B.TECH. (IT) MAJOR PROJECT PRESENTATION

Detection of Spam Email using Machine Learning Techniques

Presented by

Sagarjyoti Das - 20BTechIT14
Dimpal Das - 20BTechIT16
Kimkimbai K Marak - 21BTechLIT15
Priti Halam - 21BTechLIT16

Under the Supervision of

Dr. Bubu Bhuyan

Department of Information Technology
North-Eastern Hill University

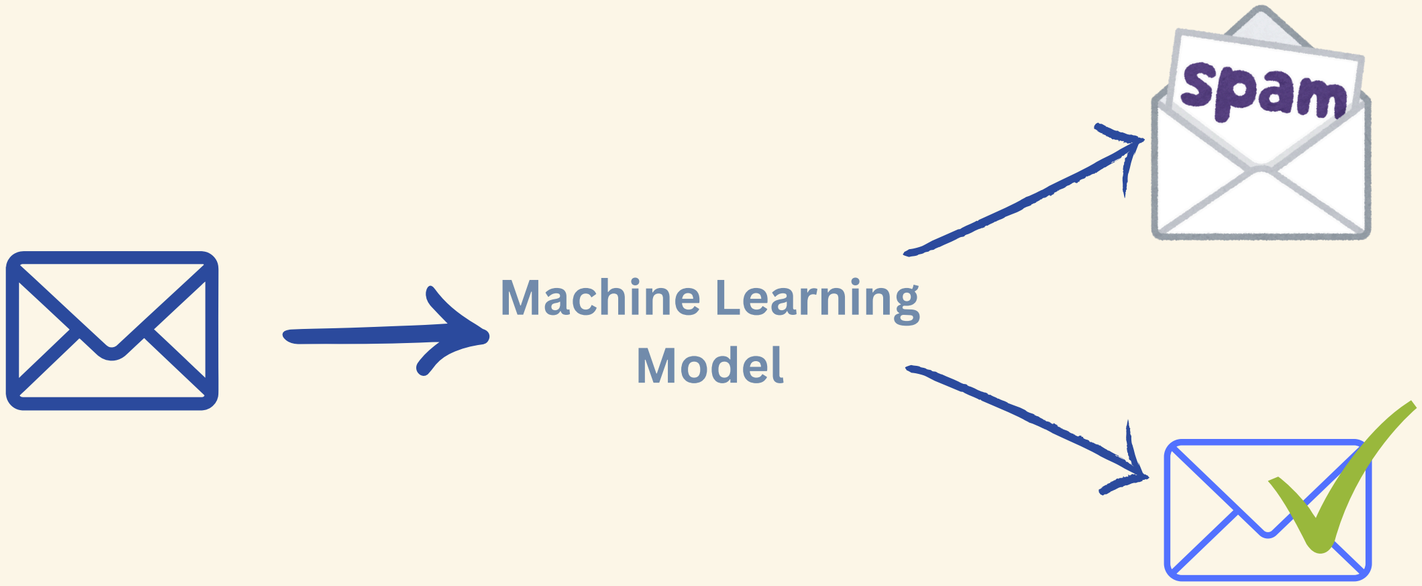
Contents

Objective

To develop an effective machine learning - based solution for detecting spam emails.

Introduction

Using machine learning algorithm particularly ***Logistic regression****,* ***Multi-Layer Perceptron*** *and* ***Naive bayes*** *can help us to accurately decide if emails are spam or real based on various features about them.*



Machine Learning Techniques Used

1

Logistic Regression

Probability-based classifier for binary outcomes.

2

Multi-Layer Perceptron

Neural network for learning complex patterns in email data.

3

Naive Bayes

Utilizes Bayes' theorem, assuming feature independence, effective for text classification.

Dataset Collection

Total emails : 5172

Ham emails : 3672

Spam emails : 1500

```
Summary of Spam Email Dataset:
Number of emails: 5172
Number of features: 3002
Number of spam emails: 1500
Number of legitimate emails: 3672

Samples of the Dataset:
  Email No.  the  to  ect  and  for  of    a  you  hou  ...  connevey  jay  \
0   Email 1    0   0    1    0    0   0    2    0    0  ...         0    0
1   Email 2    8  13   24    6    6   2  102    1   27  ...         0    0
2   Email 3    0   0    1    0    0   0    8    0    0  ...         0    0
3   Email 4    0   5   22    0    5   1   51    2   10  ...         0    0
4   Email 5    7   6   17    1    5   2   57    0    9  ...         0    0
5   Email 6    4   5    1    4    2   3   45    1    0  ...         0    0

   valued  lay  infrastructure  military  allowing  ff  dry  Prediction
0       0    0               0         0         0   0    0           0
1       0    0               0         0         0   1    0           0
2       0    0               0         0         0   0    0           0
3       0    0               0         0         0   0    0           0
4       0    0               0         0         0   1    0           0
5       0    0               0         0         0   0    0           1

[6 rows x 3002 columns]
```

Data Preprocessing

1

Data Cleaning

Removed unnecessary information and handled missing values.

