# GRAPHICAL PASSWORD AUTHENTICATION

**1.M. SWATHI REDDY,2.S NANDHINI,3.MAINAM AJAY,4.MAMILLA RITHWIK REDDY,5.NALLA AKHILA**
[1]Assistant Professor, Department of AIML, SriIndu College Of Engineering & Technology, Hyderabad.
[2,3,4,5]U.G.Scholor, Department of AIML, SriIndu College Of Engineering &Technology, Hyderabad.

**Abstract:** *A pattern-based password is an authentication mechanism in which a user selects images in a specific sequence through a graphical user interface (GUI). This approach is commonly referred to as Graphical User Authentication (GUA). Traditionally, computer systems rely on alphanumeric usernames and passwords for authentication; however, this method has notable limitations. Users often choose simple passwords that are easy to guess, while more complex passwords tend to be difficult to remember, leading to usability and security challenges. To address these issues, researchers have explored authentication techniques that utilize images and colours instead of text. In this paper, a detailed review of existing pattern-based password techniques is presented, along with the introduction of a new conceptual approach. Graphical cryptosystems are considered a promising alternative to conventional text-based authentication, as humans generally find it easier to remember and recognize visual elements such as colours and images compared to textual information. This study provides a comprehensive survey of current graphical password methods, which can be broadly categorized into two types: recognition-based and recall-based approaches. Furthermore, the paper discusses the advantages and limitations of each category and outlines potential future research directions to enhance the effectiveness and security of graphical authentication systems.*

**Keywords:** User Authentication, Memorability, Recognition, Image based Authentication, Pattern based Authentication, Cognitive Psychology, Biometrics, Cued Click Points, Shoulder Surfing, Attack resistance, NodeJs, Hashing, Front-end, Back-end, Image Processing, Data Encryption

## I. INTRODUCTION

In many computer security contexts, User authentication is a crucial element that serves as the foundation for access control and user accountability. Its purpose is to confirm the identity of a user and ensure security that only authorized users have access to sensitive information or resources. [1]There are various types of passwords that are commonly used today, and many of them require the user to either implement recognition or memorability for the correct password. For instance, in a recall-based system, the user needs to remember the password that they created during the registration process in order to regenerate it. On the other hand, the recognition-based technique involves presenting the user with a set of images that they previously selected during registration. The user is then required to identify and confirm their chosen image from the group of images presented to them.

The most common computer authentication method is for a user to submit a user name and a text password. The vulnerabilities of this method have been well known. One of the main problems is the difficulty of remembering passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember. Unfortunately, these passwords can also be easily guessed or broke. To address the problems with traditional username-password authentication, alternative authentication methods, such as biometrics, have been used. In this paper, however, we will focus on another alternative: using pictures as passwords. This paper will be particularly useful for researchers who are interested in developing new graphical password algorithms as well as industry practitioners who are interested in deploying graphical password techniques.

### 1.1 Overview of Authentication Methods

Current authentication methods can be divided into three main areas:

- Token based authentication

- Biometric based authentication
- Knowledge based authentication

Token based techniques, such as key cards, bank cards and smart cards are widely used. Many token-based authentication systems also use knowledge-based techniques to enhance security. For example, ATM cards are generally used together with a PIN number.

Biometric based authentication techniques, such as fingerprints, iris scan, or facial recognition, are not yet widely adopted. The major drawback of this approach is that such systems can be expensive, and the identification process can be slow and often unreliable. However, this type of technique provides the highest level of security.

Knowledge based techniques are the most widely used authentication techniques and include both text-based and picture-based passwords. The picture-based techniques can be further divided into two categories: recognition-based and recall-based graphical techniques. Using recognition-based techniques, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he or she selected during the registration stage. Using recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage.

### 1.2 Graphical Password

Graphical passwords refer to using pictures (also drawings) as passwords. In theory, graphical passwords are easier to remember, since humans remember pictures better than words. Also,they should be more resistant to brute- force attacks, since the search space is practically infinite. In general, graphical passwords techniques are classified into two main categories: recognition-based and recall- based graphical techniques.

