in order 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 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 has to 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 has to 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. GridImage 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 particular 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 entry is accepted according to the password length determined by the user.

Here the temporary sequence code concerning object sequence is typed in.

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 has to login again. The URL of the previously used- login page does not enable the user to access the same grid that appeared in 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. (See Figure 11.5)

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. (See Figure 11.3)

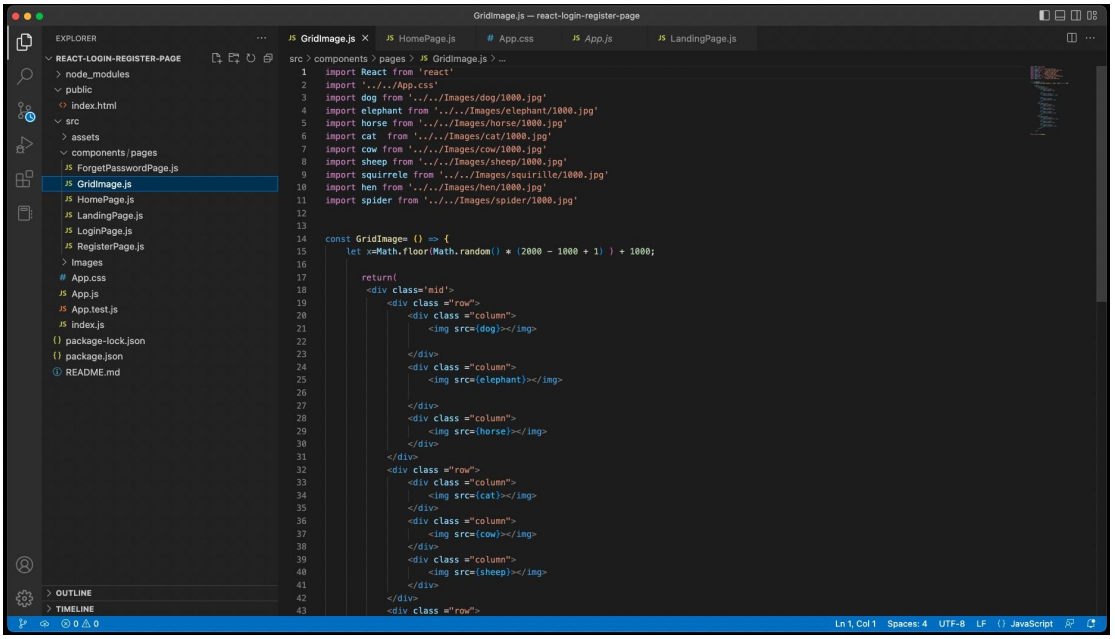


Fig. 10.1 GridImage Module

The above component (in Figure 10.1), takes in the image props and can render it in a grid fashion, this component is used in login and registration. This will be connected to the content delivery system and the randomization module from the Node.js module.

