IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

MULTI-LAYERED AUTHENTICATION SYSTEM FOR ENHANCED SECURITY AGAINST SHOULDER-SURFING ATTACKS

Shruti Rathod[1], Zarna Raval[2], Prof. Sonal Kadam[3]

[1,2] Final Year Students, [3]Professor, Dept. of Computer Science & Technology, Usha Mittal Institute of Technology, Mumbai, SNDT Women's University, Mumbai, Maharashtra, India

Abstract: Authentication is a fundamental security process that verifies user identity and can be implemented through various mechanisms, including tokens, biometrics, and text- or image-based passwords. At present single layered or double layered authentications systems are used, which may face security threats. This paper presents a multi-layered authentication framework combining textual, color-based, and image-based authentication to enhance security against cyber threats like brute-force attacks, phishing, and shoulder surfing. The system follows a three-phase authentication process**:** users enter a text password**,** select a pass-color from a hexagonal palette and complete authentication with image-based verification using the Playfair Cipher rule**.**

Index Terms - Graphical Passwords, Shoulder-Surfing Attacks, Security, Multi-Layered Authentication, Color-Based Authentication, Playfair Cipher.

I. INTRODUCTION

Authentication is the digital umbrella that provides protection against unauthorized access and ensures data security and user privacy. While traditional password-based authentication remains the most acceptable way that has all the risks of being compromised by brute-force attacks, phishing, or shoulder surfing, other methods such as biometrics, cryptographic tokens, graphical password schemes, and others have been introduced to improve security without compromising ease of accessibility and convenience.

Given these challenges, a multi-layered authentication framework is proposed in this paper which integrates other mechanisms such as text, color, and image-based authentication. Each user is supposed to go through three phases of verification, namely the text password, color-based authentication with reference to a hexagon color palette, and image verification via the Playfair Cipher rule. This multi-factor authentication is designed with usability in mind whilst hardening attack defences relevant to threats faced daily by the application without disrespecting user-friendliness.

1.1. PROBLEM STATEMENT

Traditional authentication systems are vulnerable to brute-force attacks, phishing techniques, or shoulder-surfing. Existing systems (like text-based passwords and biometric authentication) tend to struggle with security-versus-usability balance. Hence, there is a proposal to deal with the issues of traditional authentication systems by suggestion of multi-layered authentication structures that incorporate text-based, color-based, and image-based elements into secure, user-friendly systems.

1.2 Objectives

Following important objectives are considered in the proposed work

- Enhance resistance against shoulder-surfing attacks using dynamic authentication techniques.
- Improve usability while maintaining high-security standards in user authentication.

2. LITRETURE REVIEW

Similar work has been done by various researchers working in this area, some of the more related work are as listed below:

In 2017, Lip Yee Por and co-authors [2] introduced a graphical password authentication system based on the novel Digraph Substitution Rules, which defends against shoulder-surfing attacks. The authentication process involves the user selecting one pass-image from a challenge set placed in multiple consecutive rounds. Security is enhanced by the challenge sets' randomness, which keeps the time taken to log in fairly brief, thus making the system quite efficient against direct observation attacks. However, one of the main limitations of this approach is its lack of dynamic transformations of the images, which opens the need for attackers, who can watch multiple trials of authentications over time, to spot recognizable patterns and take advantage of them to amplify the risk of long-term compromise. Further, while the scheme seems to have a good tendency to defend against shoulder-surfing attacks in pretty controlled environments, its practicality and applicability in real-world settings with all kinds of user groups remains debatable.

In 2019, Harshada Shitole et al. [3] proposed a barcode-based graphical password authentication system to strengthen security and provide resistance to shoulder-surfing attacks. The system integrates barcode technology into authentication by generating a unique barcode that is sent to the user via email. The user must retrieve and scan this barcode during the login process. This method effectively combines graphical passwords with conventional authentication mechanisms, adding an extra security layer. The approach minimizes the risk of unauthorized access, as the barcode must be presented at each login attempt. However, it also introduces potential usability challenges, particularly for users who may not have immediate access to their registered email or a barcode scanning device. Additionally, reliance on external devices or network connectivity to retrieve barcodes could hinder accessibility, making the system less practical for real-time authentication needs.

