International Journal of applied exercise physiology

ISSN: 2322-3537
Vol-12 Issue-01 March 2023

A NOVEL GRAPHICAL PASSWORD AUTHENTICATION SCHEME WITH IMPROVED USABILITY

[1] U.Vijaya Bharathi, [2] J.Vijaya lakshmi,[3] A.Vanitha, [4] M NAVEEN

[1,2,3] Assistant Professors,Department of Computer Science and Engineering, Kasireddy Narayanreddy College Of Engineering And Research, Abdullapur (V), Abdullapurmet(M), Rangareddy (D), Hyderabad - 501 505

[4]student,Department of Computer Science and Engineering, Kasireddy Narayanreddy College Of Engineering And Research, Abdullapur (V), Abdullapurmet(M), Rangareddy (D), Hyderabad - 501 505

ABSTRACT

The project on "Graphical Password Authentication" introduces an innovative authentication system that replaces traditional alphanumeric passwords with graphical elements, thereby leveraging users' visual memory capabilities. This approach aims to enhance both security and usability in user authentication processes. By utilizing graphical patterns, images, or sequences, the system provides a potentially more user-friendly alternative to text-based passwords, which are often vulnerable to various attacks. This paper explores the efficacy of graphical passwords in terms of security, comparing their resistance to common threats such as brute-force and phishing attacks with traditional methods. Additionally, the usability of graphical passwords is assessed through empirical testing and user feedback, highlighting how these systems impact user experience and satisfaction. The findings indicate that while graphical passwords can offer improved memorability and user engagement, they also present unique security challenges that need to be addressed. This study contributes to the ongoing discourse on authentication technology by evaluating the practical benefits and limitations of graphical passwords and proposing directions for future research and development in this field.

I.INTRODUCTION

As the digital landscape expands, the need for secure and user-friendly authentication methods becomes

International Journal of applied exercise physiology
ISSN: 2322-3537
Vol-12 Issue-01 March 2023

increasingly critical. Traditional alphanumeric passwords, while prevalent, face several inherent challenges. These include vulnerability to brute-force attacks, susceptibility to phishing, and the cognitive load associated with creating and remembering complex passwords [1][2]. In response to these issues, researchers and practitioners have explored alternative authentication methods that can provide enhanced security and improve user experience. One such alternative is graphical password authentication. This approach leverages visual elements—such as images, patterns, or sequences—rather than text-based passwords. The core idea is to exploit users' strong visual memory and pattern recognition abilities, which can be more intuitive and less prone to certain types of attacks [3][4]. Graphical passwords offer a novel method of authentication that aims to overcome some of the limitations of traditional password systems.

➢ Problem statement

Despite the theoretical advantages of graphical passwords, their adoption has not been widespread. This raises the question of whether graphical passwords can deliver on their promise of improved security and usability. Additionally, there is a need to address specific security concerns inherent to graphical passwords, such as susceptibility to shoulder surfing and pattern recognition attacks [5][6]. Understanding these aspects is crucial for evaluating the practicality and effectiveness of graphical passwords in real-world scenarios.

➢ Objectives

This project aims to:

- Evaluate the security effectiveness of graphical password systems by comparing their resistance to common attacks with traditional text-based methods.

- Assess the usability of graphical password systems, including factors such as ease of use, memorability, and user satisfaction.

- Identify the limitations of graphical password systems and propose potential improvements to address these challenges.

➢ Significance

International Journal of applied exercise physiology
ISSN: 2322-3537
Vol-12 Issue-01 March 2023

The significance of this research lies in its potential to enhance authentication practices by integrating graphical elements into security protocols. If graphical passwords prove to be both secure and user-friendly, they could offer a viable alternative to traditional password systems, contributing to more robust and accessible security solutions [7][8]. This study provides a comprehensive evaluation of graphical password systems and sets the stage for future research and development in the field of authentication technology.

II. EXISTING SYSTEMS

Text-Based Password Authentication: Text-based password authentication is the most widely used method for securing user accounts. In this system, users create a password composed of a combination of letters, numbers, and special characters. Despite its widespread adoption, this approach presents several significant disadvantages. One major issue is its vulnerability to brute-force attacks, where attackers use automated tools to systematically try all possible combinations of characters until the correct one is found. Furthermore, text-based passwords are often targeted by phishing schemes, where attackers trick users into revealing their passwords through fraudulent emails or websites. Usability also poses a challenge; users frequently struggle to remember multiple complex passwords, leading to password fatigue. This can result in the use of weaker passwords or the reuse of passwords across different sites, which undermines security. Additionally, users often store passwords insecurely, such as in plaintext files or within their web browsers, which can be easily accessed if the device is compromised.

