

# **“Graphical Password Authentication System”**

**Major Project (Phase-II) Report Submitted**

**To**

**Chhattisgarh Swami Vivekananda**

**Technical University, Bhilai (C.G.), India**



*for*

*The award of the degree*

*of*

**BACHELOR OF TECHNOLOGY**

*in*

**COMPUTER SCIENCE & ENGINEERING**

*By*

**VIVEK YADAV**  
**B.TECH CSE**  
**Roll No.- 303302219123**  
**Enrollment No.- BH3806**

**GAURAV YADAV**  
**B.TECH CSE**  
**Roll No.- 303302219036**  
**Enrollment No.- BH3719**

Under the Guidance of  
**Mrs. Upasana Khadatkar**

Assistant Professor  
Department of Computer Science & Engineering  
S.S.I.P.M.T, Raipur



**Department of Computer Science & Engineering**  
**Shri Shankaracharya Institute of Professional Management &**  
**Technology Raipur (C.G.)**

---

**Session: 2022 – 2023**

---



**DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING**  
**SHRI SHANKARACHARYA INSTITUTE OF PROFESSIONAL**  
**MANAGEMENT & TECHNOLOGY RAIPUR (C.G.)**

---

**DECLARATION BY THE CANDIDATE**

We, the undersigned solemnly declare that the thesis entitled “**Graphical Password Authentication System**” Is based on our work carried out during the course of our study under the supervision of **Mrs. Upasana Khadatkhar**, Asst. Prof., Department of Computer Science and Engineering, Shri Shankaracharya Institute of Professional Management & Technology, Raipur (C.G.), India.

---

VIVEK YADAV  
Roll No.- 303302219123  
Enrollment No.- BH3806

---

GAURAV YADAV  
Roll No.- 303302219036  
Enrollment No.- BH3719



## CERTIFICATE OF THE SUPERVISOR

This is to certify that the incorporation in the thesis “**Graphical Password Authentication System**” is a record of research work carried out by Vivek Yadav, bearing Roll No. 303302219123 Enrollment No. BH3806 and Gaurav Yadav, bearing Roll No. 303302219036 Enrollment No. BH3719, guidance and supervision for the award of the degree of **Bachelor of Technology in Computer Science & Engineering** of Chhattisgarh Swami Vivekanand Technical University, Bhilai (C.G.) India.

To the best of our knowledge and belief the thesis

- I. Embodies the work of the candidate themselves,
- II. Has duly been completed in the specified time,
- III. Fulfil the requirement of the Ordinance relating to the B.Tech. degree of the University and
- IV. Is up to the desired standard both in respect of contents and language for being referred to the examiners.

(Signature of H.O.D.)

Dr. J. P. Patra  
Professor & HOD  
Department of CSE

(Signature of Supervisor)

Mrs. Upasana Khadatkhar  
Assistant professor  
Dept. of CSE

Forwarded to Chhattisgarh Swami Vivekanand Technical University, Bhilai (C.G.)

.....

(Signature of the Principal)

**Dr. Alok Kumar Jain**  
S.S.I.P.M.T, Raipur, C.G



**DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING**  
**SHRI SHANKARACHARYA INSTITUTE OF PROFESSIONAL**  
**MANAGEMENT & TECHNOLOGY RAIPUR (C.G.)**

---

**CERTIFICATE BY THE EXAMINERS**

This is to certify that the project thesis entitled “**Graphical Password Authentication System**” was submitted by Vivek Yadav student of B. Tech. (CSE) (Roll No. 303302219123, Enrollment No. BH3806) and Gaurav Yadav student of B. Tech. (CSE) (Roll No. 303302219036, Enrollment No. BH3719) has been examined by the undersigned as a part of the examination and hereby recommended for the award of the degree of **Bachelor of Technology in Computer Science and Engineering** of Chhattisgarh Swami Vivekanand Technical University, Bhilai (C.G.) India.

---

Internal Examiner

Date:

---

External Examiner

Date:



## ACKNOWLEDGEMENT

The real spirit of achieving a goal is through the way of excellence and serious discipline. We want to thank SSIPMT, Raipur for providing us with the necessary software, tools, and other resources to deliver our major project work.

With gratitude and humanity, we acknowledge our indebtedness to **Mrs. Upasana Khadatkar**, Asst. Prof., SSIPMT, Raipur, under whose guidance we had the privilege to complete this project work. Also, we are grateful to all the faculty members of the department of CSE, who were always there at the need of the hour and provided us with all the help and facility, we required for the completion of our project work.

We shall be failing in our duties if we do not express our duty sense of gratitude towards **Dr. J. P. Patra** Professor & Head of the Department of Computer Science and Engineering SSIPMT, Raipur.

We owe our sincere thanks to **Shri Nishant Tripathi** Chairman (B.G.) SSIPMT, Raipur, **Dr. Alok Kumar Jain**, Principal of SSIPMT, Raipur, for inspiration and constant encouragement that enabled us to present our work in this form.

Our greatest thanks go to our parents and family, who have been our driving force. Our work would not be possible without their constant inspiration, encouragement, support, and love. Above all, we render our gratitude to the almighty, who bestowed self-confidence, Ability, and strength on us to complete this work.

---

VIVEK YADAV  
Roll No.- 303302219123  
Enrollment No.- BH3806

---

GAURAV YADAV  
Roll No.- 303302219036  
Enrollment No.- BH3719



**DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING**  
**SHRI SHANKARACHARYA INSTITUTE OF PROFESSIONAL**  
**MANAGEMENT & TECHNOLOGY RAIPUR (C.G.)**

---

**ACKNOWLEDGEMENT – AICTE IDEA Lab**

We have taken efforts in this project. However, it would not have been possible without the kind support and help of AICTE-IDEA Lab at SSIPMT, Raipur. We would like to extend our sincere thanks to all the gurus, mentors and support staff of Idea lab.

## **ABSTRACT**

**Abstract—** Passwords provide protection to electronic accounts and devices from unauthorized access. This paper proposes a graphical password authentication system that uses a series of images as a password to authenticate users and provides security from brute force, dictionary, key logger and shoulder surfing attacks.

**Keywords:** Graphical Password Authentication, AES.

## Table of contents

Chapter	Title	Page No.
I.	INTRODUCTION	1-14
	1.1 Introduction	1-2
	1.2 Graphical Password	3-14
II.	LITERATURE REVIEW AND PROBLEM IDENTIFICATION	15-23
	2.1 Literature Review	15-20
	2.2 Problem Identification	21-23
III.	METHODOLOGY	24-31
	3.1 Graphical Password Authentication System Methodology	24-27
	3.2 Use Case Diagram	28
	3.3 DFD (Data Flow Diagram)	29
	3.4 Work Flow Diagram	30
	3.5 E-R Diagram	31
IV.	RESULT	32-43
	4.1 Snapshots with Description	32-43
V.	CONCLUSION	44-48
	5.1 Conclusion	44-45
	5.2 Future Scope	46-48
	REFERENCES	49-50
	PAPER PUBLICATION WITH CERTIFICATE	



## List of Figures

Figure No.	Title of figure	Page No.
Figure 3.2	Use Case Diagram	28
Figure 3.3.1	Data Flow Diagram Level 0	29
Figure 3.3.2	Data Flow Diagram Level 1	29
Figure 3.4	Work Flow Diagram	30
Figure 3.5	E-R Diagram	31
Figure 4.1	Home Page	32
Figure 4.2	Register Page	33
Figure 4.3	Home Page (Account Created Successfully)	34
Figure 4.4	Home Page	35
Figure 4.5	Login Page	36
Figure 4.6	Home Page (Login Successfully)	37
Figure 4.7	Login Page (Forgot Password)	38
Figure 4.8	Password Reset Page	39
Figure 4.9	Home Page (Email Sent Notification)	40
Figure 4.10	Password Reset Mail Sent To User	41
Figure 4.11	Password Reset Page (Create New Password)	42
Figure 4.12	Home Page (Password Changed Successfully)	43

# **CHAPTER-1**

---

## **INTRODUCTION**

## 1.1 INTRODUCTION

Authentication is the process of recognizing a user's identity. It is the mechanism of associating an incoming request with a set of identifying credentials. The credentials provided are compared to those on a file in a database of the authorized user's information on a local operating system or within an authentication server.

User authentication is a fundamental component in most computer security contexts. It provides the basis for access control and user accountability.

While there are various types of user authentication systems, alphanumeric username/passwords are the most common type of user authentication. They are versatile and easy to implement and use. Alphanumeric passwords are required to satisfy two contradictory requirements. They have to be easily remembered by a user, while they have to be hard to guess by impostor.

Users are known to choose easily guessable and/or short text passwords, which are an easy target of dictionary and brute-forced attacks.

Enforcing a strong password policy sometimes leads to an opposite effect, as a user may resort to write his or her difficult-to-remember passwords on sticky notes exposing them to direct theft. In the literature, several techniques have been proposed to reduce the limitations of alphanumeric password. One proposed solution is to use an easy to remember long phrases (passphrase) rather than a single word.

Another proposed solution is to use graphical passwords, in which graphics (images) are used instead of alphanumeric passwords.

A graphical user interface (GUI) or graphical user authentication (GUA) is a form of authentication using images rather than letters, digits, or special characters.

The type of images used and the ways in which users interact with them vary between implementations.

In a graphical password authentication system, the user has to select from images, in a specific order, presented to them in a graphical user interface (GUI).

Traditional alphanumeric passwords have been widely used for authentication purposes, but they can be vulnerable to various security threats like dictionary attacks, shoulder surfing, and password reuse. To overcome these limitations, graphical password authentication systems have emerged as an alternative approach that leverages images or visual elements to authenticate users. By utilizing graphical elements, these systems aim to enhance security, improve memorability, and provide a more user-friendly authentication experience.

Graphical password authentication systems offer several advantages over traditional text-based passwords. Firstly, humans tend to have better visual memory than textual memory, making it easier to recall images or patterns compared to complex alphanumeric combinations. Additionally, graphical passwords can offer a higher level of security by incorporating a larger password space and making it more challenging for attackers to guess or crack the passwords.

Graphical password authentication systems also incorporate various security measures to address potential vulnerabilities. These measures can include obscuring images to prevent shoulder surfing, introducing challenges to resist replay attacks, and implementing mechanisms to protect against brute-force attacks. Extensive user studies and iterative design processes are employed to ensure usability and user experience, taking into account factors such as image diversity, cultural neutrality, and accessibility for all user groups.

While graphical password authentication systems offer promising advantages, they are not without challenges. The system needs to strike a balance between security and usability, ensuring that the authentication process is both secure and efficient for users. Additionally, issues like image bias and the need for users to remember their chosen interaction patterns or image sequences pose usability concerns that require careful consideration during system design.

Overall, graphical password authentication systems represent an innovative and potentially more secure approach to user authentication. By leveraging images and visual elements, these systems offer a unique and memorable authentication experience while addressing some of the limitations of traditional text-based passwords. Ongoing research and development in this field continue to refine and improve the effectiveness, usability, and security of graphical password authentication systems.

## **1.2 Graphical Password**

A graphical password is a type of authentication method that uses images or graphical elements instead of traditional text-based passwords. It provides an alternative way for users to authenticate themselves by selecting or interacting with graphical objects on a screen.

The main idea behind graphical passwords is to leverage the human ability to remember images or spatial relationships better than random strings of characters. Users are typically presented with a set of images or a graphical grid and are required to perform specific actions or select specific images in a predetermined sequence to create their password.

There are different types of graphical password schemes, including:

1. Recognition-based: Users are presented with a set of images or icons, and they need to correctly identify or recognize specific images they previously selected during the registration process. For example, users may be asked to identify their chosen "favorite" images from a grid of random images.
2. Recall-based: Users are required to recall and reproduce a specific sequence of actions or selections performed on a graphical grid.
3. Cued-recall: Users are given a set of clues or hints to recall their password. These clues can be related to specific images or the actions performed on a graphical grid.

Overall, graphical passwords offer an alternative approach to traditional text-based passwords, but they come with their own set of advantages and challenges. The effectiveness of graphical passwords depends on the specific implementation and user education on selecting strong, memorable graphical passwords.

When implementing a graphical password system, it is essential to balance usability, security, and accessibility considerations to ensure an effective and secure authentication method for users.

### **1.2.1 Advantages of Graphical Passwords:**

1. Enhanced Memorability: Graphical passwords leverage visual cues, images, or patterns that can be more memorable than traditional text-based passwords. Users may find it easier to recall

a picture or a gesture associated with their password compared to remembering a complex string of characters.

2. Intuitive and User-Friendly: Graphical passwords can be more intuitive for users, especially those who are less technically inclined or have difficulty with text-based passwords. Selecting images or performing gestures can be more engaging and enjoyable, leading to a positive user experience.

3. Increased Resistance to Dictionary Attacks: Text-based passwords are often susceptible to dictionary attacks, where attackers systematically try common words or combinations. Graphical passwords, especially those based on unique images or personalized patterns, can provide better resistance to such attacks, as they are less likely to be found in a pre-existing dictionary of passwords.

4. Potential for Stronger and Longer Passwords: Graphical passwords allow users to create longer and more complex passwords by combining multiple images, positions, or gestures. This can increase the overall entropy of the password, making it more difficult for attackers to guess or crack.

### **1.2.2 Challenges of Graphical Passwords:**

1. Limited Password Space: Graphical password systems typically offer a limited set of images, symbols, or patterns to choose from. This limited password space can lead to weaker passwords if users tend to select common or easily guessable images or gestures.

2. Vulnerability to Shoulder Surfing Attacks: Graphical passwords are more susceptible to shoulder surfing attacks, where an attacker can observe the user's interactions or visually analyze the selected images or patterns. This compromises the confidentiality of the password and increases the risk of unauthorized access.

3. Difficulty in Standardization: Unlike text-based passwords, which have well-established standards for length, complexity, and composition, graphical passwords lack standardized guidelines. This can result in inconsistencies in password creation and difficulty in enforcing strong security practices.

4. Usability and Learning Curve: Introducing a graphical password system requires users to learn and adapt to a new method of authentication. Some users may find it challenging to

understand the rules and constraints associated with graphical passwords, leading to errors, frustration, or lower user acceptance.

5. Potential for Smudge Attacks: Smudge attacks involve analyzing residual marks or smudges left on touchscreens or other input surfaces after a user enters their graphical password. These marks can provide clues or patterns that attackers can exploit to guess or reconstruct the password.

6. System Vulnerabilities: Like any authentication system, graphical password systems are susceptible to various vulnerabilities, including implementation flaws, weak encryption, or improper storage of password data. System vulnerabilities can undermine the overall security and effectiveness of the graphical password authentication mechanism.

It is important to consider these advantages and challenges when implementing or using graphical password systems. User education, system design considerations, and ongoing research can help mitigate the challenges and enhance the security and usability of graphical password authentication.

### **1.2.3 Graphical password authentication system involves the following steps**

#### **1.2.3.1 Registration (Password Creation)**

Password registration typically refers to the process of creating a new account or user profile for a particular service or platform, where a password is required to secure the account. It is a crucial step in setting up a personal or user-specific login credential.

