Journal of Advances in Developmental Research (IJAIDR)

E-ISSN: 0976-4844 ● Website: www.ijaidr.com ● Email: editor@ijaidr.com

Intelligent Password Strength Analyzer for Secure Authentication

A. A. Patil[1], S. S. Kamble[2], S. S. Redekar[3]

[1,2,3]Engineering researchers from institutions in India

Abstract:
In the modern digital world, secure authentication is necessary to protect information from cyber threats such as hacking and data breaches. Weak passwords are one of the main causes of security vulnerabilities. This project proposes an **Intelligent Password Strength Analyzer using Machine Learning** to evaluate the strength of passwords more accurately than traditional rule-based methods. The system analyzes password features such as length, complexity, and patterns to classify passwords as weak, medium, or strong. It also provides real-time feedback and suggestions to help users create stronger passwords. This system improves cybersecurity and can be integrated into websites and applications to enhance secure authentication.

Keywords: Password Security, Authentication, Password Strength Analysis, Cybersecurity, Data Protection, Secure Login.

1. Introduction

In today's digital world, secure authentication plays a vital role in protecting personal and organizational data from unauthorized access. Passwords are the most widely used authentication method for accessing online accounts, banking systems, social media platforms, and enterprise applications. However, many users tend to create weak or easily guessable passwords, which makes systems vulnerable to cyberattacks such as brute force attacks, dictionary attacks, and credential stuffing.

Traditional password validation systems rely on simple rule-based mechanisms such as minimum length, use of uppercase letters, numbers, and special characters. Although these rules encourage stronger passwords, they often fail to accurately evaluate the real strength of a password. Attackers can still predict passwords that follow these simple rules.

To overcome these limitations, an Intelligent Password Strength Analyzer using Machine Learning can be implemented. Machine learning techniques can analyze patterns in large datasets of weak and strong passwords to identify the actual strength of a password. The system evaluates various features such as character diversity, password length, entropy, and common patterns to classify passwords as weak, medium, or strong.

The proposed system helps users create secure passwords by providing real-time feedback and suggestions. This improves the overall security of authentication systems and reduces the chances of unauthorized access.

2. Literature Review

Password security plays an important role in protecting digital systems from unauthorized access. Many researchers have studied methods to evaluate password strength and improve authentication security. Traditional password validation techniques mainly focus on basic rules such as minimum length, the use of numbers, and special characters. However, these rule-based methods often fail to

accurately measure the real strength of passwords and may still allow weak passwords to be used.
Wang et al. (2019) - This paper proposed a deep learning model for password strength prediction using neural networks.
Geng and Tian (2020) - The study introduced a hybrid machine learning approach to improve password strength classification accuracy.

3. Methodology

Intelligent Password Strength Analyzer for Secure Authentication

The methodology describes the steps followed to develop the intelligent password strength analyzer system. The system evaluates the strength of passwords using machine learning techniques and provides feedback to users.

3.1. Data Collection - In this step, a dataset containing different types of passwords such as weak, medium, and strong passwords is collected. This dataset is used to train the machine learning model.

3.2. Data Preprocessing - The collected password data is cleaned and prepared for analysis. Important features such as password length, number of characters, use of uppercase letters, numbers, and special characters are extracted from the dataset.

3.3. Feature Extraction - Relevant features that influence password strength are identified. These include password complexity, character distribution, entropy, and pattern recognition.

3.4. Machine Learning Model Training - The extracted features are used to train a machine learning model such as Logistic Regression, Decision Tree, or Random Forest. The model learns to classify passwords into categories like weak, medium, or strong.

3.5. Password Analysis - When a user enters a password, the system analyzes the password using the trained model. The system checks the password characteristics and predicts its strength.

4. Modules description

The system consists of the following main modules:

4.1. User Interface Module

This module provides the front-end interface where users enter their passwords. It also displays password strength results and improvement suggestions.

4.2. Password Data Collection Module

This module collects password datasets used to train the machine learning model. The dataset contains examples of weak, medium, and strong passwords.

4.3. Feature Extraction Module

This module extracts meaningful features from the password such as:

- Length of the password
- Character diversity
- Number of digits
- Special symbols
- Entropy calculation