D. Sathish Kumar et al. [4] developed a CAPTCHA-based graphical password authentication system that combines image-based and position-based security features. The system uses image selection by users as a part of their authentication. This approach adds computational work for brute-force and dictionary attacks within increasing combinations of options available for authentication. Incorporating CAPTCHAs adds a degree of protection against automated attacks, as human intervention is required to perform the authentication measures. However, the image-selection complexity may form a barrier to usability for some users, especially those who might have difficulty with precision types of authentication. The few users unfamiliar with image-based password schemes may also find the system less intuitive and prone to authentication errors, thus increasing login times.

The year saw the introduction by Ronak Gangwani et al. [5] of a graphical user interface for authentication using a color-based password scheme. Users select some colors in a predetermined sequence as the authentication credentials. There are other colors, the so-called decoy colors that improve security, giving rise to some resistance against keylogging and shoulder-surfing attacks. Using a color password scheme exploits abilities related to human cognition, being that colors can be simpler to memorize than complex alphanumeric passwords. Nevertheless, the viability of such a scheme is would a user be able to memorize the sequence if too complex. In addition to this, where there were predictable patterns determining the choosing of colors, statistical analysis or observational assaults might be used to take advantage of the system.

An advanced graphical password system named Cued Click Points Authentication was instituted by Devidas S. Thosar and others [6] in 2021. This modern authentication algorithm based on images makes it much more secure by dragging the user to click multiple predefined points over different images. Such assigning of authentication points across multiple pictures introduces complexity to the presaged attack, yet has considerable ease of use. Password uniqueness per user decreases the risks of pattern-based attacks,

assured through click points. Persuasive cued click points will help further steer a user into creating more secure authentication patterns for themselves. However, the system may force an added cognitive load on users who are not familiar with graphical password schemes, since they must have a good memory and accurately reproduce their own click points. Also, they may take even longer to log in because of jumping between images.

A Three-Way Authentication system was presented by Pathik Nandi et al. in 2022[7], which contains text-based, color-based, and image-based authentication factors. To log into the system, a user is required to enter a normal password, select a sequence of colors, and then pick out some images. When the authentication factors are combined, it does enhance security through some of the vulnerabilities associated with single-factor authentication. They tend to be very much resistant towards brute-force, dictionary, and shoulder-surfing attacks. But complexity comes at a price: User-friendliness. Users get to memorize different avenues to enter. It is feared they might switch off from using such a system when they are unable to, or their friends can never seem to remember how to actually put these three into use. Additionally, this multi-step authentication could also mean longer authentication times, which would not help the experience for the user.

In 2023, Meher Gulhane et al. [8] proposed the Continuous Click-Based Image Authentication system, a system by which users perform an authentication mechanism based on continuous clicks and drags across images. Security is subsequently enhanced because brute-force or dictionary-type attacks need not be considered; the authentication is based on ongoing interactions by the user and not on simply static credentials. The method exploits the recognition by the user of familiar patterns, and as such it may be an effective alternative to current password schemes. Other drawbacks include some prospects for usability problems because of the dependence on constant interaction: Users unfamiliar with click-and-drag authentication could potentially be confused with the system, allowing for a greater chance of errors in input. Besides, the method requires a fairly high fidelity of input from the user, which could prove to be challenging for individuals with motor impairments or limited dexterity.

By the Continuous Drawing System was proposed which described an exact year of introduction by Haichang Gao et al. [9]. This system involved a new and shoulder-surfing-resistant authentication in that it required users to draw continuous curves across password images. This technique further improved security through randomized image arrangements and visual degradations, thus making it harder for attackers to even guess at what the authentication patterns were. In addition, the drawing-based input method adds extra layers of complexities, thus decreasing the feasibility of replay attacks. Nevertheless, the freehand drawing may impart a degree of difficulty on the user's part because he or she must draw according to the authentication pattern accurately, which may also prolong the time of authentication beyond that of a more conventional password, thus posing an inconvenience to users.

Finally, we have the sequence rule-based graphical password system developed by Vishal Pednekar et al. [10]. In this case, the password is constructed by selecting images. The very philosophy of this approach takes advantage of the human ability to perceive and recollect sequences, thus giving a simplified authentication process for users well-acquainted with pattern-based passwords. The security is enforced by implementing sets of images in random order; thus, brute force, as well as dictionary attacks, will not be so effective. The only setback with this process is that if the selection order becomes predictable, an attacker may replay the selections. Additionally, any memorization difficulty could hinder the user's navigation of long or complex prescribed sequences.

