**Graphical Password Authentication Project Documentation**



Rahul Sharma

[rahultechip@gmail.com](mailto:rahultechip@gmail.com)

<https://github.com/mr-rahul-sharma>

<https://www.linkedin.com/in/rahul-2/>

**Index**

|  |  |
| --- | --- |
| **Sr. No.** | **Topic** |
| 1 | Introduction |
| 2 | Background |
| 3 | Objectives |
| 4 | Technical Details |
| 5 | Results |
| 6 | Conclusion |
| 7 | References |

**Introduction**

With increasing technical advancements, the world is becoming digital at a high pace and everything is happening online. From paying your bills to ticket bookings to paying the person sitting next to you, you prefer to pay online. Not only payments but all activities, be it, communication through e-mails and messaging apps, keeping your documents in a digital locker, etc happen online.

With everything turning online, the risk of cybercrimes and privacy breaches is also increasing. Passwords play a huge role in keeping your data safe online as well as offline platforms. Passwords are the default method of authentication to get access to our accounts. There are various types of authentications available for users to secure their accounts.

**Token-based authentication** includes key cards, bank cards, smart cards, etc.

**Knowledge-based authentication** includes text-based authentication and picture-based authentication.

**Biometric authentication** includes fingerprints authentication, iris scan and facial recognition.

In a graphical password authentication system, the user has to select from images, in a specific order, presented to them in a graphical user interface (GUI). According to a study, the human brain has a greater capability of remembering what they see(pictures) rather than alphanumeric characters. Therefore, graphical passwords overcome the disadvantage of alphanumeric passwords.

**Background**

Passwords are ubiquitous today on any platform, on possibly any website. But to remember so difficult passwords and that too on numerous websites seems daunting and therefore you can devise a project illustrating graphical password strategy. This will allow the user to set passwords in the form of graphical presentation in a certain pattern and later use that pattern to login o the system.

Considering the traditional username-password authentication, the alphanumeric passwords are either easy to guess or difficult to remember. Also, users generally keep the same passwords for all their accounts because it is difficult to remember a lot of them. Alternative authentication methods, such as biometrics, graphical passwords are used to overcome these problems associated with the traditional username-password authentication technique.

Graphical Password Authentication has three major categories based on the activity they use for authentication of the password:

**Recognition based Authentication**: A user is given a set of images and he has to identify the image he selected during registration.

For example, Passfaces is a graphical password scheme based on recognizing human faces. During password creation, users are given a large set of images to select from. To log in, users have to identify the pre-selected image from the several images presented to him.

**Recall based Authentication**: A user is asked to reproduce something that he created or selected at the registration stage. For example, in the Passpoint scheme, a user can click any point in an image to create the password and a tolerance around each pixel is calculated. During authentication, the user has to select the points within the tolerance in the correct sequence to login.

**Cued Recall**: Cued Click Points (CCP) is an alternative to the PassPoints technique. In CCP, users click one point on each image rather than on five points on one image (unlike PassPoints). It offers cued-recall and instantly alerts the users if they make a mistake while entering their latest click-point.

**Objectives**

In this method, the user is required to select some images (let’s say different chocolates) in a specific pattern (for example dairy milk is followed by 5 stars which is in turn followed by KitKat and so on).

Next time the user tries to log in, the images would have been shuffled, but the user will be required to follow the same pattern which was used initially.

Every time the user will have to use the same sequence while the images are placed in different ways.

This type of authentication is difficult to break since neither brute force nor dictionary attacks could breach it.

We need techniques that can be easily implemented and provide better results to this process.

