

# DETAILED PROJECT REPORT



# Password Generator

Strong Password Generator to copy

By Mrunal Somankar



## PROJECT DETAIL

Project Title

Password Generator

Technologies

Reactjs

Domain

Security Services

level

Intermediate

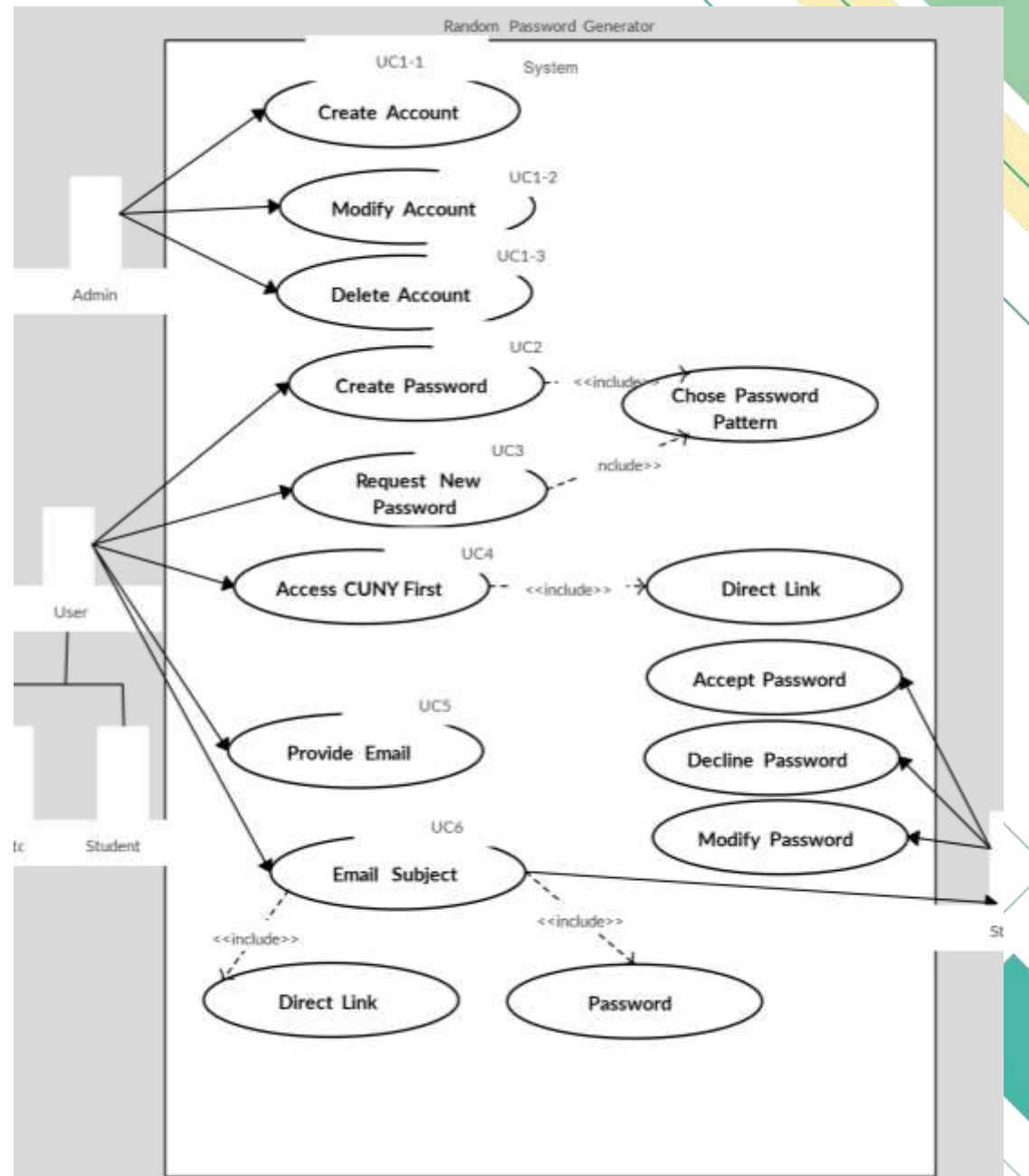
## Objective

The primary objective of the Password Generator Project is to design and implement a robust and secure password generation tool that enhances online security for users.