3. EXISTING SYSTEM

In 2017 R. Vijayakumar et. Al [1] implemented, Graphical Password Authentication with Ceaser Cipher Rules implements a graphical password authentication system aimed at preventing shoulder-surfing attacks by utilizing Ceaser Cipher Rules. The proposed scheme consists of 1200 pictures in the database to ensure a larger password space, similar to the existing system. The goal of this scheme is to enhance security and usability against shoulder-surfing attacks.

Registration Phase:
During registration, users provide their details, including:

- User Name
- Email ID
- Mobile Number
- Number of Pictures for Password

After providing these details, the user selects images as their password from the displayed image set.

Authentication Phase:
During login, the user follows these steps:

- Enter Username.
- Generate a Passcode: The system sends an encrypted passcode to the user's email and mobile number.
- Select the correct password images based on the passcode: The passcode guides the user to select the correct image by shifting positions according to predefined rules.

Limitations of Existing System:

- **High Storage Requirement** – Storing 1200 images requires significant database space and increases system complexity.
- **Limited Passcode Variability** – The use of only four movement directions (L/R/T/B) and numbers (1-4) may restrict password complexity
- **Dependence on Mobile & Email** – Users must have access to their registered email and mobile number to receive the passcode.
- **Recovery Challenges** – Resetting forgotten image passwords may require a complicated recovery mechanism, affecting usability.

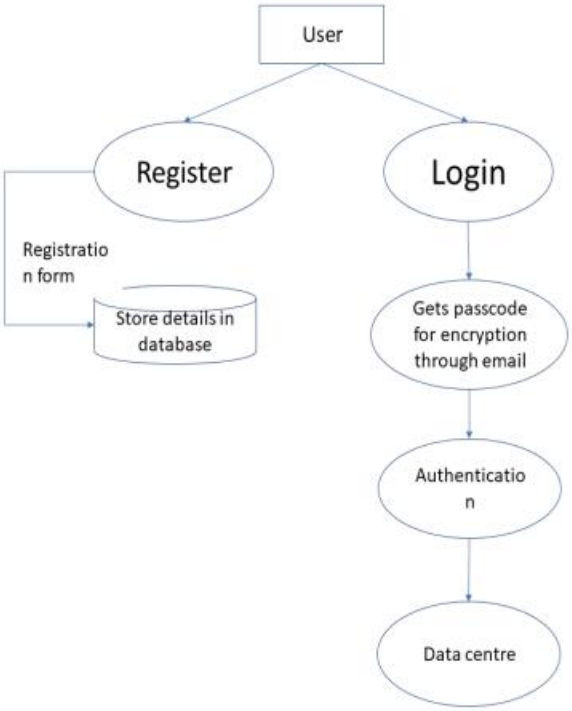

Fig1. Flowchart of Existing System

4. PROPOSED SYSTEM

To overcome the limitations of the existing system, the proposed system introduces a multi-layered authentication framework that integrates text-based, color-based, and image-based authentication using the Playfair Cipher rule**.** This approach enhances security while maintaining usability.

Registration Phase:

- Users first register with a text-based password and provide personal details.
- They select a pass-color from a hexagonal color palette and can either remember the exact color or its RGB value for authentication.
- Users then choose two images from a predefined grid as pass-images.

Authentication Phase:

The authentication process is divided into three layers to strengthen security:

- **Text-Based Authentication:** Users enter their registered email and password.
- **Color-Based Authentication:** Users either select their pass-color from the hexagonal palette or enter its RGB value for verification.
- **Image-Based Authentication Using Playfair Cipher:** Users must identify the correct pass-image from a dynamically generated challenge set. The system applies Playfair Cipher rules and alter image positions, ensuring security against pattern recognition attacks.

We are implementing a three-phase authentication system**,** consisting of text-based, color-based, and image-based authentication, each designed to enhance security and prevent unauthorized access. The following sections provide a detailed explanation of each phase.

4.1. Text-Based Password Authentication

Text-based authentication is the most widely used method for securing user accounts. It requires users to enter a unique combination of characters, including letters, numbers, and special symbols, to gain access to a system. Despite being a traditional approach, it is still prevalent due to its ease of implementation and familiarity among users.