To register a password, you typically follow these steps:

1. Visit the registration page: Access the website, application, or system where you want to create a password. Look for a "Register" or "Sign Up" button/link to initiate the registration process. In the registration page, the user is presented with a registration form that requires them to provide certain information. This may include fields such as name, email address, username, password, and any additional required details specific to the platform.
2. Provide necessary information: Fill out the required information on the registration form. This may include details such as your name, email address, username, and any other relevant information as requested by the system.

(i) Username: A username is a unique identifier chosen by a user during the registration process. It is used to distinguish one user from another within a system or platform. Usernames can be alphanumeric or may allow special characters depending on the platform's rules. Users typically use their usernames to log in to their accounts along with a password. Usernames are often public and may be displayed to others within the system, such as in online communities or forums.

(ii) Email: An email address is a unique identifier associated with an individual's electronic mailbox. During registration, users are typically required to provide an email address, which serves as a means of communication between the system and the user. Email addresses are also used as an alternative or additional identifier for logging in to an account. In many systems, email addresses are not publicly visible and are used for account verification, password reset processes, and sending notifications or updates to the user.

3. Create a password: Create a password that meets the specific requirements set by the system. These requirements may include factors such as minimum length, the use of uppercase and lowercase letters, numbers, special characters, and avoiding easily guessable passwords. It's important to choose a strong password that is difficult for others to guess or crack.

4. Additional security measures: Depending on the system's security policies, you may be required to set up additional security measures such as providing answers to security questions, enabling two-factor authentication (2FA), or verifying your email address or phone number.

5. Review and submit: Once you have provided all the necessary information and set up your password, review the registration form to ensure accuracy. If everything looks correct, submit the form to complete the registration process.

It's crucial to choose a strong and unique password that is not easily guessable. Avoid using common passwords, personal information, or easily guessable patterns. Additionally, consider using a password manager to securely store and manage your passwords.

Remember to follow any specific guidelines or recommendations provided by the system or service you are registering with to ensure your password meets their security standards. Regularly updating your password and being cautious about sharing it with others are also important practices to maintain the security of your account.



### **1.2.3.2 Password Validation**

Password validation is the process of checking whether a password meets certain criteria or requirements set by a system or application. It is an essential aspect of user authentication and helps ensure the security and integrity of user accounts. Password validation typically involves the following considerations:

1. **Length:** The password should meet a minimum length requirement, usually specified by the system. Longer passwords are generally more secure as they increase the complexity and difficulty of guessing or brute-forcing the password.
2. **Complexity:** A strong password should include a combination of different character types, such as uppercase and lowercase letters, numbers, and special characters. This helps increase the password's entropy and makes it harder to guess.
3. **Avoidance of Common Patterns:** Users should be discouraged from using common patterns or sequences, such as consecutive numbers or repeated characters, as they are easier to guess. Password validation may check for such patterns and reject passwords that exhibit them.
4. **Exclusion of Commonly Used or Easily Guessable Passwords:** Password validation should include a list of commonly used or easily guessable passwords (e.g., "password," "123456," etc.) and reject passwords that match these entries. This helps prevent users from selecting weak and easily compromised passwords.
5. **Password History:** Systems may enforce a password history policy that prevents users from reusing their recent passwords. This helps ensure that users regularly choose new and unique passwords, reducing the risk of compromised accounts.
6. **Error Handling:** Password validation should provide clear and specific error messages to users when their chosen password does not meet the requirements. This allows users to understand why their password is being rejected and make the necessary adjustments.
7. **Backend Security:** Passwords should be stored securely in a hashed and salted format to protect them from unauthorized access in case of a data breach. Additionally, secure password transmission protocols, such as HTTPS, should be used when transmitting passwords over the network.

It is important to note that password validation should be implemented alongside other security measures, such as account lockouts after multiple failed login attempts and two-factor authentication, to provide a comprehensive security posture.

Overall, password validation plays a crucial role in ensuring that users create strong and secure passwords. By enforcing specific criteria and educating users about password best practices, systems can enhance the overall security of user accounts and protect against unauthorized access.

### **1.2.3.3 Password Storage**

Storing passwords securely is crucial to protect user accounts and prevent unauthorized access. Here are some commonly used methods for password storage:

1. Hashing: Hashing is a one-way function that takes a password as input and generates a fixed-length string of characters, known as a hash value. The password is transformed using a mathematical algorithm, and the resulting hash is stored in the database. When a user enters their password during authentication, the entered password is hashed and compared to the stored hash. If the hashes match, the password is considered valid. Popular hashing algorithms include bcrypt, PBKDF2, and SHA-256.

2. Salting: Salting is a technique used in conjunction with hashing. A salt is a random value added to the password before hashing. The salt is then stored alongside the hash. Salting adds an extra layer of security by making it computationally expensive for attackers to crack multiple passwords using precomputed rainbow tables or brute force methods. Each user can have a unique salt value.

3. Key stretching: Key stretching is a process that makes the hashing algorithm slower by performing multiple iterations of the hashing function. This slows down attackers attempting to guess passwords through brute force methods. Key stretching algorithms, such as bcrypt and PBKDF2, increase the computational time required to hash a password, making it more difficult to crack.

4. Encryption: Instead of hashing, some systems encrypt passwords before storing them. Encryption uses an algorithm and a secret key to convert the password into ciphertext. Unlike

hashing, encryption allows for the decryption of the password when needed. However, encryption requires additional measures to protect the encryption key.

5. Password hashing frameworks and libraries: Instead of implementing password storage mechanisms from scratch, it's recommended to use well-established password hashing frameworks or libraries provided by reputable security experts. These frameworks handle the complexities of secure password storage, including salting, key stretching, and choosing appropriate hashing algorithms.

It's important to note that storing passwords securely is only one aspect of overall security. It's also crucial to protect against other potential vulnerabilities such as database breaches, secure network communications, and following best practices for secure coding and application development.

Furthermore, users should avoid reusing passwords across multiple accounts, enable additional security measures like two-factor authentication (2FA), and regularly update their passwords for enhanced security.

#### **1.2.3.4 Login (Password Authentication)**

Password authentication is the process of verifying the identity of a user by comparing the provided password with the stored password associated with that user's account. It is a widely used method to protect user accounts and ensure that only authorized individuals can access the system or service.

Here is a general overview of the password authentication process:

1. User Identification: The user provides their username, email address, or any other unique identifier associated with their account. User identification is essential for authentication, authorization, and tracking user interactions within a system.
2. Password Entry: The user enters their password into the designated field. The password is typically masked or hidden to protect it from being visible to others.
3. Password verification: The system takes the provided password and compares it with the stored password associated with the user's account. The stored password is typically hashed or encrypted for security purposes.

4. Hash comparison: If the password is hashed, the system hashes the provided password using the same algorithm and compares the generated hash value with the stored hash value. If the two hashes match, the password is considered valid.

5. Authentication outcome: Based on the comparison result, the system determines whether the password provided by the user is correct or not. If the password matches the stored password, the authentication is successful, and the user is granted access to the system. Otherwise, the authentication fails, and the user may be prompted to re-enter the password or take appropriate action, such as resetting the password.

6. Failed Login Attempts: To prevent brute-force attacks or unauthorized access attempts, systems often implement measures to handle multiple failed login attempts. This can include temporary lockouts, CAPTCHA challenges, or other security mechanisms.

7. Account Recovery: In case the user forgets their password, most systems provide a password recovery or reset option. This typically involves verifying the user's identity through email, security questions, or other predetermined methods. Once the user's identity is confirmed, they can reset their password and regain access to their account.

It's important to note that during the password authentication process, the actual password should not be transmitted or stored in plain text to prevent unauthorized access in case of a data breach. Instead, industry-standard practices involve storing only the hashed or encrypted version of the password and comparing the hashed values.

To enhance password security, users should follow good password hygiene practices, such as using strong and unique passwords for each account, avoiding easily guessable information, regularly updating passwords, and enabling additional security measures like two-factor authentication (2FA).

#### **1.2.3.5 Password Recovery / Reset**

Password reset is a process that allows users to regain access to their accounts when they forget their password or suspect unauthorized access. The password reset process typically involves the following steps:

1. **Initiation:** The user initiates the password reset process by clicking on the "Forgot Password" or a similar link on the login page of the system or application.
2. **User Verification:** To ensure the security of the account, the system usually requires the user to verify their identity. This can be done through various methods, such as sending a verification email to the user's registered email address, sending a verification code via SMS to a linked phone number, or answering security questions.
3. **Verification Code or Link:** The system generates a unique verification code or includes a link in the email or message sent to the user. The user is prompted to enter the code or click on the link to proceed with the password reset.
4. **Password Reset Page:** Upon successful verification, the user is directed to a password reset page. Here, the user can enter a new password for their account. Password requirements and strength indicators may be provided to help users create a strong and secure password.
5. **Password Update:** The user enters their new password in the designated fields on the password reset page. To ensure accuracy and prevent mistakes, some systems may require the user to enter the new password twice.
6. **Password Confirmation:** After the new password is entered and submitted, the system confirms the password update and notifies the user that their password has been changed successfully.
7. **Access Restoration:** With the new password in place, the user can now log in to their account using the updated credentials and regain access to their account.

During the password reset process, it is important for users to follow security best practices, such as choosing a unique and strong password, avoiding the reuse of old passwords, and protecting their account information.

System administrators should implement secure mechanisms for password reset, such as verifying user identity through trusted contact information and providing secure methods for password creation and update. Additionally, they should employ measures to prevent abuse or unauthorized access to the password reset functionality, such as rate limiting or account lockouts after multiple failed attempts.

### **1.2.4 PBKDF2**

PBKDF2 (Password-Based Key Derivation Function 2) is a key derivation function that is commonly used to derive cryptographic keys from passwords. It is designed to be computationally expensive, making it more difficult for attackers to guess passwords through brute-force or dictionary attacks.

The primary purpose of PBKDF2 is to protect the passwords stored in a system by transforming them into a cryptographic key that can be used for encryption or authentication. PBKDF2 applies a pseudorandom function, such as HMAC (Hash-based Message Authentication Code), to repeatedly hash the input password along with a salt value. The salt is a randomly generated value that is unique for each user, preventing attacks that exploit common passwords.

The primary goal of PBKDF2 is to slow down the password hashing process, making it computationally expensive for attackers to attempt a large number of password guesses. By increasing the number of iterations, the computational cost of generating the derived key is increased, which in turn slows down the password cracking process.

The security of PBKDF2 relies on using a sufficiently high number of iterations. However, it is important to balance the desired security level with the performance impact on the system. The number of iterations should be set high enough to provide an adequate defense against password cracking attacks, but not so high that it significantly impacts system responsiveness.

The PBKDF2 algorithm follows these steps:

1. Initialize the pseudorandom function (e.g., HMAC) with the password as the key.
2. Generate the first iteration of the derived key by hashing the salt concatenated with a counter value.
3. Repeat the process for the specified number of iterations, using the previous iteration's result as the input for the next iteration.
4. Concatenate the results of each iteration to obtain the final derived key.

#### **Key derivation process**

The PBKDF2 key derivation function has five input parameters:

$$DK = \text{PBKDF2}(\text{PRF}, \text{Password}, \text{Salt}, c, \text{dkLen})$$

where:

PRF is a pseudorandom function of two parameters with output length hLen (e.g., a keyed HMAC)

Password is the master password from which a derived key is generated

Salt is a sequence of bits, known as a cryptographic salt

c is the number of iterations desired

dkLen is the desired bit-length of the derived key

DK is the generated derived key

Each hLen-bit block  $T_i$  of derived key DK, is computed as follows (with + marking string concatenation):

$$DK = T_1 + T_2 + \dots + T_{\text{dklen}/\text{hlen}}$$

$$T_i = F(\text{Password}, \text{Salt}, c, i)$$

The function F is the xor (^) of c iterations of chained PRFs. The first iteration of PRF uses Password as the PRF key and Salt concatenated with i encoded as a big-endian 32-bit integer as the input. (Note that i is a 1-based index.) Subsequent iterations of PRF use Password as the PRF key and the output of the previous PRF computation as the input:

$$F(\text{Password}, \text{Salt}, c, i) = U_1 \wedge U_2 \wedge \dots \wedge U_c$$

where:

$$U_1 = \text{PRF}(\text{Password}, \text{Salt} + \text{INT\_32\_BE}(i))$$

$$U_2 = \text{PRF}(\text{Password}, U_1)$$

⋮

$$U_c = \text{PRF}(\text{Password}, U_{c-1})$$

For example, WPA2 uses:

$$\text{DK} = \text{PBKDF2}(\text{HMAC-SHA1}, \text{passphrase}, \text{ssid}, 4096, 256)$$

PBKDF2 is widely supported and can be implemented using various cryptographic libraries and programming languages. It is recommended to use a secure hash function, such as SHA-256 or SHA-512, as the underlying pseudorandom function.

The purpose of PBKDF2 is to slow down the password verification process, making it more time-consuming and resource-intensive for an attacker to guess passwords. By increasing the computational cost, PBKDF2 helps to protect against brute-force attacks and provides an additional layer of security for password storage and authentication systems.



## **CHAPTER-2**

---

# **LITERATURE REVIEW AND PROBLEM IDENTIFICATION**

## 2.1 Literature Review

“A Survey on Different Graphical Password Authentication Technique” by Saranya Ramanan, Bindhu J S [1]. In this journal, they explored many algorithms, approaches, and methodologies for graphical password authentication. These methods are divided into four groups: hybrid approaches; cued-recall methods; pure recall methods; and recognition-based methods. Graphical password schemes provide a means to make passwords that are easy for people to remember. The system's safety is extremely exceptional in this. Brute force searches and dictionary attacks are impossible. Images are easier to remember than long text and number sequences. They covered a variety of graphical password related topics to examine different attack patterns on graphical password authentication technique. The graphical password system concept is the primary subject of this publication.

“Enhancement of Password Authentication System Using Graphical Images” by Amol Bhand, vaibhav desale, Swati Shirke, Suvarna Pansambal [2]. It is suggested to improve password authentication systems with the use of graphics (images). The use of cued click points for authentication purposes supports it. The user's engagement with a succession of five images is the core idea behind this system. This system's main objective is to increase security using user-friendly methods that are more difficult for hackers to guess. The most excellent replacement for text passwords is an authentication system that uses graphics. The best replacement for the outdated graphical password system is cued click point (CCP). Pass Matrix is a cutting-edge authentication solution that uses graphical passwords to fend off shoulder surfing assaults.

“A Shoulder Surfing Resistant Graphical Authentication System” by Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh and Chia-Yun Cheng [3]. In this study, a graphic authentication system using a pass matrix was discussed, based on graphical passwords to resist shoulder surfing attacks is proposed. With a one-time valid login indicator and circulate horizontal and vertical bars covering the entire scope of pass-images, Pass Matrix offers no hint for attackers to figure out or narrow down the password even they conduct multiple camera based attacks. Implementation of a Pass Matrix prototype on Android was done and carried out real user experiments to evaluate its memorability and usability. From the experimental result, the proposed system achieves better resistance to shoulder surfing attacks while maintaining usability.

“Graphical Authentication System Using Pass Matrix” Sarojini, Priya, Bhuvaneshwari [4]. Computer security and privacy commonly use authentication-based passwords. The majority of conventional passwords are made up of letters and digits. That is immediately recognizable by those who are not authorized. Attacks that use shoulder surfing start with identification. Human error, such as selecting wrong passwords and entering passwords incorrectly, is a weak point in the process of authentication. People can access these applications anytime, anywhere, and on a variety of devices thanks to the proliferation of online and mobile applications. Pass Matrix presented to solve these issues. They addressed the issue of password failing in this publication.

