Project Design Phase-I
Proposed Solution Template

Date	19 September 2022
Team ID	8.2
Project Name	Password strength classifier
Maximum Marks	2 Marks

Proposed Solution:

S.No.	Parameter	Description
1.	Problem Statement (Problem to be solved)	Predicting the strength of passwords and estimating the time to crack them is important for evaluating and improving password security. However, doing this manually does not scale well.
2.	Idea / Solution description	We will create a machine learning model using TensorFlow and a sequential neural network architecture to automatically predict password strength as a classification problem and estimate cracking time via regression.
3.	Novelty / Uniqueness	Our solution is unique in its use of deep learning for this problem, which allows the model to learn complex password patterns. Fine-tuning the neural network architecture specifically for password data is a novel approach.
4.	Social Impact / Customer Satisfaction	More secure passwords mean better protection of user data and privacy. Our model can help guide users and systems to generate and adopt stronger passwords.
5.	Business Model (Revenue Model)	The model could be offered as a service to evaluate password security. Revenue could come from password auditing services or licensing the model itself.
6.	Scalability of the Solution	The TensorFlow implementation can scale to handle large datasets of password data. Once trained, the model can rapidly predict strength and cracking time for any input password. This is more scalable than manual or rules-based approaches.