Journal of Computer and Electrical Sciences (JCES)- Volume-1 Issue-4, April 2026
ISSN: 3049-2602

PASSWORD STRENGTH CHECKER AND GENERATOR

P.Soni[1], Dr.Y. Prakasarao[2]

[1]Student, Department of Computer & Science Engineering

Andhra Loyola Institute of Engineering and Technology, Vijayawada, Andhra Pradesh, India

[2]*Assistant Professor, Department of Computer Science Engineering*

Andhra Loyola Institute of Engineering and Technology

Andhra Loyola Institute of Engineering and Technology, *Vijayawada, Andhra Pradesh, India*

Email id:penumathsasoni@gmail.com

Abstract: Passwords are one of the most important security components in the field of cybersecurity. The password sector deals with the protection, management, and secure use of passwords to prevent unauthorized access to systems and data. Weak passwords are a major cause of cyber-attacks such as hacking, identity theft, and data breaches.

This project focuses on understanding the password sector in cyber security anddeveloping a password generator to create strong and secure passwords. The password generator produces random passwords using a combination of letters, numbers, and special characters, making them difficult to guess or crack. The project demonstrates how strong password policies and automatic password generation improve system security.

The proposed system helps users create secure passwords easily and reduces the risk of cyber threats. This project highlights the importance of password security and promotes safe digital practices among users. It is simple, effective, and suitable for basic cyber security learning at the 10th standard level.

Keywords:*Cyber Security, Password Generator, Strong Passwords, Authentication, Data Protection, Digital Security*

.1. INTRODUCTION

With the rapid advancement of digital technologies, online platforms and applications have become an essential part of everyday life. Users rely on various digital services such as banking, social media, and email, which require secure authentication mechanisms. However, this growth has also led to an increase in cybersecurity threats, especially those targeting user accounts through weak passwords.Attackers often exploit weak or easily guessable passwords using techniques such as brute-force attacks, dictionary attacks, and credential stuffing. These attacks can lead to unauthorized access, identity theft, and data breaches. Traditional password practices, such as using simple or reused passwords, increase the risk of such cyber threats.To address this issue, the **Password Strength**

https://doi.org/10.5281/zenodo.19610599

Checker and Generator system is developed. This system helps users evaluate the strength of their passwords and generate strong, secure passwords automatically. It analyzes passwords based on factors such as length, complexity, and randomness, and provides real-time feedback to improve weak passwords.The password generator creates secure passwords using a combination of letters, numbers, and special characters, making them difficult to guess or crack. By promoting strong password practices and awareness, the system enhances user security and reduces the risk of cyber-attacks.

This project highlights the importance of password security in modern digital systems and provides a simple, effective solution suitable for basic cybersecurity learning and practical applications.

2. LITERATURE SURVEY

Several research studies have explored password security mechanisms and authentication systems to protect user data. Existing systems mainly focus on basic password validation but lack advanced strength analysis techniques Some password generators create random passwords but do not evaluate their strength or provide feedback to users. Traditional password checkers analyze only simple parameters like length and character type, without considering entropy or real security risks. Advanced security tools use complex algorithms for password analysis, but they are often difficult to use and not user-friendly.From the literature, it is evident that there is a need for a simple, efficient, and user-friendly system that can both evaluate password strength and generate secure passwords effectively.

Proposed System Improvements

The proposed system addresses these limitations by:

- Providing accurate password strength analysis
- Generating strong and secure passwords
- Using entropy-based evaluation for better security
- Detecting common and weak passwords
- Giving real-time feedback and suggestions
- Offering a simple and user-friendly interface

https://doi.org/10.5281/zenodo.19610599

3. METHODOLOGY

The proposed system is implemented using multiple modules that work together to evaluate password strength and generate secure passwords. The modules in the system include:

- **User Module**
- **Password Strength Evaluation Module**
- **Password Generator Module**
- **Logging and Monitoring Module**
- **Security Module**

MODULES DESCRIPTION

User Module: The User module provides a web interface for users to interact with the system. Users can enter passwords to check their strength or request the system to generate strong passwords. The dashboard displays password strength scores, feedback, and suggestions for improvement.

Password Strength Evaluation Module: This module analyzes the user-provided passwords using criteria such as length, use of uppercase and lowercase letters, digits, special characters, and dictionary word checks. Passwords are categorized into strength levels: weak, moderate, or strong.

Password Generator Module: The Password Generator module creates secure passwords based on user-defined criteria such as length and inclusion of numbers, symbols, and mixed case letters. Generated passwords are designed to resist common attacks such as brute force or dictionary attacks.

