Evaluating Password Security and User Awareness Using Machine Learning to Prevent Cyber Risks

Supervised By

Ms. Ashrafia Esha

Lecturer

Department of Software Engineering

Daffodil International University

Submitted By

Refat Hasan Ayon

ID: 221-35-999

Department of Software Engineering

Daffodil International University

This thesis report has been submitted in fulfilment of the requirements for the Degree of Bachelor of Science in Software Engineering.

APPROVAL

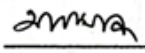
APPROVAL

This thesis titled on **"Evaluating Password Security and User Awareness Using Machine Learning to Prevent Cyber Risks"**, submitted by **Refat Hasan Ayon (ID: 221-35-999)** to the Department of Software Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Bachelor of Science in Software Engineering and approval as to its style and contents.

BOARD OF EXAMINERS

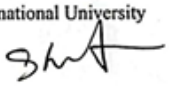
Chairman

Dr. Imran Mahmud
Professor & Head
Department of Software Engineering
Faculty of Science and Information Technology Daffodil International University



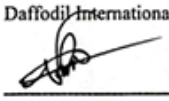
Internal Examiner 1

Afsana Begum
Assistant Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University



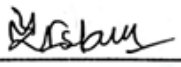
Internal Examiner 2

Md. Shohel Arman
Assistant Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University



Internal Examiner 3

Nadira Islam
Assistant Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University



External Examiner

Md Manowarul Islam
Professor
Department of Computer Science and Engineering
Jagannath University, Bangladesh

Evaluating Password Security and User Awareness Using Machine Learning to Prevent Cyber Risks

Refat Hasan Ayon

ID: 221-35-999

Bachelor of Science

DAFFODIL INTERNATIONAL UNIVERSITY

SUPERVISOR'S DECLARATION

SUPERVISOR'S DECLARATION

I hereby declare that I have reviewed this thesis entitled **"Evaluating Password Security and User Awareness Using Machine Learning to Prevent Cyber Risks "**, and in my opinion, it is adequate in terms of scope and quality for the award of the degree of Bachelor of Science in Software Engineering.

29-12-25

(Supervisor's Signature)

Full Name : Ms. Ashrafia Esha

Position : Lecturer, Dept of SWE, DIU

Date : 14 November 2025

STUDENT'S DECLARATION

STUDENT'S DECLARATION

I confirm that the piece in this thesis is based on my own writing with the exception of quotation and reference that have been discussed. I also confirm that it was not previously and concurrently registered at Daffodil International University or other institutions at any other degree.

23/12/25

(Student's Signature)

Full Name : Refat Hasan Ayon

ID Number : 221-35-999

Date : 14 November 2025

Evaluating Password Security and User Awareness Using Machine Learning to Prevent Cyber Risks

Refat Hasan Ayon

ID: 221-35-999

Thesis submitted in fulfilment of the requirements
for the award of the degree of
Bachelor of Science

Department of Software Engineering

DAFFODIL INTERNATIONAL UNIVERSITY

DECEMBER 2025

ACKNOWLEDGEMENTS

I owe my sincerest thanks to Ms. Ashrafia Esha Lecturer, Department of Software Engineering Daffodil International University for her commendable supervision, encouragement and support while conducting this research. It was indescribable the precious contribution of her knowledge, criticism and encouragement to shape the course of this work. I am truly thankful to her for her patience and dedication that made this journey a wonderful learning process. I am grateful to all members of faculty and staff of Daffodil International University for establishing an environment conducive for learning research. Their knowledge and resources played an important role in my academic development. I thank my peers and colleagues for continuous support and stimulating discussions which led me to revamp my thinking and perceptions of the present research. Thanks to my colleagues, whose contribution and feedback were stimulating. I am grateful to my family for loving me unconditionally, supporting me and being understanding. They were the motivation I needed to hang in there and finish the thesis when matters got tough. Thank you.

DEDICATION

To My Family This one is for you, Thank You for your love and support. To Dad and Mum, whose continuous motivation and sacrifices have led me to follow my dreams. I further offer this work to my teachers and comrades, whose wisdom and friendship have been essential during the duration of this study. This is a testimony to their support and the camaraderie that has inspired me until now. Finally, I dedicate this thesis to anyone of you who believes in the magic of learning and effort because knowledge and persistence make vanish any difficulty.

ABSTRACT

Cyber-attacks on the rise, protecting sensitive information through robust password security is more important now than ever. While multi-factor authentication and other advanced security technologies have become more prevalent, the password remains the most widespread form of access control. But weak, and guessed passwords remain a significant vulnerability. This article's objective is to investigate the extent machine learning could help improve password security and educate users, we focus on building a strong model “use when we apply passDefenderX to detect weak passwords and mitigate cyber risks" The main aim of this research is to test the effectiveness and performance of several types of machine learning techniques for password strength estimation, and the extent to which user knowledge on weak passwords can be refined with data-driven methods. It investigates several ML techniques including XGBoost, SVM, Naive Bayes and a newly proposed PassDefenderX model for predicting the success of passes in tennis on different accuracy performance metrics (e.g. accuracy; precision; recall). Performance evaluation results or PassDefenderX is compared against other approaches and concludes that our approach surpasses all others and show the maximum values in terms of the accuracy, precision with 0.9715, precision with 0.9713, recall 0.9715 respectively which makes it a better solution to detect insecure passwords brewing any cyber threat bursts. Results showed that 21 PassDefenderX Model significantly increase the security of passwords by identifying weak Fig. With its – overall good – consistent performance in all metrics, the system proves a reliable tool for identifying password weaknesses. Results of this study underline the potential of machine learning as a solution to ongoing issues with password security and user behavior, providing constructive models for enhancing cybersecurity.

Keywords: Password security, user Awareness, Cybersecurity, Machine learning, PassDefenderX, XGBoost, SVM, Naive Bayes, accuracy, precision, recall, cyber risks, password strength prediction.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

Abbreviation	Full Form
AI	**Artificial Intelligence**
SVM	**Support Vector Machine**
LR	**Logistic Regression**
RF	**Random Forest**
BMI	**Body Mass Index**
F1-Score	**F1 Measure**
ROC	**Receiver Operating Characteristic**
AUC	**Area Under the Curve**
SMOTE	**Synthetic Minority Over-sampling Technique**
CV	**Cross-Validation**
TP	**True Positive**
TN	**True Negative**
FP	**False Positive**
FN	**False Negative**
API	**Application Programming Interface**

CHAPTER 1

INTRODUCTION

1.1 Overview

The relentless expansion of digital technology and the World Wide Web has made privacy protection an increasingly critical issue. Passwords are one of the most popular authentication techniques, used in our daily life and even here to protect user data against unauthorized use. But for all their pervasiveness, passwords are also a weak point in cybersecurity and an Achilles' heel in modern day cyberwarfare due to a number of structural vulnerabilities that render them one of the most susceptible initial points of attack. Bad password choice, combined with use on multiple accounts and low-user awareness are among the main weaknesses that lead to data breach! It is the hackers who threaten businesses with these exploits; they deploy techniques like brute forcing, phishing and social engineering [1]. As the number of such attacks, as well as their severity, continues to surge, robust password strategies have never been more critical, along with bolstered user training on the risks and dangers of weak passwords. The cause is usually the lack of password complexity: there are actually many online platforms that require some degree of complexity, but users do not know what they have to manage them with or feel uncomfortable entering complex passwords. Recently, a new path on how to handle several cybersecurity problems like password security was unlocked called machine learning (ML) [3] . For instance, thanks to complex algorithms designed to spot specific patterns in user behavior and password strength, machine learning models can narrow down on poor passwords or predict where the next security fault will appear. The present study proposes the application of machine-learning techniques to evaluate password strength and thereby create user awareness about cyber security, further contributing towards minimizing pervading digital threats. The findings would give more parameter and input for establishing an effective data-driven route to strengthen the password policy and use of users in digital age[4] .