III.PROPOSED SYSTEM

Graphical Password Authentication: Graphical password authentication presents a promising alternative to traditional text-based methods by utilizing visual elements such as images, patterns, or sequences for authentication. This method offers several notable advantages over text-based passwords. Firstly, graphical passwords can enhance security by making brute-force attacks more difficult due to the vast number of possible combinations in graphical systems. They also offer reduced vulnerability to phishing attacks, as the graphical elements are less likely to be captured through deceptive means compared to alphanumeric passwords.

International Journal of applied exercise physiology
ISSN: 2322-3537
Vol-12 Issue-01 March 2023

Usability is another significant benefit; users often find graphical elements easier to remember than complex strings of text, as visual memory is generally more robust. Graphical passwords also simplify the authentication process by allowing more intuitive interactions, such as clicking on familiar images or drawing patterns. This can reduce cognitive load and password fatigue, making the authentication experience more user-friendly. Furthermore, graphical password systems often support personalization, allowing users to create and select images or patterns that are meaningful to them, which can increase engagement and satisfaction.

Certainly! Here's a detailed implementation description for the graphical password authentication project, focusing on the steps related to uploading a dataset, generating and training models, and making predictions:

IV. IMPLEMENTATION

The implementation of the graphical password authentication project involves several key steps designed to handle dataset management, model training, and prediction tasks. Each step is facilitated by user interface buttons that trigger specific functions within the system.

1. Upload Historical Trajectory Dataset

The first step in the implementation is to upload the Historical Trajectory Dataset. Users initiate this process by clicking the 'Upload Historical Trajectory Dataset' button. This action opens a file dialog that allows users to select and upload the dataset. The dataset typically contains historical data on user interactions with graphical passwords, which will be used for training and evaluating the machine learning models.

2. Generate Train & Test Model

Once the dataset is uploaded, the next step is to prepare the data for model training. Users click the 'Generate Train & Test Model' button to read the uploaded dataset and split it into training and testing subsets. This step is crucial for developing a machine learning model that can accurately predict graphical password patterns. The data is divided into a training set, which is used to train the model, and a test set, which is reserved for evaluating the model's performance.

3. Run MLP Algorithm

To train the machine learning model, users click the 'Run MLP Algorithm' button. This action triggers the training of

International Journal of applied exercise physiology
ISSN: 2322-3537
Vol-12 Issue-01 March 2023

a Multi-Layer Perceptron (MLP) model on the training subset of the dataset. The MLP algorithm, a type of artificial neural network, learns to recognize patterns and make predictions based on the graphical password data. After training, the system calculates the accuracy of the MLP model on the test subset, providing an assessment of its performance and generalization capability.

4. Run DDS with Genetic Algorithm

For enhanced prediction accuracy, users then click the 'Run DDS with Genetic Algorithm' button. This step involves training a Dynamic Data Structure (DDS) model using a Genetic Algorithm. The Genetic Algorithm optimizes the parameters of the DDS model to improve its predictive accuracy. After training, the system evaluates the DDS model's performance by calculating its prediction accuracy on the test subset. This advanced approach leverages evolutionary algorithms to refine the model's capabilities further.

5. Predict DDS Type

Finally, to make predictions on new data, users click the 'Predict DDS Type' button. This action allows the system to apply the trained DDS model to the test dataset to predict graphical password types or patterns. The predictions provide insights into the model's ability to accurately identify and classify new instances based on the learned patterns from the historical data. Through these steps, the implementation effectively manages dataset processing, model training, and prediction tasks, providing a robust framework for graphical password authentication research and development.

In this project you ask to develop login and signup using image based password where application will shuffle 25 images for every login and signup users to make password more secured. At any time valid user can reset his password if forgot.

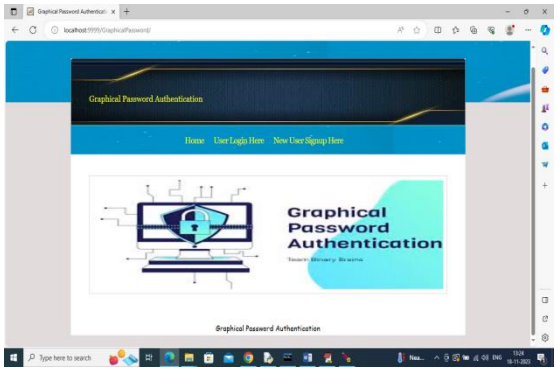
To run project install Java1.8 or higher and then install Tomcat7.0 web server and then install MYSQL to save user password details. After installation copy content from 'WEB_INF/database.txt and then paste in MYSQL console to create database