2

Feature Extraction

Used TF-IDF (Term Frequency-Inverse Document Frequency) to represent words and their importance.

3

Label Encoding

Converted labels (spam/ham) into numerical format for machine learning algorithms.

Model Training

We trained our machine learning models to recognize spam emails using the prepared data

Data Split

Divided the dataset into training and testing sets.

Algorithm Selection

Chose Logistic Regression, Naive Bayes, and MLP for their suitability.

Training Process

Fed the training data into each algorithm to learn patterns and characteristics.

Results and Analysis

After training our models, we evaluated their performance to see how well they could detect spam emails:

Logistic Regression

Accuracy : 98.2%
Precision : 99.3%
Recall : 89.4%
F1 Score : 94.1%

Multi-Layer Perceptron

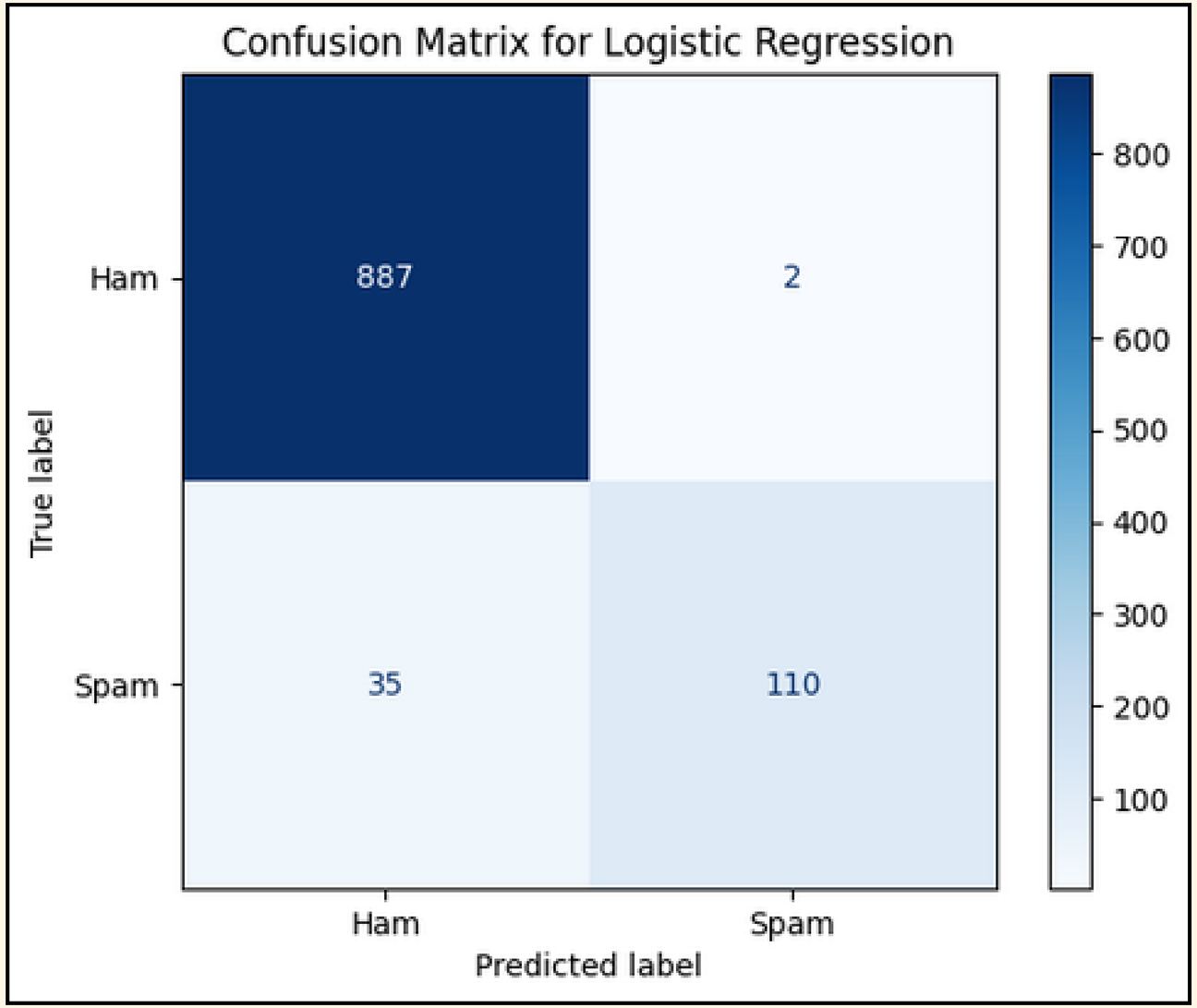
Accuracy : 99.1%
Precision : 98.7%
Recall : 96.3%
F1 Score : 97.5%