With increasing technical advancements, the world is becoming digital at a high pace and everything is happening online. From paying your bills to ticket bookings to paying the person sitting next to you, you prefer to pay online. Not only payments but all activities, be it, communication through e-mails and messaging apps, keeping your documents in a digital locker, etc happen online.

### 1.3 Recognition Based System

In recognition-based techniques, a user is authenticated by challenging him/her to identify one or more images he or she chooses during the registration stage. Recognition- based systems, also known as cognometric systems [2] or searchmetric systems [3], generally require that users memorize a portfolio of images during password creation, and then to log in, must recognize their images from among decoys. Humans have exceptional ability to recognize images previously seen, even those viewed very briefly [4]. According to Renaud [5], there are specific security and usability concerns associated with recognition-based systems. He also provides guidelines for designing recognition-based systems with a focus on usability."The authors Dhamija and Perrig proposed a graphical authentication scheme that uses the Hash Visualization technique. In their system, the user is presented with a set ofrandom pictures and asked to select a certain number of images. Later, during authentication, the user is required to identify the pre-selected images to gain access (as shown in Figure 1.3).

Fig:1.3 Dhamija and Perrig by Recognition based System

### 1.4 Recall Based System

In recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage. Recall-based graphical password systems are occasionally referred to as draw metric systems because users recall and reproduce a secret drawing. In these systems, users typically draw their password either on a blank canvas or on a grid (which may arguably act as a mild memory cue). Recall is a difficult memory task because retrieval is done without memory prompts or cues. Users sometimes devise ways of using the interface as a cue even though it is not intended as such ,transforming the task into one of cued-recall, although one where the same cue is available to all users and to attackers.

## II. RELATED WORK

A literature survey on graphical password authentication would involve a comprehensive review of existing research and publications in the field of graphical password authentication. Here are some examples of relevant studies:

1. Weinshall, D., & Kirkpatrick, A. E. (1999). “Attacking Graphical Passwords. Proceedings of the 1999 IEEE Symposium on Security and Privacy”.
2. Weinshall and Kirkpatrick [1] sketched several authentication schemes, such as picture recognition, object recognition, and pseudo word recognition, and conducted a number of user studies.
3. Xiaoyuan Suo Ying Zhu G. Scott. Owen “Graphical Passwords: A Survey” 21st Annual Computer Security Applications Conference (ACSAC 2005), 5-9 December 2005, Tucson, AZ, USA.
4. The paper discusses the strengths and weaknesses of graphical password systems, as well as potential future research directions. The authors highlight the advantages of graphical passwords in terms of usability, memorability, and user acceptance, as well as their potential to resist dictionary and brute-force attacks.
5. Egelman, S., & Renaud, K. (2008). “Visual Login: Secure and Usable Authentication Based on Image Selection.” In Proceedings of the 2008 Symposium on Usable Privacy and Security (SOUPS 2008) (pp. 1-12). ACM.
6. According to Renaud [3], there are specific security and usability concerns associated with recognition-based systems.
7. "A Survey of Graphical Password Techniques" by SaeidPourroostaeiArdakani, et al. (2015)
8. This paper provides an overview of graphical password techniques, including recognition-based and recall-based systems. It discusses the strengths and weaknesses of these techniques, and provides a comparison of various graphical password schemes.
9. "Human Ability to Grasp Images: Understanding Graphical Passwords" by Rucha Nanavati and H. V. Kul-
10. karni (2015): https://ieeexplore.ieee.org/document/7288627
11. Humans have exceptional ability to recognize images previously seen, even those viewed very briefly.
12. "A Literature Survey on Graphical Passwords" by Mohammadreza Alizadeh and Mohammadreza Bahrami (2016)
13. This study provides a comprehensive review of graphical password authentication schemes, including recognition-based, recall-based, and hybrid approaches. It discusses the advantages and disadvantages of different graphical password techniques and provides recommendations for future research.
14. "Towards More Usable and Secure Graphical Passwords: A Survey" by Yingying Chen and Xinxin Fan (2018)
15. This paper presents a survey of graphical password schemes and discusses the usability and security implications of these techniques. It provides insights into the design of more secure and usable graphical password systems.
16. "User Authentication with Graphical Passwords: A Survey" by Aqeel Mahesri and Hassan Elkamchouchi (2018)
17. This paper provides an overview of the evolution of graphical password authentication, including its history and recent advances. It surveys the existing graphical password schemes, discusses their strengths and limitations, and provides recommendations for designing more secure and user-friendly graphical password systems.
18. Graphical Password Authentication: A Survey" by Rachana Hathi and Sneha Karmarkar (2018):
19. The paper "Graphical Password Authentication: A Survey" by Rachana Hathi and Sneha Karmarkar (2018)
20. provides an extensive review of graphical password authentication methods, which are an alternative to traditional text-based passwords.

