Journal of Science Research International (JSRI)
ISSN: 2456-6365 (Online)

OPEN ACCESS

PASSGUARD: DESIGN AND EVALUATION OF A REAL-TIME PASSWORD STRENGTH CHECKER

Soly Zachariah*, Reyhan Sayyad, Nitesh Maddheshiya, Abhishek Bhairamadgi and Sairaj Jadhav

Department of Computer Science,

Pillai College of Arts, Commerce & Science (Autonomous), Navi Mumbai, Maharashtra, India 410206

**Corresponding author E-mail: solyz@mes.ac.in*

Received: 21 December 2025	Revised: 19 January 2026	Accepted: 17 February 2026	Published: 28 February 2026

DOI: **https://doi.org/10.5281/zenodo.19051146**

Abstract:

Passwords are still the most commonly used authentication method in contemporary digital systems. Nevertheless, poor password practices are still a major contributing factor to data breaches and unauthorized access. Conventional password strength verification systems are highly dependent on simple rule-based verification methods such as minimum length and the presence of numeric or special characters, which are often ineffective in identifying predictable and easily guessable patterns. PassGuard is a real-time password strength verification system proposed in this research work that aims to provide users with accurate password strength assessment and immediate feedback. The proposed system combines rule-based verification, entropy analysis, and pattern identification methods to assign a weighted strength score. PassGuard also assesses the accuracy of classification and efficiency of performance on a labeled dataset. The experimental outcome confirms that the integration of multiple assessment approaches ensures reliability and real-time performance.

Keywords: *Passwords, Authentication, Password Strength, Entropy Analysis, Pattern Identification, Real-time Security.*

1. Introduction

In the contemporary digital age, passwords are still the most commonly used technique for user authentication. This is despite the existence of more sophisticated security solutions like biometric and multi-factor authentication, which are still not widely adopted. However, weak passwords are still among the most common causes of security weaknesses. This is because many people still use passwords that are weak, easily predictable, and composed of common words. Conventional password strength analysis tools only check for the password's structural integrity, including length and character variety. This is not an effective way of testing the password's resilience to attack.

PassGuard is a new password strength analysis tool proposed in this research. It is a real-time password strength analyzer that dynamically analyzes password strength as the user is typing.

2. Problem statement

Many online sites use simple validation rules to check the acceptability of passwords. Although these rules ensure that the password structure is complex, they do not ensure that the password is not predictable or commonly used. For instance, passwords that meet the character requirements can still be sequential or dictionary-based, and hence vulnerable to attacks.

The main research question that this study tries to answer is:

How can a real-time password strength checker be designed to provide accurate, meaningful, and user-friendly feedback while maintaining fast performance?

3. Objectives

The main aims of this research work are:

i. Design and develop a real-time password strength assessment system.
ii. Combine rule-based verification, entropy calculation, and pattern recognition methods.
iii. Offer instant and useful feedback to enhance password strength.
iv. Assess the accuracy of the system using labeled password data.
v. Test the performance and response time of the system in real-time.

4. Literature review

Studies on password security have shown that users tend to have predictable patterns in password generation. These patterns include appending numbers to dictionary words, using sequential letters, and repeating patterns. These patterns greatly lower the actual strength of passwords.

Entropy models calculate the randomness of passwords using mathematical computations of character set size and password length. Although entropy provides theoretical information on randomness, it is not always a good measure of actual vulnerability, particularly against dictionary and pattern attacks.

More advanced password strength calculators use frequency analysis, common password lists, and pattern recognition algorithms. These models try to realistically model actual attacks and provide more accurate security estimates. PassGuard uses a hybrid model based on these observations.

5. Proposed methodology

The development of PassGuard follows a structured methodology

5.1 Requirement analysis

The system requirements include:

- Real-time strength assessment
- Effective classification mechanism
- Low response time
- Feedback suggestions are clear
- Performance assessment capability

5.2 System design

The system is designed using a modular architecture consisting of:

The system is developed employing a modular design with the following components:

- Input module
- Rule-based validation engine
- Entropy calculation module
- Pattern detection engine
- Weighted scoring system
- Feedback generator
- Real-time display interface

5.3 Implementation

PassGuard is developed using web technologies to make it fully responsive and cross-platform compatible.

The project structure is as follows:

- **index.html** – User interface design
- **styles.css** – Strength meter design and layout
- **src/password-analyzer.js** – Password analysis logic
- **src/app.js** – Real-time password analysis integration
- **data/password-dataset.json** – Sample passwords for analysis
- **scripts/evaluate.js** – Accuracy and performance evaluation script

The system is capable of dynamically analyzing passwords during input events.