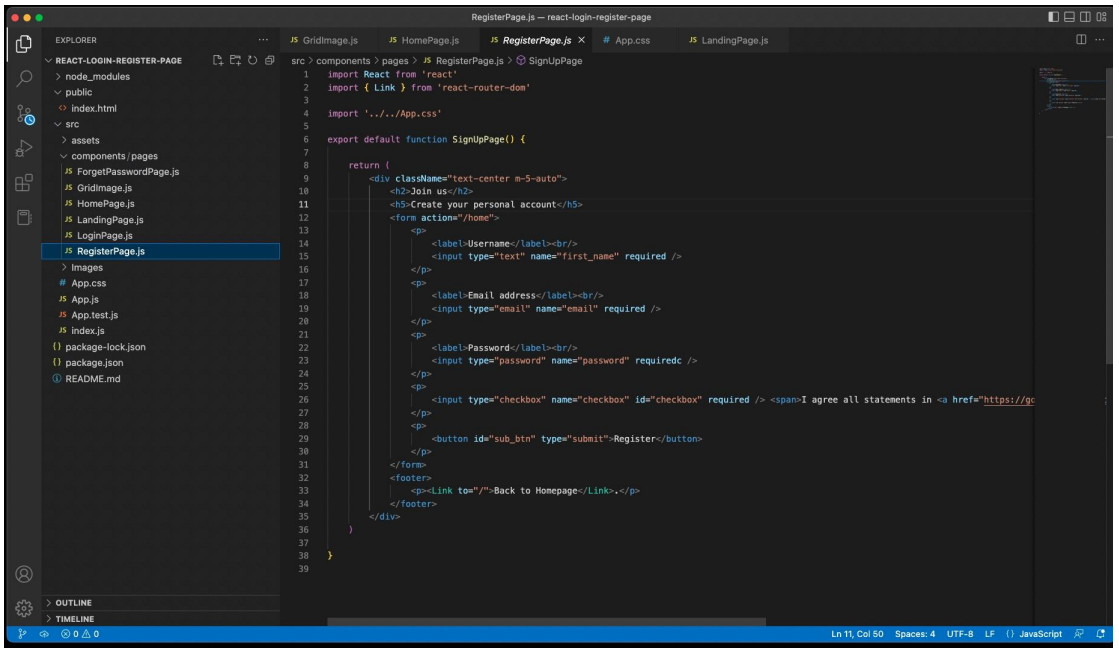


Fig. 10.2 RegistrationPage Module

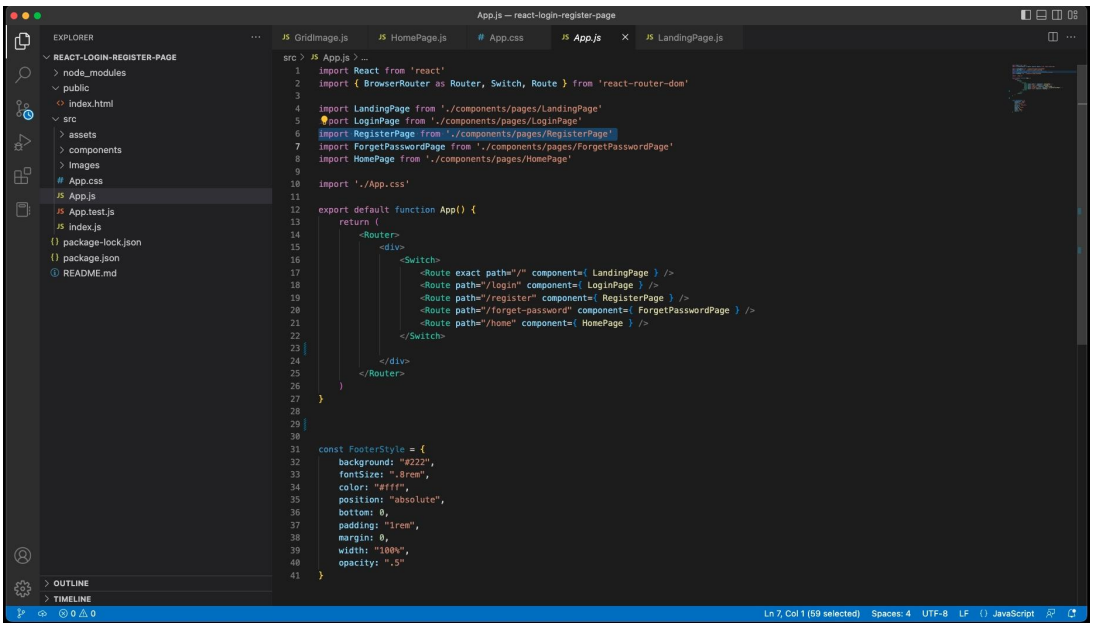


Fig. 10.3. ReactRouting Module

Using React DOM as a routing module. This will be intercepted by the node.js middleware to acquire the required data. Like username, token, and objectSet.

4.2. 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, on every sunday.

In the first week, the working of the system was explained and the Registration procedure was conducted on each participant. This included every participant to sign up using the deployed GPA system. Every participant registered using their name as the UserName, their EmailID and their RollNO as a textual Password. Later they made their SOO with the minimum Length of the SOO was at least 4 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 Signed 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 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 the data 3 login iteration of 100 users.

4.3. OUTPUT

A. Complete Registration , Login Example

As mentioned above and shown in figure 11.1, The user is required to provide credentials and 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 figure 11.3, out which 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.

During the login process, the user should provide the *Username* as shown in figure 11.2, 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 continues accordingly in the other two rows. According to the set SOO, the passcode for this particular grid shown in figure 11.4 is 2934.

