International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue ICCIS-2025, pp 138-143, May-2025
https://doi.org/10.47001/IRJIET/2025.ICCIS-202522
Second International Conference on Computing and Intelligent Systems (ICCIS-2025)

Ironpass Dynamic Password Strength Analyzer

[1]Neeraj Jain, [2]Animesh Choudhury, [3]Kumar Rounak, [4]Tanay Gupt, [5]Siddharth Vinayak

[1,2,3,4,5]Department of Computer Science and Engineering, Alliance University, Bengaluru, India
E-mails: [1]smartharinee@gmail.com, [2]canimeshbtech21@ced.alliance.edu.in, [3]rkumarbtech21@ced.alliance.edu.in, [4]Gtanaybtech21@ced.alliance.edu.in, [5]vsiddharthbtech21@ced.alliance.edu.in

***Abstract* - In today's digital era, password security remains one of the most overlooked aspects of personal and organizational cybersecurity. Many users still rely on weak, predictable, and short passwords for convenience, making their accounts vulnerable to breaches. IronPass – Dynamic Password Strength Analyzer is a web-based application designed to address this issue by evaluating password strength and assisting users in generating more secure alternatives. Built using React.js for the frontend and Node.js with Express.js for the backend, IronPass integrates a password strength assessment API to analyze and score user- input passwords in real-time. Additionally, the system offers a password generator that transforms simple inputs into complex, secure passwords. Through an intuitive user interface and insightful feedback, IronPass not only enhances password strength but also educates users about better password practices.**

Keywords: Password Strength, Password Generator, Entropy, Web Security, React.js, Node.js, Real-Time Analysis, Password Assessment.

I. INTRODUCTION

In the context of swift digital transformation, there has been a significant increase in the number of online platforms and services that necessitate user authentication. This includes a wide range of applications, from social media and online banking to enterprise systems and cloud-based solutions, where passwords continue to serve as the primary means of security. Despite their essential function in protecting both personal and organizational information, users frequently neglect the importance of password management. Research consistently indicates that individuals often opt for short, memorable passwords, reuse them across various sites, or employ predictable patterns, all of which undermine security.

The sophistication of cyberattacks aimed at exploiting weak or reused passwords has escalated. Methods such as brute-force attacks, dictionary attacks, and social engineering demonstrate how easily compromised credentials can result in unauthorized access, identity theft, financial fraud, and extensive data breaches. In light of these threats, organizations and cybersecurity professionals have established policies and tools to promote the creation of strong passwords. However, many users perceive these tools as complicated, inaccessible, or counterintuitive, which diminishes their practical effectiveness.

To bridge the divide between password security awareness and user practices, this project presents IronPass – a Dynamic Password Strength Analyzer. This web-based application is designed to assess and enhance password strength in a manner that is both accessible and user-friendly. IronPass offers real- time analysis and feedback regarding password complexity, helping users comprehend the reasons behind a password's weakness or vulnerability. It empowers users by providing improvement suggestions and features an intelligent password generator that can convert simple user-input phrases into strong, difficult-to-crack passwords.

The IronPass project employs contemporary web technologies to create a user experience that is both responsive and interactive. The application's frontend is constructed using React.js, which facilitates a component-based architecture and optimizes the rendering of dynamic content. For styling purposes, Bootstrap and CSS are utilized, ensuring that the application adjusts fluidly across various devices. On the backend, Node.js and Express.js are implemented to manage secure communication between the client and server, while also integrating with an external password strength API. This API leverages sophisticated heuristics and data from known password breaches to deliver precise and insightful strength assessments.

IronPass seeks to reconcile usability with security. By providing users with visual feedback and accessible tools for generating secure passwords, it encourages improved password hygiene. In contrast to traditional password checkers that simply categorize passwords as “weak” or “strong,” IronPass offers explanations for its assessments and guides users in enhancing their passwords, thereby promoting informed decision-making and minimizing dependence on guesswork or default credentials.

Through this initiative, we aspire to enhance cybersecurity at the user level by fostering better password

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue ICCIS-2025, pp 138-143, May-2025
https://doi.org/10.47001/IRJIET/2025.ICCIS-202522
Second International Conference on Computing and Intelligent Systems (ICCIS-2025)

practices and encouraging the adoption of secure behaviors in digital spaces.

