Developing a robust and effective password strength analyzer that can accurately assess the security of passwords against various types of attacks

Rohit Ashok Bagde
Student
bagderon@gmail.com

Roshit Hadge
Student
roshithadge5@gmail.com

Sagar Tarekar
Guide
Asst Prof. MCA
TGPCET
sagartarekar@tgpcet.com

Abstract: This research paper we have to focus on developing a robust and effective tool.

Early password strength analyzers were relatively simple, primarily focusing on length and complexity. However, as password cracking techniques have evolved, so have password strength analyzers. More recent approaches have incorporated machine learning, natural language processing, and other advanced techniques to improve accuracy and identify more sophisticated password patterns. We are focusing to final tool the security of passwords.

The main goal of this paper we have to find the create a passwords strength Analyzer that can measure a passwords security.

Keywords: Machine Learning-Based Approaches, Natural Language Processing, Context-Aware Analysis, Hybrid Approaches,

Introduction: Password strength analyzers have become an indispensable tool in cybersecurity, helping users select strong, memorable passwords that are resistant to brute-force attacks, dictionary attacks and other common password cracking techniques. These analyzers typically evaluate passwords based on various criteria, such as:

- **Length:** Longer passwords are generally considered more secure due to the increased number of possible combinations.

- **Complexity:** The presence of uppercase letters, lowercase letters, numbers, and symbols can enhance password complexity and make them more difficult to guess.
- **Dictionary words:** Passwords containing common words or phrases are more susceptible to dictionary attacks, where attackers use lists of common words to try different combinations.
- **Personal information:** Using personal information (e.g., names, birthdays) in passwords can make them easier to guess, especially if attackers have access to additional information about the user.

developments in password strength analysis:

- Rule-based approaches:
- Dictionary-based approaches:
- Machine learning:
- Natural language processing:
- Context-aware analysis.

Review of literature:

I have read many references on the interesting topic of this paper, but the reference that particularly stood out to me is the Singh and Rani (2020) study. They researched strong passwords in a different way, specifically detailing how they used machine learning – which is how Prasad and Ramesh created some new passwords in 2021.

My next reference is that in (2019), Goyal and Dahiya also worked on a strong password login system. They identified system weaknesses and then used a strong method for verification. Also, Sharma and Singh in (2018) studied how humans interact with passwords, and they clearly explained the easily identifiable patterns in passwords.

Singh and Kaur (2019) worked on a special password system for banking apps. Their system changes the password rules based on how risky the situation is. This helped make banking apps more secure and easier to use. Mehta and Sharma (2022) developed a password strength checker that used different methods together. In Indian colleges, they had tested it and found that it proved better than the older systems. Finally, in studying how people, in India, use passwords and how password attacks take place, Bhushan and Kumar (2020) came in to play. As it turns out, many people use weak or repeated passwords. According to them, passwords should be generally safer if there is more awareness and better rules.

Preliminaries:

Machine Learning-Based Approaches:

In Indian colleges, they had tested it and found that it proved better than the older systems. Finally, in studying how people, in India, use passwords and how password attacks take place, Bhushan and Kumar (2020) came in to play. In fact, they found that many users use weak or repeated passwords. It should be a better rule that rules about keeping passwords safe more awareness, they said.

Natural Language Processing:

Password strength analysis has been formalized as a problem in natural language processing (NLP), and the semantic content of passwords is analyzed. However, NLP can specify inadequate passwords related to personal information, common words, and other patterns by looking at the meaning behind the passwords. However, meaningful information can be extracted from passwords using such techniques like keyword extraction, sentiment analysis, and topic modelling.

Context-Aware Analysis:

It has been researched recently how the use of contextual information can help to improve the password strength assessment. It includes taking into account factors like where the password is used (a website or an application), on what device or platform it is entered, or user behavior. Password strength can be defined in terms of what happens with passwords in different context.

It can offer more accurate assessments and can detect possible vulnerabilities that should be removed by conventional methods.

Hybrid Approaches:

In order to tackle the problem of limitations of single method, researchers have developed hybrid approach by joining several methods. For example, using something like hybrid approach, which combines ML to find general works, and NLP to analyse specific words or phrases in passwords. Hybrid approaches can be achieved by combining the strengths of several techniques to make a more comprehensive and accurate password strength assessment.

APPLICATIONS:

Machine Learning Applications

Password strength analysis in the machine learning algorithms has become a very important area. So, some of the most common techniques are from this list:

Support Vector Machines (SVM): SVM is a supervised learning model which can classify the data points in different categories SVMs can be employed as the classifier to classify passwords as (strong) or (weak) based on password features in the context of password strength analysis.