Logging and Monitoring Module: All user interactions, including password checks and generated passwords, are logged (without storing plain passwords) to monitor system usage and identify potential misuse. The logs can be reviewed by administrators through the dashboard.

Security Module: This module ensures the system follows best practices for security. Passwords are validated in real-time, and sensitive data is handled using hashing and encryption techniques to prevent leaks.

4. IMPLEMENTATION

The system is implemented using the following technologies:

- **Python:** Core programming language for developing logic and functionality
- **PyQt6:** Used for designing the graphical user interface
- **Random & String Libraries:** Used for secure password generation
- **Hashlib / Math Libraries:** Used for entropy calculation and strength analysis

Application Includes:

- **User Interface:** Allows users to enter passwords and view results

https://doi.org/10.5281/zenodo.19610599

- **Password Strength Checker:** Analyzes password based on security parameters
- **Password Generator:** Generates strong and secure passwords
- **Entropy Analysis Engine:** Measures password randomness and strength
- **Feedback System:** Provides suggestions to improve weak passwords

User interface:

The user interface provides a centralized platform for users to check password strength and generate secure passwords. It includes input fields for entering passwords, options to display or hide the password, and buttons for generating, checking, copying, and clearing data. The interface displays password strength results along with suggestions for improvement, ensuring an easy and efficient user experience.

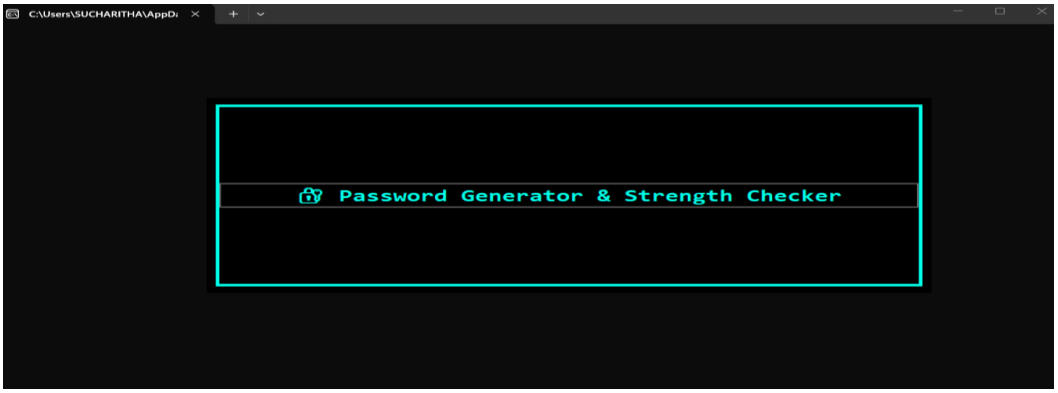

Fig 5.1: Software Design

Password Strength Checker:

The Password Strength Checker evaluates the security of a password based on length, complexity, and character types. It analyzes the use of uppercase, lowercase, numbers, and special characters. Based on this, the system classifies the password as Weak, Medium, or Strong. It also provides suggestions to improve weak passwords for better security.

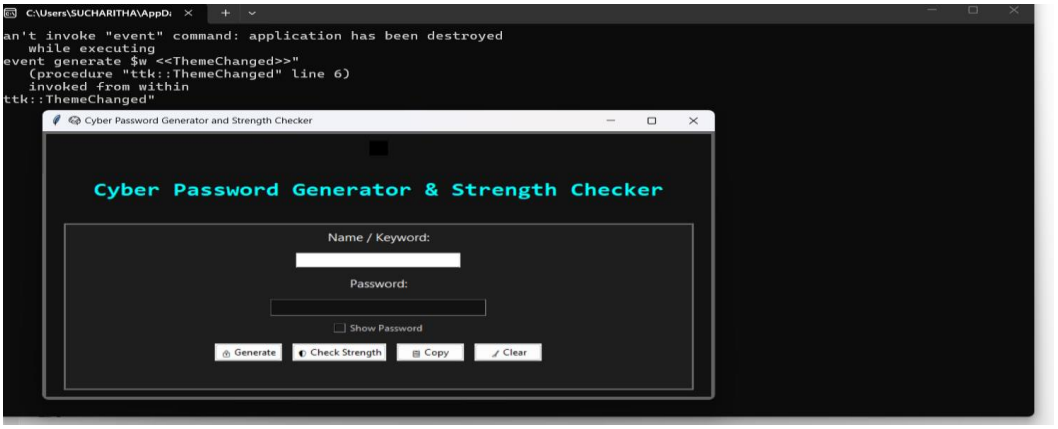

Fig 5.2:login

https://doi.org/10.5281/zenodo.19610599

Password Generator:

The Password Generator is a module that creates strong and secure passwords automatically. It generates passwords using a combination of uppercase letters, lowercase letters, numbers, and special characters. The system ensures randomness to make passwords difficult to guess or crack. This helps users easily create secure passwords and improve overall cybersecurity.

