Minor Project (21CSA697A)

Proposal (Individual Mode)

Title: Password Strength Classification
Student Name: KETHA DEVIKA
Roll No.: AA.SC.P2MCA24074048

Abstract :

Password Strength Classification describes the project's purpose, the problem it addresses (prevalence of weak passwords and associated security risks), the proposed methodology (rule-based checks, entropy calculations, potential machine learning approaches), the expected outcomes (a tool that classifies password strength and provides feedback), and the project's contribution to enhancing cybersecurity awareness.

Assumptions/Declarations:

Assumptions:
1. Passwords are input as strings.
2. Password strength is classified based on criteria like length, uppercase, lowercase, digits, and special characters.
3. Classification categories are Weak, Medium, and Strong.

*Declaration ;
- *Weak*: Does not meet at least 3 criteria.
- *Medium*: Meets at least 3 criteria but not all.
- *Strong*: Meets all criteria (length ≥ 8, uppercase, lowercase, digit, special character).

Main Objective/Deliverable:

The main objective of password strength classification is to assess and categorize passwords based on their security level, helping users create stronger passwords to protect against unauthorized access and potential security breaches

Timeline and Milestones:

	Milestones	Timeline
1.	- 1970s: Introduction of password systems - 1988: Morris worm exploits weak passwords	- 1970s: Early password systems focused on basic security. 1988: Morris worm highlights password vulnerabilities.

Tools to be used.

Software/Hardware Tools	Specifications
- zxcvbn: Open-source password strength estimator - Passfault: Password strength analysis tool - John the Ripper: Password cracking tool for testing strength - Hashcat: Password recovery tool for strength testing - OWASP Password Validator: Web-based strength checker - Python libraries: password_strength, passlib for custom checks	- Criteria: - Length: ≥ 8 characters - Uppercase: ≥ 1 letter - Lowercase: ≥ 1 letter - Digits: ≥ 1 - Special characters: ≥ 1 - Classification: - Weak: < 3 criteria met - Medium: 3-4 criteria met - Strong: All 5 criteria met - Additional checks: - Dictionary words - Sequential patterns (e.g., "abc123") - Common passwords (e.g., "password123") - Output: Strength category (Weak/Medium/Strong) and feedback

Topic	Description
- Cybersecurity companies: Offer password security solutions ($100k-$1M+ per project) - Password managers: Integrate strength classification for premium features ($10-$20/user/month) - Consulting services: Assess password policies for clients ($50-$200/hour) - Research and development: Improve classification algorithms (varies widely) - Freelance work: Offer password security assessments ($25-$100/hour)	Password strength classification evaluates passwords based on criteria like length, complexity, and unpredictability to categorize them as Weak, Medium, or Strong . - Weak: Easily guessable or crackable - Medium: Some security measures, but vulnerable - Strong: Resistant to common attacks, secure Helps users create robust passwords and protect accounts

Date :23/12/2025
Student Name : KETHA DEVIKA Signature: Devika K