## PROBLEM STATEMENT

Imagine securing your digital life is like navigating a dangerous jungle of cyber threats. Weak passwords are like poisonous berries – tempting to use but potentially disastrous. Just as identifying safe edibles requires careful observation and understanding, generating strong passwords demands a robust tool and knowledge of cybersecurity principles.

# The Architecture





# DATASET INFORMATION

**Character Sets:** Comprehensive lists of uppercase and lowercase letters, numbers, symbols, and potentially accented characters.

**Algorithm Parameters:** Specifications for password length, complexity requirements (e.g., mix of character types), and customization options.

**User Preferences (optional):** If applicable, user-provided information about desired password length, complexity, or specific character inclusions/exclusions.

**Data Generation:**

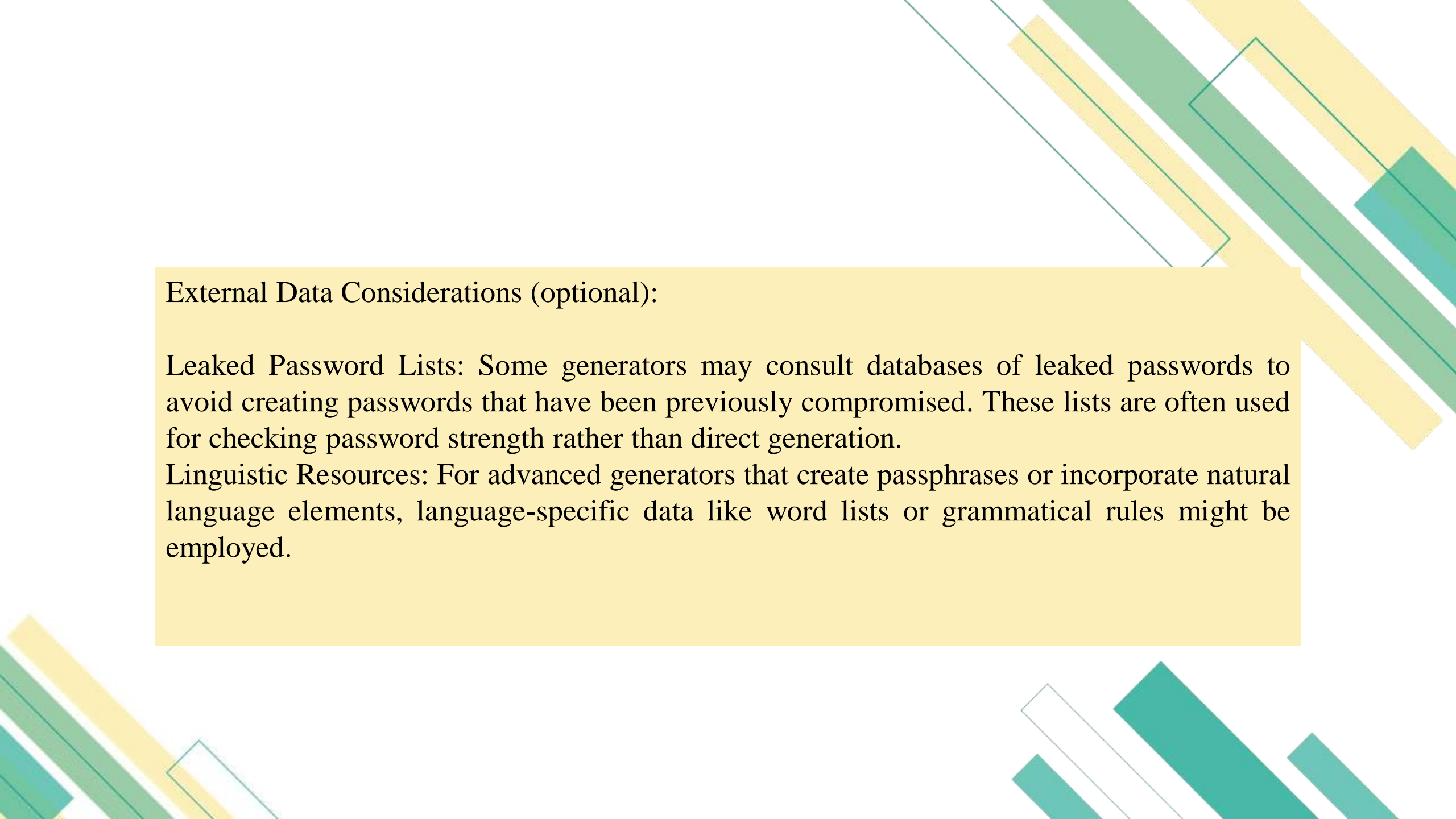
**Algorithmic Randomness:** Secure pseudorandom number generators (PRNGs) are used to create unpredictable sequences of characters for password construction.