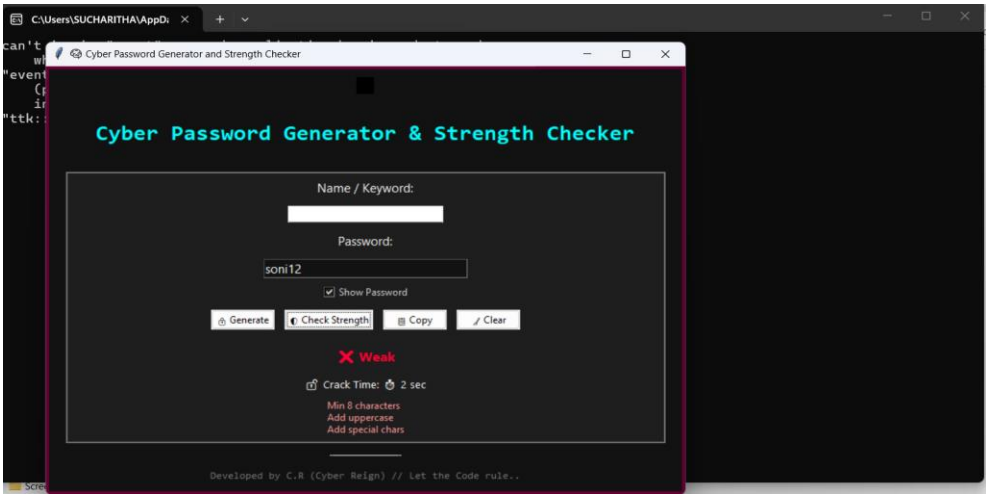

Fig 5.3:Dash Board

Entropy Analysis Engine:

The Entropy Analysis Engine measures the strength of a password by calculating its randomness. It evaluates how unpredictable the password is based on length and character variety. Higher entropy indicates a stronger and more secure password. This helps the system provide accurate strength evaluation and improve password securit

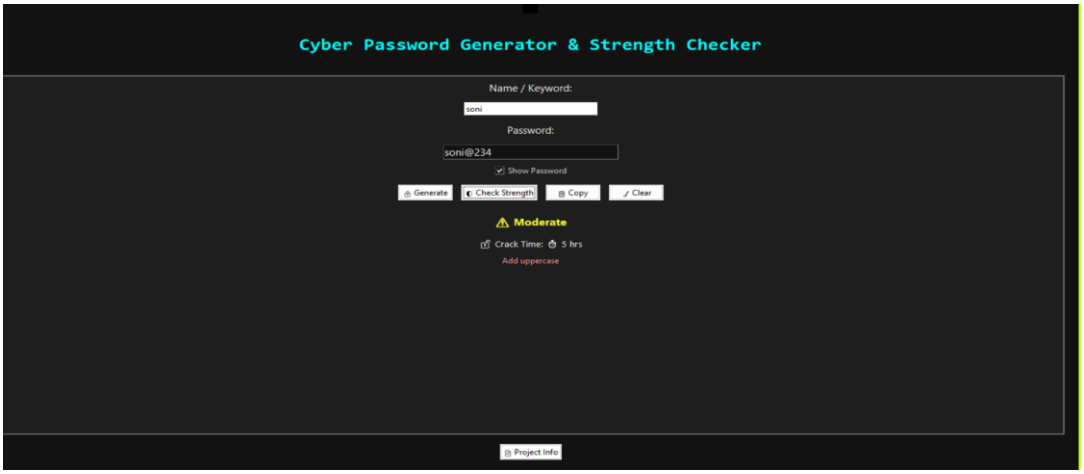

Fig 5.4:working password generator

https://doi.org/10.5281/zenodo.19610599

Feedback System:

The Feedback System provides real-time suggestions to help users improve their passwords. It identifies weaknesses such as short length or lack of character variety and recommends adding uppercase letters, numbers, or special characters. This helps users create stronger and more secure passwords.