4.4. Machine Learning Training Module

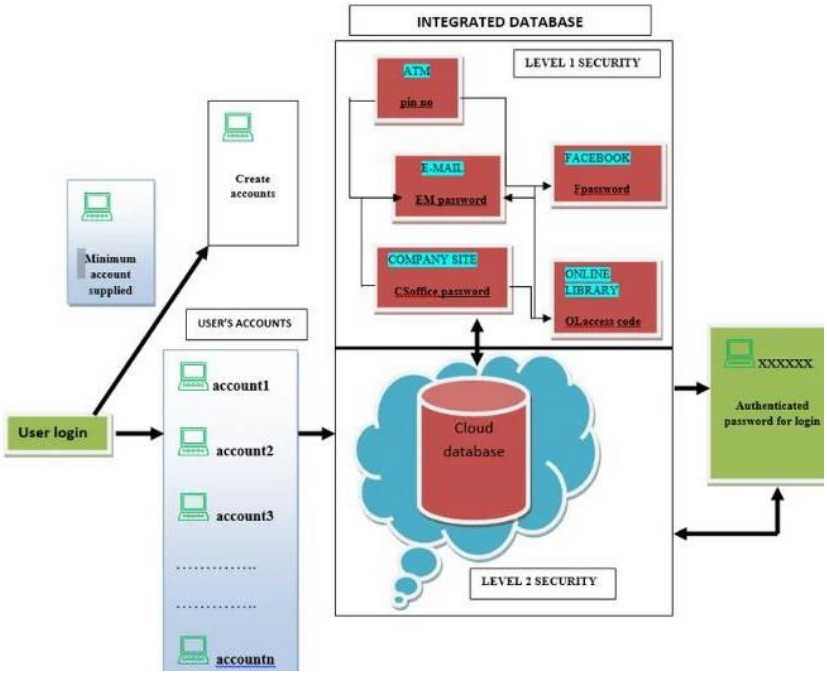
This module trains the machine learning model using the collected dataset. Algorithms such as Logistic Regression, Decision Tree, or Random Forest can be used.

Password Strength Prediction Module This module uses the trained model to predict the strength of newly entered passwords.

4.5. Feedback and Recommendation Module

The system provides suggestions to improve password strength, such as increasing length or adding special characters.

5. System Architecture



6. Performance Result

The performance of the **Intelligent Password Strength Analyzer** was evaluated using machine learning algorithms to classify passwords as **weak, medium, or strong**. The system analyzed password features such as length, complexity, character variety, and entropy.

During testing, the trained model achieved good classification accuracy in identifying password strength levels. The system was able to detect weak passwords that contain simple patterns, dictionary words, or predictable sequences. It also correctly identified strong passwords that include a combination of uppercase letters, lowercase letters, numbers, and special characters.

7. Conclusion

The **Intelligent Password Strength Analyzer for Secure Authentication using Machine Learning** provides an effective way to improve password security. Unlike traditional rule-based methods, the system uses machine learning to analyze password features such as length, complexity, and character patterns to classify passwords as weak, medium, or strong. It also provides real-time feedback and suggestions to help users create stronger passwords. Overall, the system helps reduce the risk of cyberattacks and enhances the security of modern authentication systems.

8. Future Scope

The system can be further improved by integrating advanced machine learning and deep learning techniques to increase the accuracy of password strength prediction. Future versions can also include support for multi-factor authentication to enhance security.

The analyzer can be integrated with websites, mobile applications, and cloud-based platforms to provide real-time password security analysis for a large number of users.

REFERENCES:

1. Florençio, D., & Herley, C. (2017), "A Large-Scale Study of Web Password Habits," Proceedings of the 16th International World Wide Web Conference,pp. 657–666.
2. Shay, R., Komanduri, S., Kelley, P., Leon, P., Mazurek, M., Bauer, L., Christin, N., & Cranor, L. (2014), "Encountering Stronger Password Requirements: User Attitudes and Behaviors," Proceedings of the Sixth Symposium on Usable Privacy and Security,pp. 2–20.
3. Ur, B., Kelley, P., Komanduri, S., Lee, J., Maass, M., Mazurek, M., Passaro, T., Shay, R., Vidas, T., Bauer, L., Christin, N., & Cranor, L. (2017), "How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation," USENIX Security Symposium, pp. 65–80.
4. Melicher, W., Ur, B., Segreti, S., Komanduri, S., Bauer, L., Christin, N., & Cranor, L. (2016), "Fast, Lean, and Accurate: Modeling Password Guessability Using Neural Networks," USENIX Security Symposium, pp. 175–191.
5. Ma, J., Yang, W., Luo, M., & Li, N. (2014),
6. "A Study of Probabilistic Password Models," IEEE Symposium on Security and Privacy, pp. 689–704.
7. Golla, M., & Dürmuth, M. (2018), "On the Accuracy of Password Strength Meters," Proceedings of the ACM Conference on Computer and Communications Security, pp. 1567–1582.
8. Wheeler, D. (2016), "zxcvbn: Low-Budget Password Strength Estimation," USENIX Security Conference, pp. 157–173.
9. Wang, D., Cheng, H., Wang, P., Huang, X., & Jian, G. (2019), "A Security Evaluation of Pattern Passwords," IEEE Transactions on Information Forensics and Security, Vol. 14, Issue 5, pp. 1133–1145.
10. Geng, Y., & Tian, X. (2020), "Machine Learning Based Password Strength Classification," International Journal of Computer Applications, Vol. 176, Issue 30, pp. 1–6.