INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 05, May 2023, pp : 1238-1240

e-ISSN : 2583-1062

Impact Factor : 5.725

PASSWORD GENERATOR AND MANAGER TO PREVENT CREDENTIAL STUFFING, DICTIONARY ATTACK AND BRUTE FORCE ATTACK

Arumbaka Prakash[1], Arun N [2], Jeevanraj R [3], Mr. G. Praveen Kumar[4]

[1,2,3]Student, Computer Science and Engineering, Agni College of Technology, Chennai-600 130, Tamil Nadu, India

[4]Assistant Professor, Computer Science Engineering, Agni College of Technology, Chennai-600 130, Tamil Nadu, India

ABSTRACT

The Password Generator and Manager employs advanced algorithms and security best practices to generate highly robust passwords. By utilizing cryptographic techniques and randomization, the system ensures the creation of passwords that are resistant to common hacking methods. The Password Generator and Manager addresses the vulnerability of weak and reused passwords, mitigating the risks of credential theft, unauthorized access, and data breaches. By generating complex and unique passwords, users are protected against dictionary attacks and brute force attacks, as the passwords incorporate a wide range of characters, symbols, and lengths.

1. INTRODUCTION

As the digital landscape continues to evolve, protecting sensitive information has become increasingly crucial. One of the key pillars of online security is the generation and management of strong, unique passwords.

The Password Generator and Manager utilizes advanced algorithms and security best practices to generate highly secure passwords.

By leveraging cryptographic techniques, the system ensures the creation of random, unpredictable passwords resistant to common attack vectors. Additionally, the password management functionality provides a secure repository for storing and organizing these passwords.

When it comes to security, randomization is vital in defending against attacks. For example, in password generation, randomization ensures the creation of strong, unpredictable passwords, making it harder for adversaries to guess or crack them. Randomization techniques are also used in network protocols to prevent predictable patterns and mitigate risks such as replay attacks or traffic analysis.

2. LITERATURE SURVEY

1."A Comprehensive Study of Password Management Tools" by Shuo Yang, et al. (2016) - This study compares and evaluates various password manager tools, including their features, security, and user experience.

2."Password Managers: Attacks and Defenses" by Zhiwei Li, et al. (2014) - This paper examines the security and vulnerabilities of password manager tools and proposes solutions for improving their security.

3."A Comparative Analysis of Password Generators" by Mohamed Ouanane and Abdelmalek Amine (2020) - This paper compares and evaluates different password generator techniques, including deterministic and probabilistic methods.

3 MATERIALS AND METHODS

3.1 EXISTING SYSTEM:

The existing system section describes the currently available password generator and manager tools in the market. It mentions popular tools such as LastPass, 1Password, and Dashlane and highlights some of the features they offer, such as password generation, password strength analysis, password synchronization across devices, and multi-factor authentication. However, it also acknowledges that these tools may have limitations such as subscription fees, limited features in the free version, or concerns about the security of user data.

3.2 PROPOSED SYSTEM:

The proposed system section outlines the features and functionality of the password generator and manager system that will be developed as part of this project. It mentions that the system will allow users to generate strong and unique passwords. The system will also provide options to manage passwords easily. The system will be accessible through a user-friendly web-based interface.

3.3 SOFTWARE USED:

Languages: HTML, CSS, JavaScript

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor : 5.725

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 05, May 2023, pp : 1238-1240

4 CATEGORIES OF MODULES

4.1 PASSWORD LENGTH MODULE:

The password length module is an important component of a password generator and manager. It allows the user to choose the desired length of their generated passwords.

4.2 PASSWORD SETTING MODULE:

The password setting module is a crucial component of any password generator and manager system. It provides the user with options to customize the generated passwords according to their needs.

4.3 PASSWORD GENERATION MODULE:

To ensure the strength and uniqueness of the generated passwords, the password generator will use advanced algorithms and techniques, such as randomization, entropy, and pattern recognition. This will help to prevent predictable passwords that could be easily guessed or hacked.

