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

**ARUMBAKA PRAKASH1, ARUN N 2, JEEVANRAJ R 3, Mr.G.Praveen Kumar4**

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

**1.ABSTRACT:**

The abstract provides a brief overview of the project. In this case,it highlights the importance of strong and unique passwords in ensuring online account security and introduces the concept of a password generator and manager system. It also outlines the project’s goal, which is to design and implement a password generator and manager system that can generate strong and unique passwords and securely store them for users.

**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.

5."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:**

* 1. **EXISTING SYSTEM:**

The existing system section describes the currently available password generator and manager tools in the market. It mentions populartools 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.

* 1. **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.

* 1. **SOFTWARE USED:**

Languages: HTML, CSS, JavaScript

**4. CATEGORIESOF 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:**

 

**6. RESULT & DISCUSSION:**

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, the proposed system, with its user-friendly web-based interface and advanced features, can effectively address the limitations of existing password management solutions.

**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.