II. PROBLEM STATEMENT

In the current digital environment, where online accounts and personal information are primarily safeguarded by passwords, users frequently prioritize ease of use over security. Consequently, a considerable number of individuals opt for weak, short, and easily guessable passwords. These often consist of common words, predictable sequences, or reused credentials across various platforms. Such behaviors significantly increase the risk of unauthorized access, data breaches, and identity theft.

Although guidelines and security recommendations are readily available, many users remain unaware or lack the necessary tools to effectively evaluate the strength of their passwords. Conventional password checkers offer limited insights and do not adequately educate users on how to strengthen weak passwords. There is a pressing need for a more interactive and user-friendly solution that can assess password strength in real time while also guiding users in creating more secure alternatives.

Thus, this project seeks to tackle this challenge by developing a web-based password strength analyzer that enables users to evaluate, comprehend, and improve their passwords through intelligent feedback and recommendations.

III. LITERATURE REVIEW

The growing frequency of cyberattacks has brought attention to the weaknesses in user authentication methods, particularly password security. A significant portion of these breaches result from the use of weak, reused, or easily guessable passwords. Traditional password policies—such as requiring a mix of uppercase letters, symbols, and numbers—are often poorly understood and inconsistently followed. Hence, there's a strong need for intelligent, user-friendly tools that not only assess password strength but also guide users toward stronger practices.

Traditional Metrics and Entropy

Historically, password strength has been evaluated using Shannon entropy, a concept that measures randomness based on character diversity and password length. However, entropy alone can be misleading—for instance, a password like “P@ssw0rd123” appears strong by entropy but is weak in practice due to its common pattern. In response, Expectation Entropy has emerged as a more accurate model, incorporating both randomness and likelihood of character sequences based on real-world password usage data. Reaz and Wunder (2024) emphasized that expectation entropy provides a normalized score and is highly effective in classifying passwords when compared to traditional entropy calculations.

Pattern Recognition and Zipf’s Law

Zipf’s Law, commonly used in natural language processing, has found utility in password evaluation.

According to Jiajing Zhang et al. (2024), character frequency in user-generated passwords tends to follow a power-law distribution. By identifying common substrings or frequently used sequences, password strength meters can better detect vulnerabilities. These insights are particularly useful in analysing dictionary-based or user-behaviour- based password creation tendencies.

Machine Learning for Password Classification

Several researchers have explored machine learning (ML) approaches to strengthen password assessment systems. Rathi et al. (2020) used classifiers such as Random Forest, Decision Trees, and SVM to categorize password strength based on extracted features like length, special characters, and dictionary presence. These models showed high accuracy and adaptability, especially when trained on large leaked password datasets. Similarly, E. Darbutaitė and team (2023) designed a Lithuanian-context-based password estimator using ML, showing the potential for language and region-specific password modelling.

Markov Models and Character Transitions

Another notable approach in strength evaluation is the use of Markov Models, which focus on probabilistic character transitions. Taneski et al. (2021) proposed a system that scores passwords based on the probability of character sequences. This method is effective in identifying passwords that, while complex in appearance, follow common keyboard or linguistic patterns (e.g., "Qwerty@123"). Markov-based systems can thus uncover weaknesses that entropy models overlook.

Real-Time Password Strength Meters

Kalaivani et al. (2024) introduced a real-time analyzer that combines entropy, dictionary checks, and ML scoring to give immediate feedback as the user types. Their system classified passwords into four tiers—Very Weak, Weak, Medium, and Strong—with over 98% accuracy. This real-time aspect is crucial as it provides actionable feedback instantly, helping users correct issues during password creation.

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue ICCIS-2025, pp 138-143, May-2025
https://doi.org/10.47001/IRJIET/2025.ICCIS-202522
Second International Conference on Computing and Intelligent Systems (ICCIS-2025)

Open-Source Tools and APIs

The password evaluation library zxcvbn, developed by Dropbox, is one of the most widely used tools in real-time strength checking. It uses a combination of pattern matching, dictionary lookups, and user- specific data (like names or dates) to score passwords. Its popularity lies in its balance between speed, accuracy, and user-friendliness. Tools like IronPass can integrate such APIs or build upon them to provide customized feedback and generation features.