“When the Password Doesn’t Work: Secondary Authentication for Websites” by Robert Reeder, Stuart Schechter [5]. The article examines secondary authentication methods, highlighting the value of building a toolbox of techniques that satisfy the security and dependability requirements of users. Passwords are used by almost all websites. This sites confirm that a user, who is trying to access an account is the account holder. However, passwords may be forgotten, lost, or stolen, websites must be capable enough to identify a user, who is unable to provide the correct password. For that users need to provide some sort of secondary authentication to demonstrate their identity and regain access to their accounts. There are numerous secondary authentication methods that websites can use.

“Graphical passwords” by G. Blonder [6]. This was the first scheme proposed among graphical password systems. In this scheme, the user is required to click on the pre-selected areas of the previously selected image in a sequence to input the password. Blonder’s technique has many advantages over popular text based passwords. Main advantages are, people find images easier to remember than alphanumeric strings and such password schemes provides more security than text based passwords. However, Blonder’s technique also had some limitations such as predefined regions should be easily identifiable and the number of predefined regions is small, sometimes a few dozen in an image. The password may require many clicks to enhance the security, so it will become a tedious task for the users and it is more prone to shoulder surfing attacks when compared to text based passwords.

“A new algorithm on Graphical User Authentication (GUA) based on multi-line grids” by Lashkari, A. H., Gani, A., Sabet, L. G., & Farmand, S. [8]. Seven Pure Recall-Based and five Cued Recall-Based graphical password authentication algorithms were reviewed in this study. From all these algorithms we were able to come up with a number of shortcomings that can

allow attacks to be perpetuated. Therefore, it can be concluded that the most common Lacks on the nine algorithms were, Due to users frequently being fascinated by pictures drawn by other users the common picture for passwords became obvious. After some time has elapsed users tend to forget the drawing sequence that they had used. Typically users have a tendency to choose weak passwords which are vulnerable to the graphical dictionary attack. The use of a mouse as a drawing input device for graphical password is not common. It is not easy to commit to memory and use some of the algorithms. The choice of weak passwords leads to passwords that are easily guessable or predictable. After this a GUA attack patterns survey was done in an attempt to make a comparison table for recall-based algorithms based on attack patterns. As part of future works, an algorithm that is resistant to most of the shortcomings mentioned in this paper will be proposed and developed. In conclusion, our newly proposed algorithm for a graphical password is based on multi size grids used during the login phase.

“Graphical Password Authentication Techniques: A Review” by Aakansha Gokhale, & Vijaya Waghmare [9]. Having studied different recent graphical password authentication techniques and subjecting them for usability features that is memorability, creation time and login time and comparing the security features of each of them by considering their password space (complexity), dictionary attack, shoulder surfing and brute force attack. Every method has good resistance to various password attacks, but not a single method is perfect with subject to usability. The future work is to balance the trade-off between Usability and Security.

“Guidelines for designing graphical authentication mechanism interfaces” by K. Renaud [10]. In the last few years a number of innovative graphical authentication mechanisms, which use pictures instead of alphanumeric strings, have been proposed. There is long-standing evidence that people remember pictures far better than they remember alphanumeric strings, so in terms of easing the memory load, pictures seem to offer a viable alternative. However, what is emerging from current research is that the design of such a graphical authentication mechanism interface can either make or break it, both in terms of security and usability. This paper will discuss various design options and make recommendations about how such systems should be designed in order to make them maximally efficacious while considering the level of risk associated with the resource being protected by the mechanism.

“Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems” by Antonella De Angeli, Lynne Coventry, Graham Johnson, Karen Renaud [11]. This paper reports two user studies comparing several implementations of the

graphical approach with PINs. Results demonstrate that pictures can be a solution to some problems relating to traditional knowledge-based authentication but that they are not a simple panacea, since a poor design can eliminate the picture superiority effect in memory. The paper concludes by discussing the potential of the graphical approach and providing guidelines for developers contemplating using these mechanisms.

“Improving password security and memorability to protect personal and organizational information” by K. P. L. Vu, R. Proctor, A. Bhargav Spantzel, B. L. Tai, J. Cook, and E. Schultz [12]. The present study evaluated the time and number of attempts needed to generate unique passwords satisfying different restrictions for multiple accounts, as well as the login time and accuracy for recalling those passwords. Imposing password restrictions alone did not necessarily lead to more secure passwords. However, the use of a technique for which the first letter of each word of a sentence was used coupled with a requirement to insert a special character and digit yielded more secure passwords that were more memorable.

“Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice” by Susan Wiedenbeck, Jim Water, Jean-Camille Birget, Alex Brod-skiy, Nasir Memon [13]. The human factors testing was expanded by studying two issues: the effect of tolerance, or margin of error, in clicking on the password points and the effect of the image used in the password system. The results show that accurate memory for the password is strongly reduced when using a small tolerance (10x10 pixels) around the user’s password points. This may occur because users fail to encode the password points in memory in the precise manner that is necessary to remember the password over a lapse of time. In this image study compared user performance on four everyday images. The results indicate that there were few significant differences in performance of the images. This preliminary result suggests that many images may support memorability in graphical password systems.

“Analysis and Design of Graphical Password Techniques” Xiaoyuan Suo, Ying Zhu & G. Scott Owen [14]. In this paper, they conduct a comprehensive study of the existing graphical password techniques. They propose the first taxonomy for graphical passwords methods and discuss the important elements in designing them. They present a mathematical analysis of the graphical password space.

“A Study of Graphical Password for Mobile Devices” by Xiaoyuan Suo [15]. The objective of this project is to conduct a comprehensive research into the usability; design and security of

graphical password on touch screen devices. They address the design limitation of touch screen devices and possible solutions. They also propose a simple graphical password scheme designed specifically for touch screen devices. Further, expert reviews and usability studies were used to explore user interactions in order to gain a more complete understanding on the potentials to improve the graphical password design for touch screen mobile devices.

“Password Recovery Using Graphical Method” Wafa Mohd Kharudin, Nur Fatehah Md Din & Mohd Zolisham Jali [16]. In this paper they studied on password recovery using graphical images. Authentication with images or better known as graphical password is gaining its recognition as an alternative method to authenticate users, for it is claimed that images or pictures are easier to use and remember. The same method can be applied to password recovery, with the purpose to ease the process of users in regaining their account in case of forgotten passwords. A total of 30 participants were asked to use a prototype implementation of graphical password recovery and provide feedbacks. The data gained were analyzed in terms of attempts, timing, pattern, and user feedback. Overall, it was found that participants had no problem in using graphical password recovery despite they were new to it. Most of them preferred the choice-based method, even though they agreed that it provided less security. Graphical recovery has potential to be used more widely in current technology, although more works need to be done to balance the issues of usability and security.

“Authentication Schemes - Comparison and Effective Password Spaces” Peter Mayer, Melanie Volkamer & Michaela Kauer [17]. This paper presents a comparative study in which all schemes are configured to the same effective password space (as used by large Internet companies). The experiment includes both, cued-recall-based and recognition-based schemes. The results demonstrate that recognition-based schemes have the upper hand in terms of effectiveness and cued-recall-based schemes in terms of efficiency. Thus, depending on the scenario one or the other approach is more appropriate. Both types of schemes have lower reset rates than text passwords which might be of interest in scenarios with limited support capacities.

“User Authentication with Graphical Passwords using Hybrid Images and Hash Function” by Sachin Davis Mundassery & Sreeja Cherillath Sukumaran [18]. In this paper, it is shown as per human psychology, people remember visual objects more than texts. Although many user authentication mechanisms are based on text passwords, biometric characteristics, tokens, etc., image passwords have proven to be a substitute due to its ease of use and reliability. The

technological advancements and evolutions in authentication mechanisms brought greater convenience but increased the probability of exposing passwords through various attacks like shoulder-surfing, dictionary, key-logger, and social engineering attacks. The proposed methodology addresses these vulnerabilities and ensures to keep up the usability of graphical passwords. The system displays hybrid images that users need to recognize and type the randomly generated alphanumeric or special character values associated with each of them. A mechanism to generate One Time Password (OTP) is included for additional security. As a result, it is difficult for an attacker to capture and misuse the password.

“A Hybrid Graphical Password Based System” by Wazir Zada Khan, Yang Xiang, Mohammed Y. Aalsalem & Quratulain Arshad [19]. In this age of electronic connectivity, where we all face viruses, hackers, eavesdropping and electronic fraud, there is indeed no time when security is not critical. Passwords provide security mechanism for authentication and protection services against unwanted access to resources. A graphical based password is one promising alternatives of textual passwords. According to human psychology, humans are able to remember pictures easily. In this paper, we have proposed a new hybrid graphical password based system, which is a combination of recognition and recall based techniques that offers many advantages over the existing systems and may be more convenient for the user. Our scheme is resistant to shoulder surfing attack and many other attacks on graphical passwords. This resistant scheme is proposed for small mobile devices (like smart phones i.e. ipod, iphone, PDAs etc) which are more handy and convenient to use than traditional desktop computer systems.

“Graphical Password Using an Intuitive Approach” by Rajat Mahey, Nimish Singh, Chandan Kumar, Nitin Bhagwat & Poonam Verma [20]. In this paper it is studied that users generally tend to select passwords that are easier to recall and shorter in length. This, though, makes them vulnerable to cracking attempts. A graphical password is a confirmation framework that works by having the client select pictures, in a particular order. Graphical passwords have inherent advantages over conventional textual password schemes. In this paper, we propose one such graphical password methodology which makes use of the distinct shape, color, and type of image a user chooses, for the purpose of authentication.

## 2.2 Problem Identification

Passwords play a huge role in keeping your data safe online as well as offline platforms. Passwords are the default method of authentication to get access to our accounts.

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.

With everything turning online, the risk of cybercrimes and privacy breaches is also increasing. Passwords play a huge role in keeping your data safe online as well as offline platforms. Passwords are the default method of authentication to get access to our accounts.

Considering the traditional username-password authentication, the alphanumeric passwords are either easy to guess or difficult to remember.

Also, users generally keep the same passwords for all their accounts because it is difficult to remember a lot of them. Alternative authentication methods, such as biometrics, graphical passwords are used to overcome these problems associated with the traditional username-password authentication technique.

The alphanumeric passwords can be easily cracked by guessing, permutations and combinations. Also, users generally keep the same passwords for all their accounts because it is difficult to remember a lot of them.

So to increase the security of the system, we are here introducing a graphical password authentication system.

There are several reasons why graphical password authentication systems are considered as an alternative to alphanumeric passwords:

1. Enhanced Memorability: Graphical passwords leverage visual cues, such as images or gestures, which can be more memorable than traditional alphanumeric passwords. Users may find it easier to recall a picture or a specific gesture associated with their password compared to remembering a complex string of characters.



2. **Resistance to Dictionary Attacks:** Alphanumeric passwords are often susceptible to dictionary attacks, where attackers systematically try common words or combinations. Graphical passwords, especially those based on unique images or personalized patterns, can provide better resistance to such attacks, as they are less likely to be found in a pre-existing dictionary of passwords.
3. **Usability and User Experience:** Graphical passwords can offer a more intuitive and user-friendly experience. Users tend to be more engaged and satisfied when interacting with visual elements and performing gestures rather than entering text-based passwords. This can lead to a positive user experience and reduce the likelihood of errors or frustration during the authentication process.
4. **Potential for Stronger and Longer Passwords:** Graphical password systems allow users to create longer and more complex passwords by combining multiple images, positions, or gestures. This can increase the overall entropy of the password, making it more difficult for attackers to guess or crack.
5. **Diversity and Customization:** Graphical passwords offer a wide range of options for users to choose from, including images, symbols, or gestures. This diversity allows users to create passwords that are unique and personalized to their preferences. It also provides flexibility for individuals who may have difficulty remembering or typing text-based passwords.
6. **Security through Obscurity:** Graphical passwords can provide security through obscurity by obfuscating the password input. Unlike alphanumeric passwords that reveal the characters as they are entered, graphical passwords keep the authentication process visually concealed, making it harder for shoulder surfers or unauthorized individuals to observe or guess the password.
7. **Cultural and Language Independence:** Alphanumeric passwords can sometimes be language-specific, making it difficult for users who are not fluent in a particular language to create or remember passwords. Graphical passwords, on the other hand, are often language-independent and can be equally understood and used by individuals from various cultural and linguistic backgrounds.

8. Accessibility: Graphical passwords may be advantageous for individuals with certain disabilities or impairments that make typing alphanumeric passwords challenging. By utilizing visual elements, such as selecting images or drawing patterns, graphical passwords can provide a more accessible authentication option.

However, it is important to note that graphical password authentication systems also have their own challenges and vulnerabilities. The selection of weak or easily guessable images, the potential for smudge attacks, and the need for user education and training are factors that should be addressed when implementing and using graphical password systems.

## **CHAPTER-3**

---

### **METHODOLOGY**

### 3.1 Graphical password authentication system Methodology

Graphical password authentication systems rely on visual images as a means of authentication instead of traditional alphanumeric passwords. The methodology of a graphical password authentication system typically involves the following steps:

**3.1.1 Registration:** Password registration typically refers to the process of creating a new account or user profile for a particular service or platform, where a password is required to secure the account. It is a crucial step in setting up a personal or user-specific login credential.

During the registration process, the user creates a graphical password. This password can be a series of images. The user may be provided with a set of images to choose.

1. Username or Email Address: Username or email address refers to the information that uniquely identifies a user on a particular platform, service, or website. It serves as a means of identification and helps differentiate one user from another. A username can be a custom name, often alphanumeric, that represents the individual within the system. Usernames are typically publicly displayed and used for communication or identification purposes within the platform's community. For example, on social media platforms, usernames are often used as handles or screen names. An email address consists of two main parts: a username (before the "@" symbol) and a domain name (after the "@" symbol). Email addresses are associated with specific email services or providers, such as Gmail, Yahoo, or Outlook. They serve as a means of sending and receiving electronic messages and are often used as a primary method of contact and account verification.

2. Password Creation: A password is a confidential and personalized combination of characters that serves as a security measure to protect the account from unauthorized access. The user creates a graphical password by selecting images. At the time of registration, the system will display a 3\*3 grid consist of 9 images for password. Each thumbnail image is assigned a numerical value, and the sequence of selection will generate a numerical password. A user creates a graphical password by selecting 3 images from a 3\*3 grid. The system records the password securely, often by generating a cryptographic hash or a template that represents the password.

3. Review and submit: Once you have provided all the necessary information and set up your password, review the registration form to ensure accuracy. If everything looks correct, submit the form to complete the registration process.

4. Password Validation: Password validation is the process of checking whether a password meets certain criteria or requirements set by a system or application. It is an essential aspect of user authentication and helps ensure the security and integrity of user accounts.

4. Password storage: The system securely stores the user's graphical password information, typically by encrypting or hashing it. This ensures that even if the stored data is compromised, it is difficult for an attacker to determine the original password.

It is important to choose a strong and unique password during registration and to keep it confidential to protect the account from unauthorized access or security breaches. Additionally, regularly updating and changing passwords can enhance security and reduce the risk of compromise.