5.4 Testing and evaluation

The evaluation phase includes

- Classification accuracy testing
- Performance benchmarking
- Misclassification analysis

6. System Architecture

PassGuard consists of the following components:

6.1 User input layer

- Captures password input dynamically as users type

6.2 Rule-based validation module evaluates

- Minimum length
- Character variety (uppercase, lowercase, digits, symbols)
- Basic structural compliance

6.3 entropy calculator

Computes estimated entropy in bits based on password length and character set diversity.

6.4 Pattern detection engine

Detects predictable structures including:

- Sequential characters (e.g., 1234, abcde)
- Keyboard adjacency patterns
- Repeated character sequences
- Common words and frequently used passwords

6.5 Score generator

Applies weighted scoring with penalties for detected weaknesses. The final score maps to strength labels:
Very Weak → Weak → Moderate → Strong → Very Strong

6.6 Feedback module

Generates actionable suggestions such as:

- Increase password length
- Avoid predictable sequences
- Add more character variety

6.7 Real-time display module

Updates strength meter and feedback instantly using input event listeners.

7. Evaluation Strategy

To measure effectiveness, three types of evaluation were conducted:

7.1 Accuracy testing

A labeled dataset containing weak, moderate, and strong passwords was used to calculate:

- Overall classification accuracy
- Per-class accuracy
- Misclassified samples

7.2 Performance testing

The system measured:

- Average response time
- Worst-case response time

Results indicated minimal latency, confirming suitability for real-time use. Misclassified passwords were analyzed to identify potential improvements in scoring weight

8. Results and Discussion

The combination of rule-based validation, entropy calculation, and pattern recognition led to relatively balanced strength estimates compared to standalone techniques.

The assessment script outputted:

- Uniform classification for all categories
- Low average processing time per input
- Enhanced detection of predictable passwords

These results indicate that hybrid assessment approaches are more reliable than conventional rule-based systems.

9. Key conceptual observations

- **Limitations of Rule-Based Systems**: Basic password rules (length, symbols, numbers) do not guarantee real security because predictable patterns can still exist.
- **Entropy Is Not Enough Alone**: Mathematical randomness does not always reflect practical resistance to dictionary or pattern-based attacks.
- **Human Predictability in Passwords**: Users often create passwords using common words, sequences, or repeated characters, reducing actual strength.

- **Importance of Real-Time Feedback**: Immediate strength updates encourage users to improve passwords during creation.
- **Security–Usability Balance**: An effective strength checker must ensure strong evaluation while remaining user-friendly.
- **Need for Multi-Layer Evaluation**: Combining rule validation, entropy estimation, and pattern detection provides more accurate strength assessment.

Conclusion

This work has demonstrated the design and evaluation of PassGuard, a real-time password strength analyzer that combines various analytical approaches. By doing so, the proposed system overcomes the shortcomings of existing password analyzers.

The experimental results have shown that PassGuard provides accurate classification performance while preserving real-time efficiency. The proposed system further improves user awareness by providing informative feedback.

This work has made a contribution to the development of effective password validation tools in modern web applications.

Future work

Future enhancements may include:

- Integration with breached password databases
- Machine learning-based strength prediction
- Adaptive scoring based on attack models
- Multi-language dictionary analysis
- Behavioral pattern learning for personalized feedback

References

1. Florêncio, D., & Herley, C. (2007). A large-scale study of web password habits. In *Proceedings of the 16th International World Wide Web Conference (WWW 2007)* (pp. 657–666). ACM. https://doi.org/10.1145/1242572.1242661
2. Golla, M., Dürmuth, M., & Pöpper, C. (2018). Guiding users towards better passwords: Evaluating password-strength meters. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM. https://doi.org/10.1145/3173574.3174045
3. Bonneau, J. (2012). The science of guessing: Analyzing an anonymized corpus of 70 million passwords. In *2012 IEEE Symposium on Security and Privacy* (pp. 538–552). IEEE. https://doi.org/10.1109/SP.2012.49
4. Shannon, C. E. (1948). A mathematical theory of communication. *Bell System Technical Journal, 27*(3), 379–423. https://doi.org/10.1002/j.1538-7305.1948.tb01338.x
5. Gaw, S., & Felten, E. W. (2006). Password management strategies for online accounts. In *Proceedings of the 2nd Symposium on Usable Privacy and Security (SOUPS 2006)* (pp. 44–55). ACM. https://doi.org/10.1145/1143120.1143127
6. National Institute of Standards and Technology (NIST). (2017). *Digital identity guidelines: Authentication and lifecycle management (NIST Special Publication 800-63B).* National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63B