Registration Phase:

- Users Fills the registration form and create a strong password by combining uppercase and lowercase letters, numbers, and special characters.
- The password is hashed and stored securely in the database to prevent direct access.

Login Phase:

- Users enter their registered email/username and password**.**
- The system hashes the entered password and compares it with the stored hash.
- If the hashes match, authentication is successful; otherwise, access is denied.

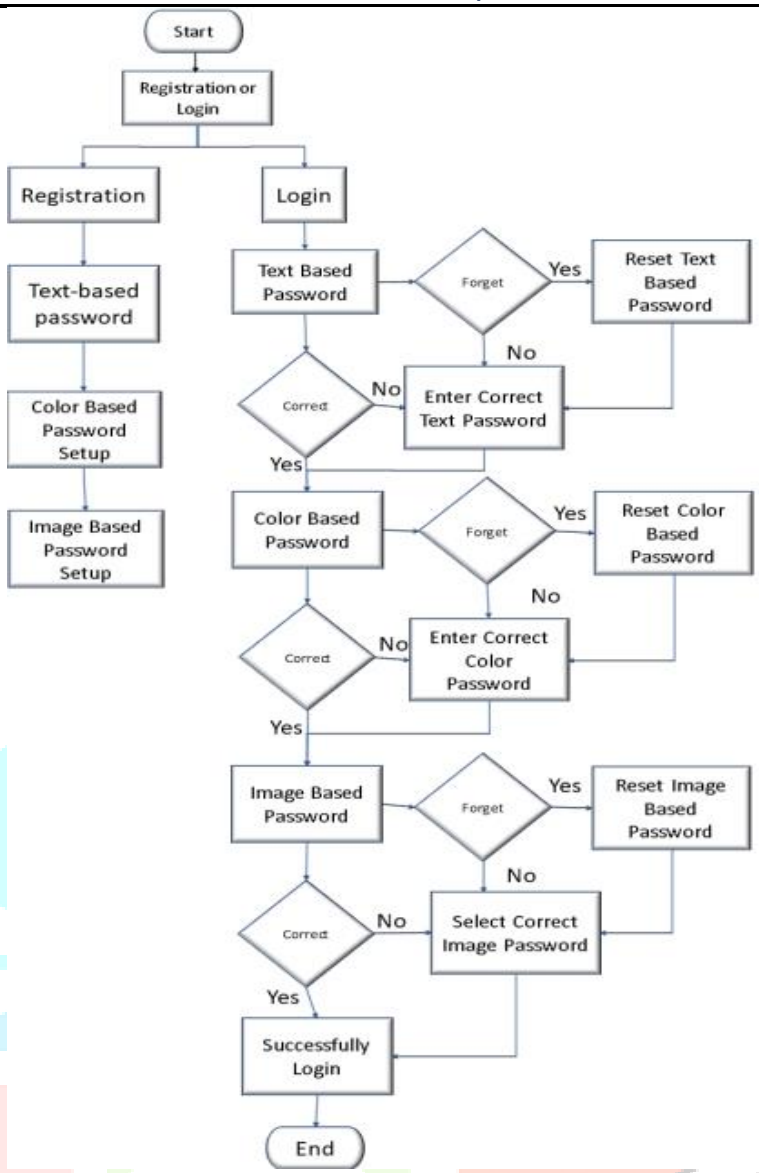

Fig 2: Flowchart of Proposed System

4.2. **Color-Based Authentication**

Color-based authentication is an intermediate layer of security that enhances the robustness of the authentication process while maintaining usability. This phase requires users to select the pass-color from a set of distinct colors arranged in a hexagonal palette, after selecting the Color user need to remember the color or Exact RGB value of the color. The system verifies the selected color against the stored credentials before proceeding to the next step.

Registration Phase:

- During registration, the user selects a pass-color from a predefined hexagonal color palette. The system securely stores the selected color along with its corresponding RGB (Red-Green-Blue) value**.**

Login Phase:

- During login**,** the user is presented with the same hexagonal color palette and must reselect their previously chosen pass-color or enter its RGB value**.**
- If the selected color matches the stored color, the authentication is successful, and the user proceeds to the next phase (Graphical-Based Authentication).
- If the user selects the wrong color, they are prompted to retry or reset their password using the password recovery mechanism.