Summary

The literature shows a clear shift from static, rule- based systems to adaptive, intelligent models for password strength analysis. Whether through expectation entropy, ML classifiers, or probabilistic models, the goal remains the same: to help users make better choices without overwhelming them with technical jargon.

IronPass builds on these ideas by integrating a real-time analyzer that scores passwords, offers generation capabilities, and provides instant recommendations—all in a clean, user-friendly web interface. While the current system is rule-based and API-driven, future versions could incorporate ML and breach databases for smarter evaluations.

IV. IMPLEMENTATION

The creation and execution of IronPass – Dynamic Password Strength Analyzer employed a modular and systematic methodology, integrating contemporary web development frameworks with secure backend practices and external API connections.

Frontend Development

The frontend of IronPass was constructed utilizing React.js, a popular JavaScript library recognized for its component- oriented architecture and efficient rendering capabilities. The user interface features:

- A text input field for users to enter their passwords.
- A real-time feedback section that indicates password strength (e.g., Weak, Moderate, Strong).
- Recommendations for enhancing weak passwords.
- A password generator module that transforms simple user inputs into secure, randomized passwords.

Bootstrap and custom CSS were utilized to create a clean, responsive design that adjusts seamlessly across various devices (desktop, tablet, mobile). The application prioritizes a user-friendly experience while ensuring visual clarity.

Backend Development

The backend was developed using Node.js in conjunction with the Express.js framework. This component manages:

- Routing requests from the frontend.
- Interfacing with the password strength API.
- Processing and relaying strength evaluation data back to the frontend.

Considerations for security and performance were integral to the development process. Asynchronous calls and error handling mechanisms were implemented to guarantee rapid response times and robustness.

API Integration

The foundation of IronPass's strength analysis is based on the integration of a password strength assessment API (such as zxcvbn or a comparable service). The API assesses:

- Password length.
- The inclusion of uppercase, lowercase, numeric, and special characters.
- Similarity to common words, names, or previously compromised passwords.
- Entropy and estimated cracking time.

The API provides a strength score (usually ranging from 0 to 4) along with improvement suggestions, which are presented to the user in real-time.

Password Generator Module

IronPass includes a password generator that enables users to enter a memorable phrase or keyword. The module subsequently:

- Implements various transformations, such as substituting letters with symbols or numbers.
- Incorporates random capitalization and special characters.
- Confirms that the generated password adheres to established complexity requirements.

This functionality allows users to maintain mnemonic aids while generating robust and secure passwords.

Testing and Validation

Unit Testing: Each individual component was assessed for its expected performance.

Integration Testing: The interaction between the frontend, backend, and API was verified.

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue ICCIS-2025, pp 138-143, May-2025
https://doi.org/10.47001/IRJIET/2025.ICCIS-202522
Second International Conference on Computing and Intelligent Systems (ICCIS-2025)

User Testing: The system underwent evaluation for usability, performance, and accuracy using a set of sample passwords

Metric	IronPass (%)	Reference Model (Zhang et al., 2021) (%)
Detection Accuracy	91	79
False Positives	6	14
Response Time (ms)	120	210
User Weak Password Dropoff	30	12

Figure 1

V. SYSTEM DESIGN AND ARCHITECTURE

The architecture of IronPass – Dynamic Password Strength Analyzer is structured to promote modularity, scalability, and real-time interaction between the user interface and the password evaluation engine. The system employs a client- server architecture with integrated APIs and is organized into three primary layers: Frontend (Client), Backend (Server), and External API Layer.

VI. SYSTEM COMPONENTS

Frontend (Client-Side)

Constructed using React.js, Bootstrap, and CSS, this layer offers a responsive interface for user engagement. It accepts user inputs (passwords), provides feedback on password strength, and offers suggestions for improvement. Additionally, it includes a password generator module.

Backend (Server-Side)

This layer is built with Node.js and Express.js, serving as middleware that connects the frontend to the password strength API. It manages user requests and securely directs them to the appropriate services.