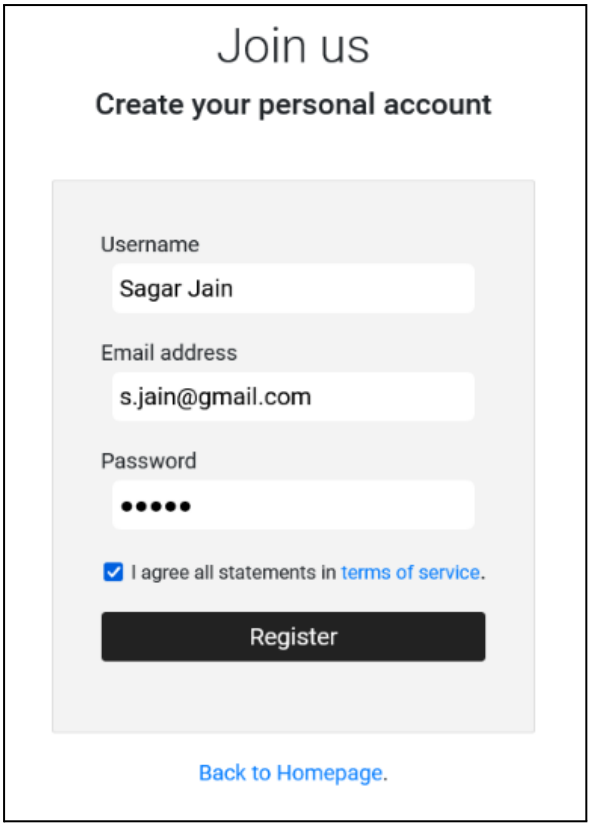


Figure 11.1. Join Us page

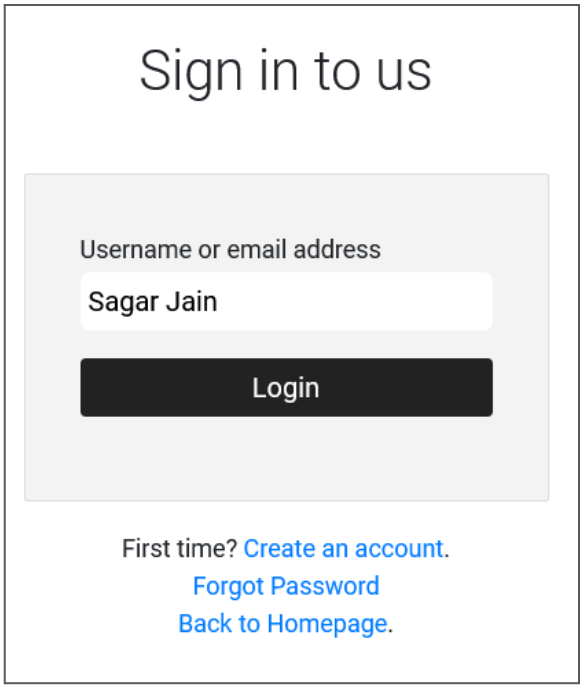


Figure 11.2 Sign in page

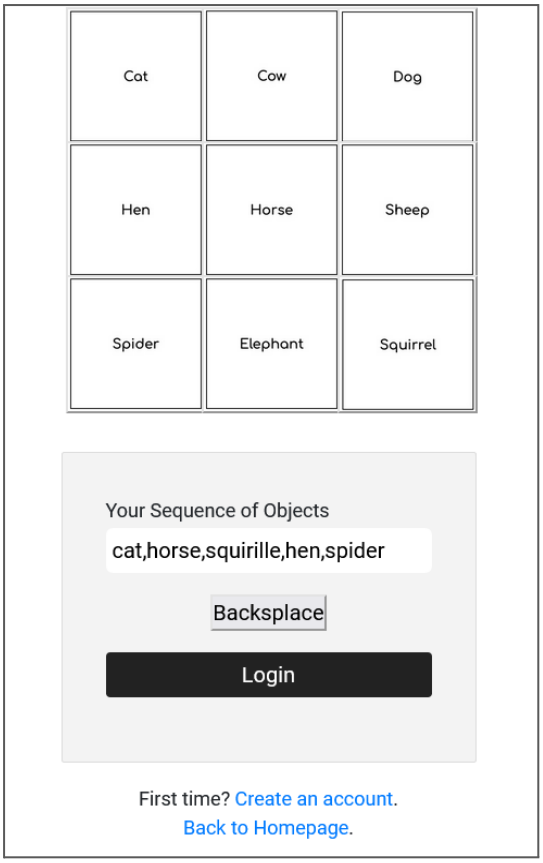


Figure 11.3. Select Password page

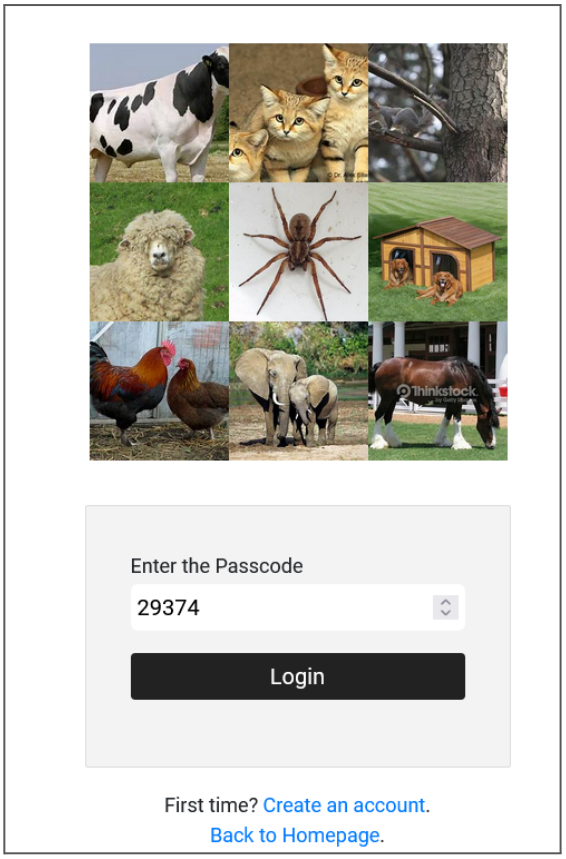


Figure 11.4. GPA Sign in page

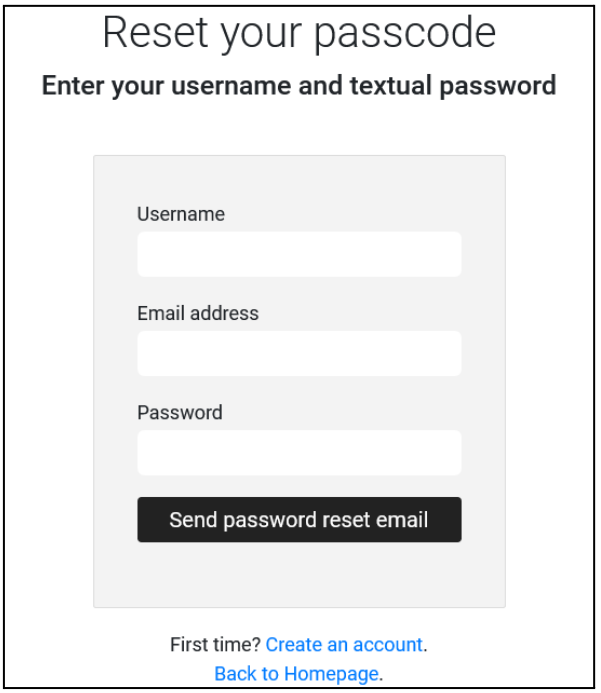


Figure 11.5. Reset Password Page

4.4. Testing

4.1.1. Software Testing

The contribution of software testing is extremely impactful, efficient and accurate. It signifies the quality of software provided to the client by the creator. It is also a scientific investigation conducted mainly to detect errors and provide assurance to the client, who is required to rely on the software.