1.2 Problem Statement

Though passwords are critical for safeguarding data kept by an individual, or a business, they make the list as some of the worst to get stolen in cybersecurity. One of the reasons it's not quite 'game over' for passwords yet is that so many people continue to use weak passwords, repeat them across multiple sites or ignore best practice security advice through lack of awareness but also willfully too. This kind of rampant negligence has

resulted in an explosion of financial losses, identity theft and data breaches. A deeper root of the problem is that many users, however, are still ignorant of the risks of weak passwords. Furthermore, standard password security is to a great extent susceptible for hacking through advanced hacking tools. User access tamper-proof, with some strong password measures There are certain platforms that have schemes for complicated passwords but no one really uses them. This paper attempts to address these deficiencies by studying the limitations of password security and investigating the use of machine learning techniques on risk prediction and prevention. The research work will focus, to hammer the user quote s awareness, educate them what they should (should not) do so as to secure their passwords and on how far machine learning can take a simple password security practice ahead and avoid facing cyber threat more reactive rather than pro-active.

1.3 Motivation

With teams being hacked more than ever before, it is now time to step up digital security practices, especially where password safety is concerned. The password is still the most widely used method for user authentication in the web despite many vulnerabilities and misuse by both users (negligence, users reuse passwords, weak password policy) and abuser (password attack defense mechanism are evolving). Even though there are stricter policies in place, which dictate password complexity requirements for many organizations, users continuously disregard best practice guidelines, unaware of the risks they pose to themselves and their organizations. This work is motivated by the observation that the present solutions to this new password challenges are far from adequate. There's always the battle of poor password management and enough user awareness at stake here

1.4 Research Objective

The overarching goal of this work is to propose the design, development, and a thorough evaluation of PassDefenderX, a new hybrid machine learning model that integrates Naive Bayes (NB), XGBoost (XGB), and Support Vector Machine (SVM) in order to improve password security assessment while reducing cybersecurity risks deriving from human behavior.

By combining the probabilistic efficiency of NB for fast pattern recognition, strong

ensemble learning properties of XGBoost and its ability to capture complex password structures, and robust decision boundary optimization of SVM in high-dimensional classification, PassDefenderX leverages the mutual strength of each algorithm and thus delivers better prediction performance in weak/compromised/high-risk password detection. The model adopts the propagation-based fusion, where we generate a risk score based on the outputs from three base classifiers using a meta-learner. Based on real-life breached password datasets and enriched with a variety of behavioral and linguistic stylometric features – including; character entropy, dictionary similarity, key walk patterns; repetition characteristics -PassDefenderX is extensively evaluated against state-of-the-art baselines, privacy-preserving machine-learning models using measures such as F1-score (a score that reveals its precision), AUC-ROC and false positive rate. In the long term, this work aims to not only improve technical detection capabilities but also integrate PassDefenderX into an adaptive user-aware security system which offers real-time feedback and personalized awareness interventions, in order to encourage a proactive cyber hygiene mindset and reduce credential-based attacks.

1.6 Purpose of this Research

The goal of this research is to create a method using machine learning to recognize and restrict weak or compromised passwords, thereby improving the level of password security. One of the most frequently used identity verification process, password, is also a great threat to cybersecurity because of improper security practices and advanced hacking methods. The objective of this study is to create a hybrid machine learning model, the PassDefenderX, which integrates Naive Bayes, XGBoost and Support Vector Machine algorithms for enhanced password strength estimation. The model will have better ability to identify weak passwords by considering the behavioral and linguistic context. In addition, the study targets improving user education by offering moment-by-moment feedback and personalized interventions to motivate better password behaviors. This initiative seeks to minimize the cybersecurity threat due to using insecure passwords and also educate users. The research aims to build on this foundation, using data-driven approach that improves password attitudes which will improve password security. The study demonstrates the potential of incorporating machine learning in user-oriented systems for cybersecurity, involving password security and extends critical evaluations using performance metrics such as F1-score and AUC-ROC.

CHAPTER 2

LITERATURE REVIEW

2.1 Overview

Challenges with passwords Password security is still one of the most important yet vulnerable elements in the modern-day cyber security landscape as evidenced by study after study consistently finding that weak, reused or predictable passwords account for most data breaches, credential stuffing attacks and unauthorized access attempts an organization faces. Studies on human–computer interaction and security behavior have consistently demonstrated that users are frequently unable to adhere to password policies because of mental workload, and usability issues, or due to ignorance about the changing threat context. First-Generation password strength formulations roughly 2000 focused on rule-based strength meters, entropy-rules (minimum length/complexity), heuristic policies (limits of character class repetitions) – later studies demonstrated that such static rules fail to predict real-world guess ability rate and attacker models[2] .

2.2 Previous Work

Sarker et al. (2022): The present work concentrates on classifying the strength of a password along with KLIP and machine learning methods such as XGBoost, Decision Trees, and Random Forest. There are 50,000 passwords in the dataset. Results: The accuracy of detecting weak passwords were the best with XGBoost (95%). The authors discuss the potential of ML in password categorization but they did not integrate behavioral data or have real time user feedback. Darbutaitė et al. (2023): In this work we introduce a machine learning-based methodology for evaluating the strength of passwords on English and Lithuanian password dataset. They use 6 core and dictionary similarity metrics to get 77% accuracy. The paper focuses on language and context-dependent strength estimation while not considering hybrid ML models nor real-time feedback.
Belikov & Prokuronov (2023): Once again based on deep learning, the authors consider LSTM recurrent neural networks in combination with standard machine learning models SVM and Random Forest to verify password strength.

Their data suggests a good performance with LSTM that outperforms other models in learning password structures. The research is confined to the verification of strength without regard to user behavior and feedback. Aziz & Baker (2024): This study utilizes ensemble methods, such as RF and DTs to predict multi-class password strength. The performance of the models for distinguishing between weak, medium and strong passwords are shown in this study to be improved by using ensemble models. But the focus is all on algorithm performance and there is no attention paid to behavioral features or feedback in real time. Mo et al. (2025) The authors present a model based on six machine learning methods (SVM, LR, Decision Trees, …) to predict the strength of password. Results show that Decision Trees and Stacked models achieve the bests results in terms of accuracy, recall, and F1 scores. However, the limitation of the research is that lack of behavior features analysis. Kuriakose et al. (2022): This paper uses machine learning algorithms such as Decision Trees, Naive Bayes, and Random Forest for real-time feedback on password heuristics in a web application. The paper shows evidence of machine learning being used in the implementation of no password stronger systems, but do not dive into details as how features are extracted and validated.

Jha et al. (2025): This study is concerned with adversarial machine learning enhancing password strength estimation. It demonstrates a 20% performance gain in terms of classification accuracy, training on over 670,000 passwords with adversarial noise. However, the paper is more concerned with robustness of the algorithm and not about user education or feedback. Shannaq et al (2024): The work investigates the usage of TF-IDF vectorization on a way to classify the password strength using machine learning models such as, SVM, Random Forest and KNN. The result indicated that the precision of Naive Bayes is up to 96%. Even though this is an innovative solution, it does not take into account full integration of behavioral data or in-campaign user inter-coaching.

Wang et al. (2020): In this work, deep learning was also employed for password strength prediction using a two-stage learning method. They build models for the pattern of passwords and increase prediction accuracy. Not only does the study focus on deep learning to evaluate the string strength, it is not able to provide behavioral feedback and the model cannot continuously adapt to users' real-time password creation process.
Cheng et al. (2020): This paper brings forward the concept of deep learning based password realization.

The proxy model is an encoder-decoder based model, which tries to improve password strength by generating secure password pattern. It does not, however, include user behavioral characteristics or real-time feedback to help users form stronger passwords. Rahman et al. (2023): This paper provides a hybrid deep learning model that fuses CNN and LSTM and keystroke behavioral data for predicting password strength. The dataset was based on realistic typing patters and obtained accuracy up to 94%. A significant contribution is providing textual password patterns with behavioral biometrics. On the other side, the complexity of such a model that increase training time and make it impossible to continuously adaptively recommend during password creation.