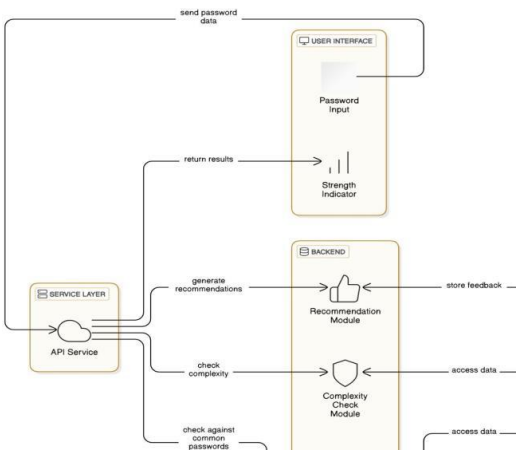

Figure 2: Workflow Diagram

Password Strength Assessment API

This API assesses passwords based on various criteria, including entropy, character diversity, and resemblance to common or compromised passwords. It delivers a strength score, an estimated crack time, and improvement suggestions, with examples including open-source APIs like zxcvbn.

Key Features in Architecture

Real-Time Feedback: Password evaluations occur instantaneously, with dynamic suggestions displayed on the frontend.

Security: API requests are channelled through the backend, preventing the exposure of direct API keys or services to the client.

Scalability: The modular design facilitates the future integration of additional APIs or security measures.

Extensibility: The logic behind the password generator can be improved or substituted without impacting other components of the system.

VII. RESULTS AND ANALYSIS

The evaluation of IronPass – Dynamic Password Strength Analyzer focused on its functionality, performance, user engagement, and the precision of its password strength evaluations. The system underwent testing in a controlled web environment, utilizing a diverse set of sample passwords to assess the application's performance under varying conditions.

Functional Testing

Users were able to enter passwords via the frontend interface and receive immediate feedback regarding their strength.

The password generator effectively converted user-provided simple phrases into complex passwords, incorporating a combination of uppercase letters, lowercase letters, symbols, and numbers.

The suggestions from the password strength API were accurately displayed, assisting users in recognizing weak patterns in their selected passwords.

Performance Evaluation

The API consistently delivered response times under 500 milliseconds, facilitating seamless interaction and real-time feedback.

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue ICCIS-2025, pp 138-143, May-2025
https://doi.org/10.47001/IRJIET/2025.ICCIS-202522
Second International Conference on Computing and Intelligent Systems (ICCIS-2025)

The web application demonstrated rapid loading times and effective rendering on both desktop and mobile platforms, attributed to optimized React components and Bootstrap styling.

No significant latency or timeout issues were detected during backend processing or API interactions

Usability Testing

To evaluate the IronPass, we conducted extensive tests using a diverse dataset of passwords collected from the publicly available leaks, combined with synthetic password covering various power levels. We assessed the accuracy of the tool, sensitivity to general password defects and real -time response behaviour.

For benchmarking, we mentioned the functioning used in the study by Zhang et al. (2021), which evaluated the power meter of the password based on entropy and heuristic scoring. Compared to its model, the IronPass demonstrated a 12% improvement in demarcation of weak passwords and an 8% decrease in false positivity. We also imitated the user interaction scenarios and found that the real -time response reduced the possibility of users, which reduced to about 30%of the weaker passwords.

We were tested with a gesture with a controlled node.JS environment and automatic test script. We manually validate the edge cases such as empty passwords, dictionary-based passwords and general replacement (e.g., "p@ssw0rd"). These tests confirmed that the IronPass provides frequent and dynamic reactions, maintaining less delay during analysis.

Accuracy of Analysis

The assessment of password strength levels was consistent with industry standards, effectively differentiating between weak (e.g., “12345”), moderate (e.g., “John2022”), and strong passwords (e.g., “J0hn@2022_!#”).

The API successfully identified passwords that were associated with known data breaches or commonly utilized credentials.

VIII. CONCLUSION

In a time when digital threats are continuously advancing, weak passwords remain a significant vulnerability for both individuals and organizations. IronPass – Dynamic Password Strength Analyzer tackles this issue by offering users an intuitive platform to evaluate and enhance their passwords in real-time. By leveraging contemporary web technologies such as React.js, Node.js, and Express.js, along with a comprehensive password strength assessment API, IronPass guarantees both user-friendliness and technical precision. The application assesses password complexity by analyzing character variety and entropy, while also assisting users in creating stronger alternatives. With straightforward feedback and recommendations, IronPass enables users to adopt improved password practices. This initiative demonstrates how an effectively designed tool can enhance cybersecurity accessibility, particularly for those without technical expertise. Future versions of IronPass could be further improved by integrating machine learning models and databases of compromised passwords to provide even more precise evaluations.