Fig 3: Color-Based Authentication Interface

Algorithm:

1.Registration Process with RGB Hashing and Color Randomization:
1. Load a set of color for selection.
2. User picks a color.
3. Convert the color to an RGB value.
4. Apply a hash function to the RGB value.
5. Store the hashed RGB with the login ID in the database.
6. Display a success message.
7. END

2. Login Process with RGB Hashing and Color Randomization:
1. 1. User selects a color.
2. Convert it to an RGB value and hash it.
3. Compare it with the stored hash.
4. Grant access if they match; deny if they don’t
5. Initialize the last failed attempt time.
6. Allow up to three login attempts.
7. User Re-selects a color or enters an RGB value.
8. Convert the selection to RGB format.
9. Hash the RGB value.
10. If the hash matches the stored value:
11.Display "Login successful!"
12.Reset failed attempts to zero.
13.Record the login time.
14. If the hash doesn’t match:
15.Increase the failed attempt count.
16.Record the time of the failed attempt.
17.If three attempts fail, deny access

4.3. Image-Based Authentication:

Image-based authentication is a graphical authentication method where users select images in a predefined pattern. This method enhances security and protects against shoulder surfing attacks, brute force attacks, and keylogging**.**

Registration Phase

- The user selects a set of images from a given image grid.
- The selected images form the user's pass-image sequence.
- The Playfair Cipher rule is applied to encode the image selection pattern.

Login Phase

- The system presents a randomized image grid.
- The user must identify and select images based on predefined selection rules (Row, Column, or Diagonal).
- If the selection matches the registered pass-images, authentication is successful.

Three Selection Rules for Image-Based Authentication

1. Row-Based Selection

If both pass-images are in the same row, the user must select the images immediately to the right of each pass-image. If at the end of the row, select the first image (wrap around).

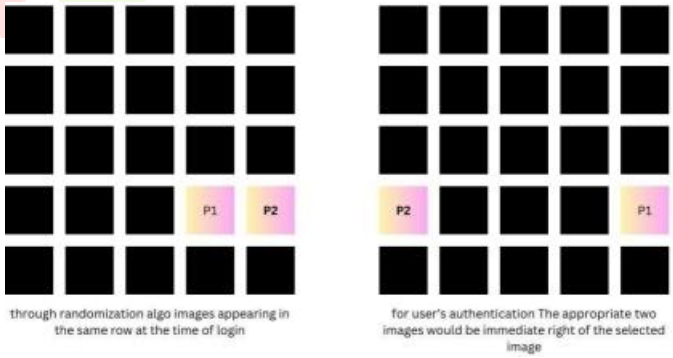

Fig 4: Play-fair Cipher Rule 1

2. Column-Based Selection

If both pass-images are in the same column, the user selects the images immediately below. If at the bottom, select the top image
(wrap around).

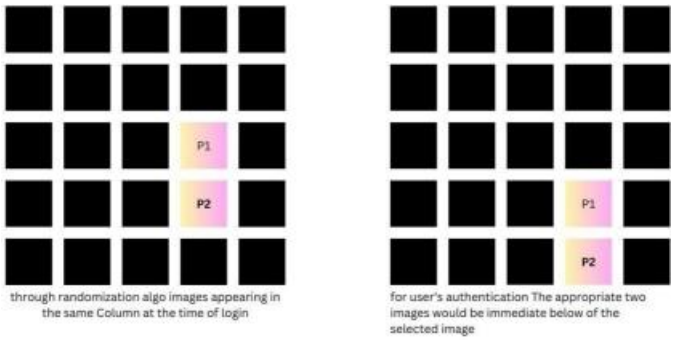

Fig 5: Play-fair Cipher Rule 2

3. Diagonal Selection

If the pass-images form a rectangle, the user selects the images on the opposite corners of the rectangle.

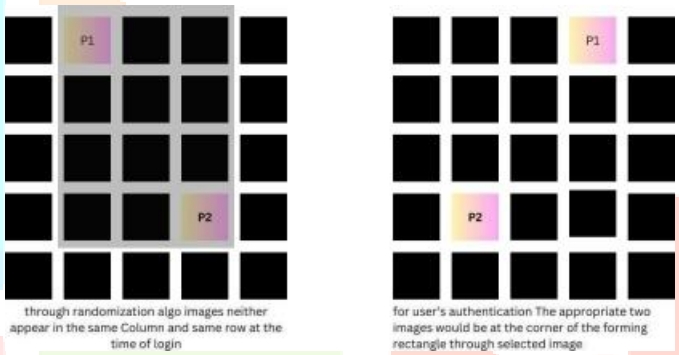

Fig 6: Play-fair Cipher Rule 3

These rules prevent direct guesswork and shoulder surfing attacks by ensuring that the pass-images are not static.