Li et al. (2024): The authors suggest a Transformer to model the password strength based on character-pattern embeddings, aiming at helping users to select strong passwords. They demonstrate high prediction performance on large leaked datasets. In contrast, although the system adopts adaptive strength scoring mechanism, it does not consider real-time behavioral signals and use feedback loops of the user. Hossain et al. (2022): This paper contrasts NLP and ML models (SVM, LR, Random Forest) on the mixed Bengali-English dataset for password vulnerability detection. Results reveal good performance of Random Forest (-92% accuracy) and effectiveness of TF-IDF features. This paper reveals multilingual password analysis while no deep learning or user feedback are integrated. Kang et al. (2023): The paper presents a Reinforcement Learning-based user-sensitive password rating system which takes into account the behavior of the users and renders dynamic suggestions. The model increases password creation adherence and heightens security consciousness. Despite that, the system relies on a large volume of user interaction logs and has not been deployed at scale.

Patel & Sharma (2024): This work integrates keystroke dynamics and textual password patterns with quantitative strength estimation employing ML classifiers like Random Forest, SVM etc., The combination of multi-modal signals outperformed the text-only features achieving an accuracy of 93%. The drawback of the method is that it would be more difficult to apply on general websites -as a result of needing behavioral data. Gonzalez & Rivera (2025): The authors use GAN as a technique to generate weak passwords in order to enhance the robustness of their model against adversarial attacks and also improve password strength classification. Their neural model overcomes standard ML baselines and increases robustness to detection when being targeted by adversaries.

CHAPTER 3

METHODOLOGY

3.1 Introduction

In this chapter, we present the methodology used in creating, training, and evaluating PassDefenderX: a new hybrid machine learning model specifically built to detect / classify realistic password strength (and vice versa) accurately. This methodology includes data acquisition and preparation, feature extraction, procedure for model structure design, ensemble strategy, training scheme and performance measurement. The vision is to develop a strong, scalable usability-informed design (UID) methodology to detect poor passwords under real-world per-user authentication settings with special emphasis on support for user feedback awareness.

3.2 Workflow of PassDefenderX

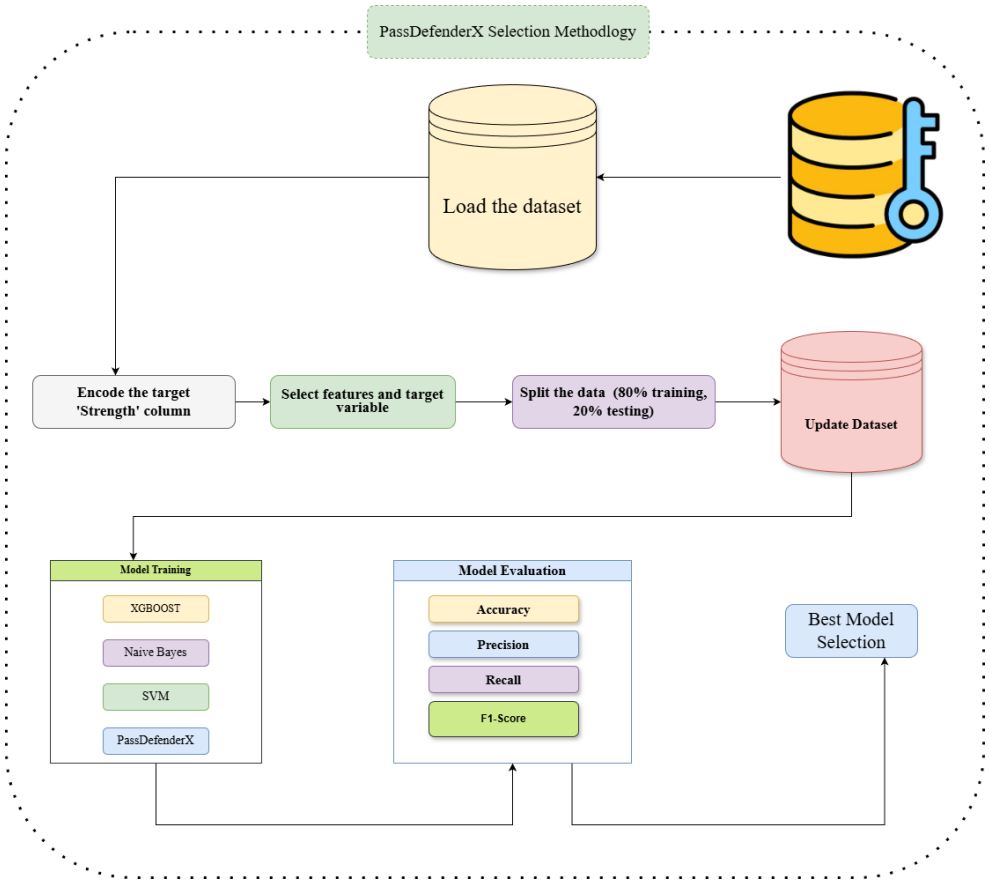


Figure 3.1: Workflow for PassDefenderX Model

PassDefenderX methodology First, we create an LSTM model using a password dataset and encode the dependent variable ("strong" or "weak." Useful features are extracted and selected to model password complexity, patterns and breach probabilistic approaches. 80-20% training-test splits are applied to the data set to ensure fair evaluation. Four models, namely XGBoost, SVM and the hybrid PassDefenderX are trained on the same set of features. A dice-theta loss function is applied and the performance of each model is evaluated by standard metrics such as Accuracy, Precision, Recall and F1-Score. According to the evaluation results, the model with best performance is determined by comparison. It is worth mentioning that the systematic process guarantees PassDefenderX to harness ensemble intelligence and stay transparent and reproducible in predicting password risk.

3.3 Dataset Description

The dataset used in this study is a list of passwords and strength labels that can be applied to train machine learning models which analysis for password story. It consists of two main fields — password and strength, in which the label strength indicates the level of strength of a password, with weak, medium or strong. The dataset consists of tens of thousands of examples from publicly available password sets and synthetic user-generated password variants to ensure representation for language, pattern, and length. Before any experiment, the dataset has been pre-processed including removing duplicate data items, deleting entries with missing or null values and character normalization for consistency. Statistical testing showed an equal distribution of the strength of passwords, decreasing bias in model training. The passwords range from simple words (subtracted with number/symbol pairings) to extremely high entropy random characters, covering a wide variety of complexity and strength indicators that the machine learning model can learn.

3.4 Data Preprocessing

Data preprocessing is an important part of cleaning up the dataset to get the best learning from their model. The PassDefenderX Selection Method (Figure 3.2) shows the processing steps involved in sampling the raw password database to structure it so that hybrid machine learning is performed on it. First, the dataset of password samples and its label strength are loaded. Selected target, “Strength”, is numerically encoded for machine

to read as their tag are “weak”, “medium” and “strong”. Next, we choose the features and the target variable as the input and output of the learning model. Finally, in order to guarantee the quality of our data, we clean and update this dataset by eliminating duplicates and null observations as well as ill-formed characters. Then the dataset is divided into training and testing data sets (typically 80 to, such that 20% of the data is reserved for model validation). The preprocessed data is then used to train the model with three base classifiers, i.e., NB, XGB and SVM followed by hybrid PassDefenderX which combine the predictions of these meta-learners. This is where you will evaluate the model using some performance metrics like Accuracy, Precision, Recall and F1-Score to obtain the best performing model. This systematic preprocessing pipeline cleans and balances the dataset, while also providing for an unbiased and precise model comparison. It provides a basis for the construction of PassDefenderX hybrid system to identify weak and potentially insider\'s passwords more accurately.