**3.1.2 Login:** Password login is the process of accessing an account or user profile on a particular platform or service by providing a valid username or email address along with the corresponding password. It is the authentication mechanism that verifies the identity of the user and grants access to the account.

Here's how password login works:

1. User Identification: The user enters their registered username or email address into the login form on the platform or service's login page.

2. Password Entry: During the authentication, the user must enter the registered images in the correct sequence to successfully login.

3. Authentication: When the user attempts to log in, the system prompts them to enter their graphical password. The user interacts with the system by selecting specific images that matches their registered password.

4. Password comparison: The system compares the entered graphical password with the stored password information. This comparison can involve various techniques, such as comparing image features, analyzing the drawn pattern, or matching templates or hashes.

5. Authentication decision: Based on the comparison result, the system determines whether the entered graphical password matches the stored password. If there is a match, the user is granted access; otherwise, the authentication fails.

6. Account Access: If the authentication process is successful, the user gains access to their account and can proceed to utilize the features and functionalities available within the platform or service.

7. Failed Login Attempts: To prevent brute-force attacks or unauthorized access attempts, systems often implement measures to handle multiple failed login attempts. In Graphical password authentication system, the user will be notified via message through email. And the further authentication through the generic URL/website is disabled for that user account, instead, they have to use the link that will be sent by the company in the notification email. This also lets the legitimate user know about the adversary.

8. Account Recovery: In case the user forgets their password, most systems provide a password recovery or reset option. This typically involves verifying the user's identity through email, security questions, or other predetermined methods. Once the user's identity is confirmed, they can reset their password and regain access to their account.

Password login is a common method used to protect user accounts and ensure that only authorized individuals can access the associated information and services. It relies on the principle that the password is known only to the account owner and serves as a means of verifying their identity. To maintain account security, it is important for users to choose strong passwords, keep them confidential, and avoid sharing them with others. Regularly updating passwords and using additional security measures can further enhance the security of the login process.

**3.1.3 Password Recovery / Password Reset:** Password reset refers to the process of regaining access to an account or user profile when the password associated with the account has been forgotten, compromised, or needs to be changed for security reasons. It allows users to reset their password to a new one, granting them the ability to log in and access their account again.

Here's a general overview of how the password reset process typically works:

1. Initiation: The user initiates the password reset process by clicking on the "Forgot password" or a similar link on the login page of the platform or service.
2. Identity Verification: To ensure the security of the account, the user is usually required to provide some form of identification. This could involve entering the registered email address, answering security questions, or confirming other personal information associated with the account.
3. Reset Instructions: Once the user's identity is verified, the system sends a password reset link or instructions to the registered email address. This link is often time-limited and valid for a specific period.
4. Setting a New Password: The user clicks on the password reset link provided in the email and is directed to a secure webpage where they can enter a new password. The system will display a 3\*3 grid consist of 9 images for new password. Each thumbnail image is assigned a numerical value, and the sequence of selection will generate a numerical password. A user creates a new graphical password by selecting 3 images from a 3\*3 grid. The system records the password securely, often by generating a cryptographic hash or a template that represents the password.
5. Password Update: After entering the new password, the system updates the account's password information, associating the new password with the user's account.
6. Password Confirmation: After the new password is entered and submitted, the system confirms the password update and notifies the user that their password has been changed successfully.
7. Account Access Restoration: With the new password in place, the user can now log in to their account using the updated credentials and regain access to their account.

The password reset process is designed to provide account security and ensure that only authorized individuals can regain access to their accounts. It is important to follow the recommended practices for creating strong and unique passwords during the password reset process to enhance account security. Additionally, it is advisable to regularly update passwords and enable additional security measures, such as two-factor authentication, to further protect user accounts.

### 3.2 USECASE DIAGRAM

A use case is a methodology used in system analysis to identify, clarify and organize system requirements. The use case is made up of a set of possible sequences of interactions between systems and users in a particular environment and related to a particular goal. The method creates a document that describes all the steps taken by a user to complete an activity.

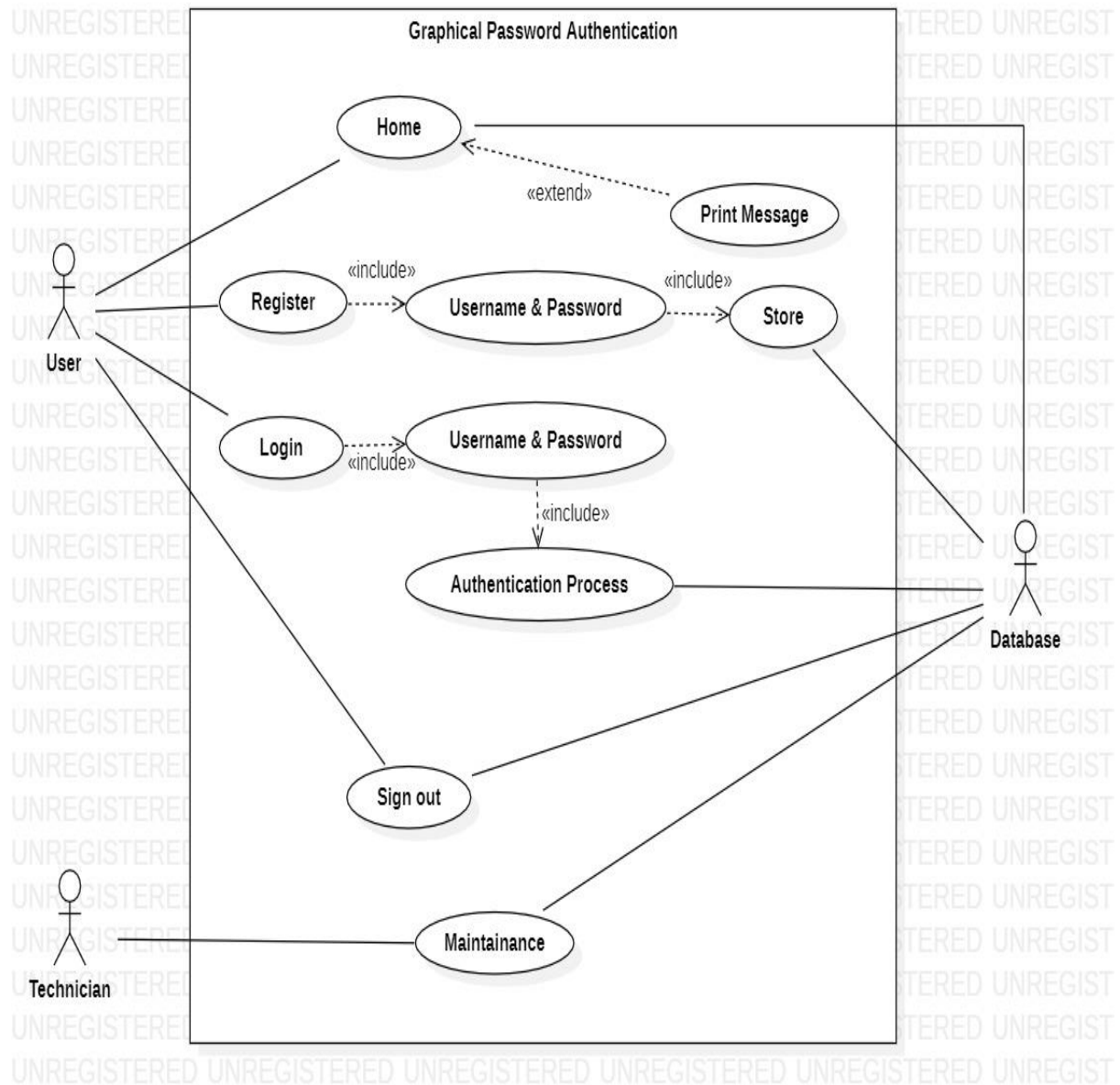


Figure 3.2 USECASE Diagram



### 3.3 DFD (DATA FLOW DIAGRAM)

Data flow diagrams are used to graphically represent the flow of data in a business information system. DFD describes the processes that are involved in a system to transfer data from the input to the file storage and reports generation. Data flow diagrams can be divided into logical and physical. Data flowcharts can range from simple, even hand-drawn process overviews, to in-depth, multi-level DFDs that dig progressively deeper into how the data is handled. They can be used to analyze an existing system or model a new one.

#### 3.3.1 DFD Level 0:-

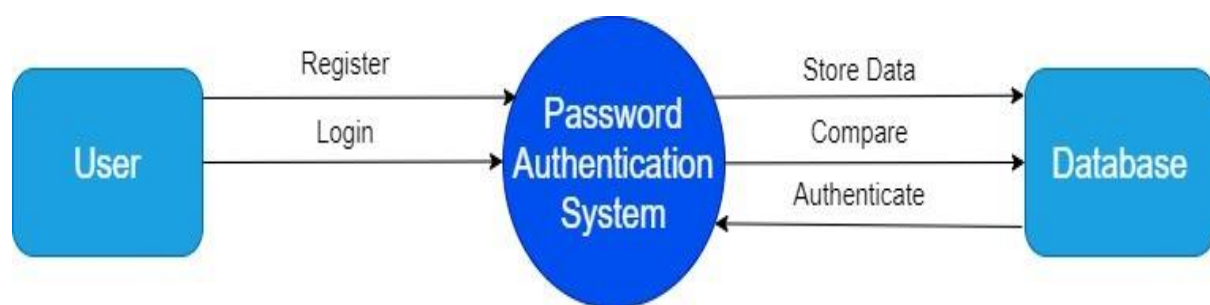


Figure 3.3.1 DFD Level 0

#### 3.3.2 DFD Level 1:-

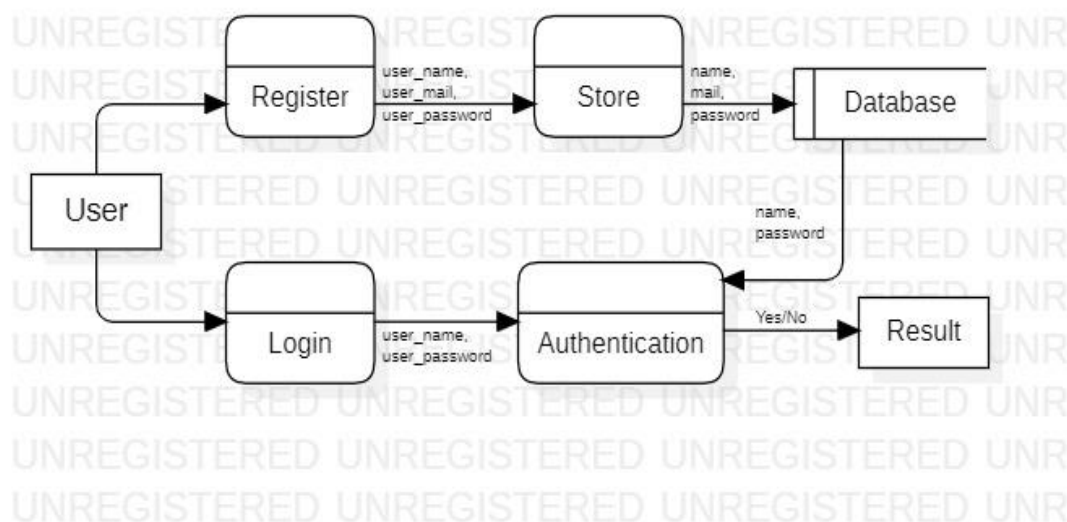


Figure 3.3.2 DFD Level 1

### 3.4 WORK FLOW DIAGRAM

A workflow diagram is a visual representation of a business process (or workflow), usually done through a flowchart. It uses standardized symbols to describe the exact steps needed to complete a process, as well as pointing out individuals responsible for each step. The “workflow” as we know today can be traced back to two American mechanical engineers, Henry Gantt and Frederick Wilson Taylor. Both were known for their contributions towards the development of scientific management.

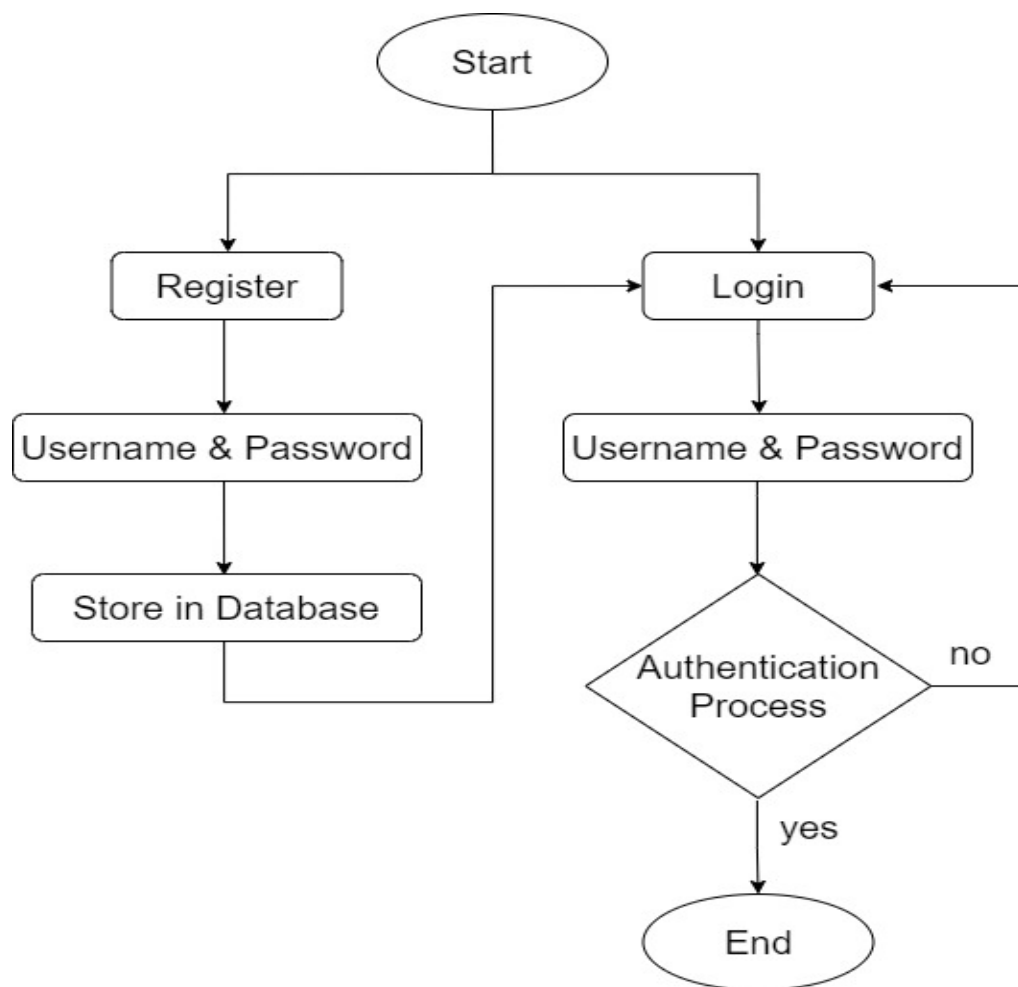


Figure 3.4 Work Flow Diagram

### 3.5 E-R DIAGRAM

The Entity Relationship Diagram explains the relationship among the entities present in the database. ER models are used to model real-world objects like a person, a car, or a company and the relation between these real-world objects. In short, ER Diagram is the structural format of the database.

