MULTIFACTOR GRAPHICAL AUTHENTICATION USING CUED CLICK POINT SYSTEM (CYBER SECURITY)

Aasha Shinde, Saloni Awasthi, Shubhangi Harnare, Divya Bhagvat, Manisha Mukhade
Computer Science And Engineering, Babasaheb Naik Collage Of Engineering, Pusa, Dist . Yawatmal, 445204, Maharashtra, India

Abstract
In today's world the password security is very important. For password protection various techniques are available. Cued Click Points are a click-based graphical password scheme, a cued-recall graphical password technique. Users Click on one point of an image. The next subsequent points can be chosen by the user as per his wish. The passwords which are easy to memorize are chosen by the users and it becomes easy for attackers to guess it, but the passwords assigned by the strong system are difficult for users to remember. In this paper, we focus on the evaluation of graphical password authentication system using Cued Click Points, including usability and security. In this authentication system, our usability goal is to support the users in selecting better passwords, thus increases the security by expanding the effective password space.Thus click-based graphical passwords encourage users to select more random, and hence more complex to guess, click points. By digging deep into how these systems handle signals and click points, we hope to make online security both safer and more user-friendly for everyone in the digital age.

Keywords: *Graphical Passwords, Cued Click Points, Authentication Systems, Security, Usability, User Experience, Digital Authentication, and Password Security.*

Introduction:

"Graphical Password Authentication Using Cued Click Points"

This foundational paper introduces the CCP scheme, where users select a single click point per image, and each click determines the subsequent image. It reports high usability (speed and accuracy) and better security compared to PassPoints, owing to its increased image sequence complexity.

This innovative approach adapts to user behaviour and evolving threats, enhancing security dynamically. Multi-Factor Authentication (MFA) further fortifies defences by combining Cued Click Points with traditional passwords or biometrics. Behavioural biometrics add another layer of security by capturing unique user patterns. Geographic security and self-destructing images mitigate risks associated with unauthorized access and prolonged image use. The motivation behind this project arises from the shortcomings of traditional password-based authentication, such as weak passwords and usability issues. By exploring Cued Click Points, we aim to enhance both security and usability. Our objectives include system design, usability evaluation, security analysis, and contributing to knowledge advancement.

Literature Review:

Graphical password schemes—especially **cued-recall** systems like Cued Click Points—leverage the strong human ability to recall images over text. In CCP, users click one point per image and the following image depends on the previous click, increasing the password's complexity by expanding the sequence and reducing predictability. Moreover, cued click points have demonstrated resilience against various security threats, including shoulder surfing and brute force attacks, as evidenced by research conducted by Biddle et al. (2012) and Yan et al. (2004). Despite their promising attributes, challenges such as usability issues and careful image selection persist. Usability concerns, such as the selection of easily guessable points and the memorability of chosen points, highlight the importance of thoughtful design considerations to ensure both security and user satisfaction. In conclusion, cued click points offer a visually intuitive authentication method that strikes a balance between security and usability. Continued research into their optimal implementation and resilience against potential attacks is necessary to fully harness their potential in enhancing online security.

Problem Statement:

Traditional text-based password systems are vulnerable to various security threats such as brute-force attacks, shoulder surfing, and phishing. Users often choose weak or easily guessable passwords due to memorability concerns, compromising system security. While graphical passwords offer a more intuitive and memorable alternative, many existing schemes are still susceptible to attacks like hotspot guessing and pattern repetition. Furthermore, single-factor authentication methods lack the robustness required to secure sensitive systems against unauthorized access. There is a growing need for a secure, user-friendly authentication mechanism that combines the strengths of graphical passwords with additional security layers.This project addresses the problem by proposing a **Multifactor Graphical Authentication System** that leverages the **Cued**

Click Point (CCP) method along with additional factors (e.g., time-based OTP or device verification). The goal is to enhance both the **usability** and **security** of authentication systems by guiding users to select less predictable click points while incorporating multifactor verification to resist common attacks.

Methodology:

Graphical password schemes can be grouped into three general categories: recognition, recall, and cued recall Recognition is the easiest for human memory whereas pure recall is most difficult since the information must be accessed from memory with no triggers. Cued recall falls between these two as it offers a cue which should establish context and trigger the stored memory.

A.Passfaces :

Passfaces is a graphical password scheme based primarily on recognizing human faces. During password creation, users select a number of images from a larger set. To log in, users must identify one of their pre-selected images from amongst several decoys. Users must correctly respond to a number of these challenges for each login. Davis et al implemented their own version called Faces and conducted a long-term user study. Results showed that users could accurately remember their images but that user-chosen passwords were predictable to the point of being insecure.

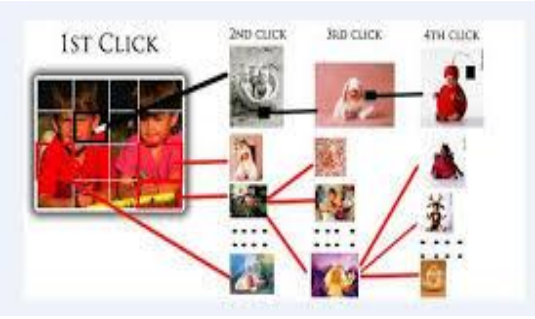
B. Story :

Davis et al proposed an alternative scheme, Story uses everyday images instead of faces, requires that users select their images in the correct order. Users were encouraged for creating a story as a memory aid. It results in somewhat worse than Faces for memorability, but user choices were much less predictable.

