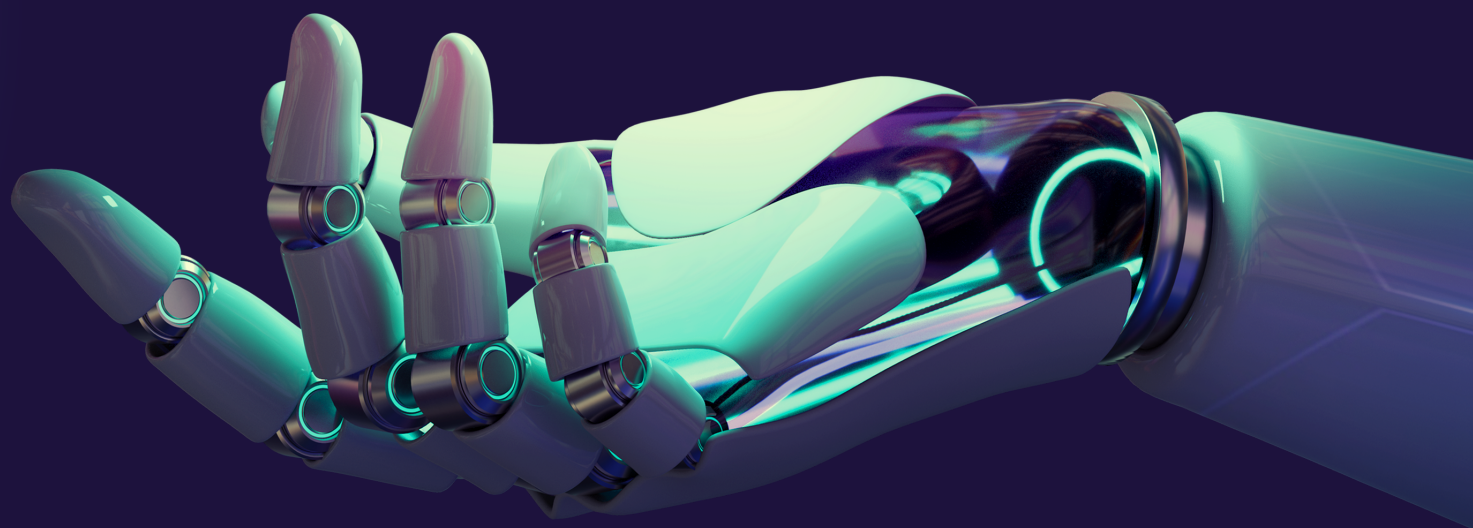
PASSWORD STRENGTH TESTER

(Third Delivrable: High Level Design of the proposed solution)



PROJECT PREPARED BY:

RIMA BEN BRAHIM
ACHRAF BEN ABDALLAH
NOUR MAALEJ
FERYEL GRITLI

The components of the solution:

1- User Interface to Password Strength Tester:

- The User Interface component sends the entered username, password, and password verification data to the Password Strength Tester component.
- This data is transmitted through function parameters.

2- Password Strength Tester:

- The Password Strength Tester component sends the validation outcomes to the Alert System component.
- The validation outcomes could be passed as function return values, event triggers, or API responses.

3 -Alert System:

- The Alert System component delivers the generated alert messages to the User Interface component.
- These alert messages are displayed on the user's screen to provide feedback on the password strength and validity.

The Data Flow of the solution:

1- User Interface sends the entered username, password, and password verification to the Password Strength Tester component:

Password Strength Tester receives the input data and performs the following checks:
a. Custom rules Check: The tester verifies if the password length falls within the specified minimum and maximum lengths and that it meets the required complexity requirements like character types.

b. Entropy check: The password strength tester verifies the entropy of a password by calculating the number of possible combinations that can be generated from a given set of characters, symbols, and length. Entropy is a measure of the randomness and unpredictability of a password, and it is calculated in bits. The formula to calculate the entropy of a password is Entropy = log2(N^L).
where N is the number of possible characters in the password, L is the length of the password, and log2 is the base-2 logarithm function.

c. Common Passwords check: check for common passwords by comparing the user's password against a list of known weak passwords that have been previously exposed in data breaches or that are commonly used.

d. Dictionary password check: The password strength tester can check for dictionary passwords by comparing the user's password against a list of words from a dictionary.

e. Brute force check: The password strength tester tries every possible combination of characters until the correct password is found by Generating a list of possible passwords based on the desired length and character set, Test each password in the list by attempting to log in to the system using that password, assigning a strength score based on the number of attempts required to find the correct password and displaying it along with an error message.

2- Match Check:

- After performing the strength password tests, the Password Strength Tester component proceeds to the Match Check step.
- The component retrieves the values of the password and password verification inputs from the User Interface component.
- It then compares these two values to check if they are identical, indicating that the user has correctly verified their password.
- If the password and password verification values do not match, it means the user has entered different passwords in the two fields.
- In this case, the Password Strength Tester component generates a validation outcome indicating that the passwords do not match.
- The validation outcome is then passed to the Alert System component, which displays an alert message to the user, notifying them that the passwords do not match.

3- Password Strength Tester generates validation results based on the checks performed.

4- The Alert System receives the validation results from the Password Strength Tester and displays relevant alert messages to the user accordingly.

5- If the password meets all the constraints, an alert message indicating a strong password is displayed. Otherwise, specific alerts are shown for each failed validation.

Exchange of Messages/Data:

- User Interface sends the username, password, and password verification data to the Password Strength Tester component.
- Password Strength Tester receives the input data, performs the necessary checks, and generates validation results.
- Password Strength Tester sends the validation results to the Alert System.
- Alert System receives the validation results and displays the appropriate alert messages to the user.