1. Problem Statement

The ubiquity of online services requires users to manage numerous passwords, leading to a critical security vulnerability. Users often resort to weak, guessable, or reused passwords (e.g., "password123," pet names, or birth dates) for the sake of memorability. These predictable passwords are the primary vector for credential stuffing, dictionary attacks, and brute-force hacking, resulting in massive data breaches and unauthorized access to personal and corporate accounts.

The core problem is the conflict between human memory limitations and the requirement for cryptographically strong, high-entropy, and unique passwords for every online account. An automated, reliable solution is needed to generate, display, and manage highly secure passwords that eliminate human predictability and significantly increase resistance to modern cyber-attacks.

2. Scope of the Project

The scope of this project is to develop a standalone, client-side application (Web, Desktop, or Mobile) that focuses exclusively on the secure, random generation of high-entropy passwords.

Inclusions (Core Scope)

Password Generation Core: Implementation of a cryptographically secure pseudo-random number generator (CSPRNG) algorithm to produce unpredictable character strings.

User Customization: Providing a clear interface for users to define password parameters (length, character sets).

Client-Side Security: Ensuring that all password generation logic occurs locally within the user's environment (client-side) and that passwords are not logged, stored, or transmitted by the application itself.

Strength Feedback: Providing real-time visual feedback on the generated password's estimated strength (entropy/bits).

Exclusions (Out of Scope for Initial Version)

Password Management: Storing or encrypting generated passwords (i.e., this is not a full-featured password manager or vault).

Browser Autofill/Extensions: Creating browser extensions or plugins for automatic filling of credentials.

Encryption/Hashing: Implementing features like AES encryption or Argon2 hashing, which belong to a separate password manager application.

3. Target Users

The primary users are individuals and professionals who manage multiple online accounts and prioritize digital security.

Everyday Internet Users

Primary Need: Need simple, one-off strong passwords for new accounts.

Context/Scenario: Signing up for a new e-commerce site, social media platform, or online subscription.

IT/Cybersecurity Professionals

Primary Need: Need to generate strong, compliant passwords for system accounts, VMs, or network devices.

Context/Scenario: Setting up root passwords, initial device passwords, or testing security policies.

Business/Enterprise Employees

Primary Need: Need to comply with company-wide password security policies (e.g., minimum length, complexity).

Context/Scenario: Updating mandatory quarterly password changes for corporate systems.

4. High-Level Features

The application will include the following core capabilities:

Generation Control

Custom Length Slider: Allow users to select a password length from a secure minimum (e.g., 8) up to a maximum (e.g., 64).

Character Set Checkboxes: Allow users to select which character types to include: Uppercase Letters (A-Z), Lowercase Letters (a-z), Numbers (0-9), and Symbols (e.g., !@#$%^&*).

Exclude Ambiguous Characters: An option to exclude characters that can be confusing (e.g., l (lowercase L), I (uppercase i), 1 (number one), 0 (number zero), O (uppercase o)).

Security & Feedback

Cryptographic Randomness: Use the browser's built-in cryptographic API (crypto.getRandomValues) to ensure true randomness.

Password Strength Meter: Real-time calculation and display of the password's entropy (in bits) and a qualitative strength rating (e.g., Poor, Fair, Strong, Excellent).

Usability

Instant Generation Button: A large, easily accessible button to generate a new password based on the current settings.

Copy to Clipboard: A one-click button to securely copy the generated password to the system clipboard, with temporary visual confirmation.

"Passphrase" Mode (Optional): A toggle to generate a more memorable, multi-word passphrase instead of a completely random character string.