# Group-3

# Three-Level Password System Using Python

## 1) ***Background/ Problem Statement***

Nowadays, we have known that computer security mostly depends on passwords to verify and authenticate users. There are many authentication schemes proposed and most of them still have weaknesses. Some of them are based on the physical and behavioural properties of the user such as voice recognition, and some others are based on knowledge of the user such as textual and graphical passwords. However, these schemes are still not secure enough and allow attackers to steal the data easily.

Our python-based Three-Level Password System is designed to overcome the problem. It is an authentication system that only allows users to access the system if they have entered the correct password. The project includes three levels of user authentication – Textual, Image and Graphical. That way there would be negligible chances of the bot or anyone else cracking the passwords, even if they crack the first or second level it would be impossible to crack the third.

## 2) ***Working of the Project***

Our python-based consists of 1 module - User. The user can register by adding and entering a conventional alphanumeric password. For second-level authentication, the user can set a password based on

colour combinations through RGB button combinations. To set the third-level authentication, the user will need to upload their desired image into the system.

To log in, the user will need to enter their email and password. Then they would need to choose the RGB combination password and at the last, they would need to choose the correct pattern or combination of the image, from the top-left arrangement, from the jumbled puzzle.

In this project, the front end involves Html, CSS and JavaScript and the back end involves Python. The database: used is MySQL Database and Django is used for the framework.

## *3) Advantages*

- The system is easy to maintain.
- It is user-friendly.
- The system is user-friendly and has a simple interface.
- Provides strong security against bot attacks or hackers.
- Users can set or upload their own images.
- Protects systems vulnerable to attacks.
-

## *4) System Description*

The system comprises 2 major modules with their sub-modules as follows:

❖ **User:**

● Register

- The user can register by adding details & entering a conventional alphanumeric password.
- For second-level authentication, they can set passwords based on colour combinations through RGB button combinations.
- For third-level authentication, they can set an Image-based password where users can upload their desired image into the system.

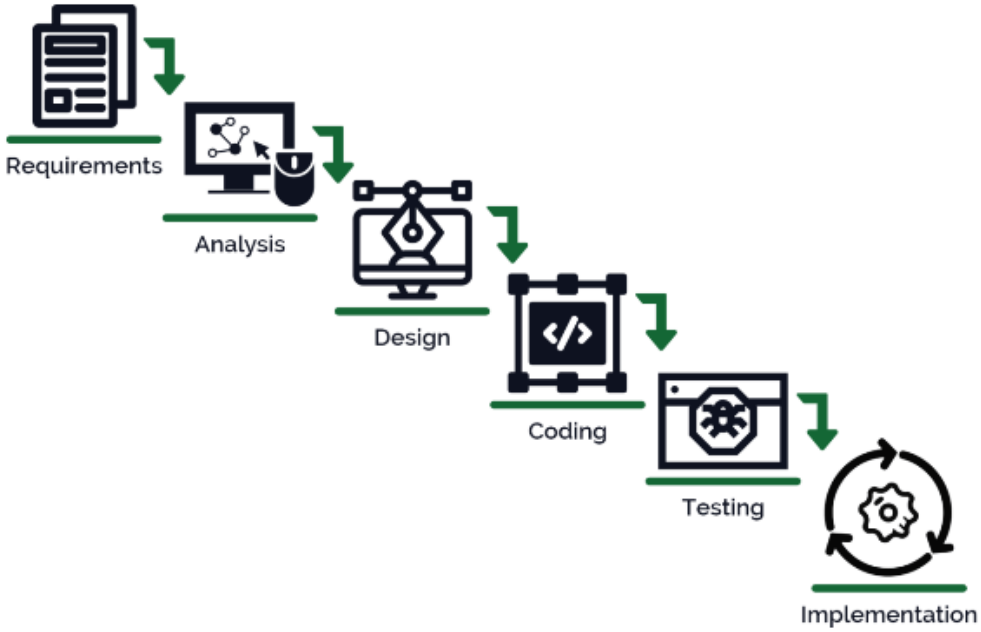
● Login

- To log in, the user would need to enter their email & password.
- For the second level, they would need to choose the RGB combination password.
- For the third level, they would need to choose the correct pattern or combination of the image from the top left arrangement, from the jumbled puzzle.

## *5) Project Life Cycle*

The waterfall model is a classical model used in the system development life cycle to create a system with a linear and sequential approach. It is termed a waterfall because the model develops systematically from one phase to another in a downward fashion. The waterfall approach does not define the process to go back to the previous phase to handle changes in requirements. The waterfall

approach is the earliest approach that was used for software development.




### *6) Limitations/Disadvantages*

- The only disadvantage is if users forget the password, it cannot retrieve it.

### *7) Application* –

- It can be used by individuals or over the internet to protect the system.
- The system can be used in website registrations.

### *8) Reference*

- ✓ *https://myfik.unisza.edu.my/www/fyp/fyp17sem2/report/039892.pdf*
- ✓ *https://www.irejournals.com/formatedpaper/1700566.pdf*
- ✓ *https://ijcrt.org/papers/IJCRT2006540.pdf*
- ✓ *https://projectchampionz.com.ng/2020/04/18/three-level-password-authentication-system/*