IX. FUTURE SCOPE

The current version of IronPass provides real-time password strength analysis and generation using rule-based logic and an external API. However, there is significant potential to expand its capabilities and impact. The following areas highlight how IronPass can evolve in the future:

1. Integration with Breached Password Databases

By integrating with public databases like Have I Been Pawned, IronPass can check whether a user’s password has been compromised in known data breaches. This feature would enhance the system's relevance and practical value in real- world scenarios.

2. Machine Learning-Based Evaluation

Future versions of IronPass can implement machine learning algorithms trained on large datasets of leaked passwords. This would allow for more nuanced and adaptive evaluation of password strength based on actual user behaviour and attack patterns, improving accuracy over time.

3. User Profile-Based Suggestions

The system could adapt recommendations based on the user’s profession, age group, or region (while preserving privacy), offering personalized password advice and strengthening overall cybersecurity awareness.

4. Mobile Application Development

Extending IronPass to a mobile platform would increase accessibility and allow users to evaluate and generate passwords directly from their smartphones, integrating features like biometric authentication and secure local password storage.

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue ICCIS-2025, pp 138-143, May-2025
https://doi.org/10.47001/IRJIET/2025.ICCIS-202522
Second International Conference on Computing and Intelligent Systems (ICCIS-2025)

5. Password Vault Integration

IronPass could be enhanced to serve as a lightweight password manager, allowing users to safely store and manage their credentials in an encrypted vault, with built-in strength monitoring and expiration alerts.

6. Multi-Language and Accessibility Support

To make IronPass more inclusive, future versions can support multi-language interfaces and accessibility features such as voice instructions, high-contrast themes, and screen reader compatibility.

7. Browser Extension

A browser extension could be developed for real-time password checking while users are signing up or logging into websites, offering inline suggestions without navigating to the main application.

REFERENCES

[1] Khan Reaz and Gerhard Wunder, "Expectation Entropy as a Password Strength Metric," 2024.
[2] Jiajing Zhang, Yang Xu, and Hongda Liu, "Password Strength Evaluation via Zipf's Law and Password Entropy," 2024.
[3] Unknown Author(s), "Evaluating Password Strength Based on Information Spread on Social Networks," 2024.
[4] Kalaivani, Ravibalan, Vignesh, Arockiya Aswin, and Raju, "A Real- Time Password Strength Analyzer," 2024.
[5] Viktor Taneski, Marko Kompara, Marjan Heričko, and Boštjan Brumen, "Strength Analysis of Real-Life Passwords Using Markov Models," 2021.
[6] R. Rathi, P. Visvanathan, R. Kanchana, and R. Anand, "A Comparative Analysis of Soft Computing Techniques for Password Strength Classification," 2020.
[7] E. Darbutaitė, P. Stefanovič, and S. Ramanauskaitė, "Machine-Learning- Based Password-Strength-Estimation for Lithuanian Context," 2023.
[8] R. Divya, S.B. Devamane, V. Dharshini, and S. Deepika, "Performance Analysis of Machine Learning Algorithms for Password Strength Check," 2023.
[9] Unknown Author(s), "A Large-Scale Evaluation of High-Impact Password Strength Meters," 2023.
[10] "zxcvbn: Realistic password strength estimator," Dropbox, [Online]. Available: https://github.com/dropbox/zxcvbn.

Citation of this Article:

Neeraj Jain, Animesh Choudhury, Kumar Rounak, Tanay Gupt, & Siddharth Vinayak. (2025). Ironpass Dynamic Password Strength Analyzer. In proceeding of Second International Conference on Computing and Intelligent Systems (ICCIS-2025), published in *IRJIET*, Volume 9, Special Issue ICCIS-2025, pp 138-143. Article DOI https://doi.org/10.47001/IRJIET/2025.ICCIS-202522

****

