GRAPHICAL PASSWORD AUTHENTICATION

Shushanth Parakala, Sri Nishant Reddy Lakkireddy,Prathap Dhamman, Sreenidhi Institute of Science &Technology**,** Telangana India
Mrs Archana Nagelli, (Guide) Assistant Professor, Sreenidhi Institute of Science & Technology , Telangana India

Abstract-Considering how difficult it is to remember alphanumeric passwords, graphical passwords are one alternative. It is simple to access and use any application when user-friendly authentication is made available. According to psychological studies, the human mind can more easily retain visuals than alphabets or digits, which is one of the main justifications for this strategy. By offering a graphical password, we are expressing the authentication granted to the application. With the help of a picture password, we have proposed a graphical security application. In order to authenticate an image, we are employing an object detection method where the password entered by the user or client during registration. Finally, this image password authentication offers application security.

I. Introduction

In the majority of computer security scenarios, user authentication is a crucial element. It serves as the foundation for user accountability and access control [1]. Although there are many different kinds of user authentication systems, alphanumeric usernames and passwords are the most popular kind. They are adaptable and simple to use and apply.

It is necessary to use alphabetic-numerical passwords to meet two conflicting demands. They must be simple for a user to remember and difficult for an impostor to guess [2]. Users frequently select passwords that are simple to decipher and/or short, making them vulnerable to dictionary and brute-force assaults [3, 4, 5]. Enforcing a strong password policy can occasionally have the opposite effect, as users may resort to writing their complex passwords down on sticky notes, leaving them vulnerable to direct theft.

Numerous methods have been suggested in the literature to lessen the restrictions of alphanumeric passwords. Use of a passphrase, rather than a single word, is one suggestion for a solution [6]. Another suggested alternative is the use of graphical passwords, which substitute images for alphanumeric passwords [7]. To do this, ask the user to choose regions from an image rather than typing characters as an in alphanumeric password approaches.

We suggest a graphical password authentication mechanism in this expanded abstract. The method mixes text-based and graphic passwords in an effort to provide the best of both worlds. We give a quick overview of graphical passwords in section 2. Section 3 then provides a description of the proposed system. In section 4, we provide a brief implementation discussion and highlight certain features of the suggested system.

GRAPHICAL PASSWORDS:

The term "graphical passwords" describes the use of images (or drawings) as passwords. Since humans remember pictures better than words, graphical passwords should be simpler to remember [8]. Furthermore, since the search space is virtually limitless, they should be more resistant to brute-force attacks.

The two primary categories of graphical password approaches are recognition-based and recall-based graphical procedures [7]. In recognition-based techniques, a user is verified by asking them to correctly identify one or more images they choose while registering. Recall-based strategies involve asking a user to duplicate what they previously made or chose while registering.

The image password authentication, as previously noted, is a recall-based system in which the user was initially asked to provide a password in the form of text that is in the shape of objects, after which they are encrypted and saved in the database after registration. When logging in, the user uses the images that were listed as objects when registering to prove their identity to the application.

How secure are graphical passwords compared to text-based passwords?

Research on the difficulty of breaking graphical passwords hasn't been done too much. Since graphical passwords are not frequently used in reality, there are no reports on actual instances of graphical passwords being broken. Here, we look at a few potential methods for cracking graphical passwords and attempt to compare them to text-based passwords.

Having a sufficiently vast password space is the primary barrier against brute force searches. The password space for text-based passwords is 94N, where N is the length of the password and 94 is the total number of printable characters, excluding SPACE. It has been demonstrated that several graphical password schemes offer a password space that is comparable to or bigger than text-based passwords. The password spaces for recognition-based graphical passwords are typically smaller than those for recall-based techniques.

A brute force assault against graphical passwords is more challenging to execute than one against text-based passwords. For recall-based graphical passwords, it is especially challenging for attack applications to automatically generate precise mouse motion to mimic human input. In general, we think that graphical passwords are more resistant to brute force attacks than text-based ones.