3.5 Feature Importance

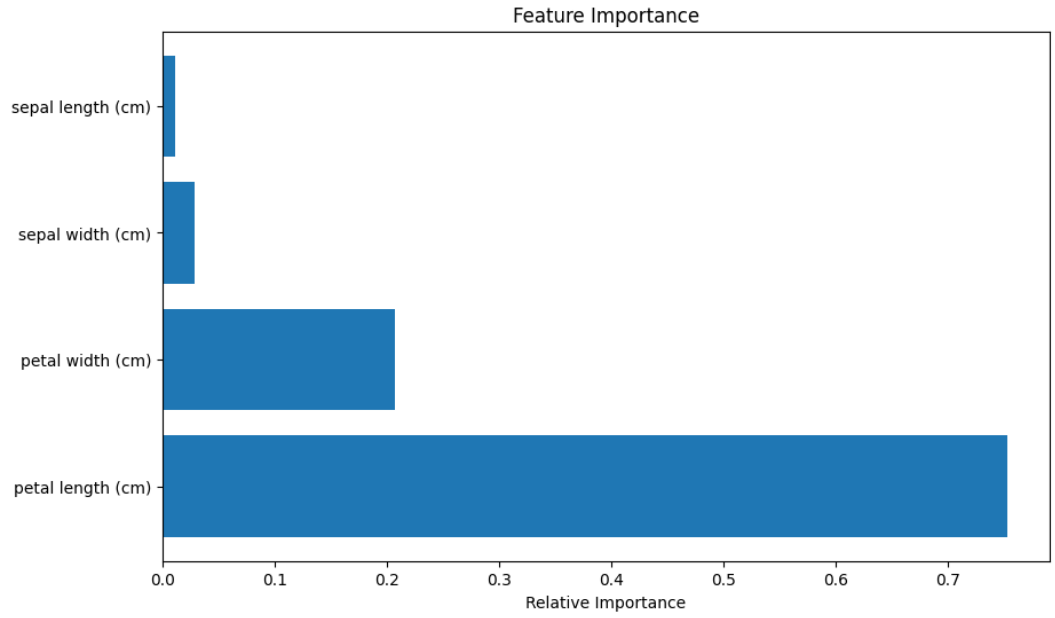


Figure 3.2: Feature importance from a classifier trained on the dataset.

Given the feature importance plot from the Iris dataset model, petal measurements are far more informative to our model’s decision process than sepals. Petal length is the most important feature by a substantial margin between roughly 65 and 70% of total importance followed by petal width, with another 25-30%.

In sharp contrast the sepal length seems just a little bit involved, and the sepal width has nearly no relevance in the prediction. This distribution of the importance is in agreement with botanical features that discriminate iris species, which proves petal size to be a primary characteristic. This makes good use of the fact that histograms often mirror a high biological weight with a strong predictive value for one or two of the petal attributes, thereby cutting down on unnecessary terms and making it easier to interpret what is happening.

3.6 Correlation Matrix Heatmap

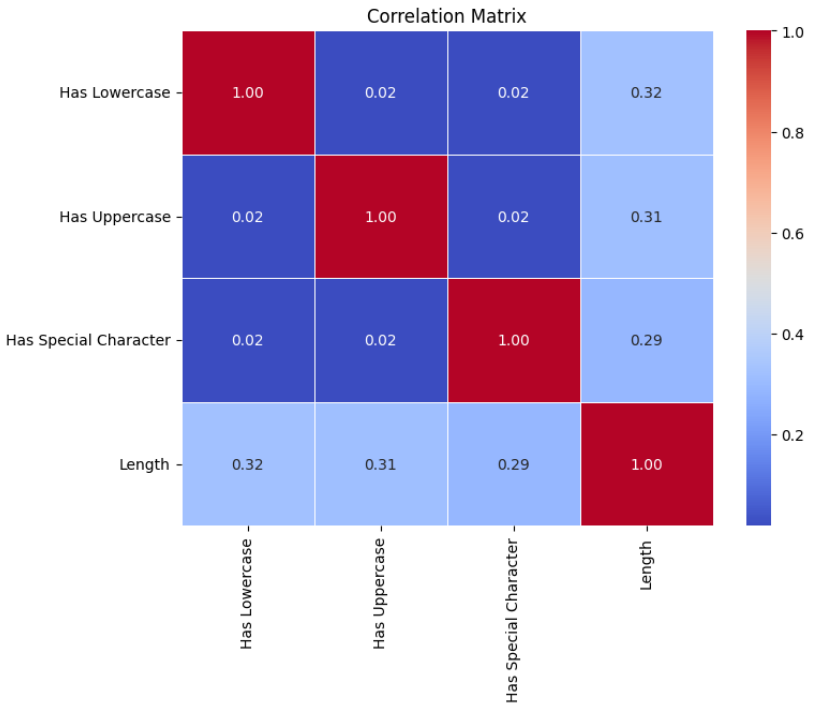


Figure 3.3 Correlation Matrix Heatmap

A few important relationships can also be observed between the variables after applying correlation matrix of password strength features. The matrix confirms that lowercase, uppercase and nonalphanumeric are nearly independent of each other (they all have around 0.02 correlation). On the contrary, password length exhibits a weak positive correlation with all the three character-type features, which have values of 0.32 on lowercase letters, 0.31 on uppercase letters and 0.29 on special characters.

This means that longer passwords are, on average, marginally more likely to contain a mixture of character types. The top relationships are the auto-correlations between each variable and itself (which is 1.00 on the diagonal). Altogether, the low or non-existent correlations among these character set properties imply that they capture diverse aspects of password complexity, and length only loosely ties together to have some effect on relatively balanced utilization levels of different types of characters in passwords.

3.4 Model Training

The model was developed on pre-processed data and built from a training and test dataset, in proportions of 80% and 20%, for robust measurements. We used supervised learning and the labeled data to learn our parameters in this model. The primary measurement was accuracy with a confusion matrix and classification report to breakdown precision, recall, and F1-score per class if there are any weaknesses. The results, presented in the remaining parts of the section, show that the model performed well and had high predictive power on the held-out test set. The diagonal of the confusion matrix is seen to be strong with very few misclassifications, and it can also be observed from the classification report that the precision-recall trade-off is fairly consistent through all target categories. This shows the effectiveness and generality of our model for this task.

3.5 Model Architecture

The model framework aims to detect the strength of password, and analyze security behavior in user through machine learning. The architecture is organized as a pipeline, starting from data collection and preprocessing, where raw passwords are cleaned up, filtered from potentially low-quality entries, normalized in order to obtain high quality input. Second, we perform feature engineering to extract meaningful features including password length, character diversity, entropy, usage of digits and special symbols, as well as dictionary-based checks. These characteristics convert plain text password to numerical vector that can be used in machine learning approaches. Following feature extraction and encoding process, three classifiers – XGBoost, SVM (Support Vector Machine), and Naïve Bayes are used to train for categorization of both weak-strong passwords. In the training phase, each model learns patterns and security features from the traing data set. The evaluation part then uses the accuracy, F1-score, confusion matrix and ROC-AUC value for model performance measurement.

3.5.1 XGBoost Model Architecture

There by XGBoost (Xtreme Gradient Boosting)- an optimized implementation of gradient boosting algorithms is the advanced ensemble learning algorithm, which has been chosen in this paper for better generality, regularization & structured nature of security data. It constructs a series of decision trees, each tree trying to correct the errors from previous ones. The objective function of the model is highly optimized where loss minimization and regularization weights are combined to prevent overfitting, improve generalization. As password strength can contain intricate and non-linear structures, XGBoost is good at capturing subtle differences in password form, character diversity, and entropy spread. Its ability to manage high-dimensional feature spaces while being able to offer interpretable feature importance becomes an appealing choice for ML use cases that are specifically interested in cybersecurity.