**Technical Details**

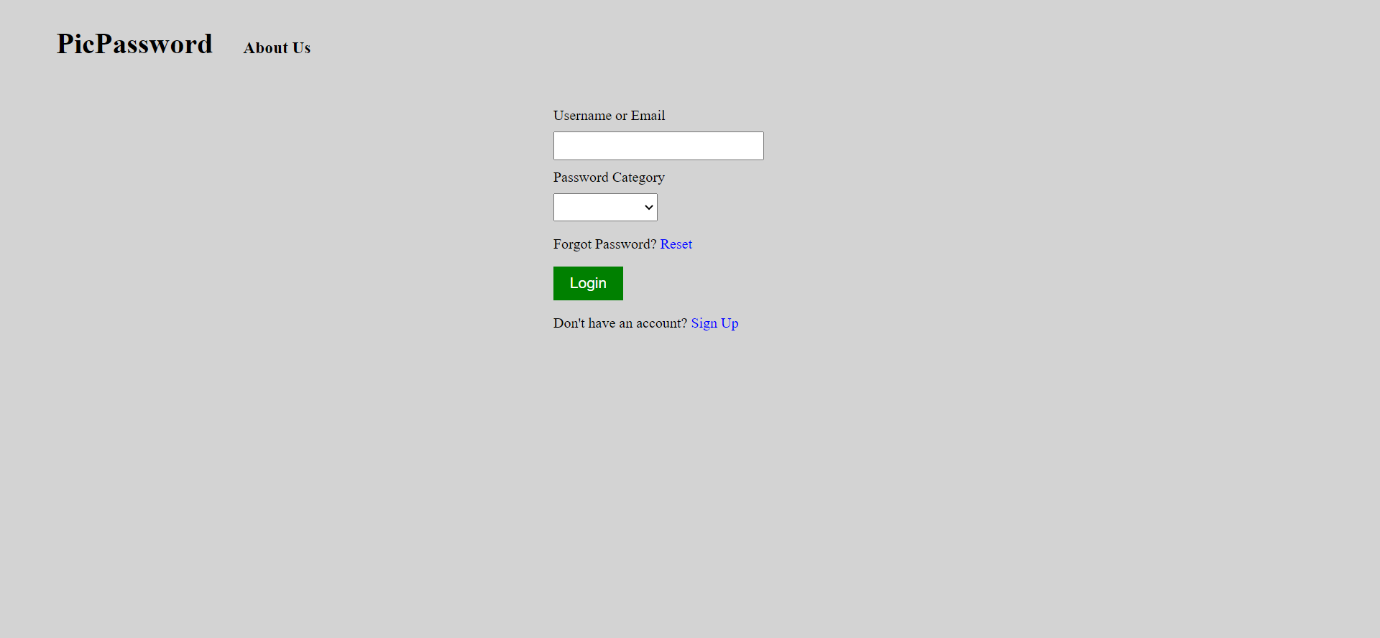
PicPassword is a web application.

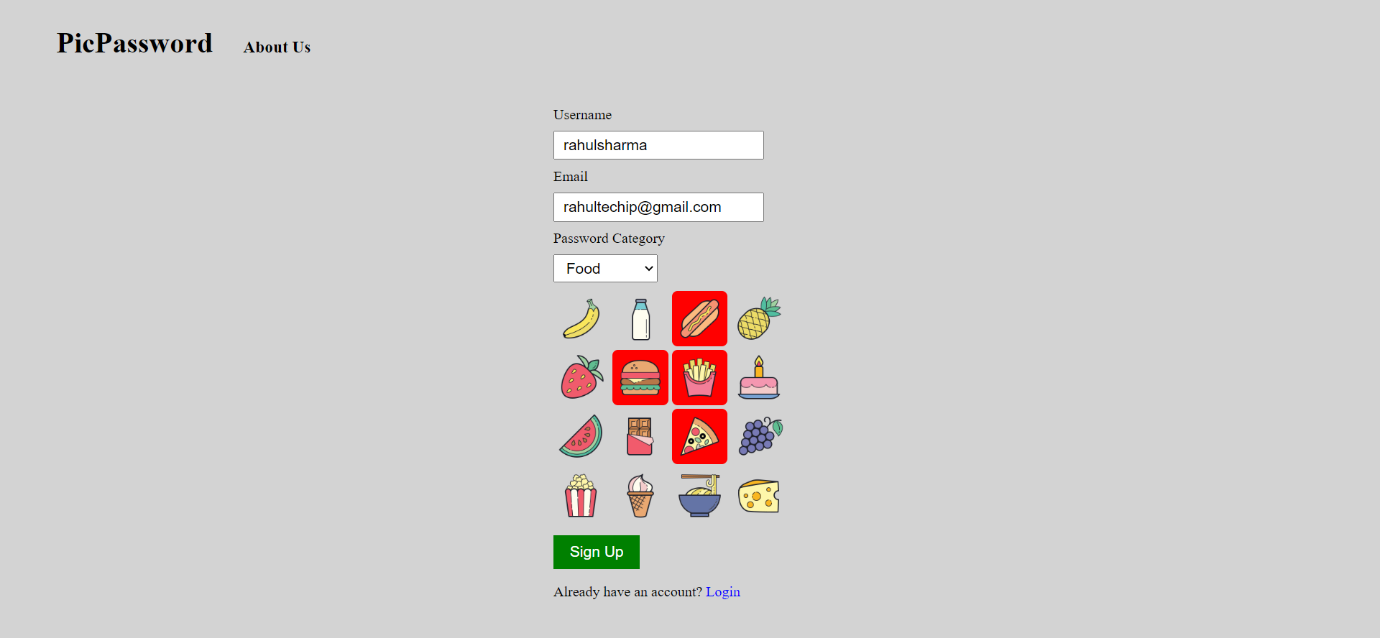
Here are some technical details about the project.