Algorithm:

Registration

1: Display a grid of 25 images in a random order.
2: Prompt the user to select two pass-images from the grid.
3: If the user selects two images:
  a. Store the following data in the database:
    → Image1_ID, Image2_ID
    → Positions of the selected images (row, column)
4: If the data is stored successfully:
  a. Display message: "Registration done successfully"
  b. Redirect the user to the login page.
5: If the selection fails:
  a. Display error message: "Selection failed. Try again."
  b. Reset the selection.

Login

1: Display a grid of 25 images in a shuffled order.
2: Prompt the user to select two pass-images from the grid.
3: If two images are selected:
Apply the Playfair Cipher Rule**:**
a. Same row: Replace each image with the one to its right (wrap around if necessary).
b. Same column: Replace each image with the one below (wrap around if necessary).
c. Rectangle: Swap along the diagonal.
4 : If the selected images match the transformed pass-images:
a. Increment the successful attempt count.
b. If successful for three consecutive attempts**:**
→ Display success message: "Login successful."
→ Redirect to the homepage/dashboard.
5: If the selected images are incorrect:
a. Reset the attempt count.
b. Display error message: "Login unsuccessful. Try again."
6: If three consecutive failures occur:
a. Display message: "Too many failed attempts."
b. Offer option to retry or reset password.

4.4. Password Recovery System:

To enhance user experience and security, our system includes a password recovery module for all three authentication methods: text-based, color-based, and image-based authentication**.** This module ensures that users can regain access to their accounts in case they forget any part of their credentials.

Text-Based Password Recovery

If the user forgets their text-based password, they can reset it using:
Security Question – Users answer a pre-selected security question set during registration.

Color-Based Password Recovery

If the user forgets their pass-color, they can recover it using a security PIN set during registration. The steps are:
The user selects the “Forgot Password” option.
They enter their security PIN.
If the entered PIN is correct, the system allows them to reset it.

Image-Based Password Recovery

If the user forgets their pass-images, they can recover it through the following steps:
The user selects the “Forgot Password” option.
They enter their security PIN. The system then presents a set of images, and the user must select a new set following the row, column, or diagonal rules**.**
Once confirmed, the new images are updated as the pass-image sequence.

Fig 7: Security – PIN system

5. RESULT AND ANALYSIS

To analyze the performance and effectiveness of the multi-phase authentication system, five major metrics were studied through graphical representations. The analysis reveals information about user behavior, system efficiency, and the success and failure of each authentication phase. The findings show how users utilized the system and how the system performed in various cases.

1. First Login Time Analysis

The graph illustrates the first login time for each user, showing significant variability in initial interaction with the system. While some users logged in within a very short time, others took considerably longer. The average first login time is around 12.5 seconds, with the fastest login taking close to 0 seconds and the slowest reaching nearly 25 seconds. The fluctuations in login times suggest differences in how quickly users adapted to the authentication process. Notably, some users showed a steep learning curve, indicating that as they gained familiarity with the system, their login times improved. The presence of peaks and drops reflects the varying levels of user experience and comfort with the multi-phase authentication method.

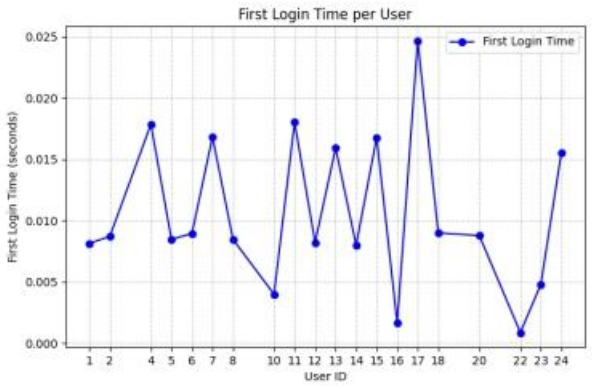

Fig 8: First Login attempt by each user

2. Comparative Analysis of Muliple Login Times for Each Users

Figure 9 illustrates the comparison of the login times of repeat users. The mean login time for repeat users fell from 12.5 seconds on the initial attempt to around 8.3 seconds after five or more successful logins. This decline is indicative of greater user familiarity and enhanced efficiency with the system. Nevertheless, a few users continued to have irregular login times even after repeated attempts, indicating that the complexity of some authentication steps—most notably the color-based and image-based steps—may need to be optimized further. The steady decrease in login time for most users reveals that the system becomes increasingly easy to use with use.