21. "A Survey of Graphical Password Authentication Techniques" by G. S. Kumar et al. (2018): https://link.springer.com/chapter/10.1007/978-981-13-1165-9_13
22. The paper presents a survey of graphical password authentication techniques. It provides an overview of various techniques including recognition-based, recall-based, cued-recall, and hybrid techniques.
23. "Security and Usability of Graphical Passwords: A Survey" by Manar Abu Talib and Hazem Hajj (2019)
24. This study reviews the security and usability aspects of graphical passwords. It provides an analysis of the current state-of-the-art in graphical password research and highlights the challenges and open issues in the field.
25. "A Robust Graphical Password Authentication Scheme Using Hybrid Features and Machine Learning Techniques" by C. M. Kumar, R. Latha, and M. SanthiPublished in: IEEE Access, vol. 9, pp. 27025-27035 (2021). This research paper proposes a new graphical password authentication scheme that uses a combination of hy- brid features and machine learning techniques to improve the security and usability of the system. The pro- posed scheme uses a set of images selected by the user as the basis for the password,

### 2.1 Existing System

Graphical password authentication methods can be divided into three categories based on the memory activity required: recognition, recall, and cued recall. Recognition is the easiest method, while pure recall is the most difficult. Cued recall falls in between by providing a cue to trigger memory

1. PassPoints: PassPoints is a graphical password system developed by Dhamija and Perrig in 2000. In this system, users select a series of points on an image to create their password.
2. PassFaces: PassFaces is a graphical password system developed by Real User Corporation. In this system, users select a sequence of faces from a grid of faces to create their password.
3. Cued Click Points: Cued Click Points is a graphical password system developed by Monrose and Rubin in 2000. In this system, users select a sequence of points on an image that are cued by a series of questions.
4. Story-Based Authentication: Story-Based Authentication is a graphical password system developed by Chiasson et al. In this system, users select a sequence of images that tell a story to create their password.

## III. PROPOSED SYSTEM

In graphical authentication there are various techniques to secure your password. Here we are proposing a new algorithm of authentication using images. We used a grid-based approach to authenticate by using image as a reference. Shoulder surfing is a major drawback of graphical password authentication. To overcome this, we have developed SSR (Shoulder Surfing Resistant) shield. The shield containing multiple fake mouse pointers are programmed in such a way that it moves randomly in an image area and the original pointer will look exactly as fake mouse pointers. This shield provides a top layer for grid clicking as well as confusing another person.

At the time of registration, user will upload his/her image or set of images along with all details; then user selected image will appear on the page with transparent grid layer on it. So, user will select certain grids to set his/her password.

### 3.1 Objectives and Purpose

The objective of graphical password authentication is to provide a secure and user-friendly alternative to traditional text-based password authentication. The purpose is to improve the overall security of computer systems and protect sensitive information from unauthorized access by utilizing human visual memory, which is considered to be stronger than traditional text-based passwords.