- Ensemble Learning Methods: Amongst the ensemble learning methods, Random forests (ensemble of decision trees) are used, as they combine multiple decision trees to achieve better accuracy and is improved over fitting on training data. It is possible to use them to recognize hidden patterns of password data.

Verbal Representations: Verbal descriptions, describing words that appear near or around a user's password, have also been shown to be an effective solution to automatic password prediction. Long range dependencies can be captured and subtle relationships between characters of the passwords can be identified by these models.

Natural Language Processing

NLP techniques offer useful information about the semantic content of passwords. Thus, NLP can analyze the words and phrases used in passwords and try to identify vulnerabilities associated such as personal information, common phrases, or patterns.

The following are some of the NLP techniques that have been applied to the password strength analysis:

- Pwd Extraction: It can be used to extract i.e. specify keywords from password and expose personal information or common patterns.
- It can be used for Sentiment Analysis to understand what users are trying to convey in their passwords. Such information allows a VPN provider to have an idea about the behavior of users and to identify possible vulnerabilities.
- Latent Topics Discovery: Passwords can also be processed by topic modeling techniques to discover latent topics on them and help to identify potential weaknesses in passwords.

Context-Aware Analysis

Password strength based on context (including the site or app, the device or platform and user behavior) is considered context aware password strength analysis. With that context, password strength analyzers are able to be more accurate as they are able to identify vulnerabilities that traditional methods miss.

However, one possible factors in context-aware analysis include:

- In which website or application the password is used matters: the type of website or application may affect its stength. Passwords for financial institution passwords may be more secure than social media passwords.
- Secondly, the type of device or platform (on the illustration of which the password is being input) could also make a difference to password strength. It is possible that passwords on the mobile devices are more prone to some types of attacks.
- Password reuse and related health: The password reuse and other such behaviors can be identified as vulnerabilities to be analyzed.

Hybrid Approaches

Thus, researchers have combined various techniques into hybrid approaches to compensate the limitations of individual techniques. An example of such approach is hybrid, which is machine learning on typical patterns and NLP on specific keywords or phrases inside passwords. Hybrid approaches combining the strength of the various techniques give more comprehensive and accurate strengths, although both are measured from the user' s perspective.

Methodology:

- Real-Time Password Strength Meters

Real time feedback is provided by many systems as users create passwords, identifying them based on their length, complexity, and those commonly used patterns.

Techniques Used:

Ingredient 2: Rule based systems to identify weaknesses (e.g., too short, commonly used word).

Dynamic feedback, such as color-coded meters or suggestions.

Example:

"Weak: Password123" → "Strong: xK9#3g!pA@z".

- **Dictionary and Pattern Analysis**

It is a method for checking whether the password has predictable words, sequences or patterns.

Common Patterns Tested:

Repeating characters ("aaaaaa").

Sequential characters ("abcd1234").

Common substitutions ("p@ssw0rd" instead of "password").

In resolving this, password pattern recognition libraries such as zxcvbn analyze password weaknesses in context.

- **AI and Machine Learning Models**

In modern crack passwords datasets are run through machine learning models trained on these datasets to determine how well the password is cracked.

Benefits:

Better detection of obscure patterns and common weaknesses.

Better feedback for creating what could only be regarded as truly unique passwords.

Example: For example, risk models can provide an understanding of why cultural or language specific problems happen.

Analysis of the study:

1. **Analyze Password Strength**

- Endpoint: POST /api/password/analyze
- Purpose: Accepts a password from the client and returns a strength assessment.
- Input:

```
{
  "password": "P@ssw0rd123"
}
```

- Response:

```
{
  "strength": "Strong",
  "feedback": [
    "Increase password length to enhance security",
    "Avoid common patterns like '123'"
  ]
}
```

2. **Validate Password Against Rules**

- **Endpoint:** POST /api/password/validate
- **Purpose:** Validates the password against predefined rules (e.g., minimum length, character complexity).
- **Input:**

```
{
  "password": "pass123",
  "rules": {
    "minLength": 8,
    "requireSpecialChars": true,
    "requireNumbers": true
  }
}
```

- **Response (if invalid):**

```
{
 "isValid": false,
  "errors": [
    "Password must be at least 8 characters long",
    "Password must include at least one special character"
  ]
}
```

3. Get Password Rules

- Endpoint: GET /api/password/rules
- Purpose: Returns the password rules (e.g., length, required characters) enforced by the system.
- Response:

```
{
 "rules": {
  "minLength": 8,
  "requireUppercase": true,
  "requireSpecialChars": true,
  "requireNumbers": true
 }
}
```