4.1.2. Unit Testing

Here, every module of the system is tested individually and is expected to function well individually and in conjunction with other modules as well.

The unit testing was conducted on the following elements:

- Grid Image module
- Randomisation 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

4.1.3. Integration Testing

All the relevant elements of the GPA system are combined and integrated to test it as a whole entity. Integration testing takes all the unit-testing-based components like modules, data, etc., and groups them to form a larger assemblage. It matters whether the system as a whole is error-free, efficient, and reliable.

4.1.4. Authentication Testing

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 the Credentials transmission over an encrypted channel/ medium. (AT-001)
- Testing for Default Credentials provided during initial authentication. (AT-002)
- Testing the poor lock-out mechanism. (AT-003)
- Testing for Authentication schema avoidance. (AT-004)
- Testing the Remember Password Functionality. (AT-005)
- Testing for Browser Cache Weakness. (AT-006)
- Testing the weak password security/policy. (AT-007)
- Testing for weak Password change/reset functionalities (AT-008)
- Testing for weaker authentication in alternative channels/mediums. (AT-009)
- Testing the login state (grid) changes on refreshing and unsuccessful login. (AT-010)

Reference. kennel209.gitbooks.io **- Owasp testing guide.**

5. RESULTS

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.

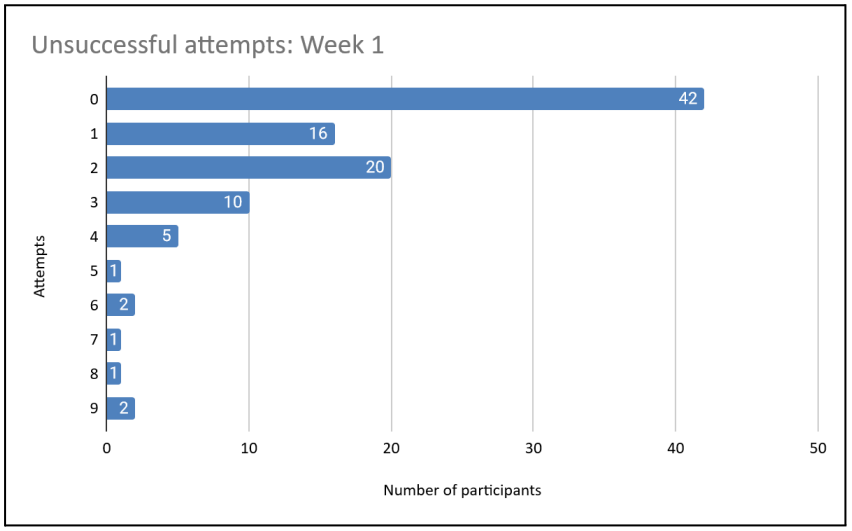


Figure 12.1. Unsuccessful attempts - Week 1

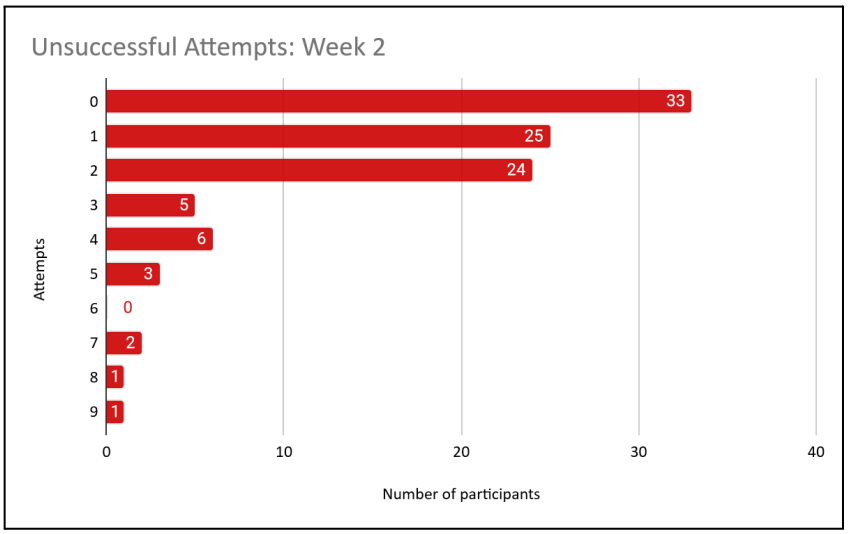


Figure 12.2. Unsuccessful attempts - Week 2

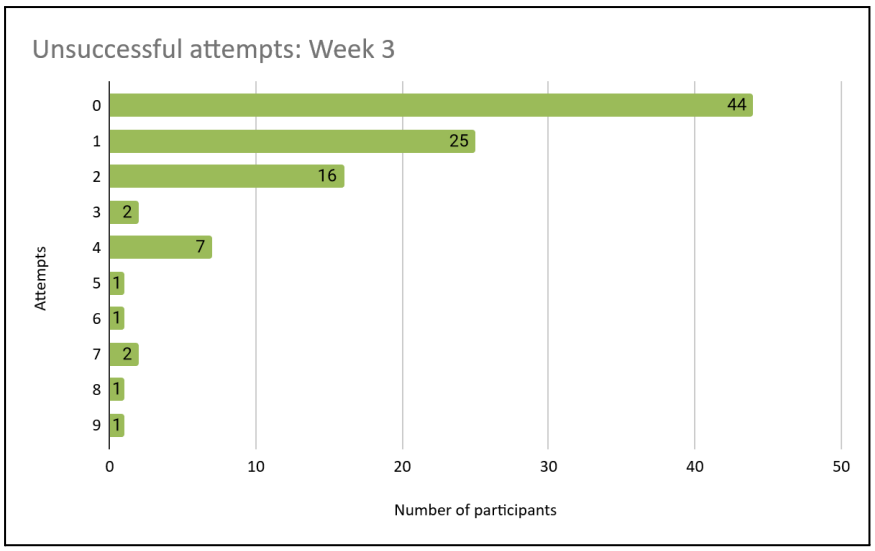


Figure 12.3. Unsuccessful attempts - Week 3

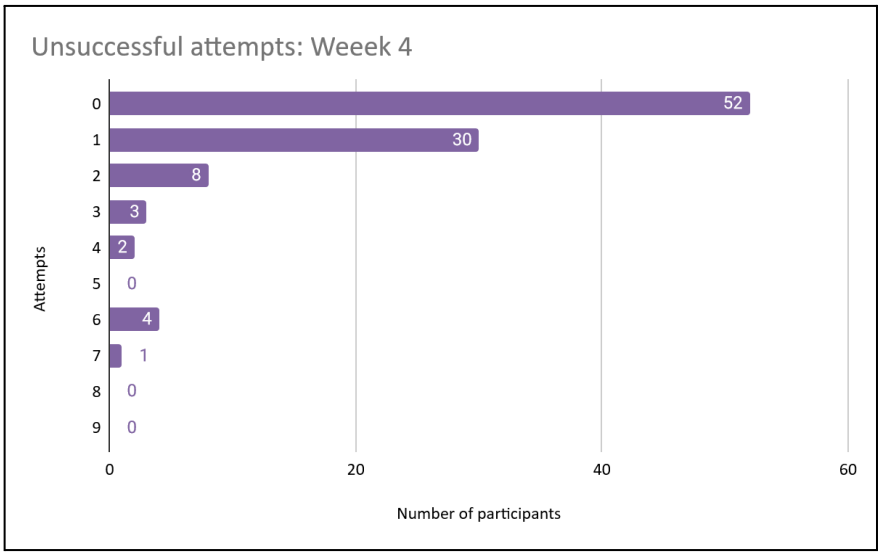


Figure 12.4. Unsuccessful attempts - Week 4

A lot of difference in the results of Week 4 and Week 5 is not observed. But the number of forgot password users were reduced this is seen due to the practice put in by the user and also a familiarity with the system. Ease-of-use is a peculiar feature that determines user retention, it does not matter whether the security provided is efficient if the system is difficult to use.

