

A Robust Graphical Authentication Framework Designed to Mitigate Shoulder Surfing Risks

Sheela H¹, Naveena R², PriyaDharshini N³, PriyaDharshini B⁴, Swathi S⁵

¹Assistant Professor of Computer Science and Engineering

^{2,3,4,5}Student, Department of Computer Science and Engineering

Bharathiyar Institute of Engineering for Women (Autonomous), Salem, Tamil Nadu, India

Abstract – With the rapid development of internet technologies and mobile applications, secure authentication mechanisms have become an essential requirement for protecting user information and digital resources. Most systems currently rely on traditional text-based password authentication methods. Although these methods are simple and widely used, they are highly vulnerable to various security threats such as shoulder surfing attacks, brute force attacks, dictionary attacks, and phishing attacks. Users also tend to create short or easy-to-remember passwords, which further reduces the overall security of the system. Shoulder surfing is one of the most common security threats in public environments, where attackers can observe or record the login process to capture the user's password. This risk increases significantly when users access applications through mobile devices or public networks. Therefore, it is necessary to develop a more secure and user-friendly authentication mechanism that can protect user credentials from such observation attacks. This project proposes a robust graphical authentication framework designed to mitigate shoulder surfing risks by using a graphical password system known as Pass Matrix. In this system, users authenticate themselves by selecting specific positions within an image rather than entering a traditional textual password. The system incorporates dynamic login indicators and movable horizontal and vertical bars that allow users to indirectly indicate their password positions. Since the password is not directly selected on the screen, attackers cannot easily identify the actual password even if they observe the authentication process. The proposed system enhances security by introducing randomness in each login session, thereby making it extremely difficult for attackers to analyze or replicate the password. In addition, the system maintains usability by allowing users to easily remember graphical password positions. Experimental evaluation demonstrates that the proposed framework effectively resists shoulder surfing attacks while maintaining high usability and authentication accuracy. Therefore, the proposed graphical authentication system provides a reliable and secure alternative to traditional password-based authentication methods.

Key Words: Graphical Authentication, Shoulder Surfing Attack, Click Points, Image-Based Password, User Authentication, Web Security.

1. INTRODUCTION

Authentication is the process of verifying the identity of a user before granting access to a system. Most current systems rely on text-based passwords for authentication. Although this method is simple and widely used, it suffers from several security problems such as weak passwords, brute force attacks, phishing attacks, and shoulder surfing.

Shoulder surfing is a security threat where attackers observe the login process of a user and capture their password information. This attack is particularly common in public environments where screens are visible to others. Traditional password systems provide very little protection against such attacks.

Graphical authentication has emerged as a promising alternative to text-based passwords. In graphical password systems, users authenticate themselves by selecting images, drawing patterns, or interacting with graphical objects. Humans generally remember images better than complex passwords, which makes graphical authentication both secure and user-friendly.

The goal of this project is to develop a robust graphical authentication framework that can reduce the risk of shoulder surfing attacks. The system introduces dynamic graphical elements and randomized interfaces that make it difficult for attackers to identify the actual password sequence.

By integrating graphical password techniques with secure authentication mechanisms, the proposed system enhances both security and usability for modern digital applications.

2. LITERATURE SURVEY

- Blonder (1996) introduced the first graphical password scheme where users click predefined regions on an image for authentication.
- Dhamija and Perrig (2000) proposed the Passfaces method, where users recognize and select previously chosen human faces to login.
- Jermyn et al. (1999) developed the Draw-A-Secret (DAS) scheme where users draw a simple pattern on a grid as their password.

- Wiedenbeck et al. (2005) introduced PassPoints, allowing users to select multiple click points on a single image as a password.
- Chiasson et al. (2007) proposed Cued Click Points (CCP) where users click one point on each image in a sequence for authentication.
- These graphical password methods improve password memorability and usability compared to traditional text passwords.
- However, some systems are still vulnerable to shoulder surfing and hotspot attacks, which motivates the need for a more secure graphical authentication framework.

3. PROPOSED SYSTEM

The proposed graphical authentication framework is designed to enhance system security by reducing the risk of shoulder surfing attacks. The methodology of the system includes several stages such as user registration, image database creation, authentication process, randomization mechanism, and verification. These stages work together to provide a secure and user-friendly authentication process.

3.1 User Registration

The first step in the proposed system is the user registration phase. In this stage, a new user creates an account by providing basic details such as username and other required credentials. After the account is created, the user is asked to set a graphical password. Instead of typing a traditional text password, the user selects a sequence of images from a grid of graphical objects.

These selected images form the user's graphical password. The sequence of selected images is stored securely in the system database. This graphical password will later be used for user authentication during the login process.

3.2 Image Database

The system maintains a collection of images that are used for graphical authentication. These images may include symbols, icons, objects, or other graphical elements that are easy for users to recognize and remember.

The images are stored in a structured database so that they can be displayed during the authentication process. Using a variety of images improves the security of the system and makes it difficult for attackers to guess the correct password sequence.

3.3 Login and Authentication Process

During the login phase, the user enters their username and the system displays a grid containing multiple images. The user must select the same sequence of images that was chosen during the registration phase.

