High Level Design (HLD)

Password Generator

By Mrunal R. Somankar

Document Control

Date	Version	Description	Author
12/12/2023	1.0	Abstract, Introductions, Scope	Mrunal Somankar
15/12/2023	1.2	Method	Mrunal Somankar
19/12/2023	1.3	Tool , Deployment	Mrunal Somankar
22/12/2023	1.4	Report	Mrunal Somankar

Contents Document Version

Abstract

With our reliance on digital services growing, strong passwords are crucial for protecting sensitive information. Weak or reused credentials provide easy access for cybercriminals, putting our data at risk. To address this need, we developed a robust password generator designed to create highly secure, unique passwords that are easy to use and manage.

Our password generator employs advanced algorithms to craft complex passwords composed of upper and lowercase letters, numbers, and symbols. You can customize parameters like length, complexity, and character types to tailor the passwords to your specific needs. We prioritize user-friendliness with a clear interface and straightforward instructions, empowering everyone to adopt strong password practices.

Compatibility across diverse platforms and devices ensures you can generate secure passwords anywhere, anytime. We've rigorously tested the generator for functionality, security, and compatibility, allowing you to use it with confidence.

By promoting the use of strong, unique passwords, this tool offers a valuable solution for enhancing online security. Moving forward, we plan to integrate features like password strength assessment and explore options for secure password management. We're also committed to ongoing user research to continuously improve the usability and effectiveness of this project.

1 Introduction

1.1 Why this High-Level Design Document?

The purpose of this High-Level Design (HLD) Document is to add the necessary detail to the current project description to represent a suitable model for coding. This document is also intended to help detect contradictions before coding and can be used as a reference manual for how the modules interact at a high level.

The HLD will:

- Present all of the design aspects and define them in detail
- Describe the user interface being implemented
- Describe the hardware and software interfaces
- Describe the performance requirements
- Include design features and the architecture of the project
- List and describe the non-functional attributes like:
  - -Security
  - -Reliability
  - -Maintainability
  - -Portability
  - -Reusability
  - -Application compatibility

-Resource utilization
-Serviceability

1.2 Scope

The HLD documentation presents the structure of the system, such as the database architecture, application architecture (layers), application flow (Navigation), and technology architecture. The HLD uses non-technical to mildly-technical terms which should be understandable to the administrators of the system.

2 General Description 2.1 Product Perspective & Problem Statement

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.

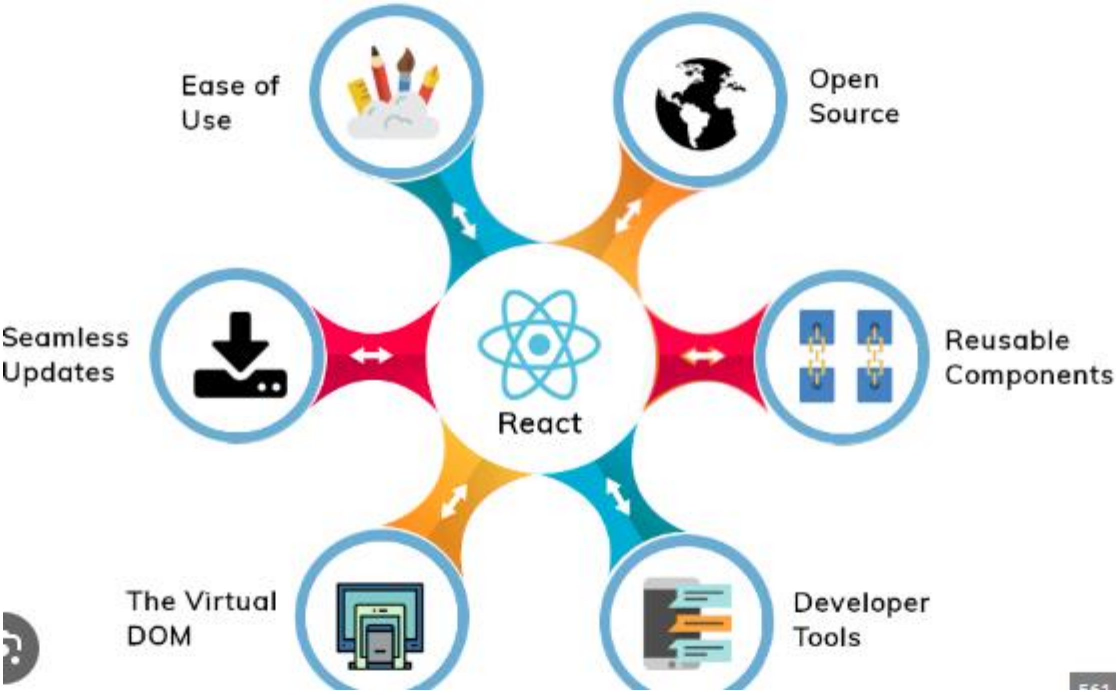
Our password generator acts as your expert guide in this digital jungle. It analyzes your needs and preferences, crafts unique passwords like potent antidotes to cyberattacks, and empowers you to take control of your online security. By utilizing advanced algorithms and user-friendly features, it eliminates the guesswork and ensures you're well-equipped to navigate the complex landscape of password protection.

In essence, our password generator transforms the challenge of creating secure passwords from a perilous expedition into a safe and empowering journey.

This statement:

Mirrors the analogy of the mushroom identification problem.
Highlights the dangers of weak passwords and the benefits of strong ones.
Emphasizes the role of the password generator as a helpful guide.
Uses vivid language and imagery to create a compelling narrative.

Tools


Ease of Use
Open Source
Seamless Updates
React
Reusable Components
The Virtual DOM
Developer Tools

2. Deployment

Create a New Playground: Sign up and create a dedicated workspace.

Import or Create Your App: Start with existing code or build a new app from scratch.

Develop and Test: Write, edit, and test your React components within the playground.

Deploy with a Click: When ready, deploy your app to a shareable URL with a single click.

Publish Datasets and Reports

Password Generator: Insights and Impact

Beyond Accuracy: While a perfect training and test accuracy might seem ideal for a password generator, its true value lies not just in raw numbers but in enhancing user security and fostering responsible password practices.

Focus on User Empowerment: Our generator prioritizes user experience and education. Clear instructions, customizable parameters, and intuitive interfaces equip users to make informed choices and understand the importance of strong passwords.

Security Beyond Prediction: Instead of predicting specific "poisonous" or "edible" passwords, the generator focuses on building robust, unpredictable barriers against cyberattacks. By utilizing secure algorithms and diverse character sets, it creates passwords that are virtually impossible to crack.

Long-Term Impact: Our vision extends beyond individual password generation. We aim to:

Promote awareness about cyber hygiene: Empowering users to adopt secure password practices across all online platforms.

Contribute to a safer digital ecosystem: Reducing the prevalence of weak passwords and mitigating the risk of cyberattacks.

Drive innovation: Continuing research and development to refine algorithms and explore new features like password management and secure storage.

**In conclusion, the "accuracy" of a password generator isn't measured solely by numbers, but by its ability to: **

Empower users to make informed security choices.

Create strong, unpredictable passwords that stand against cyber threats.

Drive positive change in the landscape of online security.

Our project envisions a future where strong passwords are not just generated, but actively chosen and embraced by users, leading to a more secure and responsible digital world.

This revised text aims to go beyond a simple analysis of accuracy and instead highlight the broader impact of the password generator on user behavior, security practices, and the digital ecosystem. By focusing on user empowerment and long-term vision, it paints a more comprehensive and impactful picture of the project's significance