

# Presentation



**Title: An Explainable Password Strength Meter Addon via Textual Pattern Recognition**

- **Course Code: CSE-4302**
- **Course Title : *Computer Graphics and Pattern Recognition Sessional.***

- ***Submitted By***

**1. Name: Chandan Sourav Mallick**  
ID:2020106510

**2. Name: Saifur Rahman**  
ID:20201165010

**3. Name: Sajib Bhattacharjee**  
ID:2020107010

*Department of Computer Science and Engineering*

- ***Submitted To***

**Name: M. Raihan**

**Assistant Professor**

**Department of Computer Science and  
Engineering**

*Department of Computer Science and Engineering*

# Abstract

Addon enhances PSMs for textual password vulnerabilities, offering detailed pattern feedback to improve user comprehension. Study on Alexa's top 100 sites reveals a lack of such platforms. Identifies twelve weak password patterns from 70 million leaked passwords. Evaluation confirms effectiveness in aiding users for more secure passwords.

# 1. Introduction

This paper delves into Internet password vulnerabilities, focusing on users' inclination toward weak and reused passwords. It underscores limitations in current password policies and strength meters. The introduced PSM addon offers detailed feedback on weaknesses, spotlighting common patterns using data from 70 million leaked passwords. The study assesses the addon's efficacy in addressing PSM issues and improving user security awareness. Key contributions include the addon introduction, PSM survey insights, and positive user study results, concluding with future work considerations.



## 2. Related Work

Previous studies focused on password strength meters (PSMs), often using simplistic methods that lead to inaccuracies. Traditional models, like NIST's entropy-based approach, struggle with evaluating user-chosen passwords.

Research explores alternatives like password cracking and behavior modeling. Solutions like zxcvbn and Ur et al.'s meter reduce weak password patterns but lack detailed explanations. Our novel PSM addon emphasizes pattern passwords for enhanced user understanding and potential behavior improvement. It detects regional patterns, phone numbers, and date variants, providing comprehensive feedback. Tailored for Chinese users, it suggests client-side deployment to boost awareness of weak passwords.



### 3. Explainable Password Strength Meter Addon

Enhancing password security through email pattern matching and addressing vulnerabilities in pure letter and digit patterns. Utilizing regular expressions and a Two-Pattern Combination Matching Algorithm for Pinyin+Date, Pinyin+Phone, wire phone numbers, and pure letter+digit. Exclusion of three-pattern combinations reduces user burden. Leaked password analysis from sites like CSDN, Tianya, Duduniu, 7k7k, and 178.com offers insights into password patterns and security.



## Password



Use 8 or more characters with a mix of letters, numbers & symbols.

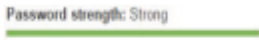
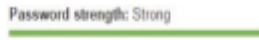
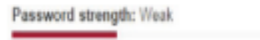
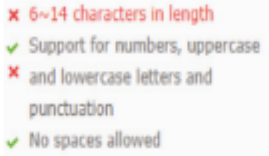
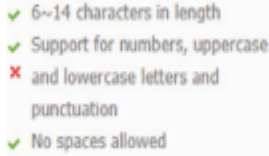
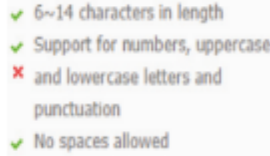









## 4. Evaluation

Evaluation reveals PSM shortcomings on top Alexa websites, with only three offering guidance and causing user confusion. A study exposes deficiencies in some sites, jeopardizing access control. The leaked password analysis emphasizes pattern matching's importance, showcasing the addon's superior detection, including Pinyin patterns. The dataset of 70 million passwords highlights prevalent patterns like pure digits and Pinyin+date. In conclusion, the evaluation stresses the need for user-friendly PSMs, praising the addon's broader pattern detection, crucial for enhancing password security, especially for Chinese users.





TABLE 3: A table to show the difference between PSMs of Alexa top 10 sites and ours.

	haorenyishengpingan	19951231	qwertyuiop
our explainable meter	Status Code: 402 Pattern: Pinyin Proportion: up to 5.4%	Status Code: 302 Pattern: Dates Proportion: up to 12.9%	Status Code: 201 Pattern: Keyboard proportion: up to 10.3%
Google			
Facebook	no hint	no hint	no hint
Baidu			
Reddit			
Yahoo	no hint	no hint	no hint
Tencent			
Amazon	no hint	no hint	no hint
Taobao	strength: medium	the password does not meet requirements	medium: weak
Twitter			

## 5. User Study

The user study with 50 college students found that the explainable PSM addon effectively influenced password habits, emphasizing common use of digit+letter combinations. Participants were willing to change behaviors based on addon warnings, showcasing improved security awareness. Other identified pattern passwords indicated a potential shift toward more secure practices. In summary, the study demonstrated the addon's impact on fostering awareness and encouraging safer password practices.