By using images, users are more likely to remember their password and less likely to write it down or choose weak passwords. Additionally, graphical passwords can be more resistant to guessing attacks and can be tailored to specific user preferences, such as favorite images or personal experiences. Overall, the objective and purpose of graphical password authentication is to enhance the security and usability of password-based authentication systems.

1. Secure way of Login
2. Hassle Free Login
3. Users can protect the data

4. User Friendly

**Features**

There are advanced features of this system:

1. Colour Pattern Password
2. Image Sequencing
3. Data is Encrypted
4. Easily Expandable
5. User friendly
6. User Interface

**Components**

The components of graphical password authentication typically include the following:

1. Registration: This involves the process of user enrolment, where the user selects a set of images or draws apattern to create their graphical password.
2. Login Interface: This is the interface presented to the user during login, which includes a set of images or agrid where the user needs to click or draw their password.
3. Authentication Server: This is the server that validates the user's graphical password during login and grantsaccess if the password is correct.
4. Password Database: This is the database that stores the users' graphical passwords and associated information,such as their username and other authentication data.
5. User Feedback: This includes the feedback provided to the user during password creation and login to ensurethat they are correctly following the process and entering the correct password.

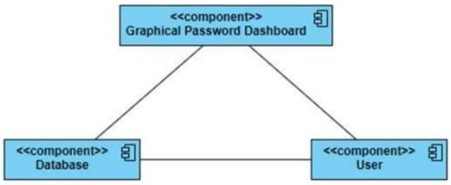


Fig:3.3 Component Diagram for the Graphical Password Authentication

## IV. METHODOLOGY

### 4.1 Model Used in the Project

The Waterfall model for SDLC is useful in graphical password authentication system development because it provides a structured and systematic approach to development. It ensures that each phase of the development process is completed before moving on to the next phase, which helps to minimize errors and ensure that the final product meets the required specifications.

1. Requirements gathering and analysis: This phase involves gathering requirements from stakeholders and analysing them to understand the scope of the project.
2. Design: In this phase, the system architecture and design are created based on the requirements gathered in theprevious phase.
3. Implementation: This phase involves coding and programming the system according to the design specifications and NodeJS and algorithm implementation.
4. Testing: In this phase, the system is tested to ensure that it meets the requirements and specifications.
5. Deployment: This phase involves deploying the system to the production environment and making it availableto end-users.

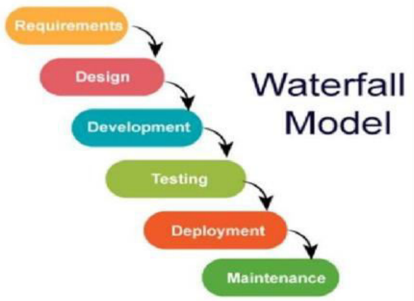


Fig:4.1 Waterfall Method implemented by Proposed System

### 4.2 Algorithms Used In this System

1. Hashing Algorithm: Hashing algorithms play a crucial role in graphical password authentication by securely storing and verifying user passwords.
2. The password entered by the user is converted into a hash value using a hashing algorithm, and the hash value is then stored in the database.
3. During authentication, the entered password is again hashed using the same algorithm and the resulting hash value is compared with the hash value stored in the database.
4. If the two hash values match, the user is granted access, otherwise, access is denied.

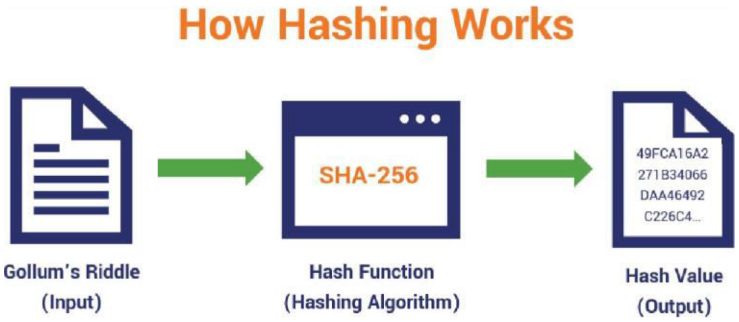


Fig:4.2 Hashing Algorithm used for security and password checking

RGB Colour Pattern Algorithm (using hashing): The RGB colour pattern algorithm in graphical password authentication involves the use of a grid of cells, where each cell is assigned, a unique colour based on the RGB (Red, Green, Blue) colour model.