4. Check Common Passwords

- Endpoint: POST /api/password/check-common
- Purpose: Checks if the submitted password is in a list of common/weak passwords (e.g., "password123", "123456").
- Input:

```
{
 "password": "password123"
}
```

- Response:

```
{
 "is Common Password": true,
 "message": "This password is too common and can be easily guessed."
}
```

5. Real-Time Feedback API (Optional)

- Endpoint: POST /api/password/feedback
- Purpose: Analyzes the password and provides real-time feedback as the user types.
- Input:
- {

```
"partialPassword": "P@ss"
}
```

- Response:

```
{
  "feedback": [
    "Add more characters for better security",
    "Include numbers to strengthen the password"
  ]
}
```

Concluson:

Ensuring the user creates a secure and resilient password is a critical element of the password strength analysis, which has an important role to play in raising the cybersecurity of the system. A weak password is indeed a significant vulnerability that most cybercriminals take advantage of in brute force, dictionary, and credential leaks attacks. The use of password analysis systems provides individuals and organisations, however, a way to lower the likelihood of an unauthorized access or a data breach.

Ideally, a password strength analysis tool designed well evaluates password complexity, length, character diversity and entropy as well as weakness and common passwords occurrence. Moreover, incorporation of cutting edge security strategies like AI (artificial intelligence) centricly analyzed systems, several options of multifactor authentication (MFA) and real time breach detection will help to strengthen the entire security system as a whole.

Looking forward, though cyberspace is dynamic, so too must the rules or policies to which cyber users conform become dynamic, and adapt to evolving cyber threats. While we may be moving towards password less future of authentication, strong password still plays a role in securing users' digital identities and their confidential information until then.

Thus, password strength analysis is an important aspect of enhancing the security of cybersecurity and technology is constantly evolving for further strengthening of password security measures.

Password strength analysis is an important aspect of increasing cyber security to determine the strength of user passwords that safeguard their private information from incorrect usage. One of the leading causes of security breaches is weak passwords, so evaluating strong credentials is becoming an ever more important task for users.

Finally, password strength analysis allows individuals or organizations less security risk, no breach of data, and maximum digital safety by best practices. As with most areas in technology, future enhancements in password security and the authentication methods will further greatly improve online power.

Future scope of the study:

- Continuous Learning: Change the analyzers into ones which learn continuously and adapt to new password cracking techniques.

- Password strength analysis with biometric authentication: This shall help in integrating biometric authentication in password strength analysis thus increasing security and concurrently offering a user friendly experience.

1. Privacy Preserving Techniques: Focus on the techniques to protect user privacy while maintaining strong password strength analysis

- Assessment of user input: Developing analyzers that make user input easy to enter and provide straightforward feedback that helps users make further judgments.

Addressing ethical considerations regarding the use of password strength analyzers, i.e. privacy and discrimination.

If these challenges are addressed in conjunction with taking advantage of the most recent technological advances, password strength analyzers will be able to remain an important means of safeguarding user accounts and data from access by unauthorized individuals.

References:

1. Singh, R., & Rani, P. (2020). A Comparative Study on Password Strength Estimation Techniques. International Journal of Computer Applications, 176(16), 17– 21.

2. Prasad, S. V., & Ramesh, V. (2021). A Framework for Evaluating Password Strength using Machine Learning Techniques. Journal of Emerging Technologies and Innovative Research (JETIR), 8(2), 150– 155.
3. Goyal, M., & Dahiya, A. (2019). Password-Based Authentication: International Journal of Engineering and Advanced Technology (IJEAT), 8(5), 1762– 1766.
4. Sharma, P., & Singh, S. (2018). Password Security: A Study of Password Creation Policies and Their Effectiveness. Proceedings of the 3rd International Conference on Computing, Communications and Networking Technologies (ICCCNT), IIT Delhi.
5. Singh, V., & Kaur, R. (2019). Enhancing User Authentication Security in Indian Banking Apps using Adaptive Password Systems. International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), 4(1), 179– 184.
6. Mehta, A., & Sharma, R. (2022). Improving Password Strength Estimation using Hybrid Algorithms: A Case Study in Indian Universities. International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), 11(3), 22– 27.
7. Bhushan, B., & Kumar, A. (2020). An Overview of Password Attacks and Defense Mechanisms with Indian User Trends. International Journal of Computer Sciences and Engineering, 8(6), 74– 78.