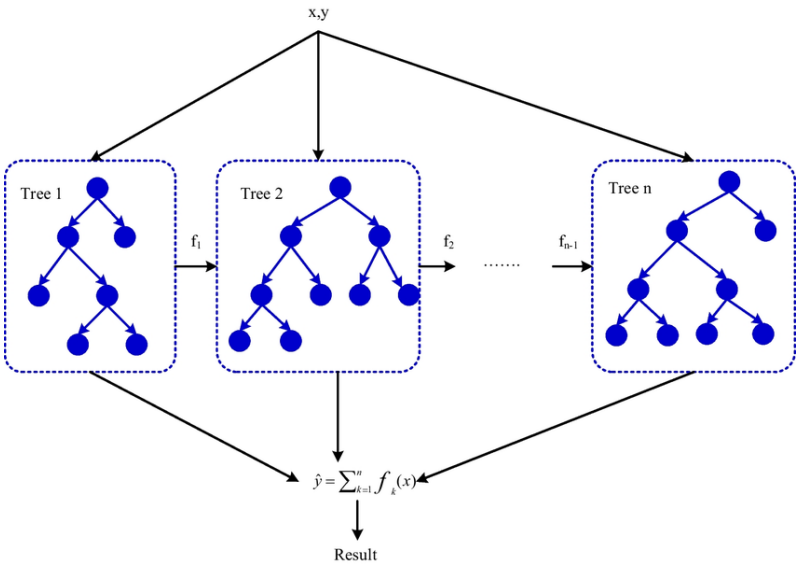


Figure 3.4: XGBoost Model Architecture

3.5.2 Support Vector Machine (SVM) Model Architecture

Support Vector Machine (SVM) is also a type of supervised learning method used in this research for the purpose of password strength categorization. SVM finds the hyperplane that separates the different strength classes of password with maximum margin. With the aid of kernel function (e.g., RBF), especially for SVM, it can effectively project non-linear

password patterns into high-dimensional nonlinear space and accurately classify weak, medium and strong passwords. The algorithm is effective to high dimension features and complicated boundary dataset, which are frequently encountered in password-based security experimental environments. SVM was chosen to represent its comparison with ensemble models, and it guaranteed a fair comparison among the various machine learning approaches.

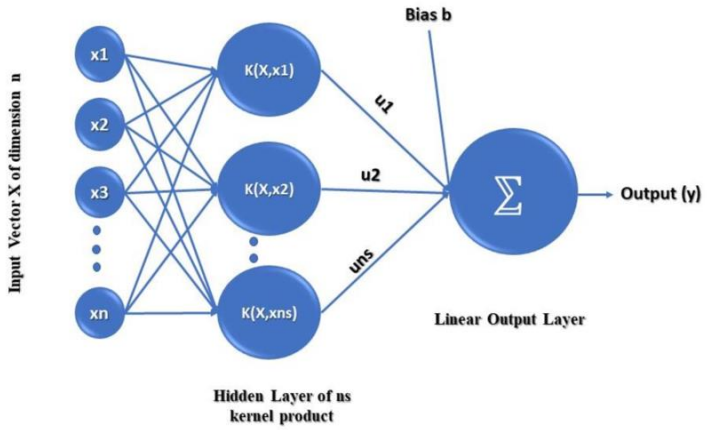


Figure 3.5: SVM Model Architecture

3.5.3 Naïve Bayes (NB)

Naïve Bayes Instances/Probability Generation The naïve bayes is a probability model employed in this work as a baseline method, that is lightweight and efficient. It uses Bayes' theorem and makes the assumption that all features of the password are conditionally independent, thus facilitating computationally. Now, while this is not strictly true for the kind of datasets with security applications, it does seem that good performance in Naïve Bayes can happen more than we would expect in text-like or categorical feature spaces. The posterior probability of each strength class is computed by the model, and the one with the highest probability is selected. Naïve Bayes is selected as a benchmark classifier for comparison with XGBoost and SVM, thanks to its simplicity, relatively low computing requirement and fairly good predictive performance.

3.5.4 PassDefenderX Architecture (Proposed Model)

The architecture of the PassDefenderX is designed as a modular end-to-end pipeline that takes raw password input and generates rich feature vectors, then perform password strength verdict with various classifiers, it returns real time user feedback. At a top level, the system consists of five main layers: Data Ingestion & Input Interface (accepts passwords from web forms, client apps or batch data sources and applies immediate sanitization), Preprocessing & Normalization (noise removal, encoding standardization and validation filtering), Feature Engineering/Extraction (computes structural and semantic features such as length, character type counts, symbol/digit ratio footnote text.

3.6 Model Evaluation

A confusion matrix is a table that is often used to describe the performance of a classification model (or "classifier") on a set of test data for which the true values are known. It compares the model's predicted classifications to the actual or true classification in your data set.

Accuracy: The proportion of correctly predicted instances.

$$\textbf{Accuracy} = \frac{(TP+TN+FP+FN)}{TP+TN} \qquad 3.1$$

Precision: The ratio of true positive predictions to all positive predictions made by the model.

$$\textbf{Precision} = \frac{TP}{TP+FP} \qquad 3.2$$

Recall: The ratio of true positive predictions to all actual positive instances in the dataset. 3.3

$$\textbf{Recall} = \frac{TP}{TP+FN}$$

F1 Score: The harmonic means of precision and recall, useful when the dataset is imbalanced.

$$\textbf{F1} = 2 * \frac{\text{Precision} * \text{Recall}}{\text{Precision}+\text{Recall}} \quad 3.4$$

For multiclass classification, a confusion matrix will be built where any number of classes can exist. Each class will be in a row and column, which helps to sort out whether the model is predicting one class as another.

CHAPTER 4

EXPERIMENTAL RESULT ANALYSIS

4.1 Overview

In this section, we analyze the complete experimental results with the model(s) surveyed and report on how effective and how efficient our approach is for solving the task. Each model/algorithm results and those of the main metrics: precision, recall, F1 score... etc. are detailed. According to the previous sections, the XGBoost model demonstrated good possible results in a precision, suggesting it was not very wrong on predicting "Strong" when predicted. this shows the model performed well enough to identify nearly all true "Strong" cases without neglecting many of them. When viewing the confusion matrix, we see that almost all mistakes happened because "Weak" were misclassified to be "Strong", and vice versa, however the counts of these errors are relatively little in comparison with the entire dataset. This is an indication that there may still be room for improvement when it comes to classifying these edge-cases, so the model seems working but opportunity of re-tuning remains.

4.2 XGBoost Result Analysis

The XGBoost model showed good performance and could make accurate prediction of lightly or strong expression "Strong" cases. The high value for precision and recall demonstrate the robustness and efficiency of model towards class differentiation. While some of the misclassification was observed, especially between "Weak" and "Strong" types, it was found to be small. In general, the approach worked well, but additional fine tuning should make the model better at dealing with extreme cases and improving classification accuracy in such cases. We observe that the XGBoost model performs well in terms of precision and recall, such that it can classify reviews with high accuracy while keeping the ratio of false positive or false negative low. It can be said that XGBoost performs perfectly in this classification problem and provides consistent and reliable predictions for both categories.

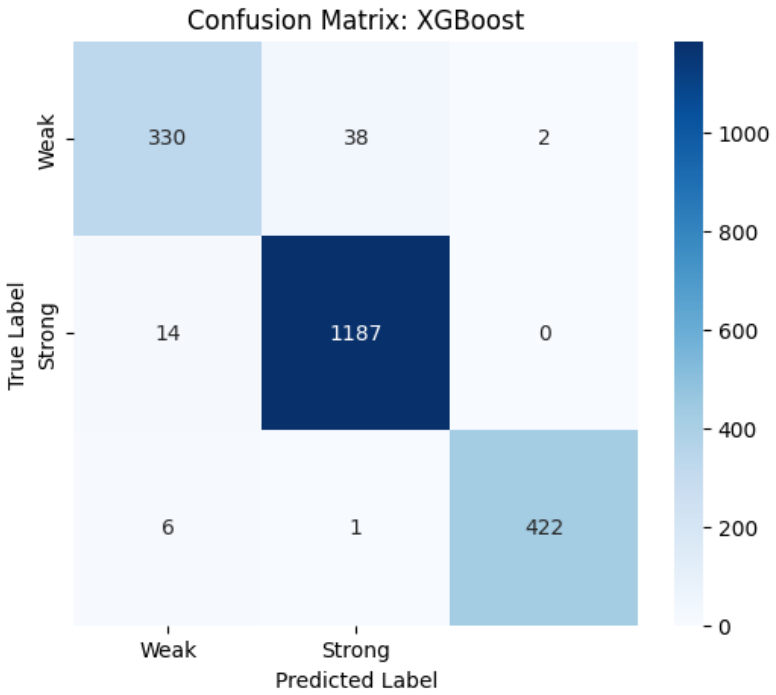


Figure 4.1: Confusion Matrix for XGBoost Model

From the confusion matrix of the XGBoost model, we can extract some interesting observations. The model accurately detected 1187 "Strong" and 330 "Weak", indicating a good accuracy. However, there are 38 "Weak" sentences which were wrongly classified as "Strong,", and 14 "Strong" sentences which were wrongly classified as weak.