The use of dictionary attacks against recognition-based graphical passwords is difficult since they require mouse input rather than keyboard input. It is feasible to employ a dictionary attack on some recall-based graphical passwords, but an automated dictionary attack will be significantly more difficult than a text-based dictionary assault. In this area, more investigation is required. In general, we think that graphical passwords are more resistant to dictionary attacks than text-based passwords.

II. RELATED WORKS

A graphical password or graphical user authentication uses graphics rather than letters, numerals, or other special characters to authenticate users. There are differences across implementations in the types of images utilised and how users interact with them.

A. Image series:

- Graphical passwords usually demand the user to reply to images that are shown in a specific order or select images in a specific order.

B. Image generated text:

- A randomly generated grid of images is used in another graphical password method to produce a one-time password. The user searches for images that fall into their pre-selected categories each time they need to authenticate, then enters the randomly generated alphanumeric character that appears in the image to create a one-time password.

B. Face recognition:

- One approach makes use of the power of the human brain to quickly recall faces by asking users to choose a series of faces as a password.

C. Draw a secret:

- A graphical password called Draw-a-Secret requires the user to sketch a picture over a grid. To be authenticated, the user must precisely recall the gestures that the user has sketched. Since it is more difficult for an attacker to copy the strokes and the order in which they are performed, a higher stroke count equates to greater security.

III. PROPOSED SYSTEM

Traditional text-based passwords are frequently replaced with graphic passwords. To authenticate users, it makes use of images, symbols, or patterns. A suggested solution for graphical password authentication is provided here.

To achieve login into the application the user must enter his credentials which will then be compared to the ones stored in the database if the credentials exist the user will be directed to the application

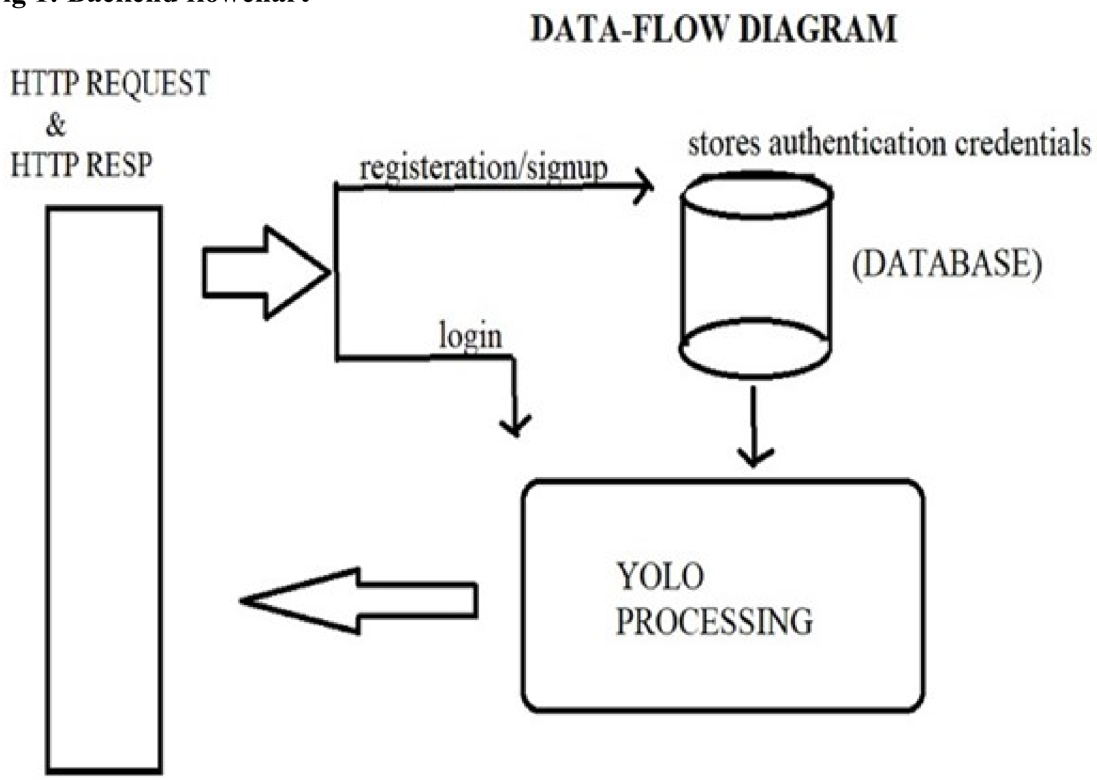
Registration:

The user enters a password during registration that contains the objects. Animals, landscapes, and abstract patterns are all examples of possible visuals. In order to register with the application, the user must select a text format that contains objects that will function as both their password and other general credentials. The password that is stored by the system is encrypted before being stored in a database.

Login

Authentication: The user is shown an image to log in. On the application's login page, they are prompted to choose the image they previously used to log in after providing text descriptions of the items during registration. To strengthen security, the photos can be displayed in a random one that includes the item. The user is given access to their account after choosing the image.

Fig 1: Backend flowchart



We are utilizing the algorithm to accomplish the project's objective. You merely glance once. A technique for object detection is called You Only Look Once (YOLO). It is the algorithmic approach used by the code to identify items in the image.

In our conventional framework, we divide the image into segments and analyze various portions of the image repeatedly at various scales to find an object within the image.

The YOLO algorithm's fundamental concept is to divide the input image into a grid of cells, forecast a bounding box and class probabilities for each cell, and then combine these predictions. These predictions are made by the algorithm using a single neural network, which makes it extremely quick.

Convolutional neural networks (CNN) are used by the YOLO method to extract information from the input image. A sequence of fully linked layers that forecast the bounding box come after the CNN.

The YOLO algorithm is renowned for its excellent accuracy and ability to detect small objects. The YOLO algorithm's ability to detect items that are quite close to one another is one of its drawbacks.

Overall, the YOLO method is a potent tool for object detection tasks and has been implemented in a variety of systems, such as robots, surveillance systems, and self-driving cars.

Security Requirement:

Security precautions: The system can put the following security measures into effect:

1. Timeouts: The user is automatically logged out after a predetermined amount of inactivity.
2. Error Limits: The number of times a user may enter an erroneous series of photos before being locked out of their account may be limited by the system.
3. Captchas: The system may demand that users complete a captcha before logging in to thwart automated assaults.
4. Traditional two-factor authentication techniques, including sending a verification code to the user's email or mobile phone, can also be used by the system.

IV. RESULT

A successful or unsuccessful authentication is the outcome of graphical password authentication. In other words, the user-provided password is either accepted or rejected by the system.

The system will authenticate the user and grant access if they correctly enter the graphical password they previously chose during the registration procedure. This authentication is regarded as successful.

On the other hand, the system will reject the authentication attempt and refuse access if the user inputs an incorrect graphical password. This is regarded as a failed authentication.

The system may also keep track of the amount of failed authentication attempts and take appropriate action, such as locking out the user from their account or requesting additional security checks, such two-factor authentication, before regaining access.

In general, the outcome of graphical password authentication is a crucial component of a system's security because it determines whether or not a person is permitted access to sensitive information and resources.

IMPLEMENTATION AND DISCUSSIONS:

The YOLO (You Only Look Once) principle was used to implement the suggested system it contains Three main classes make up the implementation:

Registration-info: Username , text-based password and related methods

Login-Info: Contains username, graphical password,and related methods.

Graphical Password: Contains graphical password information and related methods

INPUT & OUTPUT SCREENS:

Fig-2 Registration page

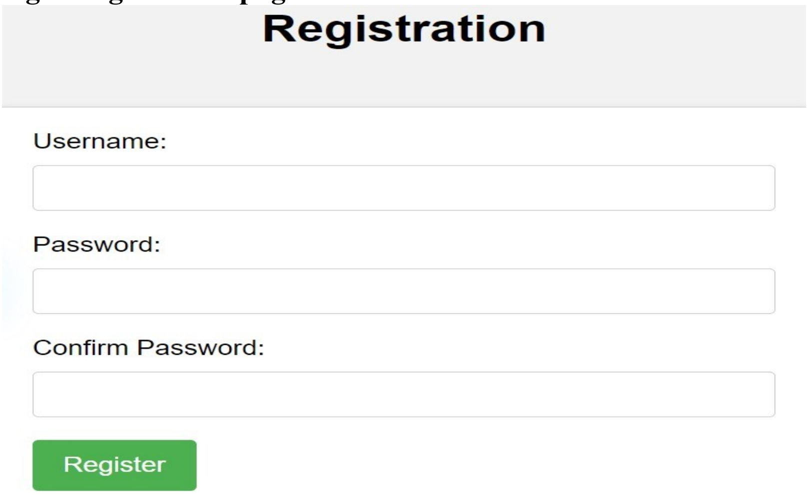
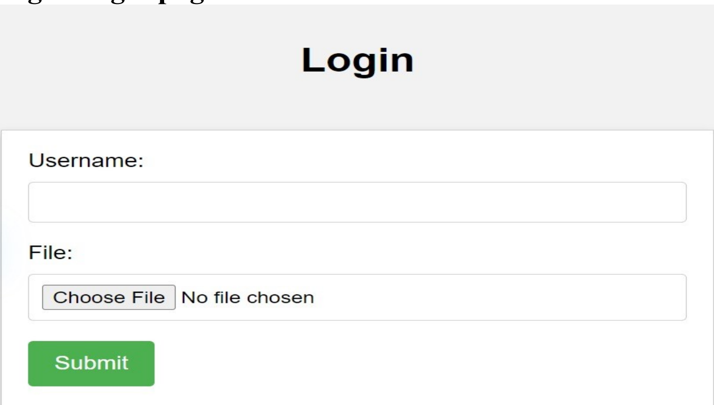


Fig-3 Login page



Login

Username:

File:

Choose File No file chosen

Submit

Case of Successfully login

Fig-4

Yay! welcome to the Appliaction:)

Case of unsuccessful login

Fig-5

x

Your password is incorrect!

V. CONCLUSION AND FUTURE SCOP

The basic goal of graphical password authentication is to offer a reliable signature in a graphical system and lower the likelihood that the password would be forgotten. Hotspots are another issue that exists. Areas of the image known as hotspots are more likely to be chosen by users as password click-points.

In order to authenticate a picture, we employ an object detection technique(yolo) where the user or client registers their password during registration. Finally, this Image password authentication offers application Security.

While passwords are generated by authentication methods, they are still vulnerable to attacks like dictionary attacks, brute force attacks, and shoulder surfing. Supporting users in choosing a stronger password is a key usability objective of an authentication system.

VI. REFERENCES

[1] William Stallings and Lawrie Brown. ComputerSecurity: Principle and Practices. Pearson Education,2008.

[2] Robert Morris and Ken Thompson. Password securitya case history. Communications of the ACM, 22:594– 597, November 1979.

[3] Daniel V. Klein. Foiling the Cracker: A Survey of, and Improvements to, Password Security. In Proceedingsof the 2nd USENIX UNIX Security Workshop, 1990.

[4] Eugene H. Spafford. Observing reusable passwordchoices. In Proceedings of the 3rd Security Symposium. Usenix, pages 299–312, 1992.

[5] Sigmund N. Porter. A password extension for improved human factors. Computers &security

[6] Xiaoyuan Suo, Ying Zhu, and G. Scott Owen. Graphical passwords: A survey. In Proceedingof Annual Computer Security Applications Conference, pages463–472, 2005.

[7] Antonella De Angeli, Lynne Coventry, Graham John-son, and Karen Renaud. Is a picture really worth athousand words? exploring the feasibility of graphicalauthentication systems. International Journal ofHuman-Computer Studies, 63:128–152, July 2005.

[8] Real User Corporation. The science behind passfaces,June 2004.

[9] G. E. Blonder. Graphical password. U.S. Patent5559961, Lucent Technologies, Inc. (Murray Hill,NJ), August 1995.