- During the password creation process, the user selects a sequence of cells, each associated with a specificRGB colour value.
- To log in, the user is presented with a cell, each with a different RGB colour value.
- The user must correctly select the cells in the correct sequence to authenticate.
- The RGB colour pattern algorithm is designed to leverage the human ability to remember colours andtheir associated values, making it a potentially strong and memorable password authentication scheme.

Grid Based Image Sequencing Algorithm (using hashing): Grid-based image sequencing is a graphical password authentication algorithm that requires users to select a sequence of images from a grid. The grid is usually a 2D matrix of images, and users are required to select a specific sequence of images to create their password.

The algorithm typically involves the following steps:

- The user selects a sequence of images from the grid.
- The sequence of images is converted into a password by a hashing algorithm.
- The hashed password is stored on the server.
- During login, the user is presented with the same grid of images and asked to select the images in the correct sequence.
- The user's selected sequence is hashed and compared with the stored hashed password. If the two hashed

passwords match, the user is authenticated and granted access.

### 4.3 Technologies used in the System

NODEJS: NodeJS is a popular server-side runtime environment that can be used for building web applications. To create a graphical password authentication system using NodeJS, you would need to usea combination of front-end technologies, such as HTML, CSS, and JavaScript, and back-end technologies, such as NodeJS, ExpressJS, and a database (e.g., MongoDB, MySQL).

- In this proposed system, users would be prompted to create a graphical password during registration. They would select a set of images from a larger set and arrange them in a particular sequence to create their password.
- To log in, users would be presented with a grid of images and asked to select the images that correspond to their password in the correct sequence.
- On the server-side, the system would use NodeJS and ExpressJSto handle user authentication andvalidation of the graphical password. The system would also need to store user account information, including the graphical password, in a database.

Bootstrap: Bootstrap is a popular front-end framework for building responsive web applications.

- It provides a set of CSS and JavaScript components that can be easily customized and integrated into web pages. In the context of graphical authentication.Bootstrap can be used to design and implement user interfaces for graphical password schemes that are both visually appealing and user-friendly.
- By using Bootstrap's responsive design features, graphical password interfaces can be optimized for different screen sizes and device types, making them accessible to a wider range of users.
- Additionally, Bootstrap provides pre-built UI components such as buttons, forms, and icons that can be used to enhance the user experience of graphical password authentication systems.

Persuasive Cued Click PointsAlgorithm: Users will choose a specific section of an image to verify their identity.

- The persuasive cued click system presents a set of images that can be selected once or multiple times, and they can be selected in any order. The primary benefit of this approach is that users can randomly choose the images without any restrictions.
- The key benefit of PPCP is that attackers have to make more informed guesses. Users are required to select a click point within the highlighted viewport and cannot click outside the viewport unless they choose to shuffle the position of the viewport randomly.
- During password creation, users have the option to shuffle as many times as they want, but it may prolong the password creation process.
- We have implemented this algorithm in level-2, where colours can be chosen randomly and in any number of click points.

Shoulder Surfing Shield Resistant Algorithm:Shoulder surfing is a social engineering tactic used to obtainconfidential information such as passwords, PINs, and other sensitive data by observing the victim'skeystrokes or listening to their conversations.

- The attackers do not require technical expertise to perform this activity and can obtain the information by closely observing the victim's typing patterns and surroundings.
- To counter this problem, the shield algorithm is implemented at level-3. The shield provides an additional layer of security by using grid clicking and confusing another person. In level-3, the images are arranged in a different order to provide an extra layer of security against shoulder surfing attacks.