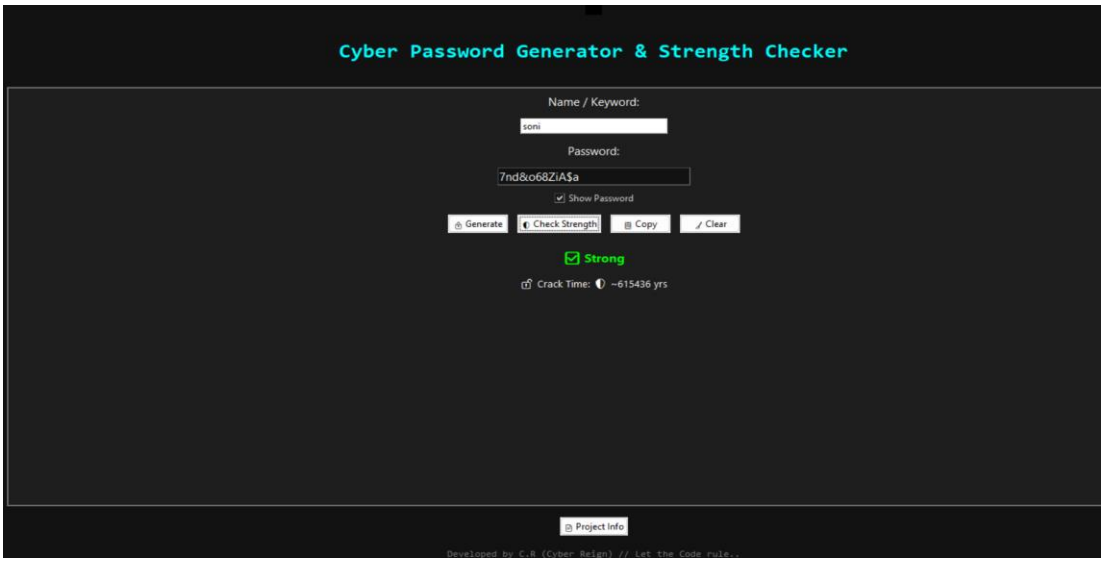

Fig 5.4:password generator

5. CONCLUSION

The Web-based Password Strength Checker and Generator was developed to help users create and evaluate secure passwords easily. Traditional methods of password creation often rely on guesswork or weak patterns, which can compromise security. The proposed system provides a web-based platform using modern web technologies, offering a simple and user-friendly interface for password management.

The system evaluates password strength based on multiple criteria, provides actionable feedback for improvement, and generates strong passwords according to user preferences. It ensures password security by incorporating best practices, such as using a mix of letters, numbers, symbols, and avoiding dictionary words.

The platform includes features such as real-time strength analysis, customizable password generation, logging of user activity for auditing, and an intuitive dashboard for monitoring usage. Overall, the system enhances cybersecurity by helping users adopt stronger passwords, reduces the risk of unauthorized access, and promotes safe password practices.

https://doi.org/10.5281/zenodo.19610599

REFERENCES

1. *Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F., "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes," In 2012 IEEE Symposium on Security and Privacy (SP), pp. 553–567, San Francisco, CA, USA (2012).*
2. *Weir, M., Aggarwal, S., Collins, M., & Stern, H., "Testing metrics for password creation policies by attacking large sets of revealed passwords," In ACM Conference on Computer and Communications Security (CCS), pp. 162–175, Chicago, IL, USA (2010).*
3. *Nadi, S., & Jahankhani, H., "Password security: Trends and challenges," In International Journal of Computer Science and Information Security (IJCSIS), 16(3), pp. 45–53 (2018).*
4. *Florêncio, D., Herley, C., & Van Oorschot, P. C., "An administrator's guide to Internet password research," In Proceedings of the 28th Large Installation System Administration Conference (LISA 2014), pp. 35–52, Seattle, WA, USA (2014).*
5. *Kelley, P. G., Komanduri, S., Mazurek, M. L., Shay, R., Vidas, T., Bauer, L., Christin, N., Cranor, L. F., & Lopez, J., "Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms," In 2012 IEEE Symposium on Security and Privacy (SP), pp. 523–537, San Francisco, CA, USA (2012).*
6. *Zhang, K., Monrose, F., & Reiter, M. K., "The security of modern password expiration: An algorithmic framework and empirical analysis," In ACM Transactions on Information and System Security (TISSEC), 13(4), pp. 1–38 (2010).*
7. *Ur, B., Kelley, P. G., Komanduri, S., Lee, J., Maass, M., Mazurek, M. L., Patel, S., Pesce, M., & Cranor, L. F., "How does your password measure up? The effect of strength meters on password creation," In Proceedings of the 21st USENIX Security Symposium, pp. 65–80, Bellevue, WA, USA (2012).*

https://doi.org/10.5281/zenodo.19610599