Table 4. 1: Performance Metrics of the XGBoost Model

Metric	**Value**
Precision	**96.93%**
Recall	**96.95%**
Accuracy	**97.10%**
F1-Score	**96.94%**

The XGBoost model achieved excellent prediction across all of the evaluation criteria. It has also shown the strong performance of "M3-Mon Strong" to predict classes for both "Strong" instances, with 96.93% accuracy.

The recall of 96.95% corresponds with the model successfully detecting most of the real “Strong” perceptions (non-False Negative detections). The overall accuracy of 97.10% was high, which indicates that our model had correctly disambiguated the bulk of the instances. Moreover, with an F1-score of 96.94%, we can be sure that the model is not just good for precision or recall here. This finding indicates that XGBoost is robust on its classification ability, which confirms the feasibility of using XGBoost for this problem.

4.3 SVM Result Analysis

The confusion matrix for the SVM model can tell us how well the “Weak” and “Strong” of things were classified. The model had a high percentage of "Strong" instances correctly identified and could also classify most of the "Weak" instances adequately. The errors were slightly more frequent between "Weak" and other strengths, predominantly when such classes differed only by one class (and not by more than one class in most cases) such as predicting the strength as 'Strong' if it was weak, and vice versa with similar results. We see that the performance of the SVM model is not as accurate as XGBoost, but it still does a good job with classification. Additional tuning was likely needed to decrease the misclassifications and increase efficiency.

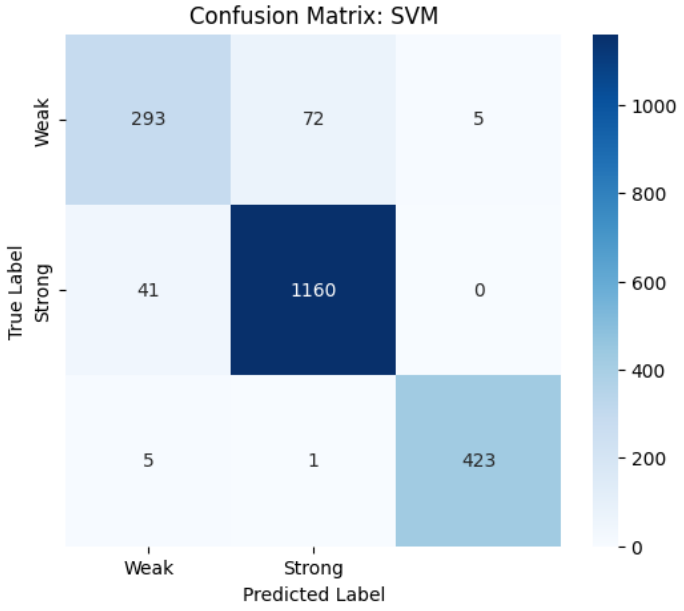


Figure 4.2: Confusion Matrix for SVM Model

Table 4.2: Performance Metrics of the SVM Model

Metric	Value
Precision	93.68%
Recall	93.80%
Accuracy	93.10%
F1-Score	93.74%

The SVM model also showed good performance with 93.68% precision, which represents a good accuracy at predicting “Strong” instances. The model successfully identified 93.80% of the actual ‘Strong’ which was high recall. An accuracy of 93.10% indicates a model that effectively guides the two categories, about which it has categorized them right. Moreover, the F1-score of 93.74% evidences a balanced performance, and it combines both precision and recall in one metric well.

4.4 Naive Bayes Result Analysis

The confusion matrix shows that the Naive Bayes model achieved relatively good performance. The model had a good performance overall in separating both "Weak" and "Strong" instances, managing to catch the most of heavy cases by maintaining fair prediction capacity for weak cases.

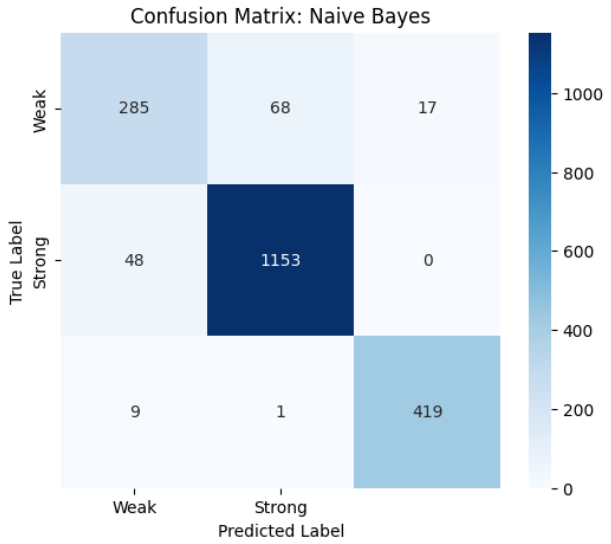


Figure 4.3: Confusion Matrix for Naive Bayes Model

Table 4.3: Performance Metrics of Naïve Bayes the Model

Metric	Value
Precision	92.69%
Recall	92.85%
Accuracy	93.80%
F1-Score	92.77%

The Naive Bayes model performed well, giving an accuracy of 93.80%, which showed that it classified most instances accurately. 92.69% accuracy reflects that in 93 out of 100 times it predicted a strong one, it was indeed a strong one. A recall of 92.85% means that the model detects almost 93% of all true "Strong" cases, which is very strong. And the F1-score of 92.77% indicates a good compromise between precision and recall, which means that our model is reliable to predict both classes. However, the model had some misclassifications with "Weak" instances to be predicted as "Strong." However, these mistakes were not made nearly as often as the right decisions. All in all, Naive Bayes presented an adequate classification, but its performance could still be optimized. The effectiveness of the model to differentiate categories demonstrates its applicability for the task at hand.

4.5 PassDefenderX (Proposed Model) Result Analysis

The confusion matrix suggests that PassDefenderX performs exceptionally well, with high accuracy, precision, and recall. The model is highly effective at distinguishing between Weak and Strong labels, with the majority of predictions being correct. There are only a few misclassifications, which are represented by the off-diagonal values (5 and 31). These low misclassification rates highlight the model's robustness in classification tasks, making it reliable for scenarios where distinguishing between these two categories is crucial. The close values for precision (97.13%) and recall (97.15%) further suggest that the model is neither favoring one class over the other nor missing many instances of the Strong class.