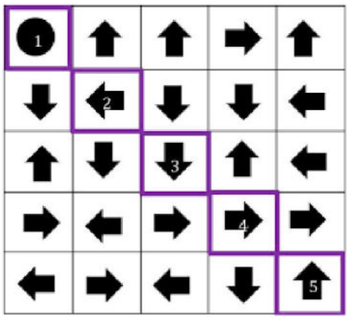


Fig:4.3 Persuasive Cued Click Points used for avoiding Shoulder Surfing

### 4.4 Working

To register a new account, the user must complete three levels of password creation.

- The first level is a text-based password that follows a recall system.
- The second level involves an RGB colour pattern, where the user selects the order of the colours (red, green, and blue), and any colour can be chosen more than once.
- In the third level, the user creates a grid-based image sequencing password using a recall pattern. Once all three passwords are created, they are stored in the database using a hashing algorithm.
- To log in, the user must enter all three passwords, and the hashing algorithm matches the entered passwords with its data. If there is a match, the login is successful; otherwise, an error message is displayed.

### 4.5 Flowchart Representation

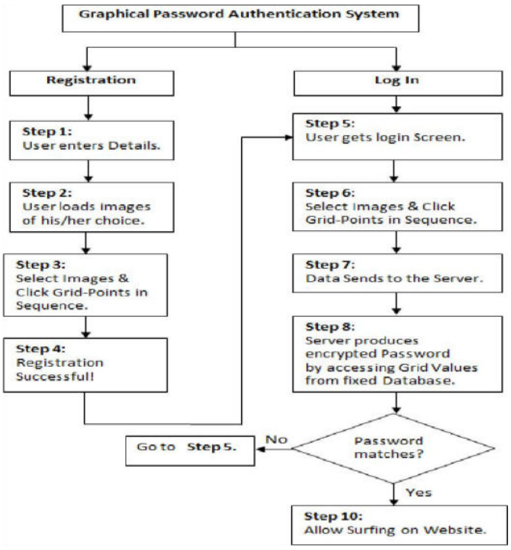

Graphical Password Authentication System
Registration
Log In
Step 1: User enters Details.
Step 2: User loads images of his/her choice.
Step 3: Select Images & Click Grid-Points in Sequence.
Step 4: Registration Successful!
Step 5: User gets login Screen.
Step 6: Select Images & Click Grid-Points in Sequence.
Step 7: Data Sends to the Server.
Step 8: Server produces encrypted Password by accessing Grid Values from fixed Database.
Password matches?
No
Go to Step 5.
Yes
Step 10: Allow Surfing on Website.

Fig:4.4 Usability and Security

As shown in the figure below researchers aretrying to stabilize the goal in text-based system. However, the text-based approach is not able to achieve the goal because as the password strength increases usability decreases.

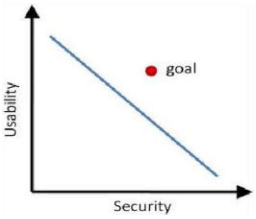


Fig:4.5 System Working Flowchart of the proposed system

## V. RESULTS AND DISCUSSION

### 5.1 Implementation

The implementation method consists of three levels. We created a registration page for new users and a login pagefor existing users. The three-level password authentication system is prioritized according to the application used.

- Level 1 involves a conventional alphanumeric password that consists of letters or numbers.
- Level 2 involves the selection of colours in a specific order during registration and requires the same colour sequence during login.
- Level 3 involves the drag and drop of images into their corresponding grids without any particular sequence.