The password generate module will also provide an option to test the strength of the generated passwords. This will help users to assess the security of their passwords and make any necessary adjustments.

4.4 PASSWORD STRENGTH ANALYSIS MODULE:

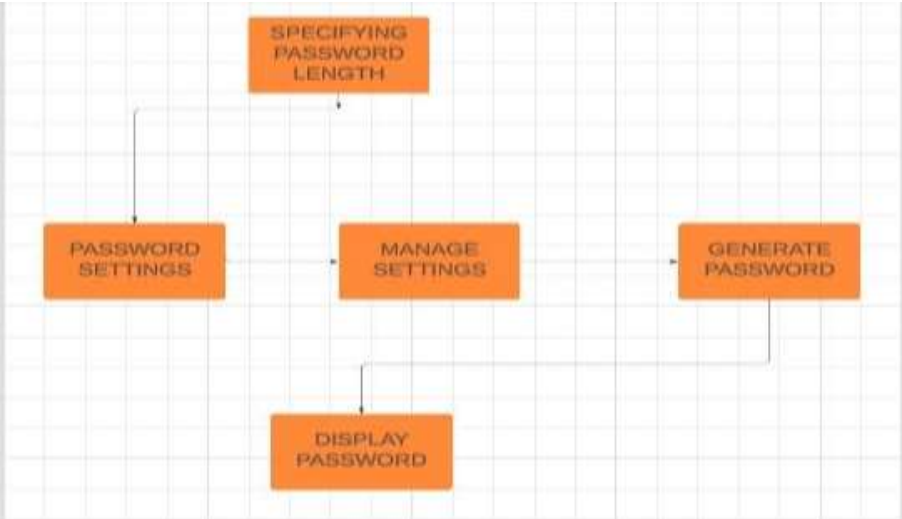
The system can analyze the strength of passwords entered by users and provide feedback to encourage the use of strong passwords

4.5 PASSWORD COMPLEXITY RULES MODULE:

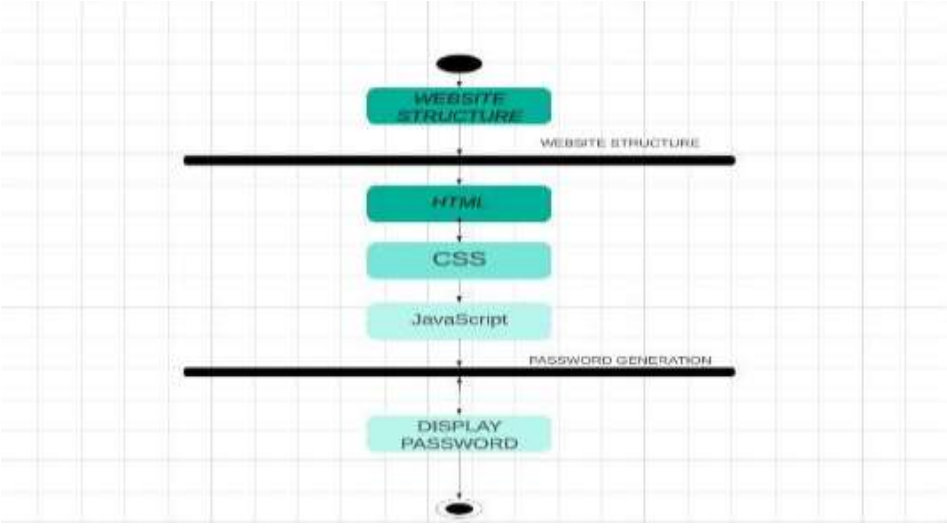
The system can enforce password complexity rules to generate strong and unique passwords. These rules can include requirements for minimum length, the use of uppercase and lowercase letters, numbers, and special characters

5 MODELING AND ANALYSIS

5.1 WEBFLOW DIAGRAM



5.2 SYSTEM ARCHITECTURE:



INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor : 5.725

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 05, May 2023, pp : 1238-1240