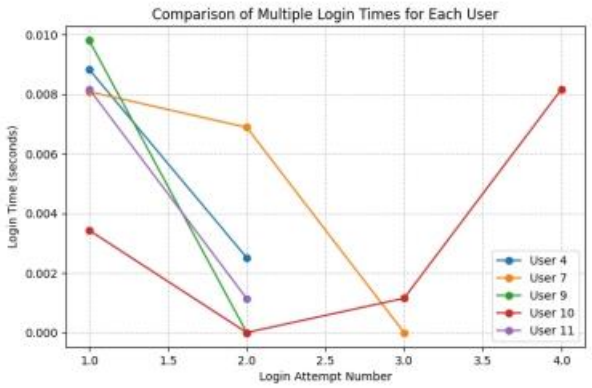

Fig 9: Comparison of multiple login attempt

3. Rate of Success and Failure

The pie chart illustrates the distribution of successful versus failed login attempts in the authentication system. The majority of login attempts were successful, accounting for 93.5% of the total, while failed login attempts made up only 6.5%**.** This indicates that most users were able to log in without difficulty, suggesting an efficient authentication process. The relatively low percentage of failed attempts suggests that users quickly adapted to the multi-phase authentication system. However, the presence of some failed attempts highlights the need for further analysis to determine if specific factors contributed to login difficulties, such as unfamiliarity with the system or errors in credential input.

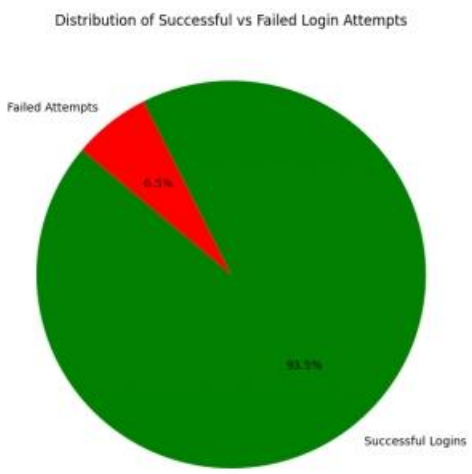

Fig 10: Success vs Failure Rate

4. Success and Failure Rates in Phase-Wise

The bar chart presents the success vs. failure rates across three authentication phases.

- Phase 1 and Phase 2 show a 100% success rate, indicating that all users successfully passed these stages without failure.
- Phase 3 shows a slight drop in success, with a few failures observed. While the majority of attempts in Phase 3 were successful, a small portion of users faced difficulties, suggesting that the third phase might be more complex or challenging compared to the previous ones.

This data highlights that the authentication system functions efficiently in the early stages but may require improvements or user guidance in the final phase to reduce failure rates.