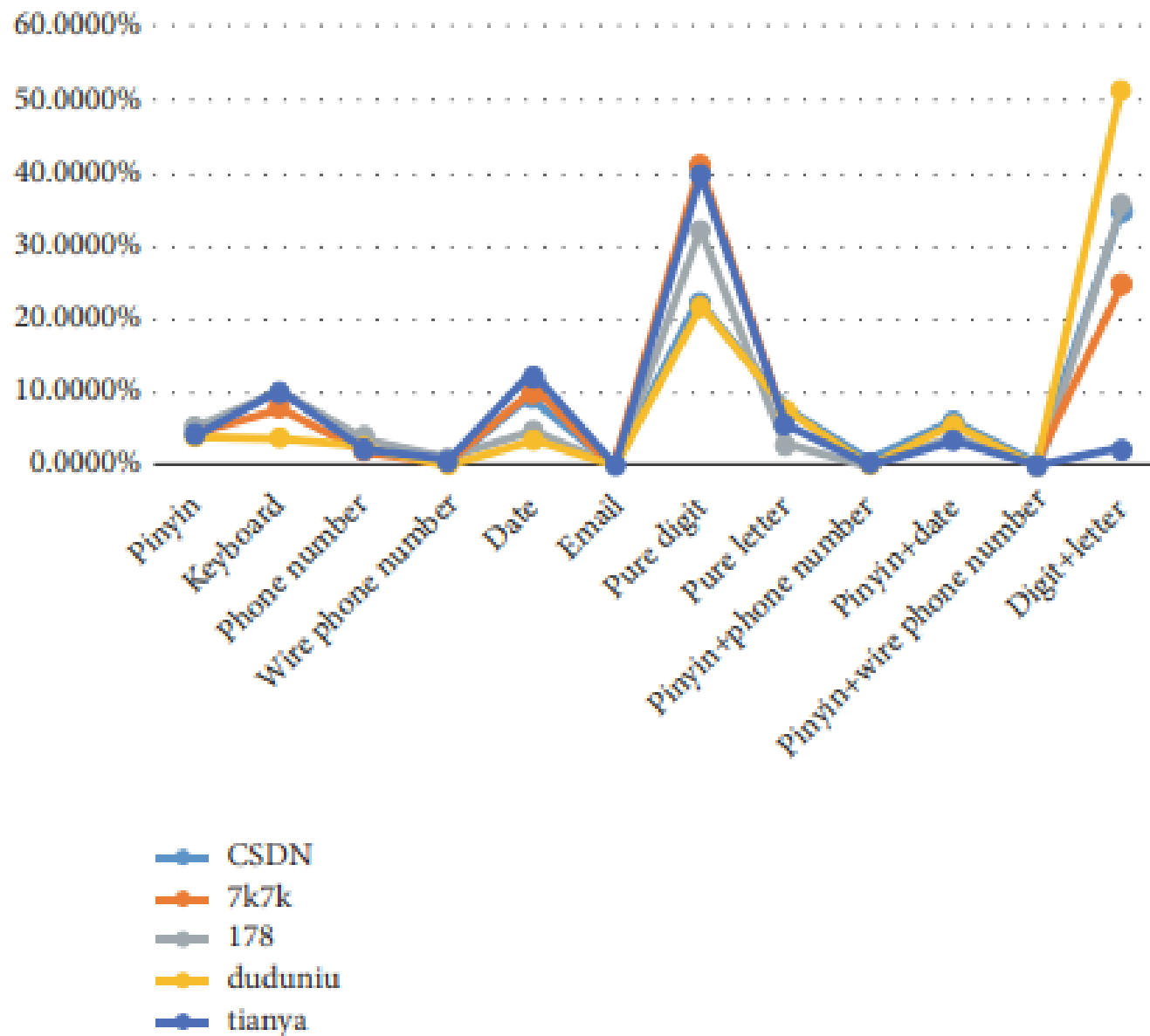


FIGURE 1: The proportion of pattern passwords among 70 million leaked passwords.

## 6.Conclusion

In summary, our study highlights PSMs' role in encouraging users to adopt stronger passwords. The user study affirms the effectiveness of our addon in enhancing usability. Despite only three top Alexa websites providing limited pattern information, our integrated addon outperforms in detecting more patterns, especially keyboard patterns in leaked passwords.



# Thank you