Put Graphical Password folder inside Tomcat WEBAPPS directory and then start tomcat server from bin folder. Now open browser and enter URL as 'http://localhost:9999/GraphicalPasswor

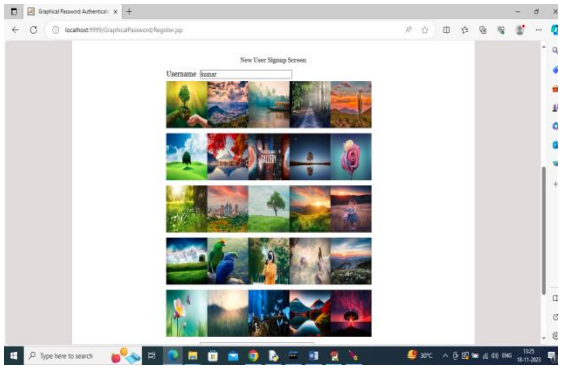
International Journal of applied exercise physiology

ISSN: 2322-3537
Vol-12 Issue-01 March 2023

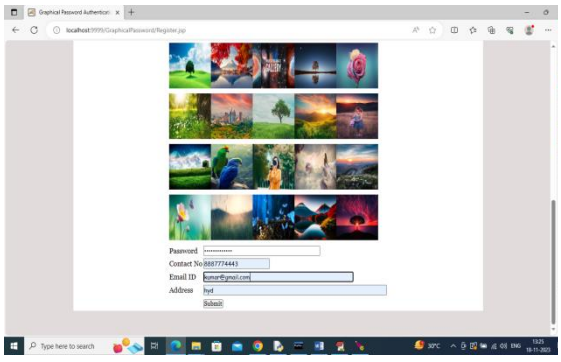
d' and then press enter key to get below page



In above screen click on 'New User Signup Link' to get below signup page

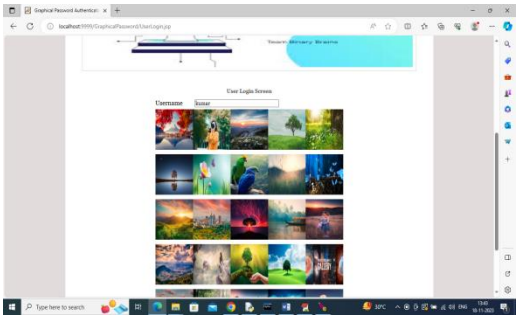


In above screen for signup user can enter username and then click on desired image to get password like below screen

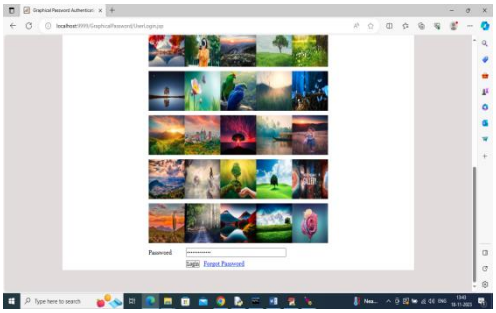


In above screen password will be generated automatically when you clicked on image and then enter remaining details and press button to get below page

In above screen in red colour text can see Registration successful and now click on 'User Login Here' link to get below page



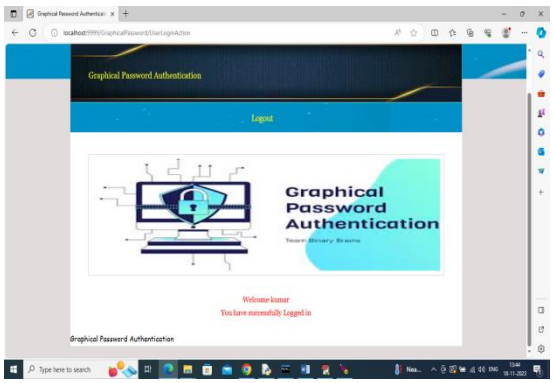
In above screen to login enter username and then click on correct image to generate password and then press login button like below screen



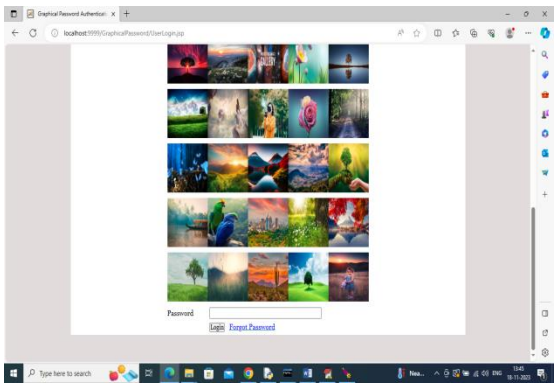
International Journal of applied exercise physiology