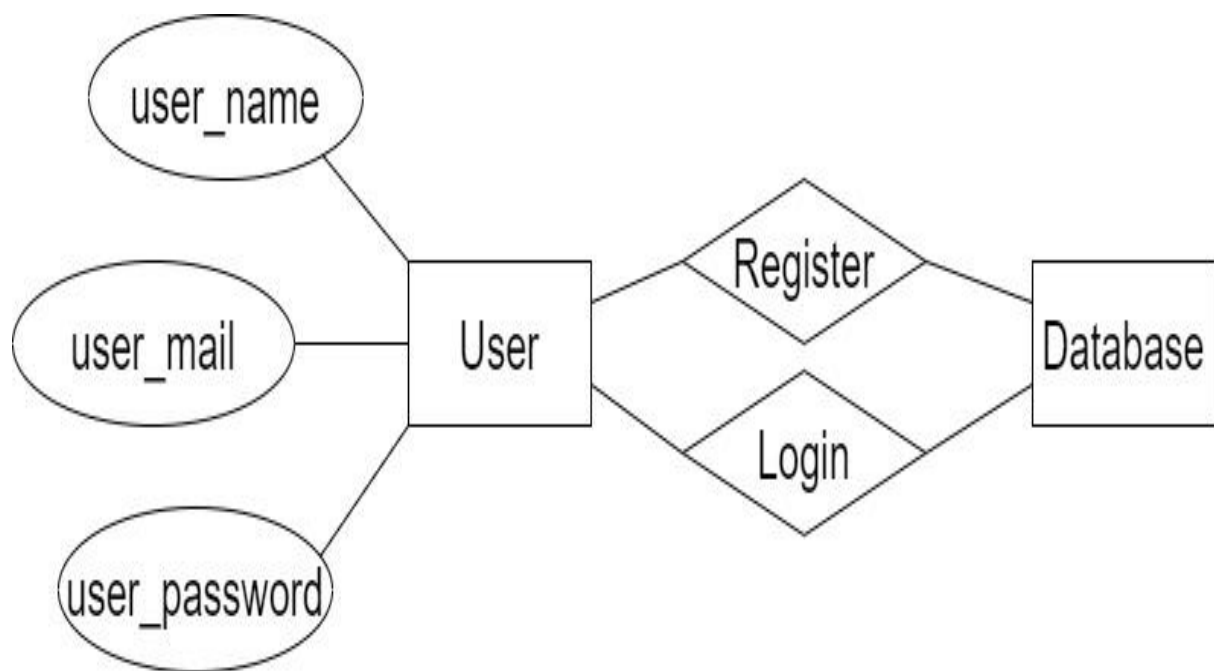


Figure 3.5 E-R Diagram

## **CHAPTER-4**

---

### **RESULT**

## 4.1 Snapshots with Description

Steps in Graphical Password Authentication Process is as follows

Step 1:- User has to open the browser.

Step 2:- In the browser User has to open Graphical Password Authentication page.

Step 3:- First user has to register themselves.

Step 4:- Click on “**Register**”.

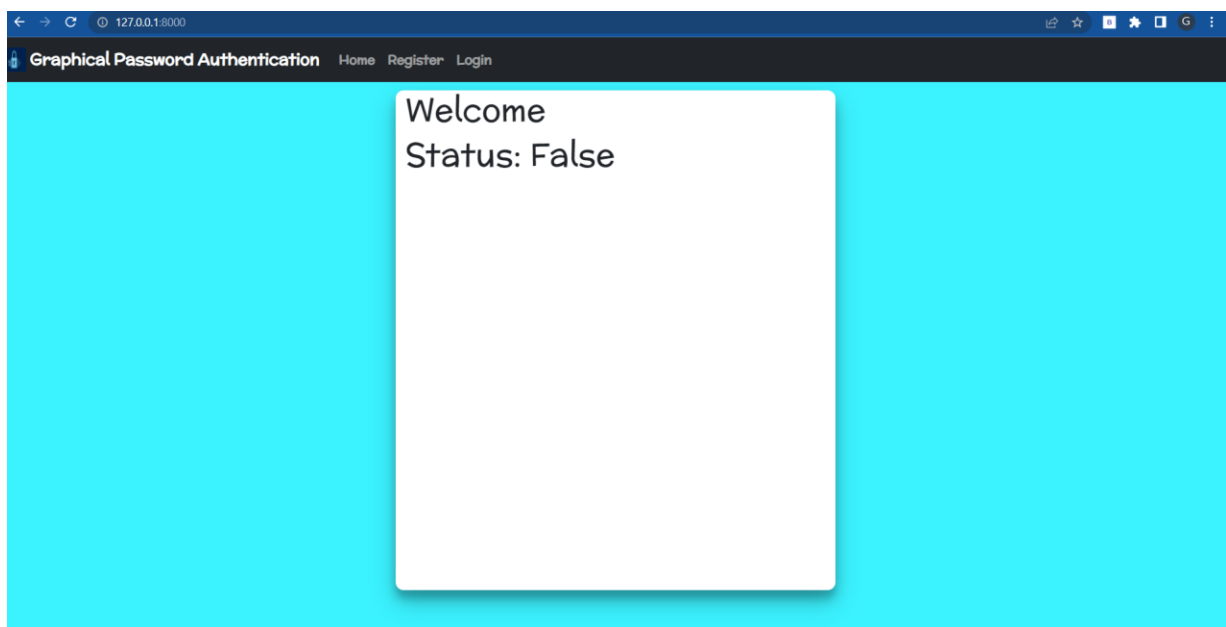


Figure 4.1 Home page

Step 5:- User will see the Register page.

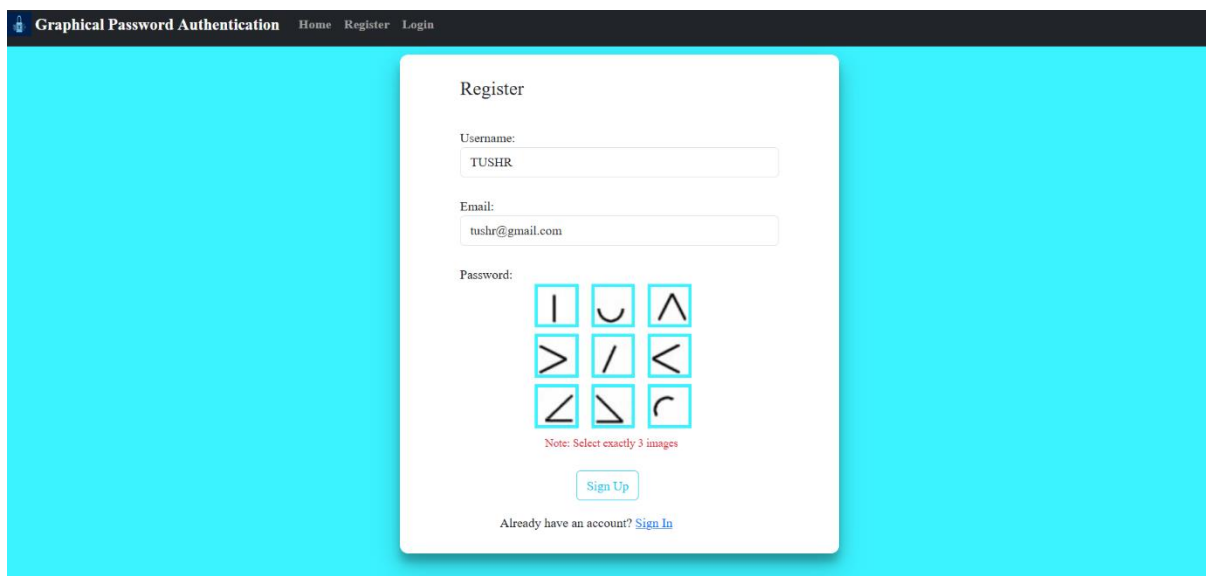
Step 6:- User has to fill the Basic details required to proceed.

i) Enter the Name.

ii) Enter the Email.

iii) Create a Password (User has to select exactly 3 images in a specific order as a password).

Step 7:- Then click on “**Sign Up**”.



The screenshot shows a web application titled "Graphical Password Authentication" with a navigation bar containing "Home", "Register", and "Login". The main content area is a light blue gradient. In the center, there is a white "Register" form. The form contains three input fields: "Username:" with the value "TUSHR", "Email:" with the value "tushr@gmail.com", and "Password:". The password field is a 3x3 grid of nine square boxes, each containing a different black graphical symbol. Below the grid, a red note states "Note: Select exactly 3 images". At the bottom of the form is a blue "Sign Up" button. Below the button, it says "Already have an account? [Sign In](#)".

Figure 4.2 Register page

Step 8:- User will be notified as “**Account created successfully**”, if the account with the same name already exists user will get the notification “**Username already exist**”, in this case user has to register himself/herself again with a different username.

Step 9:- After successfully account creation user will be redirected to home page.

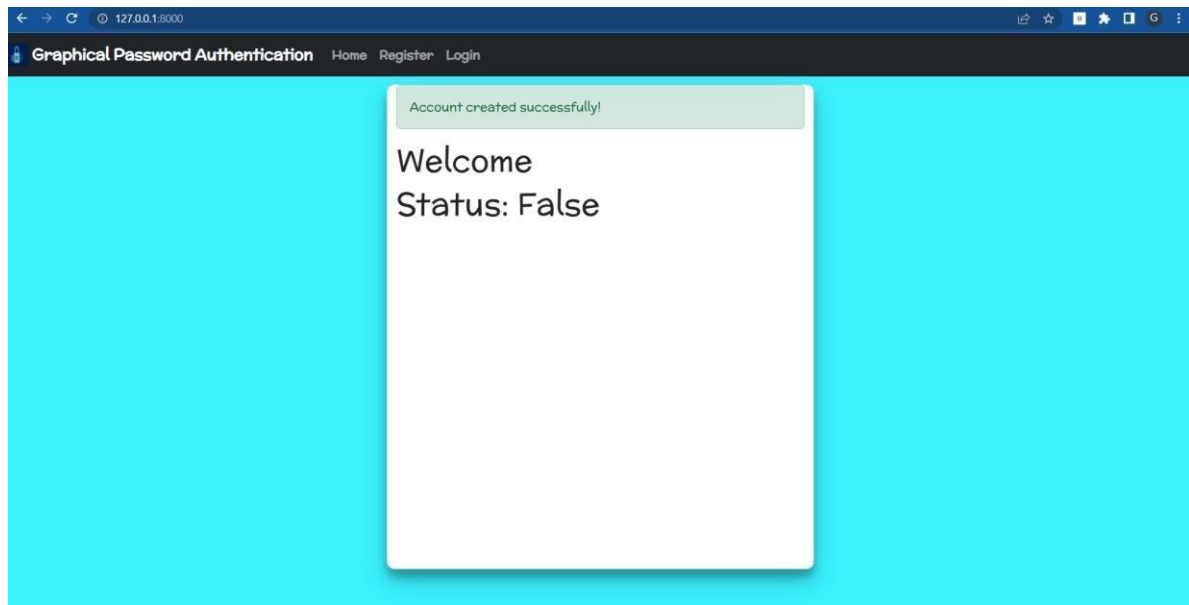


Figure 4.3 Home page (Account created successfully)

Step 10:- If new User has Enter the site then user has to repeat the above steps (steps 4-8).

If the user has already registration himself/herself, then go to the next step.

Step 11:- Click on “**Login**” that is at top right corner.

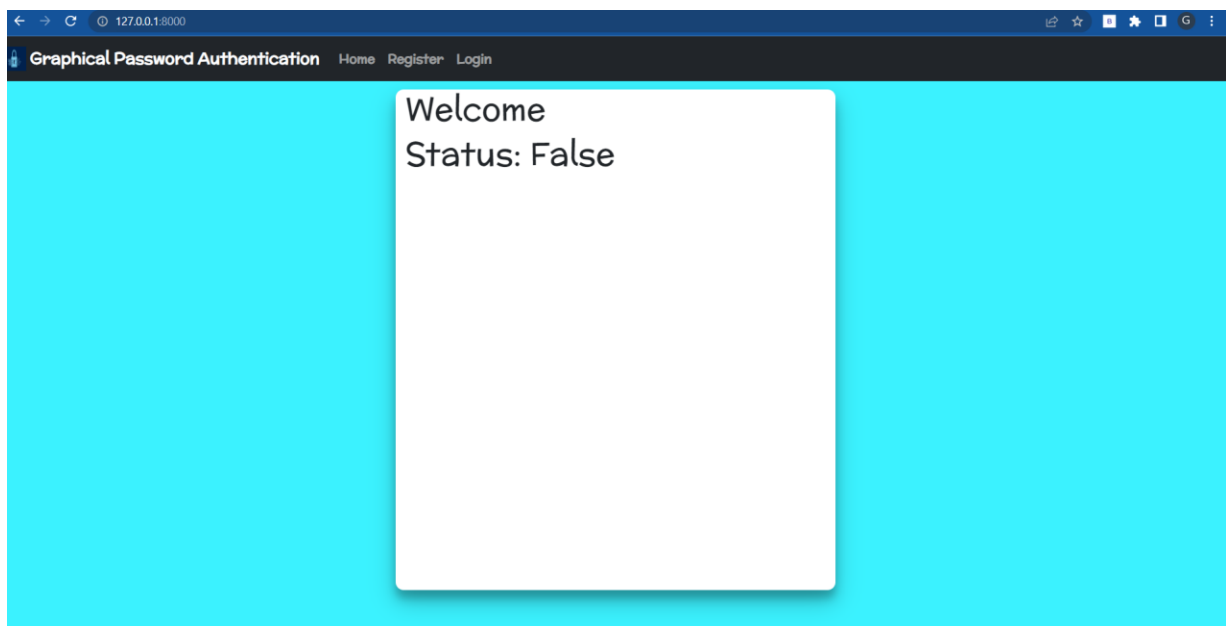


Figure 4.4 Home page



Step 12:- User has to fill the details required to proceed for login.

i) Enter the Username.

ii) Select the Password (User has to select exactly same images that he/she has chosen during registration time).

Step 13:- Click on “**Sign In**” tab.