**User-Driven Customization:** Users may be able to influence password generation through adjustable parameters or direct input.

**Data Quality and Security:**

**Randomness Testing:** PRNGs undergo rigorous testing to ensure generated passwords are truly unpredictable and resist pattern-based attacks.

**Protection of User Data:** Any sensitive user preferences are stored securely and used solely for password generation purposes.

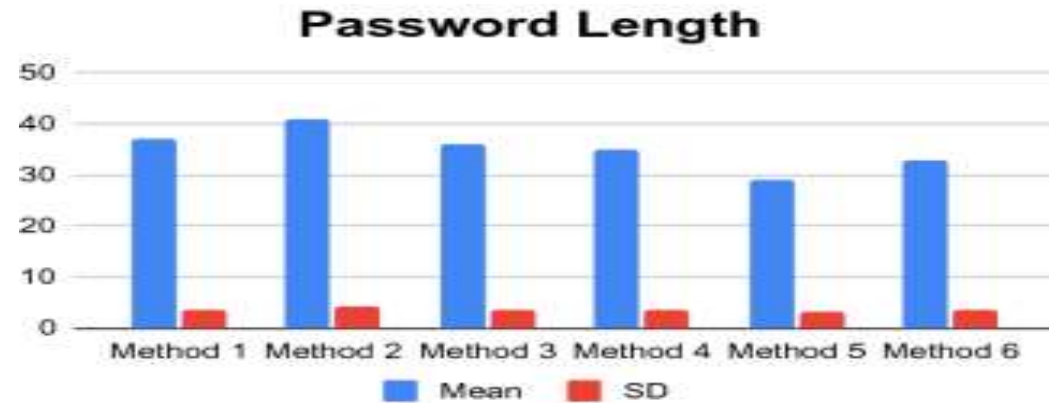
The background of the slide features abstract geometric shapes in shades of green and yellow, primarily located in the top-right and bottom-left corners. These shapes include various rectangles and parallelograms, some with thin black outlines, creating a modern, layered effect.

## External Data Considerations (optional):

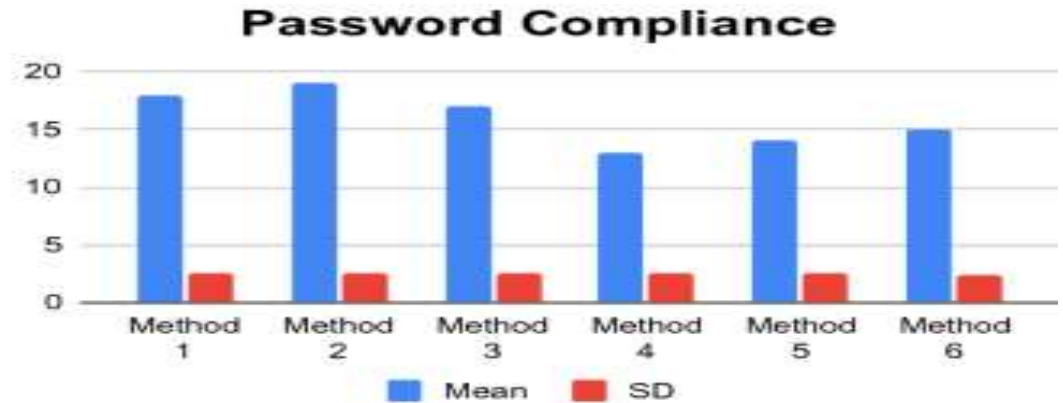
**Leaked Password Lists:** Some generators may consult databases of leaked passwords to avoid creating passwords that have been previously compromised. These lists are often used for checking password strength rather than direct generation.