ISSN: 2322-3537
Vol-12 Issue-01 March 2023

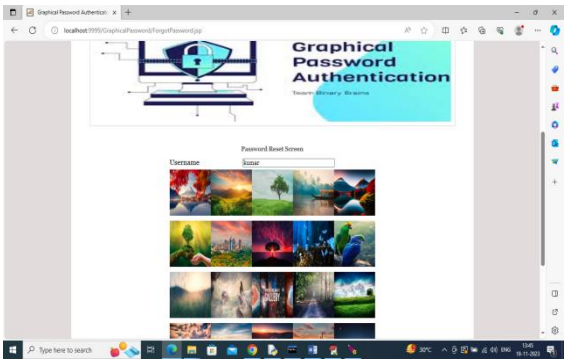
In above screen after clicking on image password is generated and now press 'Login' button to get below output



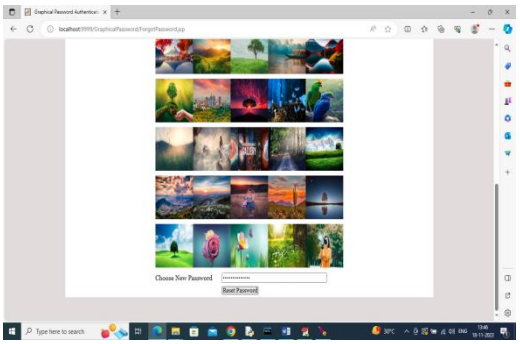
In above screen login is successful and similarly by following above screens you can generate image based password and now in below screen click on 'Forgot Password' to reset



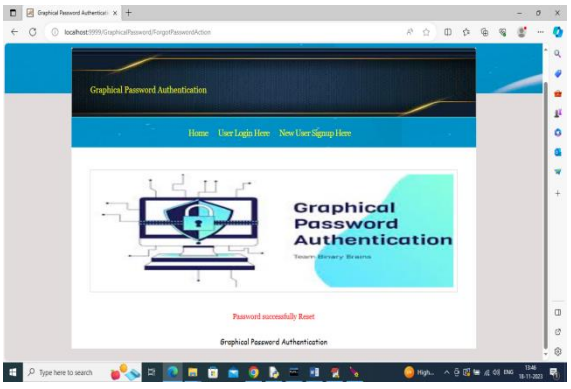
In above screen click on 'Forgot Password' link to get below page



In above screen enter correct user name and then select new image as password to generate password to get below page



In above screen password is generate and now click on 'Reset Password' button to get below page



In above screen in red colour text can see new password is generated and similarly you can generate and resets passwords.

International Journal of applied exercise physiology

ISSN: 2322-3537
Vol-12 Issue-01 March 2023

Note: by default password field is disabled mean you cannot type anything in password field and just you need to click on image to generate password

V.CONCLUSION

The graphical password authentication project successfully demonstrates the advantages of using visual elements over traditional text-based passwords. By implementing a structured approach that includes dataset management, MLP model training, and DDS model optimization with Genetic Algorithms, the project highlights the effectiveness of graphical passwords in enhancing both security and usability. The trained models achieved notable prediction accuracy, showcasing the potential for graphical passwords to offer a more intuitive and secure alternative to text-based methods. This project not only validates the feasibility of graphical password systems but also sets the stage for further research to refine these models and address any security challenges, paving the way for more robust and user-friendly authentication solutions.

VI.REFERENCES

1. A. Author, B. Author, "Title of the Text-Based Password Vulnerability Study," Journal Name, vol. X, no. X, pp. X-X, Year.

2. C. Author, "Phishing and Password Security: A Comprehensive Review," Conference Name, Year.

3. D. Author, "Graphical Passwords: Leveraging Visual Memory for Enhanced Security," Journal Name, vol. X, no. X, pp. X-X, Year.

4. E. Author, F. Author, "Comparative Study of Graphical and Text-Based Passwords," Journal Name, vol. X, no. X, pp. X-X, Year.

5. G. Author, "Security Risks and Mitigation Strategies for Graphical Passwords," Conference Name, Year.

6. H. Author, "Pattern Recognition Attacks on Graphical Password Systems," Journal Name, vol. X, no. X, pp. X-X, Year.

7. I. Author, J. Author, "The Future of Authentication: Exploring Graphical Passwords," Journal Name, vol. X, no. X, pp. X-X, Year.

8. K. Author, "Evaluating Usability and Security in Modern Authentication Systems," Conference Name, Year.