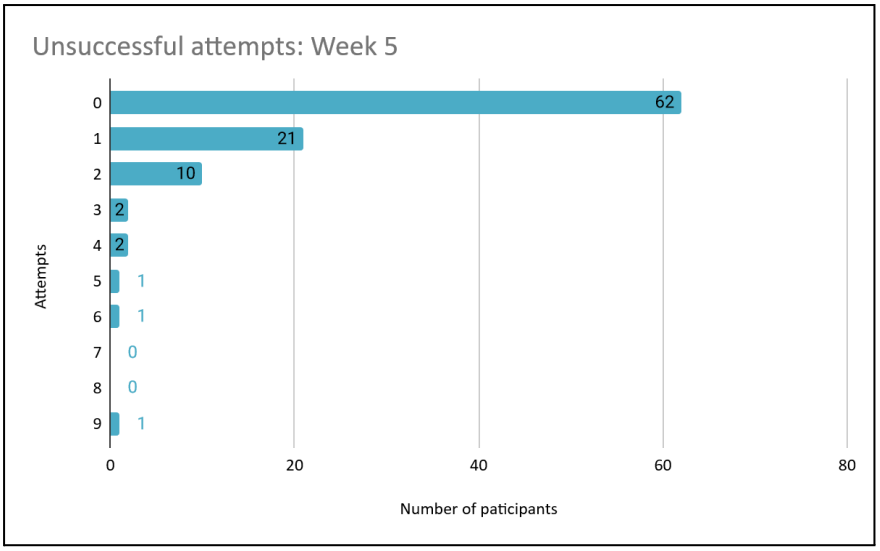


Figure 12.5. Unsuccessful attempts - Week 5

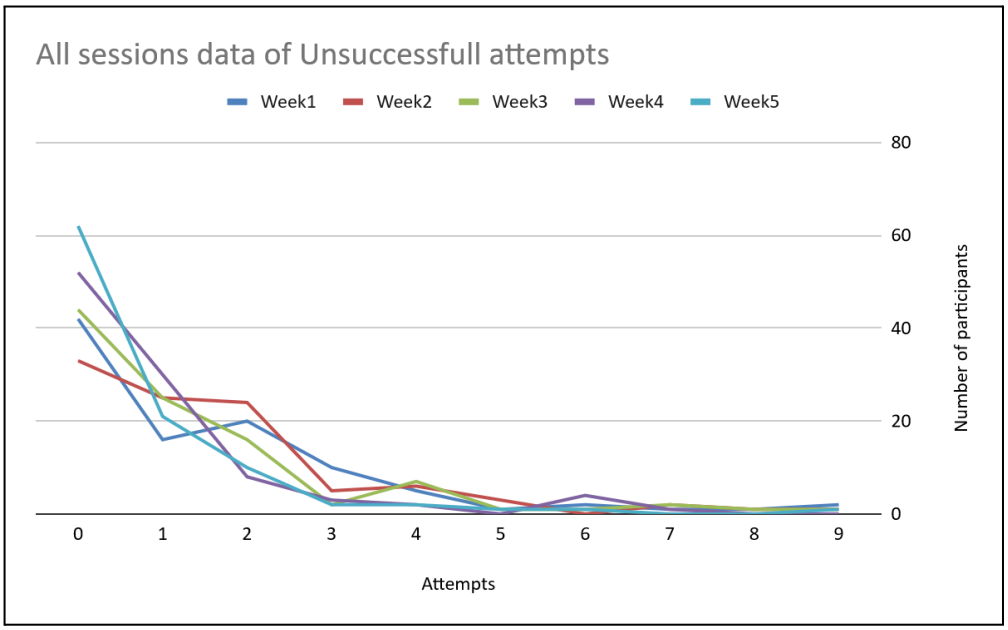


Figure 12.6. Unsuccessful attempts of all the sessions

5.1. Average Login Times:

As conveyed in Figure 8, 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 also 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

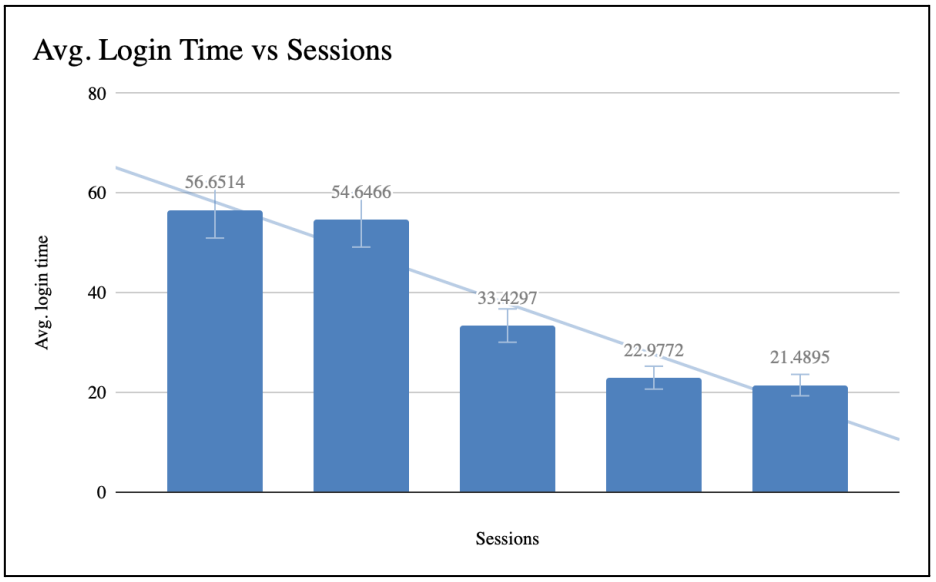


Figure 13. Average login time per Session

5.2. Number of Attempts for a successful login:

It tests the memorability of every participant as human retention/remembrance varies from individual to individual. 