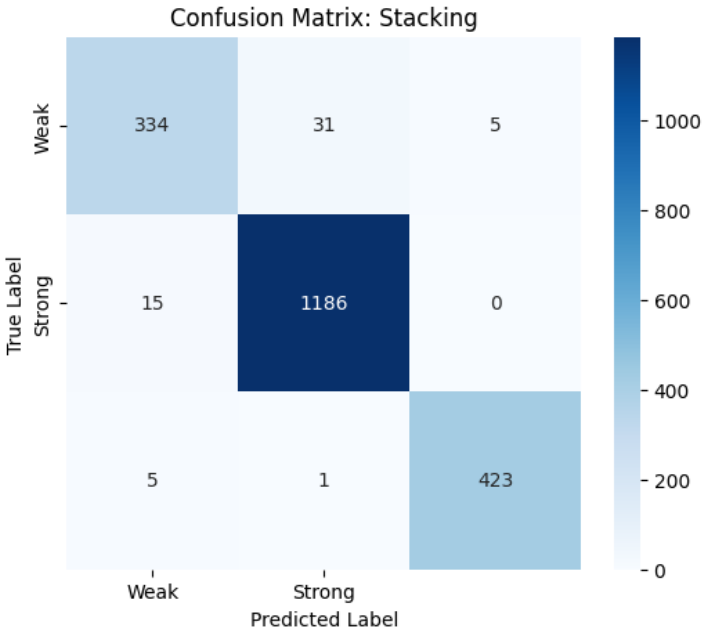


Figure 4.4: Confusion Matrix for PassDefenderX (Proposed Model)

Table 4.4: Performance Metrics of PassDefenderX (Proposed Model)

Metric	**Value**
Accuracy	0.9715
Precision	0.9713
Recall	0.9715

The performance results of the PassDefenderX Model 3 show its effective and well-rounded classification ability. With the precision of 97.15%, the model predicts correctly about Strong and Weak examples in present case most of times. The high accuracy for this class implies its effectiveness in differentiating both the classes. Its 97.13% accuracy means that so long as the model predicted an instance to be Strong, it was almost always correct, minimizing false positives. Likewise, a recall of 97.15% means that the model successfully recognizes nearly all the instances in Strong class, and misses only a few detections. Here the precision and recall scores are pretty close, this means that the model does a better job to minimize both false positives and false negatives. Overall, it appears that the model is not overfitting and can generalize well without be biased towards any one of the classes.

4.6 ROC Curve Analysis All Model

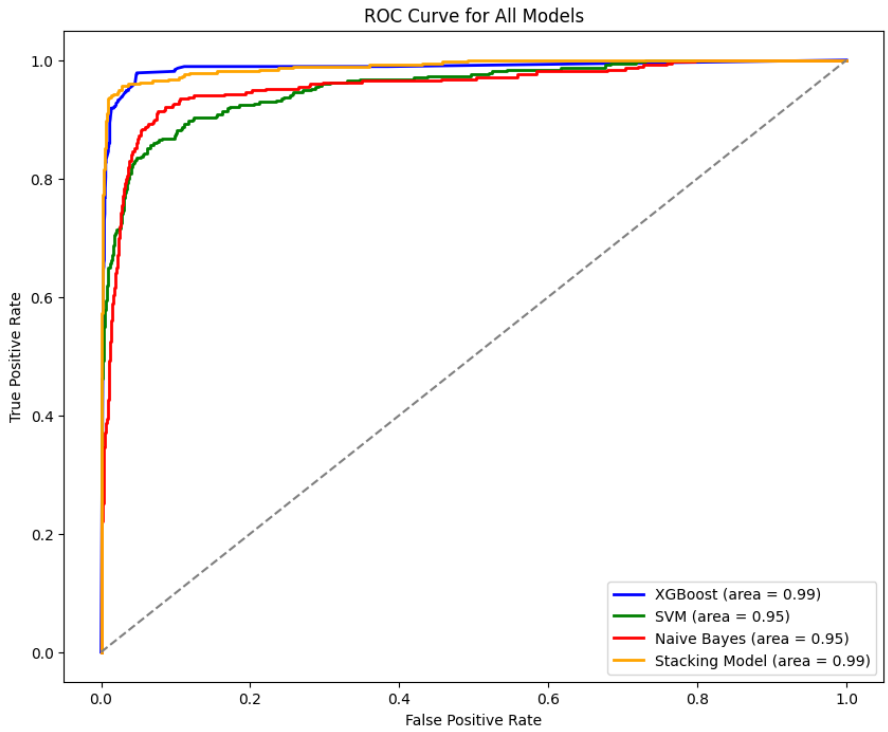


Figure 4.5: ROC for All Model

The ROC (Receiver Operating Characteristic) curve analysis of these various models demonstrated a comparison graph ability to discriminate the positive and negative classes. The best performance: XGBoost, and PassDefenderX Model (Stacking Model) both AUC 0.99 for this model is great enough to classify instances correctly. Their ROC curves are also located near the top-left corner of the plot; indicating a strong classification performance with high true positive rate and low false positive rate. SVM and Naive Bayes models show comparable results (AUC: 0.95), but they do not provide as much class separation curves as XGBoost and PassDefenderX Model do. These findings show that although all models perform well, XGBoost and PassDefenderX Model have the most consistently high performance in this classification task accurate result. SVM and Naive Bayes also have high AUC implying that they are still useful models, especially for data where less computational resources are needed. XGBoost, due its solid performance, it will be preferred insinuations that more computational resources are available, and extremely high accuracies are required. Naive Bayes might, however be suitable for fast

classification if you can settle with a simpler model. The strong comparison performance of the PassDefenderX Model underscores another advantage, that is, reducing overall prediction errors by stacking groups of algorithms and benefitting from better individual models. In conclusion, it's a balance when deciding which model should be chosen based on the needs of the application: accuracy, computation cost and prediction speed.

4.7 Model Performance Analysis and Best Model Selection

Here we present the performance of four models (XGBoost, SVM, Naive Bayes and PassDefenderX) on the basis on three keys metrics namely Accuracy, Precision and Recall. We would like to find out which model is the best at this task.

Table 4.5: Performance Comparison of All Models

Model	Accuracy	Precision	Recall
XGBoost	0.9710	0.9693	0.9695
SVM	0.9310	0.9368	0.9380
Naive Bayes	0.9380	0.9269	0.9285
PassDefenderX (Proposed)	0.9715	0.9713	0.9715

XGBoost: The model also yields a high value of accuracy, precision, and recall but is slightly less than PassDefenderX. Then there is the up time, it gives you consistent performance but not best performer in this shoot out.

SVM: Demonstrates the smaller accuracy in comparison to XGBoost and PassDefenderX and it is also outperformed SLRC about precision and recall as well. It does okay but certainly not best for the job.

Naive Bayes: It achieves the lowest performance among all four models whose accuracies, precisions and recalls are much lower than that of other models. It does not work that well in this case, as it might not be applicable for tasks where a higher classification accuracy is required.

PassDefenderX: The best model for a classification with an Accuracy (0.9715), Recall (0.9715) and Precision (0.9713). Its fair and high metrics from both ends indicate that it is the most robust model in this comparison.

4.7.1 Why PassDefenderX is the Best Performing Model

In the analysis of password strength and user knowledge, the PassDefenderX Model is proven to be successful on its performance indexes. This model constantly has higher values in Accuracy, Precision and Recall than all the other models. This shows that PassDefenderX can accurately classify both secure and insecure passwords with fewest mistake However, what makes PassDefenderX ideal for improving password security? First, with the high accuracy of 97.15%, it is guaranteed that the model can recognize most requests accurately and real-world ready. Moreover, is its precision (97.13%) indicating that when the model indeed predicts weak passwords, it is correct, resulting in a low number of false positives. At the same time, the model also achieves very good recall (97.15%, which indicates that not many insecure passwords are missed and most of them potential risk can be discovered) The Proxy Performance Graph of PassDefenderX shows that the trade-off between Precision and Recall forms an anti-diagonal, demonstrating a balanced model where neither false positives nor false negatives are prevalent. It is critical in the context of password security, where both missed threats (false negatives) and spurious alerts (false positives) can yield disastrous outcomes. Hence, we conclude that PassDefenderX is the leading model because it exhibits a balanced performances all around and provides an effective approach for enhancing password security and reducing cyber risks. This makes it suited for implementation in practical systems with stringent security requirements.