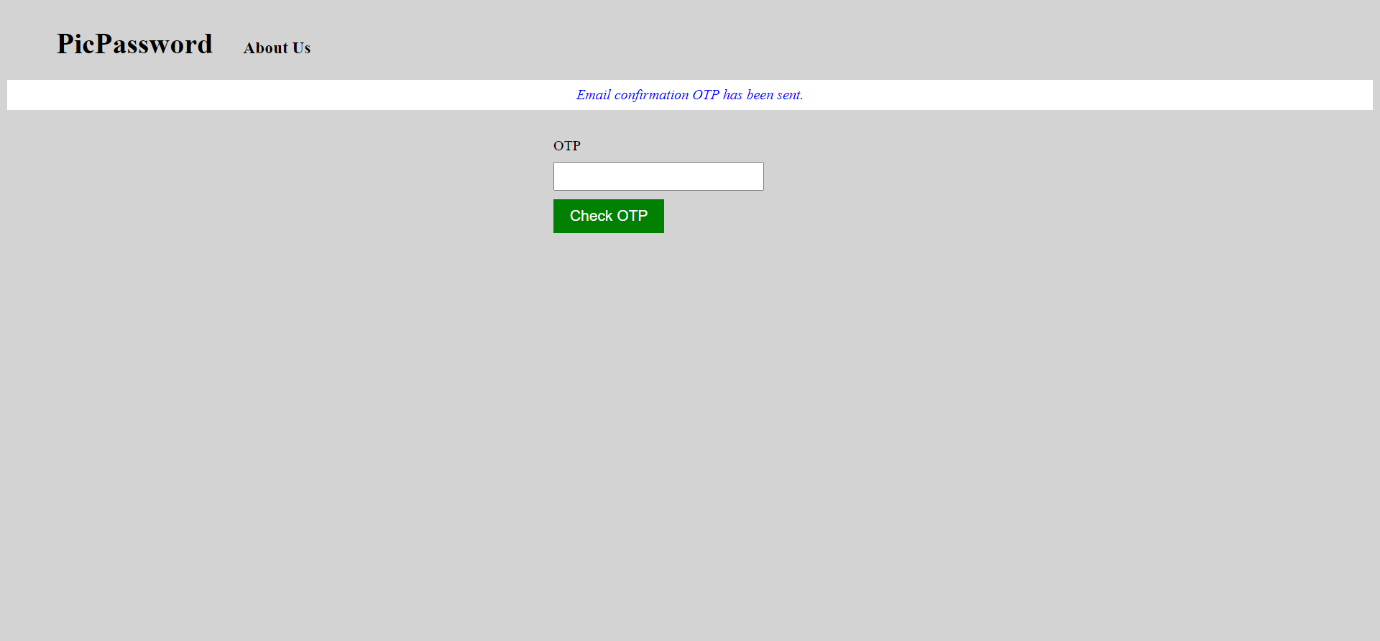
|  |  |
| --- | --- |
| Programming Language | Python |
| Web Framework | Django |
| Database | SQLite |
| User Model | Django default User model |
| Web Languages | HTML, CSS, JavaScript |
| Project Location | <https://github.com/mr-rahul-sharma/picpassword> |
| Project Website | <https://picpassword.herokuapp.com> |