34 participants never entered the wrong password or chose the forgot password option, i.e. they did not fail any login attempts; 45 of the participants made several attempts to successfully login and also did not opt to change the password. They had 4.6 average unsuccessful login attempts in all the sessions.

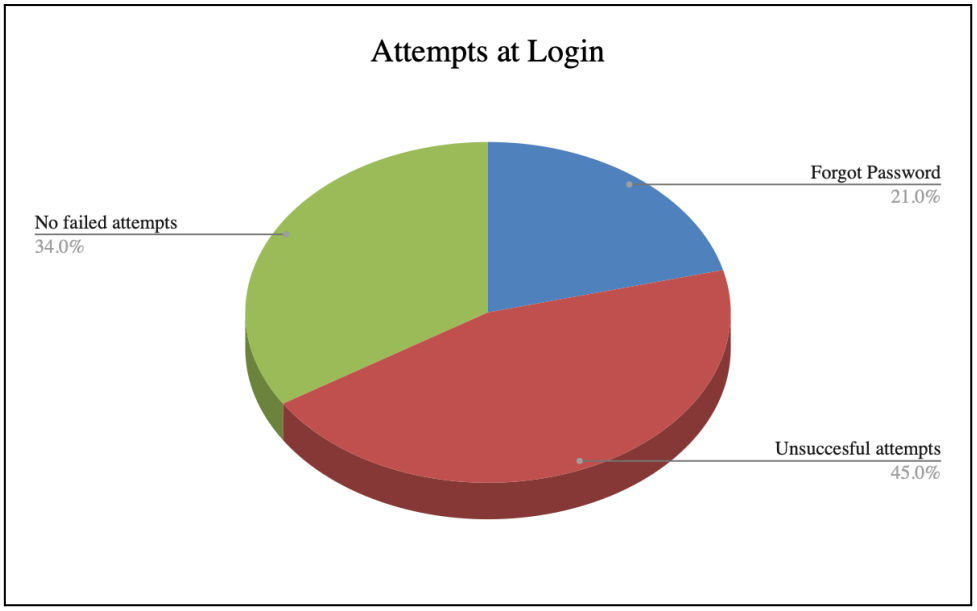


Figure 14. Attempts at Login

5.3. Number of Forgot Password Route Users:

21 participants, after several failed attempts, resorted to choosing the forgot password option and changing their password.