**Linguistic Resources:** For advanced generators that create passphrases or incorporate natural language elements, language-specific data like word lists or grammatical rules might be employed.

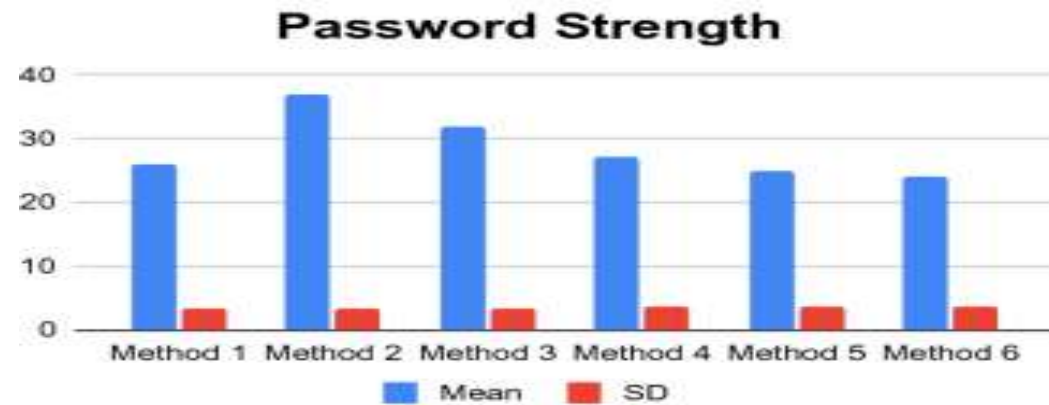
## 2-D Categorical Graphs



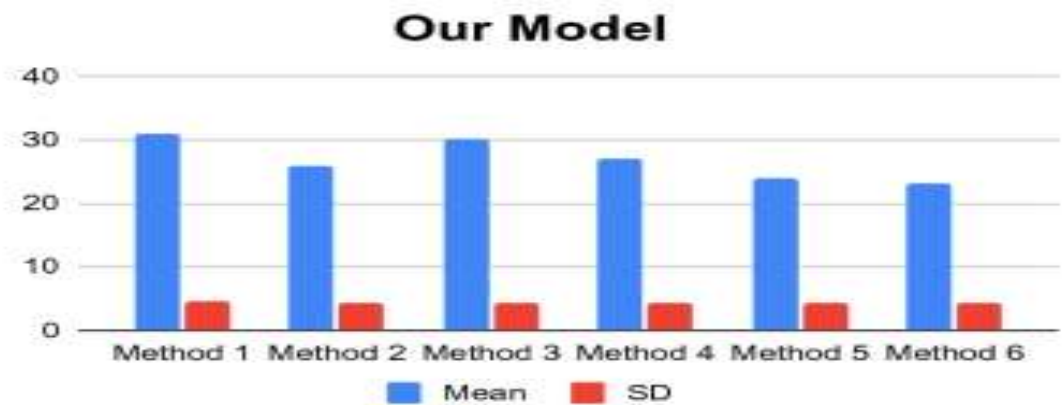
**(a)** Password Length Score



**(b)** Password Compliance Score



**(c)** Existing Strength Estimator Score



**(d)** Proposed Strength Estimator Score



# Result

### Password Generator

Password length

20

Include Uppercase Letters

☐

Include Lowercase Letters

☐

Include Numbers

☐

Include Symbols


☐

Generate Password



## Conclusion

The development and implementation of this strong password generator project have significantly enhanced our digital security landscape. By prioritizing complexity, uniqueness, and randomness, the generator ensures that users can create robust passwords that resist common hacking techniques. The project's success lies in its ability to strike a balance between user-friendliness and security, providing a practical solution for individuals and organizations alike. As we navigate an increasingly interconnected world, the importance of safeguarding our online identities cannot be overstated. This strong password generator stands as a crucial tool in fortifying our defenses against cyber threats, promoting responsible digital practices, and ultimately contributing to a safer and more secure online environment.





**Thank You**