### 5.2 Results

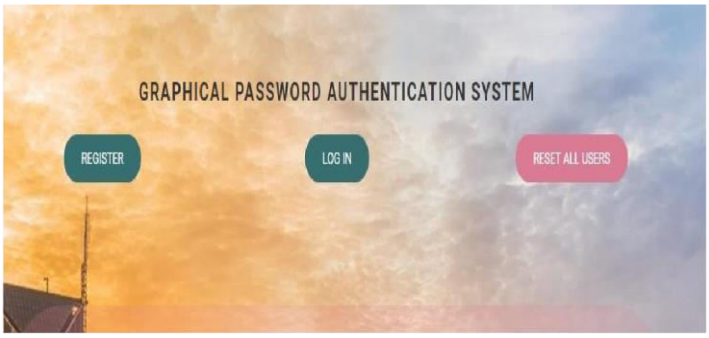
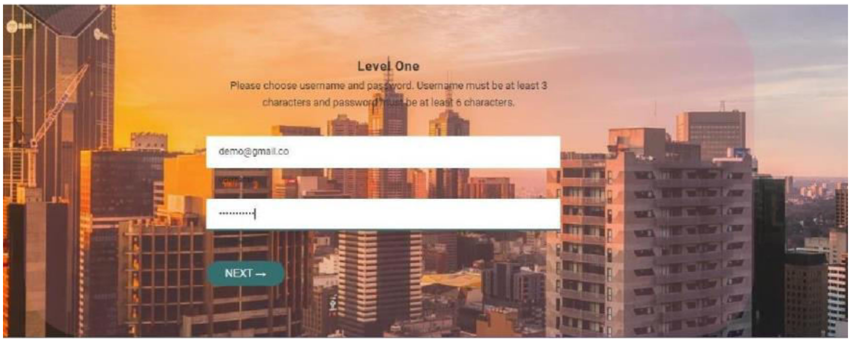


**Fig:5.2.1 USER INTERFACE SCREEN (consists of Register, Login and Reset data)**



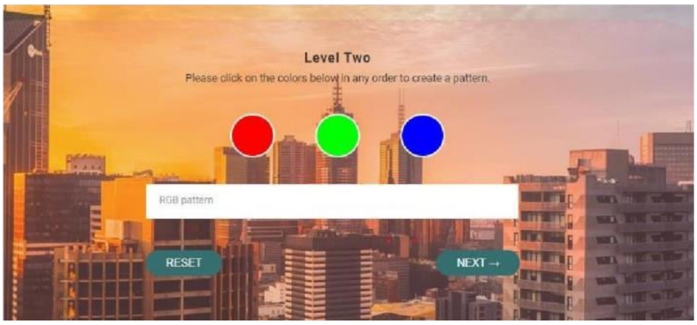
Level One

Please choose username and password. Username must be at least 3 characters and password must be at least 6 characters.

demo@gmail.co

••••••••••

Fig:5.2.2 LEVEL ONE: TEXT PASSWORD(conventional textual password)

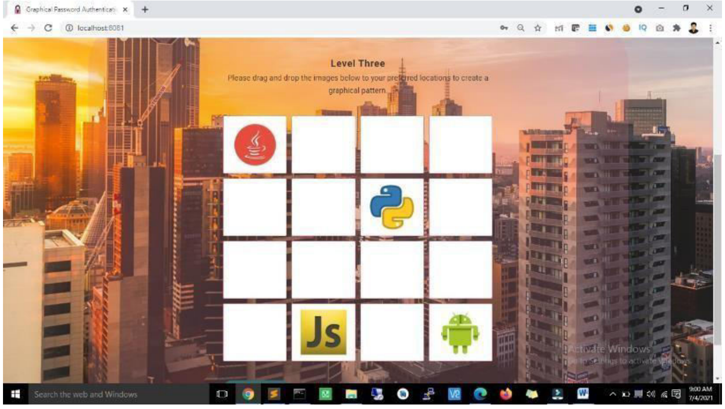


Level Two

Please click on the colors below in any order to create a pattern.

RGB pattern

**Fig:5.2.3LEVEL TWO: RGB PATTERN(selection of colour pattern from red, green and blue.)**



Level Three

Please drag and drop the images below to your preferred locations to create a graphical pattern.