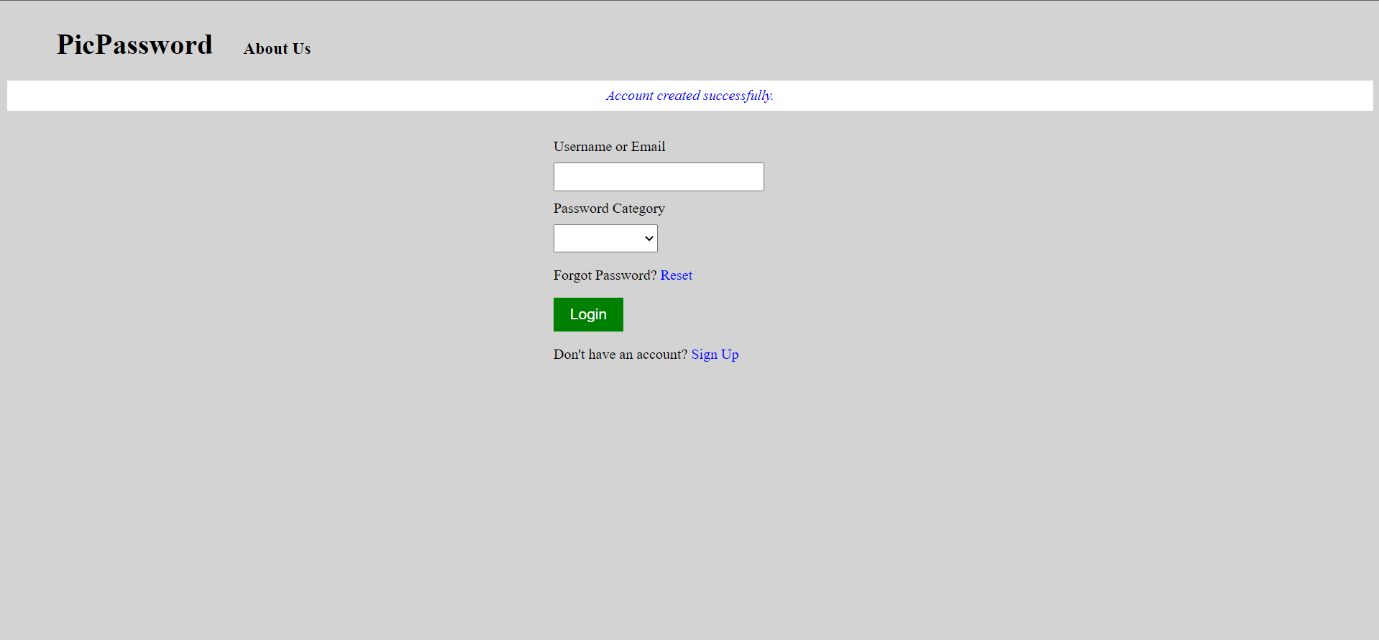
Project location and website may be unavailable.