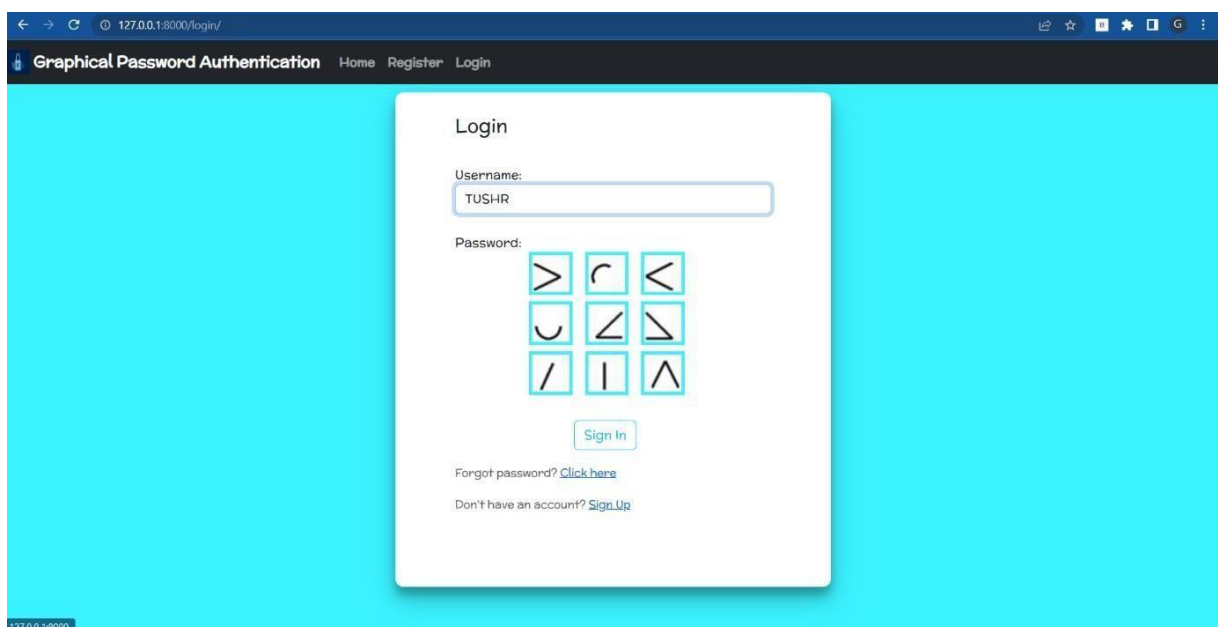


Figure 4.5 Login page

Step 14:- User will be notified as “**Login successfully**”, if user has given wrong password then the he/she will get the notification “**Wrong Password**”, in this case the user has to Login himself/herself again with Correct Password.

Step 15:- User will enter the site.

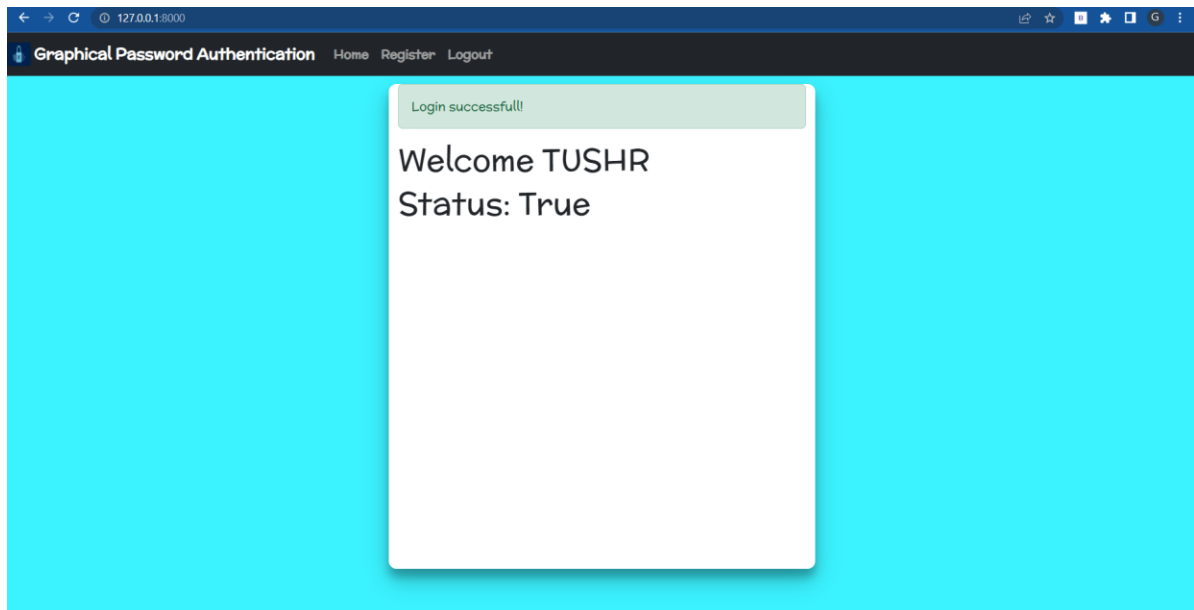


Figure 4.6 Home page (Login successfully)

Step 16:- If the user has forgot his/her password (then click on “**forgot password**”).

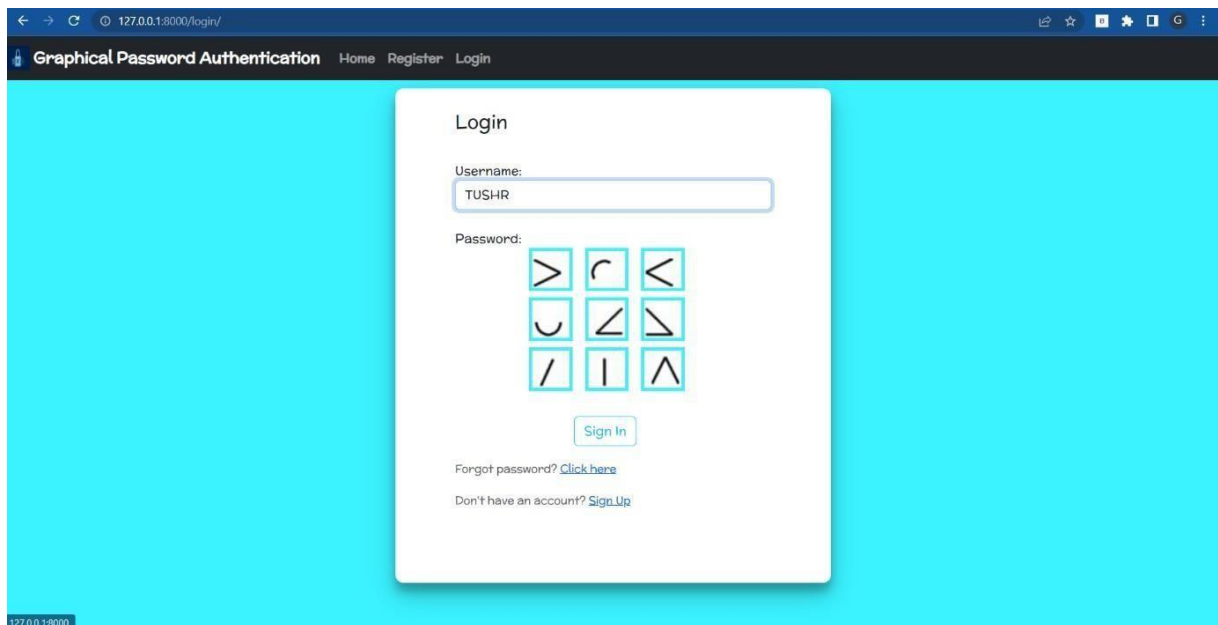


Figure 4.7 Login page (forgot password)

Step 17:- User has to fill the details required to proceed for reset password.

i) Enter the Username.

Step 18:- Click on “**Request**” tab.

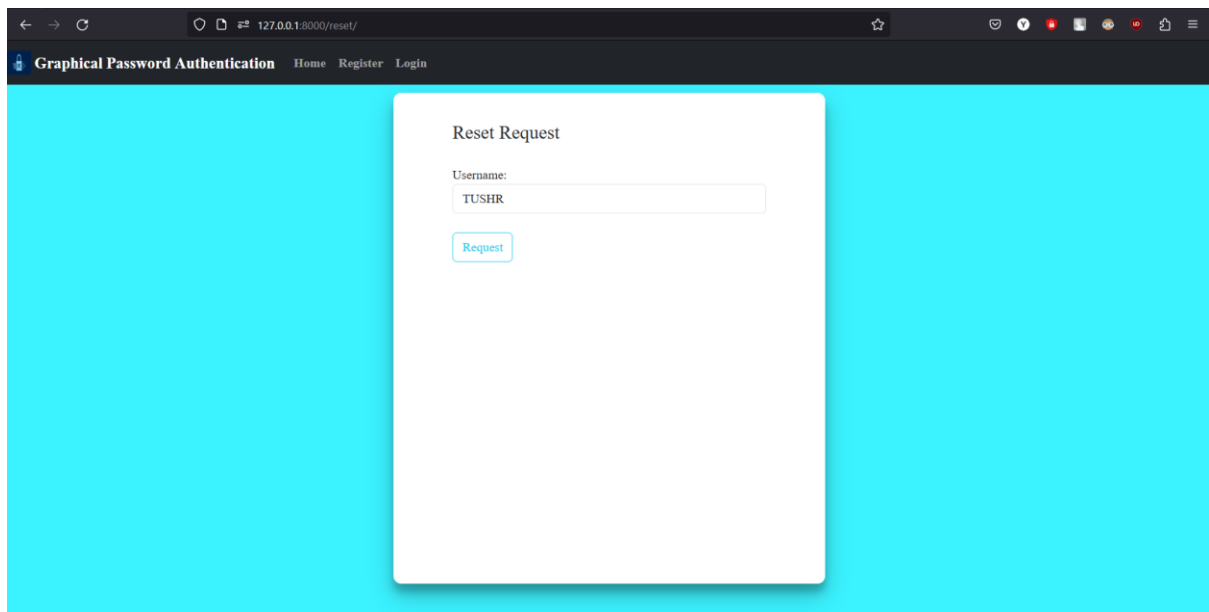
A screenshot of a web browser displaying a password reset page. The browser's address bar shows the URL "127.0.0.1:8000/reset/". The page has a dark blue header with the text "Graphical Password Authentication" and navigation links "Home", "Register", and "Login". The main content area has a light blue background. In the center, there is a white rectangular box titled "Reset Request". Inside this box, there is a label "Username:" followed by a text input field containing the text "TUSHR". Below the input field is a blue button with the text "Request".

Figure 4.8 Password Reset Page

Step 19:- A password reset link will be sent to user's email.

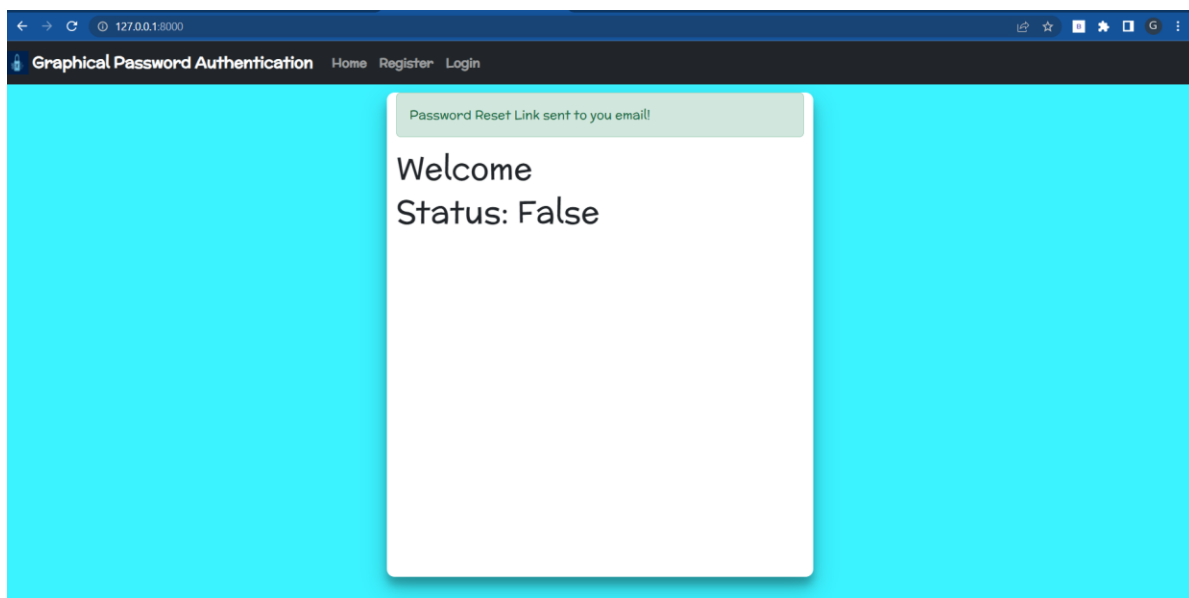


Figure 4.9 Home page (email sent notification)

Step 20:- User need go to his/her email and he/she will see the email attached with a link.

Step 21:- User need to click on “LINK”.

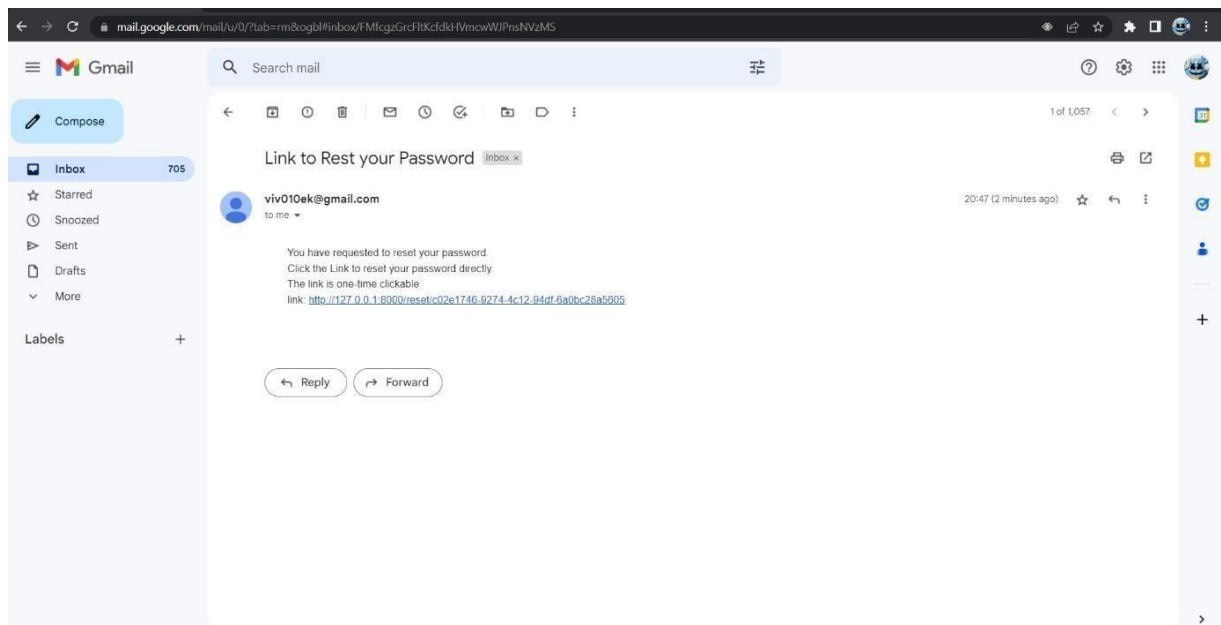


Figure 4.10 Password Reset Mail sent to user

Step 22:- Link will be opened in the browser.

Step 23:- User will have to create a new Password (User has to select exactly 3 images in a specific order as a password).

Step 24:- Click on “**Reset**”.