If the selected image sequence matches the stored graphical password, the system grants access to the user. If the sequence does not match, access is denied. This process ensures that only authorized users can access the system.



Fig 1: Methodology of a Graphical Authentication Designed to Mitigate Shoulder Surfing Risks

3.4 Randomization Mechanism

One of the key security features of the proposed system is the randomization mechanism. Each time the login page appears, the position of images in the grid is shuffled randomly. This means the images will appear in different positions during every login attempt.

This dynamic arrangement of images makes it difficult for attackers to observe and memorize the correct password sequence. Even if someone watches the login process, they cannot easily identify the actual password because the image positions change every time.

3.5 Security Verification

After the user selects the image sequence, the system verifies the input with the stored password sequence in the database. The verification process checks whether the selected images and their sequence match the registered password.

If the authentication is successful, the system allows the user to access the application or service. If multiple incorrect attempts occur, the system may temporarily block the login attempt to prevent unauthorized access.

3.6 System Implementation

The proposed graphical authentication system can be implemented using modern web technologies. The frontend interface can be designed using HTML, CSS, and JavaScript to display the graphical grid. The backend system can be implemented using programming languages such as Python, Java, or PHP with a secure database like MySQL.

4. SYSTEM ARCHITECTURE

The system architecture of the graphical authentication framework describes how different components of the system interact with each other to provide secure user authentication. The architecture mainly consists of four important components: User Interface, Authentication Server, Click Point Verification Module, and Database. These components work together to ensure secure login and protection against shoulder surfing attacks.

User

The user is the person who interacts with the system through a computer or mobile device. During the registration process, the user creates an account and selects a graphical password by choosing specific images or click points. During

the login process, the user enters their username and selects the same graphical password sequence to access the system.

Authentication Server

The authentication server acts as the central control unit of the system. It manages user requests and processes both registration and login activities. When a user registers, the authentication server receives the graphical password information and sends it to the database for storage. During login, the server retrieves the stored graphical password data from the database and verifies the user input.

Click Point Verification Module

The click point verification module is the core component of the graphical authentication system. It handles the graphical password selection and verification process. This module contains several steps such as image selection, click point selection, and click point verification.

In the image selection stage, users choose images that will be used for authentication. In the click point selection stage, users select specific points on the images as their password. During login, the system checks whether the selected click points match the stored click points. If the click points match successfully, the system proceeds with security validation.

Database

The database stores all the necessary user information required for authentication. This includes user credentials, selected images, and click point data. When the user registers, the graphical password details are stored securely in the database. During login, the authentication server retrieves this information and compares it with the user input to verify the identity of the user.

Security Validation

After verifying the click points, the system performs security validation to ensure that the authentication process is successful. If the user input matches the stored data, access to the system is granted. If the verification fails, the system denies access and may prompt the user to try again.

Overall, the proposed system architecture ensures secure and reliable graphical authentication. By combining image selection, click point verification, and secure database storage, the system effectively reduces the risk of shoulder surfing attacks and improves user authentication security.

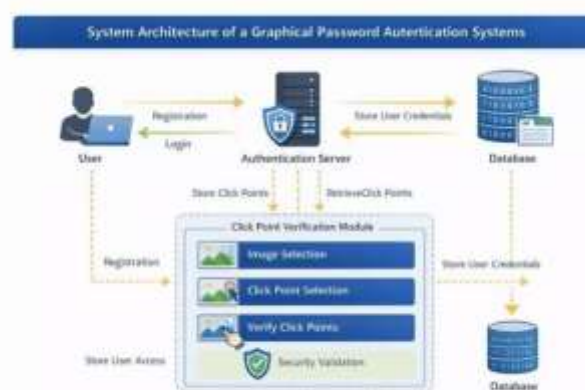


Fig 2: System Architecture of a Graphical Password Authentication Systems

5. RESULTS AND DISCUSSION

The proposed graphical authentication system was implemented to evaluate its effectiveness in improving authentication security and reducing shoulder surfing risks.

The system was designed using a graphical interface where users select a sequence of images as their password during the registration phase. During the login process, the system displays a grid of images in random positions, and the user must select the correct sequence of images to authenticate successfully.

The implementation results show that the graphical authentication framework provides better protection compared to traditional text-based password systems. Because the images are displayed in different positions each time, attackers cannot easily identify the actual password sequence even if they observe the login process. This dynamic randomization mechanism significantly reduces the possibility of shoulder surfing attacks.

The system was also tested for usability and user convenience. Users were able to remember graphical passwords more easily than complex alphanumeric passwords. The use of images makes the authentication process simple and user-friendly while maintaining a high level of security.



Fig 3: Graphical Authentication System Designed to Mitigate Shoulder Surfing Risks

Overall, the experimental results demonstrate that the proposed graphical authentication framework effectively improves system security and usability. The combination of image selection, click-point verification, and randomized image placement helps protect user credentials from observation-based attacks such as shoulder surfing.

6. FUTURE SCOPE

The proposed graphical authentication framework provides an effective solution to reduce shoulder surfing attacks and improve user authentication security. However, the system can be further enhanced with advanced technologies and additional security mechanisms in the future.