**Results**

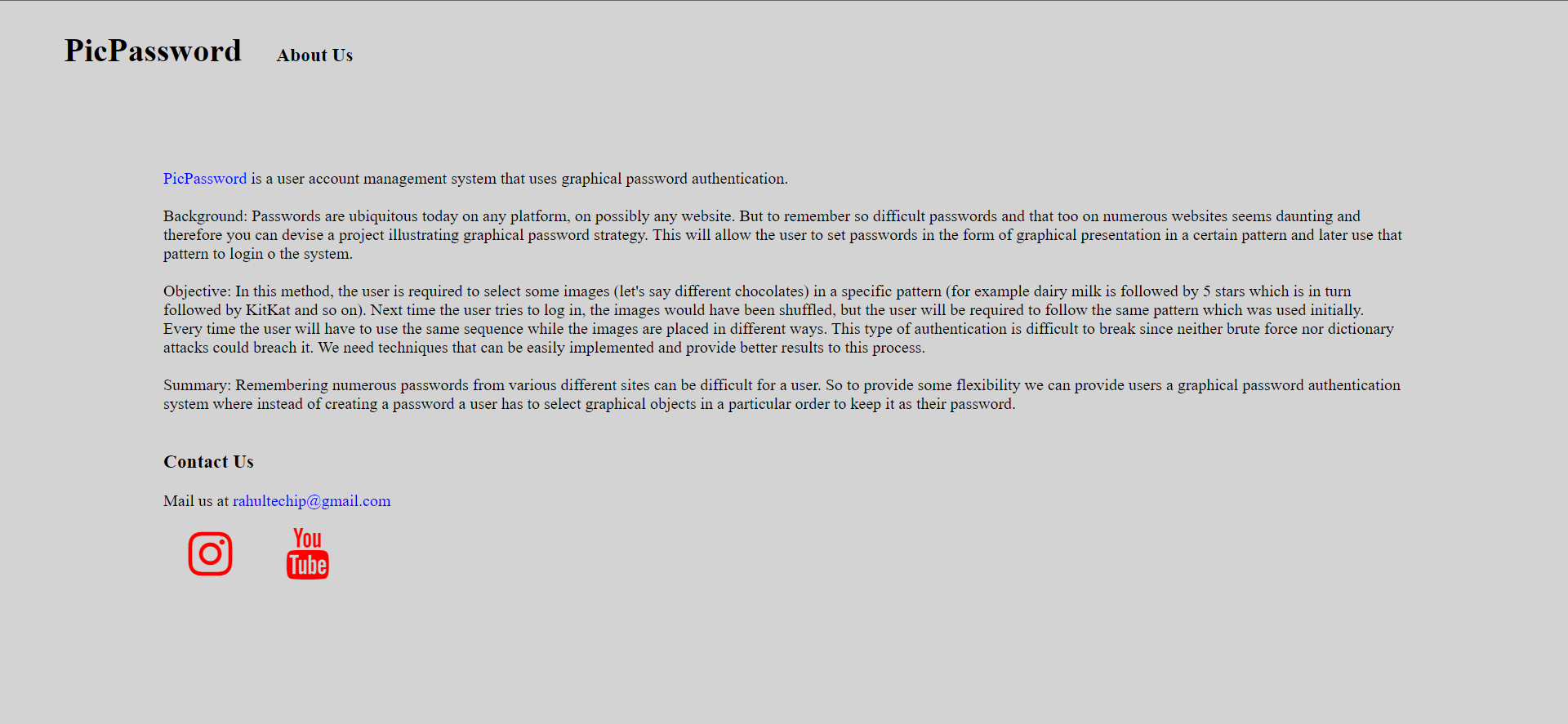












**Conclusion**

Graphical passwords provide a promising alternative to traditional alphanumeric passwords. They are attractive since people usually remember pictures better than words. Remembering numerous passwords from various different sites can be difficult for a user. So, to provide some flexibility we can provide users a graphical password authentication system where instead of creating a password a user has to select graphical objects in a particular order to keep it as their password.

In general, graphical passwords techniques are classi-

ﬁed into two main categories: recognition-based and recall-

based graphical techniques [7]. In recognition-based tech-

niques, a user is authenticated by challenging him/her to

identify one or more images he or she chooses during the

registration stage. In recall-based techniques, a user is asked

to reproduce something that he or she created or selected

earlier during the registration stage

In general, graphical passwords techniques are classi-

ﬁed into two main categories: recognition-based and recall-

based graphical techniques [7]. In recognition-based tech-

niques, a user is authenticated by challenging him/her to

identify one or more images he or she chooses during the

registration stage. In recall-based techniques, a user is asked

to reproduce something that he or she created or selected

earlier during the registration stage

In general, graphical passwords techniques are classi-

ﬁed into two main categories: recognition-based and recall-

based graphical techniques [7]. In recognition-based tech-

niques, a user is authenticated by challenging him/her to

identify one or more images he or she chooses during the

registration stage. In recall-based techniques, a user is asked

to reproduce something that he or she created or selected

earlier during the registration stage

In general, graphical passwords techniques are classi-

ﬁed into two main categories: recognition-based and recall-

based graphical techniques [7]. In recognition-based tech-

niques, a user is authenticated by challenging him/her to

identify one or more images he or she chooses during the

registration stage. In recall-based techniques, a user is asked

to reproduce something that he or she created or selected

earlier during the registration stage

In general, graphical passwords techniques are classiﬁed into two main categories: recognition-based and recall-based graphical techniques. In recognition-based techniques, a user is authenticated by challenging him/her to identify one or more images he or she chooses during the registration stage. In recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage.

This method is beneficial because

It is user-friendly.

It provides higher security than other traditional password schemes.

Dictionary attacks are infeasible.

CCP makes attacks based on hotspot analysis more challenging.

**References**

Graphical Password: Wikipedia

<https://en.wikipedia.org/wiki/Graphical_password>

Graphical Password Authentication: GeeksforGeeks

<https://www.geeksforgeeks.org/graphical-password-authentication/>

Python Documentation

<https://docs.python.org/3/>

Django Documentation

<https://docs.djangoproject.com/en/4.0/>