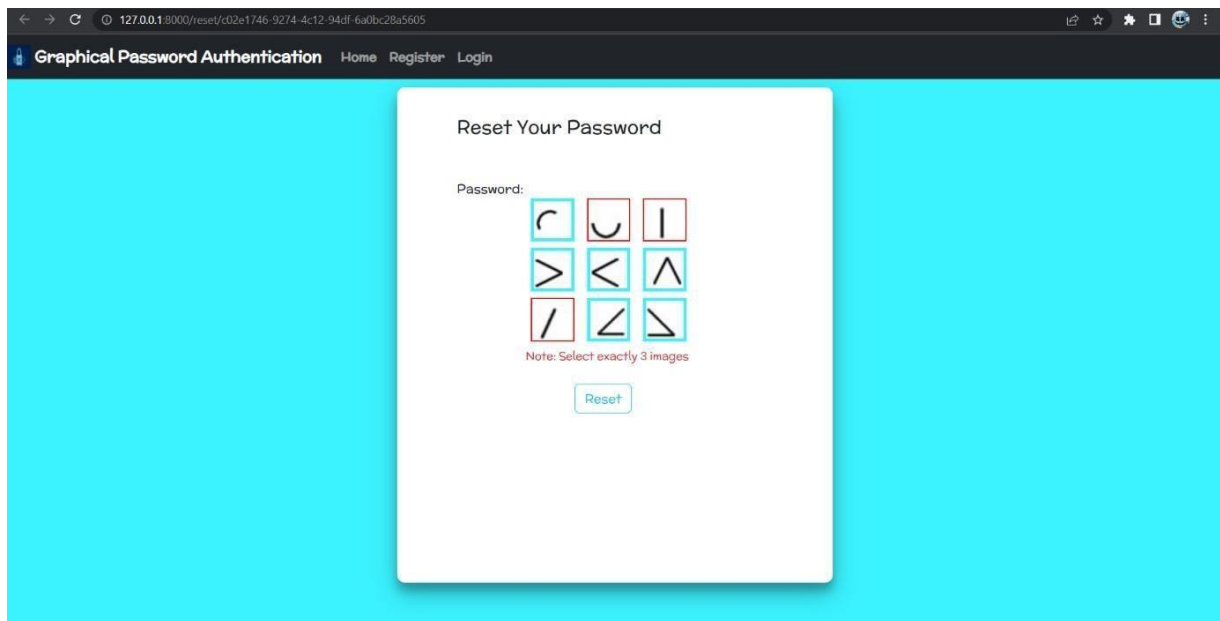
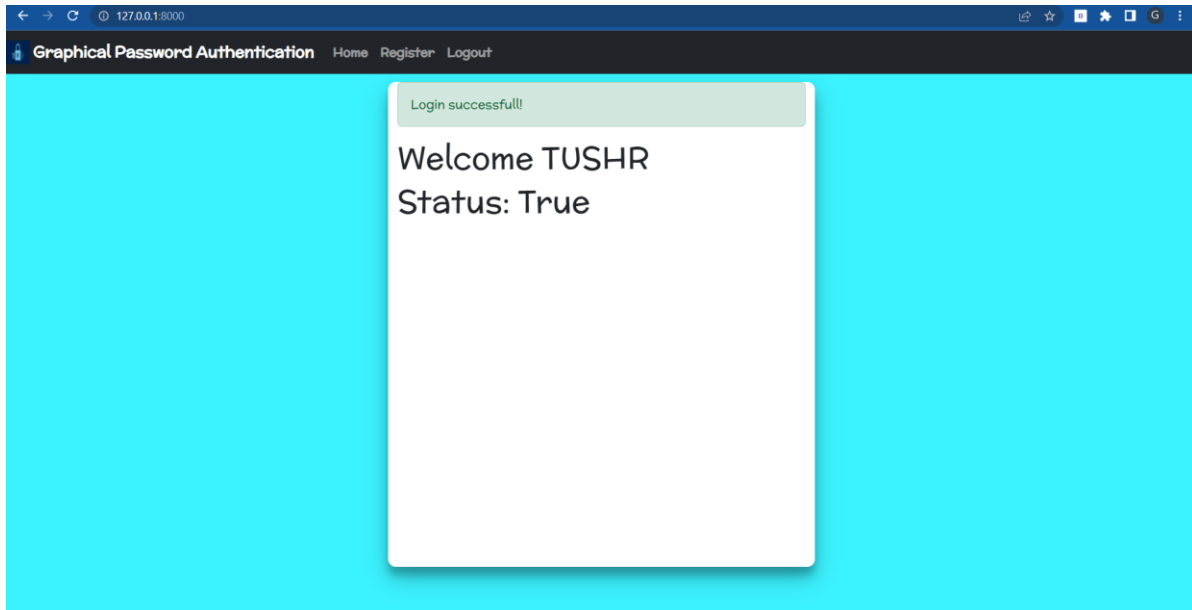


Figure 4.11 Password Reset Page (Create New Password)

Step 25:- User will get the notification “**Password Changed Successfully**”.

Step 26:- Click on “**Login**” button(repeat the step 11-13 for login).



#### 4.12 Home Page (Password Changed Successfully)



## **CHAPTER-5**

---

## **CONCLUSION**

## 5.1 Conclusion

Alphanumeric passwords are used by the majority of programs and websites to verify users. Unfortunately, this lacks security and leaves the system open to several types of attacks. Although alphanumeric passwords appear secure in theory, most users will wind up creating straightforward, widely used passwords that are regularly reused across many programs or accounts. This can be exploited by bot assaults or hackers who then conduct dictionary attacks, attempt to brute force the password, or utilize other techniques to compromise user accounts. Standard alphanumeric passwords can be replaced with graphical passwords, which are more secure and don't dramatically reduce usability. We can eliminate the issue of keystroke logging and obtain security from social engineering and dictionary assaults by using graphical password authentication.

In summary, graphical password authentication systems offer an innovative and potentially more user-friendly approach to user authentication compared to traditional alphanumeric passwords. By leveraging images or visual elements, Graphical Password Authentication System aims to enhance security, improve memorability, and provide a more user-friendly authentication experience.

While they present both advantages and challenges, ongoing research, advancements in technology, and user education can contribute to addressing the challenges and further enhancing the security, usability, and effectiveness of graphical password authentication systems in the future.

Throughout the literature review, various studies have highlighted the strengths and weaknesses of different Graphical Password Authentication System techniques, evaluated their usability and security, and explored potential future developments. The research has shown that graphical passwords have the potential to offer better memorability, increased password space, and resistance against common password attacks.

In conclusion, graphical password authentication systems offer an alternative approach to traditional alphanumeric passwords, aiming to enhance security, usability, and user experience. They utilize images, symbols, or gestures as password components, allowing users to create unique and memorable passwords. However, like any authentication system, graphical password authentication has its advantages and challenges.

The advantages of graphical password authentication systems include improved memorability, resistance to dictionary-based attacks, and potential for increased password strength. They also have the potential to provide a more intuitive and engaging user experience compared to alphanumeric passwords. Additionally, graphical password authentication systems offer opportunities for multimodal authentication, context-awareness, and integration with emerging technologies like biometrics and augmented reality.

However, there are challenges that need to be addressed. These challenges include the potential for weak or predictable image selection, limited password space, susceptibility to shoulder surfing and smudge attacks, and the need for user education and training. Additionally, standardization and interoperability across different systems and platforms can be a challenge for graphical password authentication.

To improve graphical password authentication systems in the future, various strategies can be implemented. These include expanding the password space, exploration of advanced authentication techniques, multi-factor authentication integration, integrating biometrics, usability and accessibility improvements, incorporating advanced behavioral analysis, adopting continuous authentication, enhancing the user interface and guidance, leveraging machine learning for threat detection, ensuring strong encryption and data protection, conducting regular security assessments and updates, promoting standardization and interoperability, integration with emerging technologies, and seeking user feedback for iterative design improvements. Ongoing research and development in these areas will contribute to the maturation and wider adoption of Graphical Password Authentication System.

Overall, Graphical Password Authentication System represents a promising alternative to text-based passwords, providing a more engaging and secure authentication experience. As technology evolves and research progresses, Graphical Password Authentication System has the potential to become a mainstream authentication method, addressing the limitations of traditional passwords and enhancing the security of digital systems.

## 5.2 Future Scope

Picture passwords are an alternative to textual alphanumeric password. Most of the existing authentication system has certain drawbacks for that reason graphical passwords are most preferable authentication system where users click on images to authenticate themselves.

As authentication techniques generate passwords but they have to face attacks like dictionary attacks, brute force attacks, shoulder surfing. An important usability goal of an authentication system is to support users for selecting the better password.

User creates memorable password which is easy to guess by an attacker and strong system assigned passwords are difficult to memorize. So researchers of modern days have gone through different alternative methods and concluded that graphical passwords are most preferable authentication system.

By implementing encryption algorithms and hashing for storing and retrieving pictures and points, one can achieve more security. Picture password is still immature more research is required in this field.

So, the future scope of graphical password authentication systems holds promising opportunities for further advancements and applications. Here are some potential areas of development in the future:

1. **Advanced Behavioral Analysis:** Future graphical password authentication systems may incorporate advanced behavioral analysis techniques to enhance security. By analyzing user behavior patterns, such as the speed and pressure of gestures or the sequence of image selection, the system can detect anomalies and unauthorized access attempts, providing an additional layer of security.
2. **Contextual Authentication:** Contextual authentication involves considering various contextual factors, such as user location, device information, or time of login, to determine the authenticity of the user. Future graphical password systems can leverage contextual information to dynamically adjust the authentication requirements based on the specific context, enhancing both security and usability.
3. **Multimodal Authentication:** Combining multiple authentication factors, such as graphical passwords with biometric authentication or knowledge-based authentication, can strengthen

the overall security of the system. Multimodal authentication systems offer a layered approach, leveraging the strengths of different authentication methods to mitigate vulnerabilities and provide a more robust user authentication experience.

4. Continuous Authentication: Continuous authentication aims to authenticate users throughout their entire session by continuously monitoring their behavior and interactions. Future graphical password systems may employ continuous authentication techniques to ensure ongoing user verification, reducing the risk of unauthorized access or session hijacking.

5. Augmented Reality (AR) and Virtual Reality (VR) Integration: The integration of graphical password authentication with AR and VR technologies can provide innovative and immersive authentication experiences. Users can authenticate themselves by interacting with virtual objects, navigating through virtual environments, or performing specific gestures in augmented or virtual reality settings.

6. Machine Learning and Artificial Intelligence: Machine learning and AI techniques can play a significant role in enhancing the security and usability of graphical password authentication systems. These technologies can be employed to analyze user behavior, detect patterns, identify potential threats or attacks, and adapt the authentication process accordingly.

7. Blockchain-Based Authentication: Blockchain technology offers decentralized and tamper-resistant authentication mechanisms. Future graphical password systems could leverage blockchain to securely store and manage user authentication data, ensuring transparency, integrity, and privacy in the authentication process.

8. Standardization and Interoperability: Establishing standardized guidelines, protocols, and interoperability frameworks for graphical password authentication systems would foster compatibility and seamless integration across different platforms and applications. Standardization efforts can facilitate widespread adoption and ensure consistent security practices.

9. Usability and User Experience Improvements: Future developments in graphical password authentication should focus on improving the overall user experience and usability. User-centric design approaches, user studies, and feedback loops can help refine the graphical password interfaces, making them more intuitive, accessible, and user-friendly.

10. Security Assessment and Testing: Continuous research, security assessment, and testing are essential to identify and address potential vulnerabilities in graphical password authentication systems. Evaluating the resistance of these systems against advanced attacks, such as machine learning-based attacks or adversarial examples, will be critical to ensure their robustness and effectiveness in real-world scenarios.

In summary, the future scope of graphical password authentication systems lies in their evolution to incorporate advanced technologies, provide enhanced security, adapt to diverse contexts, and deliver a seamless and user-friendly authentication experience. Continued research, industry collaboration, and user feedback will shape the development and adoption of these systems in various domains and applications.

## REFERENCES

## REFERENCES

- [1] Saranya Ramanan, Bindhu J S, “A Survey on Different Graphical Password Authentication Technique”, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 12, December 2014.
- [2] Amol Bhand, Vaibhav desale, Swati Shirke, Suvarna Pansambal (Shirke), “Enhancement of Password Authentication system using Graphical Images”. 2015 International Conference on Information Processing (ICIP) Vishwakarma Institute of Technology. Dec 16-19, 2015.
- [3] Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh and Chia-Yun Cheng, “A Shoulder Surfing Resistant Graphical Authentication System” DOI 10.1109/TDSC.2016.2539942 IEEE.
- [4] Sarojini, Priya, Bhuvaneshwari, “Graphical Authentication System Using Pass Matrix” .International Journal of Computer Trends and Technology(IJCTT) Special Issue April – 2017.
- [5] Robert Reeder, Stuart Schechter, “When the Password Doesn’t Work: Secondary Authentication for Websites”. IEEE Security & Privacy (Volume: 9, Issue: 2, March-April 2011).
- [6] G. Blonder. “Graphical passwords”. United States Patent, 5,559,961, 1996.
- [7] D. Davis, F. Monroe, and M. K. Reiter, “On user choice in graphical password schemes” in Proceedings of the 13<sup>th</sup> Usenix Security Symposium. San Diego, CA, 2004.
- [8] Lashkari, A. H., Gani, A., Sabet, L. G., & Farmand, S. (2010). “A new algorithm on Graphical User Authentication (GUA) based on multi-line grids.” Scientific Research and Essays, 5(24), 3865–3875.
- [9] Aakansha Gokhale, & Vijaya Waghmare. (2013), “Graphical Password Authentication Techniques: A Review”. 7.
- [10] K. Renaud, “Guidelines for designing graphical authentication mechanism interfaces,” International Journal of Information and Computer Security, vol. 3, no. 1, pp. 60–85, June 2009.
- [11] A. De Angeli, L. Coventry, G. Johnson, and K. Renaud, “Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems,” International Journal of Human-Computer Studies, vol. 63, no. 1-2, pp. 128–152, 2005.



- [12] K.-P. L. Vu, R. Proctor, A. Bhargav-Spantzel, B.-L. Tai, J. Cook, and E. Schultz, “Improving password security and memorability to protect personal and organizational information,” *International Journal of Human-Computer Studies*, vol. 65, pp. 744–757, 2007.
- [13] Susan Wiedenbeck, Jim Water, Jean-Camille Birget, Alex Brod-skiy, Nasir Memon, “Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice”.
- [14] Xiaoyuan Suo, Ying Zhu & G. Scott Owen “Analysis and Design of Graphical Password Techniques”.
- [15] Xiaoyuan Suo “A Study of Graphical Password for Mobile Devices”.
- [16] Wafa Mohd Kharudin, Nur Fatehah Md Din & Mohd Zalisham Jali. “Password Recovery Using Graphical Method”.
- [17] Peter Mayer, Melanie Volkamer & Michaela Kauer “Authentication Schemes - Comparison and Effective Password Spaces”.
- [18] Sachin Davis Mundassery & Sreeja Cherillath Sukumaran “User Authentication with Graphical Passwords using Hybrid Images and Hash Function”.
- [19] Wazir Zada Khan, Yang Xiang, Mohammed Y. Aalsalem & Quratulain Arshad “A Hybrid Graphical Password Based System”.
- [20] Rajat Mahey, Nimish Singh, Chandan Kumar, Nitin Bhagwat & Poonam Verma “Graphical Password Using an Intuitive Approach”.