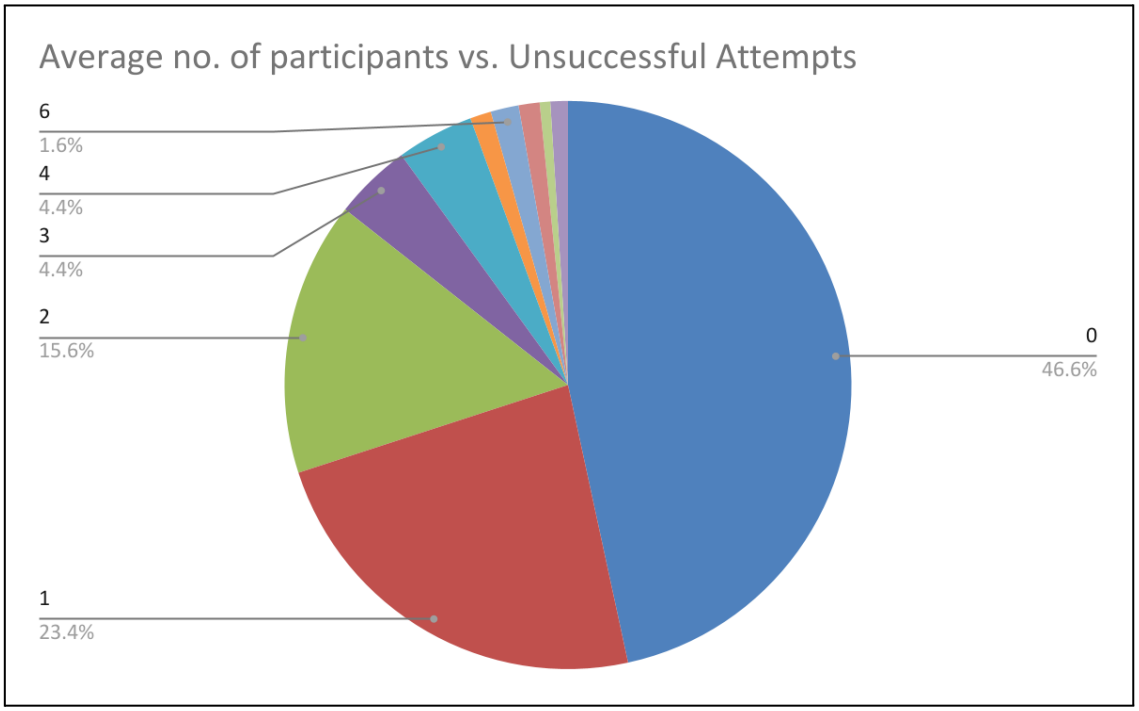


Figure 15. Average number of participants vs. Unsuccessful attempts

As depicted in the above figure, 46.6% of participants had zero unsuccessful attempts on average in all five sessions. Participants with 8, and 9 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 resistant to shoulder-surfing and brute force attacks. Nine unsuccessful attempts trigger the verification procedure to reset the password. 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 1/9. The success probability of an accidental login in an attempt is (PAL), 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 to be 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):

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

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

6. LIMITATIONS

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.

Smaller Object DataBase:

The proposed system utilizes 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.

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).

CONCLUSIONS

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, sniffing, 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 III. Both Passfaces 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.

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 in order 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 also the need to periodically change passwords. After testing, it was also found to be error-free, efficient, convenient and reliable.

FUTURE SCOPE

This authentication scheme can be further developed and 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.

6. 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).

[2] Gokhale, M. A. S., & Waghmare, V. S. (2016). The shoulder surfing resistant graphical password authentication technique. Procedia Computer Science, 79, 490-498.

[3] Gyorffy, J. C., Tappenden, A. F., & Miller, J. (2011). Token-based graphical password authentication. International Journal of Information Security, 10(6), 321-336.

[4] Towhidi, F., Masrom, M., & Manaf, A. A. (2010). An enhancement on Passface graphical password authentication (Doctoral dissertation, Universiti Teknologi Malaysia).

[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.

[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.

[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).

[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.

[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.

[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.

[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.

[12] Almulhem, A. (2011, February). A graphical password authentication system. In 2011 world congress on internet security (WorldCIS-2011) (pp. 223-225). IEEE.

[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.

[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).

[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.

[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)*.

[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.

[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).

[19] Nali, D., & Thorpe, J. (2004). Analyzing user choice in graphical passwords. *School of Computer Science, Carleton University, Tech. Rep. TR-04-01*.

[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.

[22] Dhamija, R., & Perrig, A. (2000). Deja {Vu--A} User Study: Using Images for Authentication. In *9th USENIX Security Symposium (USENIX Security 00)*.

[23] Sobrado, L., & Birget, J. C. (2002). Graphical passwords. *The Rutger Scholar*, *4*.

[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.

[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.

[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)

[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. doi: 10.3390/s22041349. PMID: 35214251; PMCID: PMC8962968.

[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.

[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.

[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

[31] Y. Zhu, G. Owen and X. Suo, "Graphical Passwords: A Survey," in Computer Security Applications Conference, Annual, Tucson, Arizona, 2005 pp. 463-472.

[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. doi: 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. doi: 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.