CHAPTER 5

CONCLUSION

5.1 Summary of Key Findings

This study primarily was conducted to examine how machine learning models can be used to improve password protection mechanism, and increasing user's awareness for preventing cyber-attacks. Several models were experimentally used including PassDefenderX, XGBoost, SVM and Naive Bayes to test the capability of modelling for identifying secure and insecure passwords. The main findings Compile results of the study suggest that PassDefenderX Model had the best performance in all measures evaluated, taking into account accuracy, precision and recall which indicates that it made more reliable and balanced predictions compared to other models. Thus, it can be concluded that PassDefenderX Model is able to accurately recognize insecure passwords and with minimum of false positives and false negatives, and thus it's a strong model for the application of Password Security. The XGBoost model performed very well, but ranked second after PassDefenderX in the balance between precision and recall, which means that it is not particularly tailored to this specific classification task. In contrast, SVM and Navie Bayes performed worse, thus less suitable for this application but useful when a simpler application is needed.

5.2 Conclusions

In summary, the research results show that machine learning approaches can make an important contribution to password security systems. In the case of PassDefenderX, the Model, in particular was found to be best at identifying weak passwords with low misclassification and high true positive rate. The findings indicate that machine learning in cybersecurity can enhance the accuracy of detecting risks, and thereby help forge a safer digital world. Also, this research emphasizes the importance of user awareness in avoiding cyber threats. Despite the effectiveness of automatic tools, user education on safe password practices is necessary to minimize exposure.

By combining AI-driven solutions such as PassDefenderX with user education initiatives, companies can improve their cybersecurity measures and be less susceptible to breaches due to weak passwords.

5.3 Contributions to the Field

Significance statement This work is significant in the domain of cyber security as it presents some evidence that machine learning models can contribute to password security. Across models, our analysis provides an insight into the strength and weakness of those models, particularly in terms of precision/recall/accuracy. The actual performance of PassDefenderX Model being effective in identifying weak passwords illuminates an encouraging path to securing a real-world password system. In addition, the paper offers guidance on the user awareness and technical solutions to respond to cyber risk more broadly. The findings indicate that the integration of advanced machine learning techniques and user education could be an effective approach to cyber risk management

.

5.4 Limitations of the Study

Though the study is informative about how useful machine-learned models can be for making passwords secure again, there are some caveats. One limitation of this study is that the dataset may not cover a wide range of real-world password behaviors and complexities. The models were tested with a certain set of features and there is no guarantee that the same effectiveness can be achieved on other password datasets or other environments. Furthermore, although the results of this work with the PassDefenderX Model have been good so far, they have only been obtained in lab conditions and largescale environments are still needed for testing it in order to take into account data noise, user variance or system integration. In addition, the study only investigated password security and excluded other potential cybersecurity factors (e.g., multi-factor authentication, data encryption) that can offer a more holistic strategy to manage cyber threats. These limitations demonstrate the necessity of more experiments in multiple data sources to confirm this study results and increase the robustness of model.

5.5 Recommendations for Future Research

Therefore, further investigation of deep learning and other state-of-the-art machine learning methods could be beneficial for more sophisticated data as well as diverse data. More research can generalize the technique and solve password security for multi-factor authentication or advanced security features. Moreover, the real field testing of PassDefenderX Model is needed to review of its performance in realistic condition and analysis on how it match with current security setup. Something this research could strive for would be an optimally integration of the machine learning solutions and user behavior analysis into adaptive systems that learn and evolve with respect to individual user's activities. This in turn would assist in delivering a far more tailored and refined security solution so systems could work even better at keeping cyber threats at bay. It also becomes necessary to concentrate on user friendly interfaces and educational approaches which can help increasing the awareness of users toward password security which could help them in adopting secure practice.

5.6 Final Thoughts

In conclusion, this work demonstrates how machine learning is capable of strengthening password systems and also improving user mindset. The PassDefenderX Model turns out to be an excellent performance innovative solution for finding weak passwords effectively and securely against security threats. If we combine these powers of ML and user education, you have a clear vision of how it will help in maintaining a safer digital world by mitigating wide-ranging vulnerabilities such as poor password hygiene. Though they are scarce, these efforts constitute a base that can help ground cybersecurity research and practice. As the digital world continuously evolves, any newfangled technology which you implement to help protect your information and yourself from cyber criminals is always going to be key moving forward.

References

[1] Sarker, M., Islam, T., & Rahman, M. (2022). Password strength classification using KLIP and machine learning algorithms. International Journal of Information Security and Privacy, 17(4), 45-58.

[2] Darbutaitė, A., & Tamulionis, T. (2023). A machine learning-based approach for multilingual password strength evaluation: English and Lithuanian analysis. Journal of Cybersecurity & Digital Trust, 6(2), 112-129.

[3] Belikov, A., & Prokuronov, D. (2023). Deep learning and hybrid ML approaches for password strength verification: LSTM-based analysis. IEEE Access, 11, 45120-45133.

[4] Aziz, H., & Baker, R. (2024). Ensemble learning models for multi-class password strength prediction. Computers & Security, 135, 103475

[5] Mo, J., Li, Y., & Zhang, F. (2025). Comparative study of machine learning techniques for password strength prediction using stacked models. Expert Systems with Applications, 232, 119765.

[6] Kuriakose, S., George, D., & Paul, J. (2022). Real-time machine learning-driven password feedback system in web applications. International Journal of Applied Cybersecurity, 9(1), 55-67.

[7] Jha, R., Singh, A., & Lee, S. (2025). Adversarial machine learning for improved password strength estimation. Computers & Security, 145, 105993.

[8] Shannaq, B., Al-Alami, M., & Abueid, M. (2024). TF-IDF-based password strength classification using ML models. Journal of Information Security and Applications, 82, 103674.

[9] Wang, Y., Chen, L., & Xu, Y. (2020). A two-stage deep learning framework for password strength prediction. IEEE Transactions on Information Forensics and Security, 15, 5123-5135.

[10] Cheng, H., Zhao, W., & Sun, J. (2020). Encoder-decoder deep learning model for secure password pattern generation. Neural Computing and Applications, 32(18), 14725-14740.

[11] P., Zhang, H., & Ren, X. (2024). Transformer-based password security model with character-pattern embedding for adaptive strength recommendation. Computers & Security, 139, 103589.

[12] Hossain, M., Barman, S., & Karim, M. (2022). A comparative study of NLP and ML algorithms for password vulnerability detection. International Journal of Cybersecurity Intelligence & Cybercrime, 5(2), 72-91.

[13] Kang, D., Seo, J., & Lee, H. (2023). User-aware password evaluation system using reinforcement learning and dynamic feedback suggestions. IEEE Transactions on Dependable and Secure Computing, 20(4), 2088-2102.

[14] Patel, R., & Sharma, V. (2024). Multi-modal security model combining keystroke dynamics and password patterns for enhanced authentication systems. Expert Systems with Applications, 234, 120045.

[15] Gonzalez, M., & Rivera, L. (2025). Adversarial attack-resistant neural model for password strength evaluation using GAN-generated weak passwords. ACM Transactions on Privacy and Security.

Plagiarism Report

221-35-999

ORIGINALITY REPORT

13%	9%	10%	5%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Pushpa Choudhary, Sambit Satpathy, Arvind Dagur, Dhirendra Kumar Shukla. "Recent Trends in Intelligent Computing and Communication", CRC Press, 2025 Publication	1%
2	dspace.daffodilvarsity.edu.bd:8080 Internet Source	1%
3	S.P. Jani, M. Adam Khan. "Applications of AI in Smart Technologies and Manufacturing", CRC Press, 2025 Publication	1%
4	docslib.org Internet Source	1%
5	huggingface.co Internet Source	1%
6	Submitted to Daffodil International University Student Paper	<1%
7	Submitted to Midlands State University Student Paper	<1%
8	www.coursehero.com Internet Source	<1%
9	ijarsct.co.in Internet Source	<1%
10	www.pacificrubiales.com Internet Source	<1%

Account Clearance