C. Passpoint:

Wiedenbeck et al proposed PassPoints, where passwords could be composed of several points anywhere on an image. They also proposed a "robust discretization" schema, with number of overlapping grids, allowing for login attempts that were closely resembling correct to be accepted and converting the entered password into a cryptographic verification key.

D. Cued Click Point:



Cued Click Points (CCP) is a proposed alternative to PassPoints. In CCP, users click one point on each image rather than on five points on one image. It offers cued-recall and introduces visual cues that instantly alert valid users if they have made a mistake when entering their latest click-point. It also makes attacks based on hotspot analysis more challenging.

Implementation:

Technologies Used:

The graphical password authentication system leverages a suite of technologies optimized for web development, database management, and security. Key technologies include operating system such as Windows 7,Windows 8 and Upper version. We also used web server such as IIS and Visual Studio as an IDE tools. Frameworks such as NET, while frontend libraries enhance user interface responsiveness.

Backend Development:

Backend development involves several crucial steps. Firstly, database design establishes the schema for storing user data, click point sequences, and audit logs. Authentication service development focuses on validating user credentials, and processing authentication requests securely. Setting up an image repository enables the storage of images used for graphical password authentication. For backend we use C# that is a popular programming language that uses secure password hashing algorithms to store passwords.

Frontend Development:

Frontend development revolves around user interface design, client-side validation, and session management. Designing intuitive interfaces for registration, login, and authentication screens ensures a seamless user experience. We use HTML/CSS/Bootstrap/Javascript for frontend development.

System Design:

The system designed consists of three modules: user registration module, picture selection module and system login module.

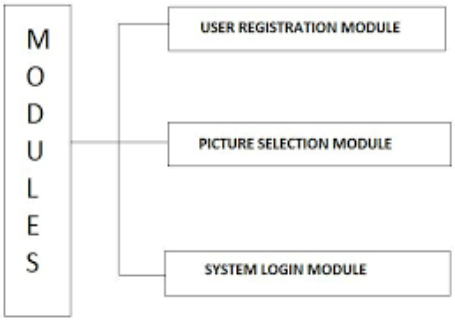


Fig: System Design Modules.

In user registration module user enters the user name in user name. When user entered the all user

details in registration phase, this user registration data is stored in data base and used during login phase for verification. In picture selection phase there are two ways for selecting picture password authentication.

1. User defines pictures: Pictures are selected by the user from the hard disk or any other image supported devices.

2. System defines pictures: pictures are selected by the user from the database of the password system.

In picture selection phase user select any image as passwords and consist of a sequence of five click-points on a given image. Users may select any pixels in the image as click-points for their password. Users must select a click-point in the image and proceed on the next image. During system login process, images are displayed normally, without shading or the viewport, and repeat the sequence of clicks in the correct order, within a system-defined tolerance square of the original click-points.

REGISTRATION:

1. Accessing the Registration Page:

- To get admission to the registration web page, navigate to the graphical password authentication system the use of Cued Click Points. This may be carried out through an internet browser or a devoted application.

2. Creating a New Account:

- Click on the "Register" or "Sign Up" button to begin the registration process.

- You will need to offer the following facts:

- Username: Choose a unique username for logging into the system. - Email Address: Enter a valid e-mail address for verification and communication purposes.

- Password: Create a strong and memorable password that meets specified standards

.3. Selecting Click Points:

- Follow on-display screen commands to select a chain of click factors at the furnished photo.

- Pay attention to the pointers or clues to help consider your click factor series.

4. Confirmation and Submission:

- Review the entered facts for accuracy and completeness.

- Once happy, put up the registration form to create your account.

Login:

1. Accessing the Login Page:

- Navigate to the login web page of the graphical password authentication device, accessible through a web browser or committed application.

2. Entering Credentials:

- Enter your registered username and password into the respective input fields on the login form. - Ensure correct credentials are entered to continue with authentication.

3. Click Point Authentication:

- After entering legitimate credentials, you will be offered a photo containing click-on points.

- Click on predefined click on points within the sequence decided on in the course of registration.

4. Authentication Result:

- If the clicking point sequence suits the one associated with your account, you may be successfully authenticated and granted access.

Conclusion:

The graphical password authentication system provides a simple and secure solution for digital authentication. Using simple registration methods, users can effortlessly access their accounts ensuring strong protection against unauthorized access The system is designed well enough to meet user expectations and implement stringent safety standards through comprehensive functional testing and safety analysis. Continuous improvements and adaptations to emerging threats ensure that the system remains effective and resilient in the face of evolving cybersecurity challenges. Going forward, the new system approach has the potential to revolutionize digital trust across platforms, delivering a simple and reliable approach to protecting user data and privacy Focused attention controlling user feedback, and iterative improvement.

References:

[1] Sonia Chiasson, Elizabeth Stobert, Alain Forget, Robert Biddle, P. C. van Oorschot, "Persuasive Cued Click-Points: Design, implementation, and evaluation of a knowledge-based authentication mechanism", IEEE Trans, Vol 9, Issue 2.

[2] Smith, J. (2018). Graphical Passwords: A Comprehensive Review of Security and Usability. Journal of Cybersecurity, 5(2), 123-137.

[3] Rangari, S., & Ingole, K. R. (2022). Implementation of Graphical Password Authentication Technique for Security Using Cued Click Points Algorithm. International Journal of Human-Computer Interaction, 35(8), 648-662.