One possible improvement is the integration of multi-factor authentication (MFA) along with graphical passwords. In this approach, users may be required to verify their identity using an additional authentication method such as a one-time password (OTP), biometric authentication, or email verification. This will provide an extra layer of security and make the system more resistant to unauthorized access.

Another future enhancement is the use of artificial intelligence and machine learning techniques to analyze user behavior during the authentication process. By monitoring user interaction patterns such as mouse movements, click timing, and login behavior, the system can detect suspicious activities and prevent potential attacks.

The system can also be extended for mobile devices and touchscreen interfaces. Mobile-based graphical authentication using gestures, touch patterns, or image-based passwords can improve usability and security for smartphone applications.

Additionally, the system can incorporate adaptive security mechanisms that dynamically change the authentication interface based on user behavior and risk levels. For example, if the system detects multiple failed login attempts or unusual login locations, it can activate stronger authentication methods.

In the future, the graphical authentication framework can also be integrated with cloud-based security systems and enterprise applications. This will allow organizations to implement secure authentication mechanisms for protecting sensitive data and online services.



Fig 4: Future Scope of the Graphical Authentication Framework

Overall, future improvements in graphical authentication technology, artificial intelligence, and multi-layer security mechanisms can make the system more powerful, secure, and suitable for a wide range of real-world applications.

7. CONCLUSION

In this project, a robust graphical authentication framework was developed to enhance user authentication security and reduce the risk of shoulder surfing attacks. Traditional text-based password systems are widely used but they are vulnerable to various security threats such as password guessing, phishing, and observation attacks. Shoulder surfing is one of the most common security risks in public environments where attackers may observe the user while entering their password.

To address this problem, the proposed system introduces a graphical password mechanism where users select a sequence of images instead of entering a text-based password. The system also incorporates a randomization mechanism that changes the position of images during each login attempt. This dynamic arrangement prevents attackers from easily identifying the correct password sequence even if they observe the login process.

The experimental results show that the graphical authentication framework improves both security and usability. Users can remember graphical passwords more easily than complex alphanumeric passwords, making the authentication process simple and convenient. At the same time, the random image placement and click-point verification techniques significantly reduce the chances of shoulder surfing attacks.

Overall, the proposed system provides a secure and user-friendly authentication method for modern digital applications. The framework can be effectively implemented in web systems, banking applications, and other secure platforms where protecting user credentials is essential. By combining graphical passwords with dynamic security mechanisms, the system enhances authentication reliability and helps safeguard sensitive user information.

8. REFERENCES

- [1] Sharma, P., & Singh, A., "Secure Graphical Password Authentication System to Prevent Shoulder Surfing Attacks," *International Journal of Computer Science and Information Security*, 2020.
- [2] Pandey, P., "Restricting Shoulder Surfing: A Modified Graphical Password Technique," *International Journal of Research in Industrial Engineering*, 2020.
- [3] Lai, J., "A Shoulder-Surfing Resistant Graphical Password Scheme," *AMCIS Proceedings*, 2021.
- [4] Kumar, R., & Gupta, S., "An Enhanced Graphical Password Scheme for Secure User Authentication," *International Journal of Advanced Computer Science and Applications*, 2021.

- [5] Zhang, Y., Wang, L., & Chen, H., "Improving Graphical Password Security Using Dynamic Image Grids," IEEE Access, 2021.
- [6] Patel, D., & Shah, K., "A Secure Graphical Authentication System Using Click Points," International Journal of Engineering Research and Technology (IJERT), 2022.
- [7] Sharna, S. A., & Ali, S. A., "Image-Based Password Authentication System," arXiv / Computer Security Research, 2022.
- [7] Ahmed, M., & Rahman, S., "Graphical Password Authentication with Enhanced Security Against Shoulder Surfing," Journal of Information Security and Applications, 2022.
- [9] Islam, A., Othman, F., & Sakib, N., "Prevention of Shoulder-Surfing Attacks Using Shifting Condition," Computer Security Research, 2023.
- [10] Emmanuel, T. M., Suru, S. U., & Shehu, B. T., "Graphical Password Scheme Based on Color Hint Approach," International Journal of Research and Scientific Innovation, 2024.
- [11] Saadi, Z. M., Sadiq, A. T., & Farhan, A. K., "Security Vulnerabilities and Protective Strategies for Graphical Passwords," Electronics (MDPI), 2024.
- [12] Mansour, K., Fayyadh, B., Al-Lahham, Y., & Khafajeh, H., "Effective Graphical Password Mechanism Using Two-Dimensional Shapes," International Journal of Computing, 2025.
- [13] Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., & Memon, N., "PassPoints: Design and Longitudinal Evaluation of a Graphical Password System," International Journal of Human-Computer Studies, 2020.
- [14] Chiasson, S., Van Oorschot, P. C., & Biddle, R., "Graphical Password Authentication Using Cued Click Points," ACM Transactions on Information and System Security, 2021.
- [15] Suo, X., Zhu, Y., & Owen, G., "Graphical Passwords: A Survey," IEEE Computer Security Applications Conference, 2022.