## **WEBSITES**

- <http://www.gobbeldygook.co.uk>
- <https://www.geeksforgeeks.org/graphical-password-authentication/>
- [https://www.youtube.com/watch?v=jBzwzrDvZ18&t=1s&ab\\_channel=freeCodeCamp.org](https://www.youtube.com/watch?v=jBzwzrDvZ18&t=1s&ab_channel=freeCodeCamp.org)

# **Paper Publication with Certificate**

# GRAPHICAL PASSWORD AUTHENTICATION

Gaurav Yadav

Department of Computer Science &  
Engineering  
Shri Shankaracharya Institute of  
Professional Management &  
Technology  
Raipur, India

Mrs. Upasana Khadatkar  
Assistant Professor

Department of Computer Science &  
Engineering  
Shri Shankaracharya Institute of  
Professional Management &  
Technology  
Raipur, India

Vivek Yadav

Department of Computer Science &  
Engineering  
Shri Shankaracharya Institute of  
Professional Management &  
Technology  
Raipur, India

**Abstract**—This paper presents a comprehensive study on Graphical Password Authentication. A graphical password or graphical user authentication uses a set of images rather than letters, numerals, or other special characters as a password to authenticate users. Different implementations use different kinds of images and interact with them in different ways. In a graphical password authentication system, the user must choose from images that are shown to them in a graphical user interface (GUI), in a particular order.

**Keywords**— Graphical User Interface (GUI).

## I. INTRODUCTION

The process of verifying a user's identification is known as authentication. It is the system that links a set of identifying credentials to an incoming request. The submitted credentials are compared to those stored in a database on a local operating system or within an authentication server that has information about the authorized user. In the majority of situations involving computer security, user authentication is a crucial element. It serves as the foundation for user accountability and access control. Although there are many different kinds of user authentication methods, alphanumeric usernames and passwords are the most used. They are adaptable, simple to use, and easy to apply. To meet two opposing requirements for security. Password must be easily recalled by the user while being difficult for the impostor to guess. Users are known to choose easily guessable and/or short text passwords, which are an easy target of dictionary and brute-force attacks. Enforcing a strong password policy can occasionally have the reverse effect, as users may turn to sticky notes to store their difficult-to-remember passwords. them to direct theft. In the literature, several techniques have been proposed to reduce the limitations of alphanumeric passwords. One proposed solution is to use graphical passwords, in which graphics (images) are used instead of alphanumeric passwords. This can be achieved by asking the user to select from images, in a specific order, presented to them in a graphical user interface rather than typing characters as in alphanumeric password approaches. A graphical password or graphical user authentication uses graphics(images) rather than letters, numerals, or other

special characters as a password to authenticate users. Different implementations use different kinds of images and interact with them in different ways. In a graphical password authentication system, the user must choose from images that are shown to them in a graphical user interface (GUI), in a particular order

## II. LITERATURE REVIEW

A Journal titled "A Survey on Different Graphical Password Authentication Techniques"[1] was published in 2014 by Saranya Ramanan and Bindhu J S. They explore many algorithms, approaches, and methodologies for graphical password authentication in this study. These methods are divided into four groups: hybrid approaches, cued-recall methods, pure recall methods, and recognition-based methods. Graphical password schemes provide a means to make passwords that are easier for people to remember. The system's safety is extremely exceptional in this. Brute force searches and dictionary attacks are impossible. Images are easier to remember than long text sequences. After that, they made an effort to examine attack patterns and frequent attacks in graphical password authentication techniques. Finally, they covered a variety of graphical password-related topics.

The graphical password system concept is the primary subject of this publication [2]. It is suggested to improve password authentication systems with the use of graphics (images). The use of cued click points for authentication purposes supports it. The user's engagement with a succession of five images is the core idea behind this system. This system's main objective is to increase security using user-friendly methods that are more difficult for hackers to guess. The greatest replacement for text passwords is an authentication system that uses graphics. The best replacement for the outdated graphical password system is cued click point (CCP).

Pass Matrix is a cutting-edge authentication solution that uses graphical passwords to fend off shoulder surfing assaults [3]. Pass Matrix provides no suggestion for attackers to find out or narrow down the password even if they execute

several camera-based attacks. It has a one-time valid login indicator and rotating horizontal and vertical bars encompassing the complete scope of pass-images.

In this study, a graphic authentication system using a pass matrix was developed [4]. Computer security and privacy commonly use authentication-based passwords. The majority of conventional passwords are made up of letters and digits. That is immediately identifiable by those who are not authorized. Attacks that use shoulder surfing start with identification. Human error, such as selecting poor passwords and entering passwords incorrectly, is seen to be the weakest link in the authentication process. People can access these applications anytime, anywhere, and on a variety of devices thanks to the proliferation of online and mobile applications. A novel authentication method called Pass Matrix resist shoulder surfing assaults was presented to solve these issues.

They addressed the issue of password failure in this publication [5]. Passwords are used by almost all websites that manage user-specific accounts to confirm that a user trying to access an account actually is the account holder. Websites must be able to recognise users who are unable to supply the correct password, though, as passwords may be misplaced, forgotten, or even stolen. Users will then need to provide some sort of secondary authentication to demonstrate their identity and regain access to their accounts. There are numerous secondary authentication methods that websites can use. The article examines secondary authentication methods, highlighting the value of building a toolbox of methods that satisfy the security and dependability requirements of users.

### III. PROPOSED METHODOLOGY

Everything is happening online as a result of the rapid digitalization of the globe brought on by rising technology breakthroughs. The risk of cybercrimes and privacy breaches is rising as more and more things go online. Your data is greatly protected by passwords on both online and offline platforms. The standard authentication technique for accessing our accounts is passwords. Users can secure their accounts using a variety of authentication methods.

#### Types of Authentication

- Token-based authentication methods includes key cards, bank cards, smart cards, etc. as authentication.
- Knowledge based authentication methods includes text based authentication and picture-based authentication
- Biometric authentication methods include facial recognition, iris scanning, and fingerprint verification.
- Recognition-based authentication, a user is presented with a set of images and asked to choose the one he registered with from among them. Users can choose from a wide selection of photos when creating passwords. Users must choose the pre-selected image from the range of images displayed to them in order to log in.

We proposed a graphical password system that provide more security than alphanumeric password. During the registration, the system will display a 3\*3 grid consisting of 9 images for passwords. Each thumbnail picture has a numerical value assigned to it, and the order of selection will

produce a numerical password. A user creates a graphical password by selecting 3 images from a 3\*3 grid. In graphical password, During the login, to authenticate himself/herself, the user must enter the registered images in the correct sequence to successfully log in. For the authentication of the password Advanced Encryption Algorithm (AES) has been used.

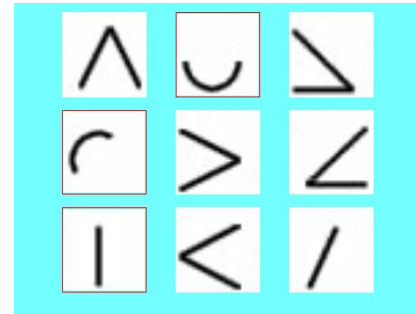


Fig 1:- Grid of 3x3 images

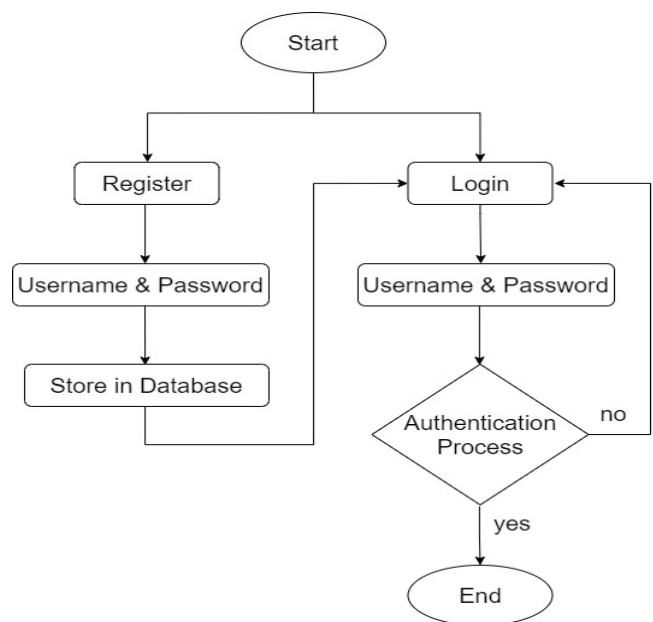


Fig. 2:- Flow Chart

### IV. SCOPE IN THE FUTURE

There is an alternative to text-based alphanumeric passwords: graphical passwords. Graphical passwords, in which users click on images to authenticate themselves, are the most preferred authentication method because the majority of the existing authentication systems have certain shortcomings. As alphanumeric password techniques generate passwords but they have to face attacks like dictionary attacks, brute force attacks, and shoulder surfing. Supporting users in choosing a stronger password is a key

usability objective of an authentication system. The strong system-given passwords are challenging to remember, but user-created memorable passwords are simple for an attacker to guess. Therefore, researchers in the current era have investigated several alternative techniques and concluded that graphical passwords are the most preferred authentication scheme. By implementing encryption algorithms and hashing for storing and retrieving pictures and points, one can achieve more security.

## V. RESULT

Alphanumeric passwords are either difficult to remember or easy to guess when using conventional username-password authentication. Additionally, because it can be challenging to remember a lot of passwords, users typically use the same one for all of their accounts. A study found that the human brain is better at recalling visual information (images) than alphanumeric characters. As a result, the drawback of alphanumeric passwords is overcome by graphical passwords. In comparison to other conventional password schemes, it offers greater security.

- **Brute Force Attacks:**-The attacker systematically checks all possible passwords and passphrases until the correct one is found. After reaching max tries, the user will be notified through an email attached with a new login link. And further authentication through the generic website is disabled for that user account. This also lets the legitimate user know about the adversary.
- **Dictionary Attacks:**-These types of attacks use a predefined set of combinations of values. Even though the images used at registration may have an impact on the password combination selected, the images in the grid always vary from the database. Thus the occurrence of the same grid which was at the time of selecting the passwords is very low.
- **Key loggers:**-Key-loggers secretly capture keystrokes and transfer, but if the spyware wants to track the mouse movements, it can be tracked, but the adversary wouldn't know which part of the graphical password is the mouse action.
- **Shoulder Surfing:**-Shoulder surfing is a type of social engineering technique used to obtain information such as personal identification numbers (PINs), passwords, and other confidential data by looking over the victim's shoulder. The system we adopt is invisible on the screen when the users draw it during login. Because of this, it is very difficult for the attacker to see the images that the user clicks on the grid.

## VI. CONCLUSION

Alphanumeric passwords are used by the majority of programs and websites to verify users. Unfortunately, this lacks security and leaves the system open to several types of attacks. Although alphanumeric passwords appear

secure in theory, most users will wind up creating straightforward, widely used passwords that are regularly reused across many programs or accounts. This can be exploited by bot assaults or hackers who then conduct dictionary attacks, attempt to brute force the password, or utilize other techniques to compromise user accounts. Standard alphanumeric passwords can be replaced with graphical passwords, which are more secure and don't dramatically reduce usability. We can eliminate the issue of keystroke logging and obtain security from social engineering and dictionary assaults by using graphical password authentication. This method of user authentication also calls for user involvement, which serves to confirm that a user is a real person rather than using the CAPTCHA.

## REFERENCES

- [1] Saranya Ramanan, Bindhu J S," A Survey on Different Graphical Password Authentication Technique", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 12, December 2014.
- [2] Amol Bhand, Vaibhav desale, Swati Shirke, Suvarna Pansambal (Shirke), "Enhancement of Password Authentication system using Graphical Images". 2015 International Conference on Information Processing (ICIP) Vishwakarma Institute of Technology. Dec 16-19, 2015.
- [3] Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh and Chia-Yun Cheng, "A Shoulder Surfing Resistant Graphical Authentication System" DOI:10.1109/TDSC.2016.2539942 IEEE.
- [4] Sarojini, Priya, Bhuvaneshwari, "Graphical Authentication System Using Pass Matrix". International Journal of Computer Trends and Technology (IJCTT) Special Issue April – 2017.
- [5] Robert Reeder, Stuart Schechter, "When the Password Doesn't Work: Secondary Authentication for Websites". IEEE Security & Privacy (Volume: 9, Issue: 2, March-April 2011).
- [6] William Stallings and Lawrie Brown. Computer Security: Principle and Practices. Pearson Education, 2008.
- [7] D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in Proceedings of the 13th Usenix Security Symposium. San Diego, CA, 2004.
- [8] Lashkari, A. H., Gani, A., Sabet, L. G., & Farmand, S. (2010). A new algorithm on Graphical User Authentication (GUA) based on multi-line grids. Scientific Research and Essays, 5(24), 3865–3875.
- [9] Aakansha Gokhale, & Vijaya Waghmare. (2013). Graphical Password Authentication Techniques: A Review. 7.
- [10] K. Renaud, "Guidelines for designing graphical authentication mechanism interfaces," International Journal of Information and Computer Security, vol. 3, no. 1, pp. 60–85, June 2009.
- [11] A. De Angeli, L. Coventry, G. Johnson, and K. Renaud, "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems," International Journal of Human-Computer Studies, vol. 63, no. 1-2, pp. 128–152, 2005.
- [12] K.-P. L. Vu, R. Proctor, A. Bhargav-Spantzel, B.-L. Tai, J. Cook, and E. Schultz, "Improving password security and memorability to protect personal and organizational information," International Journal of Human-Computer Studies, vol. 65, pp. 744–757, 2007.
- [13] Rupavathy, N., Carmel Mary Belinda, M. J., & Nivedhitha, G. (2018). A shoulder surfing resistance using graphical authentication system. International Journal of Engineering and Technology (UAE), 7(1.7 Special Issue 7), 169174. <https://doi.org/10.14419/ijet.v7i1.7.10644>

**ICSRESM  
2022**

**3rd International Conference on  
Sustainable Research in Engineering  
Science and Management**

Paper ID - 16

***CERTIFICATE***

This is to certify that

**Vivek Yadav**

**Shri Shankaracharya Institute of Professional Management and Technology Raipur Chhattisgarh, India**

has contributed a paper titled

**Graphical Password Authentication**

in 3rd International Conference on Sustainable Research in Engineering Science and Management (ICSRESM-2022) held during December 16, 2022 on Shri Shankaracharya Institute of Professional Management and Technology, Raipur, Chhattisgarh, India We wish the authors all the very best for future endeavors.



**Dr. Suman Kumar Swarnkar**  
Convener (ICSRESM-2022)



**Dr. J P Patra**  
Coordinator (ICSRESM-2022)



**Dr. Alok Kumar Jain**  
Principal,SSIPMT



**ICSRESM  
2022**

**3rd International Conference on  
Sustainable Research in Engineering  
Science and Management**

Paper ID - 16

**CERTIFICATE**

This is to certify that

**Gaurav Yadav**

**Shri Shankaracharya Institute of Professional Management and Technology Raipur Chhattisgarh, India**

has contributed a paper titled

**Graphical Password Authentication**

in 3rd International Conference on Sustainable Research in Engineering Science and Management (ICSRESM-2022) held during December 16, 2022 on Shri Shankaracharya Institute of Professional Management and Technology, Raipur, Chhattisgarh, India We wish the authors all the very best for future endeavors.



**Dr. Suman Kumar Swarnkar**  
Convener (ICSRESM-2022)



**Dr. J P Patra**  
Coordinator (ICSRESM-2022)



**Dr. Alok Kumar Jain**  
Principal,SSIPMT