Fig:5.2.4 LEVEL THREE: IMAGE SEQUENCING (selecting images on grid)

## VI. CONCLUSION

The purpose of this abstract is to introduce an improved authentication system that is both user-friendly and resistant to shoulder surfing attacks. The system incorporates both text-based and graphical-based approaches and aims to reduce the memory efforts required by the end-user. The current technological advancements suggest that system security will be a critical aspect of the next era, and graphical passwords may become a prevalent authentication method.

The system is designed as a recognition and recall-based model, making it more usable and secure compared to previous graphical password authentication systems. Its password space is extensive, providing robust security against brute force attacks. Password creation and memorization are easy, and randomization in both authentication steps offers high security against shoulder surfing and other possible attacks

The system can be used for highly secure applications. A future addition to the system could be the implementation of a password retrieval feature through email and mobile messages, ensuring users can receive system updates even when offline.

Overall, the system aims to provide both security and ease of access, with potential future improvements for even greater security.

## VI. FUTURE SCOPE

In Future we will add some more features to our application to make it more secure and useful.

1. Extend this project with any application
2. Addition of OTP verification feature
3. Notification Alert during Login
4. Adding token based (cards) and biometric (like fingerprint or face) authentication techniques. And many more.

## REFERENCES

**[1].** Weinshall, D., & Kirkpatrick, A. E. (1999). Attacking Graphical Passwords. Proceedings of the 1999 IEEE Symposium on Security and Privacy.

**[2].** Xiaoyuan Suo Ying Zhu G. Scott. Owen “Graphical Passwords: A Survey” 21st Annual Computer Security Applications Conference (ACSAC 2005), 5-9 December 2005, Tucson, AZ, USA.

**[3].** Egelman, S., & Renaud, K. (2008). Visual Login: Secure and Usable Authentication Based on Image Selection. In Proceedings of the 2008 Symposium on Usable Privacy and Security (SOUPS 2008) (pp. 1-12). ACM.

**[4].** "A Survey of Graphical Password Techniques" by SaeidPourroostaeiArdakani, et al. (2015)

**[5].** "Human Ability to Grasp Images: Understanding Graphical Passwords" by Rucha Nanavati and H. V. Kulkarni (2015): https://ieeexplore.ieee.org/document/7288627

**[6].** "A Literature Survey on Graphical Passwords" by Mohammadreza Alizadeh and Mohammadreza Bahrami (2016)

**[7].** "Towards More Usable and Secure Graphical Passwords: A Survey" by Yingying Chen and Xinxin Fan (2018)

**[8].** "User Authentication with Graphical Passwords: A Survey" by Aqeel Mahesri and Hassan Elkamchouchi (2018)

**[9].** Saikumar, B. (2023). Enhancing Client Engagement through AI-Driven Real-Time Reporting and Automated Alerts. International Journal of Enhanced Research in Science, Technology &amp; Engineering, 12(11), 111–117. https://doi.org/10.55948/ijerste.2023.1115

**[10].** "A Survey of Graphical Password Authentication Techniques" by G. S. Kumar et al. (2018): https://link.springer.com/chapter/10.1007/978-981-13-1165-9_13

**[11].** "Security and Usability of Graphical Passwords: A Survey" by Manar Abu Talib and Hazem Hajj (2019)

**[12].** "A Robust Graphical Password Authentication Scheme Using Hybrid Features and Machine Learning Techniques" by C. M. Kumar, R. Latha, and M. SanthiPublished in: IEEE Access, vol. 9, pp. 27025-27035 (2021).

**[13].** https://idoc.pub/download/seminar-report-on-graphical-password-authentication-6nq8j11wppnw

**[14].** http://www.geeksforgeeks.com/graphical-password-authentication/

**[15].** https://ieeexplore.ieee.org/document/468240860000

**[16].** https://www.researchgate.net/publication/2210464r4286_Graphical_Passwords_A_Survey

**[17].** https://ieeexplore.ieee.org/abstract/document/5749855000/