G-PAS

Introduction

Authentication is the process of determining that the person requesting a resource is the right person. Most of the authentication systems nowadays use an integration of username and password. The problem with the password is that it requires the user to remember it and it should be kept secret. Each authentication system has its own guidelines and limitations like password length, password must contain alphanumeric and special characters. These passwords are mostly text-based passwords. Either user use passwords that are easy to remember like license plate number, parent name, phone number, sometimes their own name which are very much predictable or complex passwords which they overlook so they might use the same password for different accounts or they jot down their password somewhere.

Objectives

- To develop an API for graphical password authentication
- To provide better and secure method for login systems
- To create a system in which passwords are easy to remember
- To provide the sound signature in a graphical password authentication system and reduce
- the chances to forget the password.
- To use and implement Graphical Password Authentication in web based system

Methodology

The program will work as a graphical password authentication system that will store different images, and use them as a way of authentication for the convenience of the users.
The basic idea of the proposed system is that at the time of registration, the user enters his/her credentials(name,email, mobile number), after he fills in this information he is redirected to the next page where he is shown a set of 16 images(4*4 matrix) from which he has to select at least 4 images (user must remember the pattern in which images were selected for the login) on the next page the same set is given to the user so to confirm the password by selecting the previously selected images. If the user selects the correct pattern then he is successfully registered and his password has been stored(hashed password). If both the fields don't match then the user is asked to create the password again.

Materials and Methods

We have used HTML, CSS, Javascript and Bootstrap to develop the frontend of the website and we used ejs template engine,express and Node Js,MongoDB and SHA256 for the Backend of the website.

Figure 2: Frontend Login Page

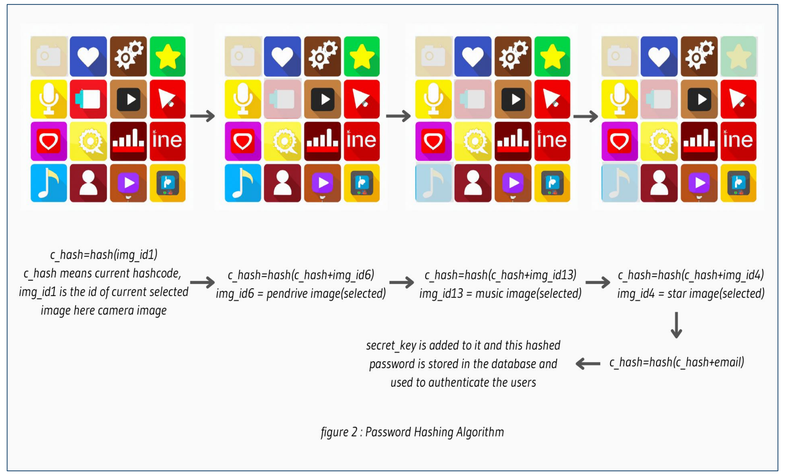

Figure 1: Dataflow diagram

Result

This system aids in increasing the security and protection required in this system. It also gives users many different advantages in many different aspects In addition, it ensures that the authentication is user-friendly and authentic.

Figure 3: Frontend SignUp Page

Abstract

A graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI). This approach is called graphical user authentication (GUA). The most common computer authentication method is to use alphanumeric usernames and passwords. This method has many significant disadvantages.On the other hand, if a password is difficult to guess, then it is often difficult to remember. To overcome this problem, Authentication methods are developed by researchers that use images as passwords.

Survey of existing system

- System #1 by Pathik Nandi, Dr. Preeti Savant :-Since the password space is very large, it offers security against brute force attacks. It's easy to use. Passwords can be easily created and recall.Shoulder navigation attack is subject to safety precaution.
- System #2 by Ahmad Almulhem:-In the proposed system, a user freely chooses a picture, POIs and corresponding words. The order and number of POIs can be enforced for stronger authentication. Together, these parameters allow for a very large password space.

Conclusion

This system is designed for the actual implementation of Graphical Password Authentication to allow users to easily access their account just by remembering an image pattern. The aim of the project was to create a website which would be able to create a graphical password from its user,store them into a database and create a graphical login page. The authentication in our system will be highly secure and it can reduce all the extra efforts of maintaining the records.

References

Towseef Akram, Vakeel Ahmad, Israrul Haq, Monisa Nazir, Graphical Password Authentication

Arash Habibi Lashkari, Abdullah Gani, Leila Ghasemi Sabet and Samaneh Farmand, A new algorithm on Graphical User Authentication(GUA) based on multi-line grids

arode, Sanket Mistry and Saurabh Chavan, Graphical Password Authentication System

Geeta M. Rane, Graphical Password Authentication:Methods and Schemes

Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A., & Memon, N., PassPoints: Design and longitudinal evaluation of a graphical password system

Contact Info

@abdulrehmantahmani20168@acropolis.in
Abdul Rehman Tahami
@ankitaarya20550@acropolis.in
Ankita Arya
@abhisheksharma20465@acropolis.in
Abhishek Sharma
@alokitsharma20401@acropolis.in
Alokit Sharma