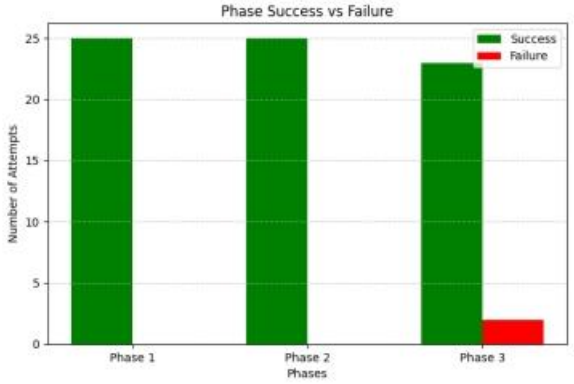

Fig 11: Phase Success vs failure rate

Statistical Overview of Multi-Stage Authentication System

Statistically, the multi-stage authentication system shows an increasing trend of user adoption and effectiveness over time. The average login time dropped from 12.5 seconds during the first attempt to about 8.3 seconds following multiple uses, reflecting a high level of user familiarity and convenience. This decline in login time indicates that users readily adjusted to the authentication process, rendering it more intuitive and effective with multiple uses.The system is seen to exhibit a 93.5% success rate, showing high reliability and efficiency. The 6.5% failure rate implies that although the majority of users completed the authentication process without issues, some small number encountered difficulties, especially during Phase 3. Graphical analysis also supports that the multi-phase authentication system achieves a balance between security and usability successfully. The increasing success rate and decreasing login time reveal that users continue to enhance their performance with increased experience, producing a more efficient authentication process. The findings based on these figures and graphical patterns form a solid basis for enhancing future system development, emphasizing efficiency, security, and user flexibility to enhance authentication performance even further Discussion. The findings validate that the multi-phase authentication system is successful in offering a secure and reliable user verification process. The statistical findings indicate that the learning curve of the system is moderate with steady improvements in user performance with time. The graphical analysis points out that although the text-based phase is fairly easy for users to complete, the color-based and image-based phases add extra complexity that influences overall completion time and success rate.The results indicate that enhancing the visual guidance and feedback processes in the color-based and image-based stages would have a substantial impact on system efficiency and user satisfaction. In addition, the high rate of login attempts reflects high user interest and confidence in the system. The overall balance between security and usability attests that the multi-phase strategy successfully resolves typical authentication issues while ensuring a user-friendly interface.

6. CONCLUSION

With a system of multi-layered authentication that combines text, colored, and image-based methods, this research aims to keep your systems secure from shoulder-surfers, brute-force attacks, and phishing. The defined verification schedule systematically divides into three phases, each phase ensuring a unique dynamically-formed set of challenges, each with randomized image positions, and colored authentication permitting stronger defense against attacks. An additional password recovery feature is included for usability without sacrificing security. Protection against shoulder-surfing attacks-centered points of usability while maintaining a high standard of security have been effectively accomplished. The system can also be optimized further to fit growing authentication security requirements.

7. REFERENCES

[1] R.Vijayakumari, K.Gangadhara Rao 2, B.Basaveswara Rao 3, International Journal of Computer Science and Information Security (IJCSIS), Vol. 15, No. 9, September 2017

[2] Lip Yee Por, Chin Soon Ku, Amanul Islam, and Tan Fong Ang, "Graphical Password: Prevent Shoulder-Surfing Attack Using Digraph Substitution Rules," Frontiers of Computer Science, 2017

[3] Harshada Shitole, Priyanka Chaure, Pradnya Thorat, Ashwini Gaikwad, and Vrushali Sonar, "Graphical Password to Avoid Shoulder Surfing," International Journal for Scientific Research & Development (IJSRD), Vol. 7, Issue 01, 2019

[4] D. Sathish Kumar, R. Rajkumar, and R. Kalpana, "Graphical Image Based Password Authentication System," International Journal of Research and Analytical Reviews (IJRAR), Vol. 6, Issue 2, 2019

[5] Ronak Gangwani, Shantanu Girme, Kiran Kharat, and Jangam D.Y., "Graphical Password to Avoid Shoulder Surfing," International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE), Vol. 7, Special Issue 1, June 2019

[6] Devidas S. Thosar and Dhanraj Verma, "A Modern Image Authentication Algorithm Using Image Click Points To Resist Shoulder Surfing Attack," Webology, Vol. 18, No. 4, 2021

[7] Pathik Nandi and Preeti Savant, "Graphical Password Authentication System," International Journal for Research in Applied Science & Engineering Technology (IJRASET), Vol. 10, Issue IV, April 2022

[8] Meher Gulhane, Amey Andurekar, Vaidehi Kute, Achal Maldhure, and Sharwari Kale, "Graphical Password Authentication," International Research Journal of Engineering and Technology (IRJET), Vol. 10, Issue 03, March 2023

[9] Haichang Gao, Zhongjie Ren, Xiuling Chang, and Xiyang Liu, "A New Graphical Password Scheme Resistant to Shoulder-Surfing," Software Engineering Institute, Xidian University, 2010

[10] Vishal Pednekar, Sayli Tawhare, Arundhati Pradhan, Nidhi Shettigar, Bharati Singh, and Amisha Sahu, "Graphical Password Authentication," Excelssior Education Society's K.C. College of Engineering & Management Studies & Research, 2023