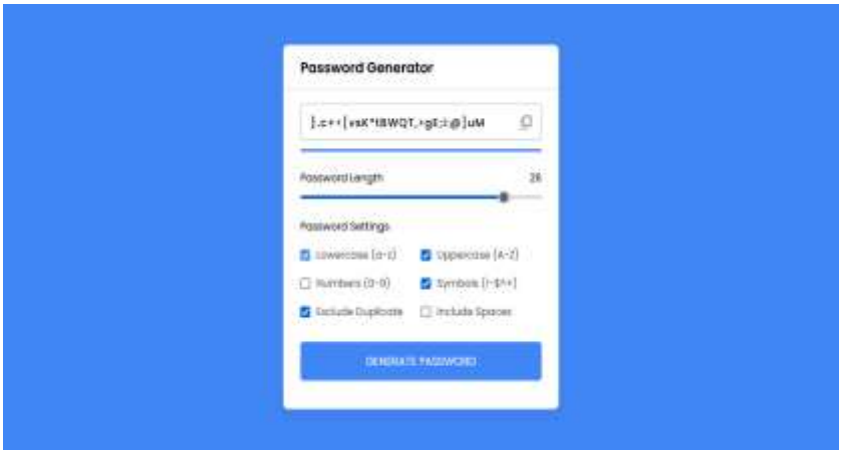
6 RESULT & DISCUSSION

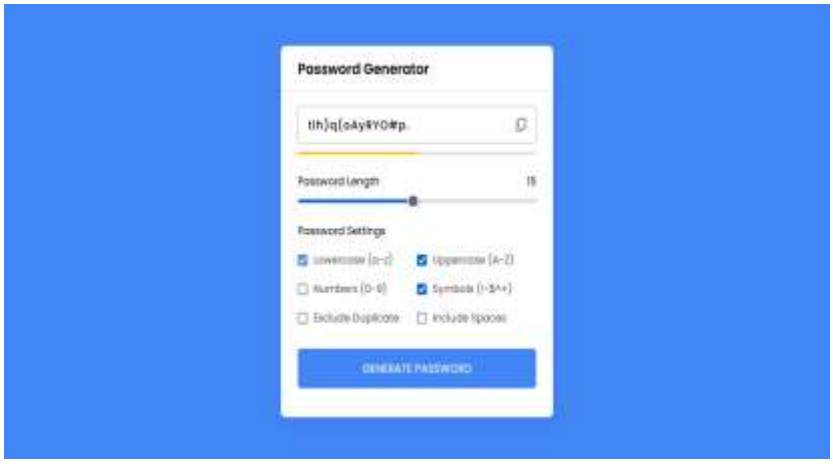
Password generators create strong and random passwords based on user-defined complexity options, ensuring that passwords are difficult to guess or crack

By utilizing password generators, users can create complex and unique passwords, while password managers simplify the management of these passwords.

Overall, the password generator and manager system can effectively prevent attacks such as credential stuffing, dictionary attacks, and brute force attacks.

6.1 SCREENSHOTS





7 CONCLUSION

In conclusion, password generators and managers are essential tools for enhancing online security and managing multiple passwords effectively. In future as new technologies emerge, password generators and managers can be integrated with block chain technology to provide decentralized and tamper-proof password storage or leverage machine learning algorithms to improve password strength analysis and prediction.

8 REFERENCE

[1] Li, X., Wu, D., Zou, D., Liu, J., & Zhang, Y. (2019). An Improved Password Manager Based on AES and SHA-256 Algorithms. In International Conference on Cloud Computing and Security (pp. 177-187). Springer, Cham.

[2] Chatterjee, A., Chakraborty, S., & Maitra, S. (2020). Design and development of a password manager application with advanced security features. Journal of Ambient Intelligence and Humanized Computing, 11(11), 5289-5304.

[3] "Towards a Better Understanding of Password Managers" by Martin Kleine and Sascha Fahl (2017) - This study investigates the usability and security of password managers, as well as user perceptions and attitudes towards them.

[4] "A Survey of Usable Security Technologies" by Simson Garfinkel, et al. (2005) - This survey examines various usable security technologies, including password managers, and discusses their effectiveness and limitations.