

# Form 1: Project Information Form

1. Team No: 09

2. Project Title:

A Password Strength Evaluation Algorithm

3. Team Details:

Sl. No	Hall ticket Number	Name
1	20EG105404	B. Mounika
2	20EG105418	K. Suxya Teja
3	20EG105434	P. Manvitha
4	-	-

4. Problem Statement

To improve the security of password authentication system and to investigate how user's personal information is used in passwords.

5. Source of IEEE paper - 2020 International Conference on Project: Trust, Security and Privacy in Computing and Communications

6. Final Outcome: To present a sensitivity personal information coverage evaluation function that represents correlation between user's password and their personal information.

7. What are parameters consider for project evaluation

user friendly interface  
strength of the password  
security enhancement

8. Development Environment:

Python 3.10 IDLE  
Visual Studio Code

Signature Team Members

- 1 B. Mounika
- 2 K. Suxya Teja
- 3 Manvitha P

Signature Supervisor

KM  
CDK. K. Madhuri

## FORM 2: LITERATURE DOCUMENTS

1. Team No: 09

2. Project Title: A Password Strength Evaluation Algorithm.


### Comparison of Existing Methods.

Sl No	Author(s)	Method	Advantages	Disadvantages
1	Mariam.M.Taha Taqwa.A.Alhaj Ala.E.Moktar Azza.H.Salim Settana.M.Abdullah	Password entropy. Password quality indicator. A dictionary attack using a second-order Markov model.	Measures password strength in terms of its entropy, and its PQI at the lowest possible cost.  Detects high entropy password that doesn't pass dictionary attack.	Limited scope  Generalization of rules.
2	Sivapriya K Deepthi L.R	Segmentation algorithms: Maximum matching algorithm Triangular matrix algorithm Password segmentation algorithm.	Consideration of User Attributes.  Optimal segmentation algorithm.  Correlation analysis.	Ethical concerns  Complexity.
3	Vijaya MS Jamuna KS Karpagavalli S	Machine Learning algorithms: Multilayer perception Decision tree induction Naive Bayes classification Support Vector Machine	Higher accuracy.  Handling complex patterns.  Feature Importance.	Dependency on training data.  Overfitting.  Data privacy concerns.

Signature Team Members

1. B. Mounika
2. K. Sumpatja
3. Kavithe P

Signature Supervisor

  
(Dr. K. Madhuri)  
28/7/2023

### Form 3: Project Requirement and Progress Document

1. Team No:09

2. Project Title: A Password Strength Evaluation Algorithm

3. Functional Requirements:

Actors	Use cases	Scenarios
Users	Evaluate password strength	Enters password The system checks if the password meets the requirements. The system provides feedback to the user.
System	Provide password requirements	The user requests password creation guidelines. The system displays the minimum requirements. The system provides examples of strong passwords.

4. Functionality Status

SI NO	List of functions	Status
1	Finding Dataset	Completed
2	Analysis of passwords	Completed
3	Building the algorithm	In progress
4	Bidirectional matching algorithm	Not yet started
5	Structure segmentation algorithm	Not yet started
6	Determining the strength of the password.	In progress
7	User interaction and interface.	In progress

Signature-Team members

1. B. Mounika.  
2. Manvitha P  
3. K Suryateja

Signature-Supervisor

Dr. K. Madhuri



#### FORM-4: Functional Test Cases

1. TEAM NO: 09
2. PROJECT TITLE: A PASSWORD STRENGTH EVALUATION ALGORITHM
3. TEST CASES:

SI NO	USE CASE	FUNCTION BEING TESTED	INITIAL SYSTEM STATE	INPUT	EXPECTED OUTPUT	TEST RESULT
1	Initial preprocessing and comparison of algorithms.	Logistic regression XG boost Naive Bayes, Decision Tree.	Imported libraries- pandas Numpy Seaborn Matplotlib Tfidfvectorizer Logistic regression XGboost MultinomialNB DecisionTreeClassifier	Dataset is provided	Provides the most accurate algorithm.	XG boost and Decision Tree are proven to be the most accurate.
2.	Categorize passwords into parts.	Structure segmentation of passwords based on personal categories	Installed python	Name Birthdate Identity number Email Telephone number	Segmented information	Separated information from provided input.
3	Matching personal information in the password to the input.	Bidirectional matching of passwords to give the type of information it incorporates.	Installed python	Name Birthdate Identity number Email Telephone number Password	Tag and the length of the password	Gives the kind of personal information used in the password.
4	Evaluate password strength	The score is assigned to eventually be categorized into strength levels	Installed python	Name Birthdate Identity number Email Phone number Password	Score and classification	It gives the score of the password and categorizes it into levels.
5.	User Feedback	User feedback is provided after the password is given.	Installed python	Name Birthdate Identity number Email Phone number Password	Password strength and suggestion	It gives the strength of the passwords and provides the user with what more to be added to make it strong.

TEAM  
SIGNATURE

1. B. Mounika.  
2. K. Suryateja  
3. Mani tha. P

  
SUPERVISOR  
SIGNATURE

Dr. K. Madhuri

#### FORM 5: JUSTIFICATION AND CONCLUSION

1. TEAM NO: 09
2. PROJECT TITLE: A PASSWORD STRENGTH EVALUATION ALGORITHM
3. JUSTIFICATION:

SI NO	PARAMETER	EXISTING VALUE	IMPROVED VALUE	JUSTIFICATION
1	Accuracy in scores of passwords.	Logistic regression and Naive Bayes give less value of accuracy	XG boost and DecisionTree give more accuracy for strength of passwords.	XG boost, and Decision Tree give the most accurate result among all.
2.	Strength of passwords.	Only the behavior of passwords are analyzed in previous methods.	The scoring algorithm gives the level of password along with the score	The password provided is immediately given its level of strength so that the user can give a better password.
3.	User Feedback	No feedback is provided in existing algorithms.	The user feedback algorithm gives suggestions to improve the password.	The suggestion given can save time for the user and help them choose a strong password.

#### 4. CONCLUSION

This password strength evaluation system provides a basic analysis of passwords, and it explores the behavior of personal information in passwords. It gives the strength of the password chosen and also suggests making changes to make the password strong enough. It improves the understanding level and saves time for the user.

#### TEAM SIGNATURES

1. B. Mounika.
2. K. Suryateja.
3. Mounika. P

#### SUPERVISOR SIGNATURE

Dr. K. Madhuri

## Industry-Oriented Mini-Project

### Project Report Supervisor Evaluation sheet

**Project Title:** A PASSWORD STRENGTH EVALUATION ALGORITHM


**Team Members:**

H. No	Name of the Student
20EG105404	B.Mounika
20EG105418	K.Surya Teja
20EG105434	P.Manvitha

Section	Should include	(✓/×)
1. Introduction	Explain problem with one illustration	✓
2. Literature Survey	Comparison literature	✓
3. Proposed methods	Explain solution with one illustration	✓
4. Implementation	1. List of program files, explain each attributes and functionality on it 2. Dataset Description 3. Other support files	✓
5. Experimental Results/Observations	1. Experimental setup 2. Parameters with formulas	✓
6 Discussion of Results	1.Compare results(in graph/table )	✓
7 Summary, Conclusion and Recommendations	Justification of your findings	✓

✓  
**Recommendation:** Approved/Not Approved

**Remarks** Project work is completed as per the requirements.

  
Signature of Supervisor

Dr. K. Madhuri.