[35] https://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=1025&context=computer_science_facpubs

[36] https://www2.cose.isu.edu/~minhazzibran/resources/MyPapers/PasswordStudy_2022_Published.pdf

[37] https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9387325

[38] https://www.diva-portal.org/smash/get/diva2:1321294/FULLTEXT01.pdf

[39] https://faculty.ontariotechu.ca/vargas/papers/EEG_PredictPMemorability-ICCC2019.pdf

[40] https://link.springer.com/article/10.1007/s10207-019-00429-y

[41] https://faculty.ontariotechu.ca/vargas/papers/InsideOut-JISA2019.pdf

[42] https://github.com/OWASP/ASVS/blob/master/4.0/en/0x11-V2-Authentication.md#v21-password-security-requirements

[43] https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Authentication_Cheat_Sheet.md#implement-proper-password-strength-controls

[44] https://wiki.owasp.org/index.php/Testing_for_Bypassing_Authentication_Schema_(OTG-AUTHN-004)

[45] https://mobile-security.gitbook.io/mobile-security-testing-guide/general-mobile-app-testing-guide/0x04e-testing-authentication-and-session-management

[46] https://www.researchgate.net/profile/Mohammad-Alshammari-2/publication/336266496_Design_and_Learning_Effectiveness_Evaluation_of_Gamification_in_e-Learning_Systems/links/5daee953a6fdccc99d92b461/Design-and-Learning-Effectiveness-Evaluation-of-Gamification-in-e-Learning-Systems.pdf#page=442

ANNEXURE I

Review paper for the said project has been *accepted* in the 3rd International Conference on Nanoelectronics, Machine Learning, Internet of Things & Computing Systems (NMIC-2023).

Paper title:

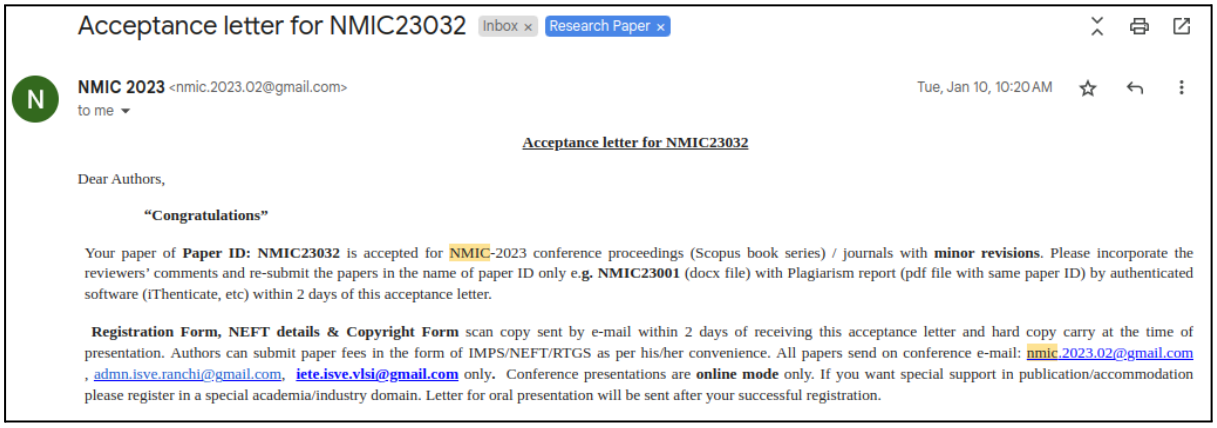
A Review of Graphical Password Authentication

Abstract:

In the current scenario, everyone is highly reliant on technology in numerous ways, such that their everyday chores are not complete without technological intervention, logically so due to modernization and advancements in technology. There are software systems available for every venture that the users require and utilise, which needs a proper mechanism to validate the users' identity for security purposes. The key terms associated with 'security' are confidentiality, integrity and authentication. And in the present age of cyber security, due to great developments in the field of computer science, authentication plays a key role in data security. Authentication is a process to validate the user's credentials in order to provide access to the system only with use of passwords, which preferably must be unique or distinct and confidential to the user only. There are several kinds of authentication systems categorised on the basis of the type of passwords used (See section II). Graphical passwords are cognition dependent, these employ the images of objects, people, sceneries, etc. These are image based authentication means that are not as burdensome on the users' memorability as the text-based passwords. Not as rigid as the biometric-based passwords, since an individual's physical features can hardly be duplicated. Graphical passwords can improve ease-of -use (usability), reduce password space as well, but only with much research and development of improved GPA systems. This paper provides a detailed study of graphical passwords, existing GPA techniques and relevant advancements in the domain of authentication systems pertaining to improved security of the system, also the users' convenience.

Authors:

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



Acceptance letter for NMIC23032 Inbox × Research Paper ×

N **NMIC 2023** <nmic.2023.02@gmail.com> Tue, Jan 10, 10:20 AM

to me

Acceptance letter for NMIC23032

Dear Authors,

"Congratulations"

Your paper of **Paper ID: NMIC23032** is accepted for NMIC-2023 conference proceedings (Scopus book series) / journals with **minor revisions**. Please incorporate the reviewers' comments and re-submit the papers in the name of paper ID only e.g. **NMIC23001** (docx file) with Plagiarism report (pdf file with same paper ID) by authenticated software (iThenticate, etc) within 2 days of this acceptance letter.

Registration Form, NEFT details & Copyright Form scan copy sent by e-mail within 2 days of receiving this acceptance letter and hard copy carry at the time of presentation. Authors can submit paper fees in the form of IMPS/NEFT/RTGS as per his/her convenience. All papers send on conference e-mail: nmic.2023.02@gmail.com , admn.isve.ranchi@gmail.com, **iete.isve.vlsi@gmail.com** only. Conference presentations are **online mode** only. If you want special support in publication/accommodation please register in a special academia/industry domain. Letter for oral presentation will be sent after your successful registration.