Naive Bayes

Accuracy : 97.3%
Precision : 99%
Recall : 86.7%
F1 Score : 92.8%

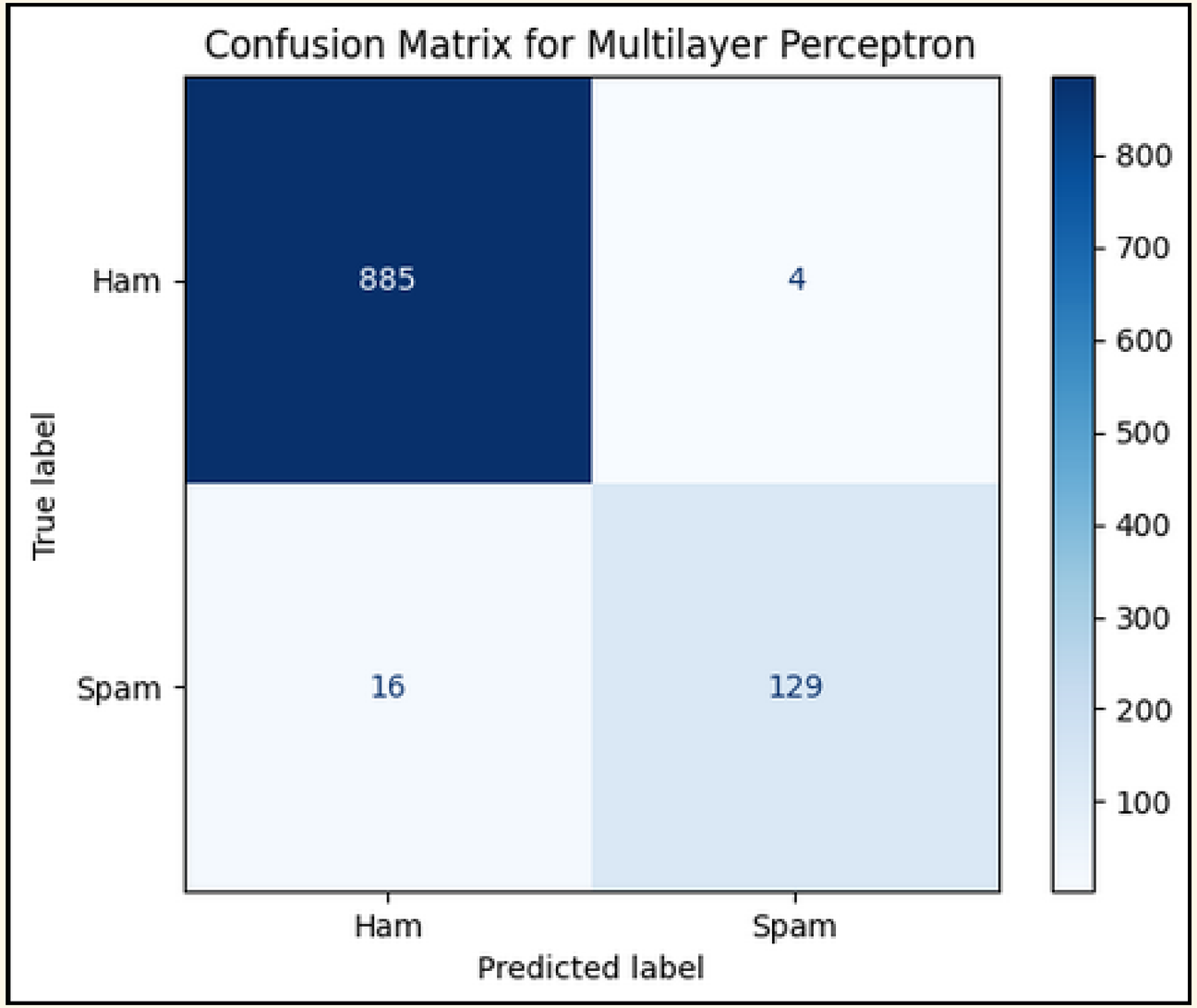
Logistic Regression

Testing Phase Result



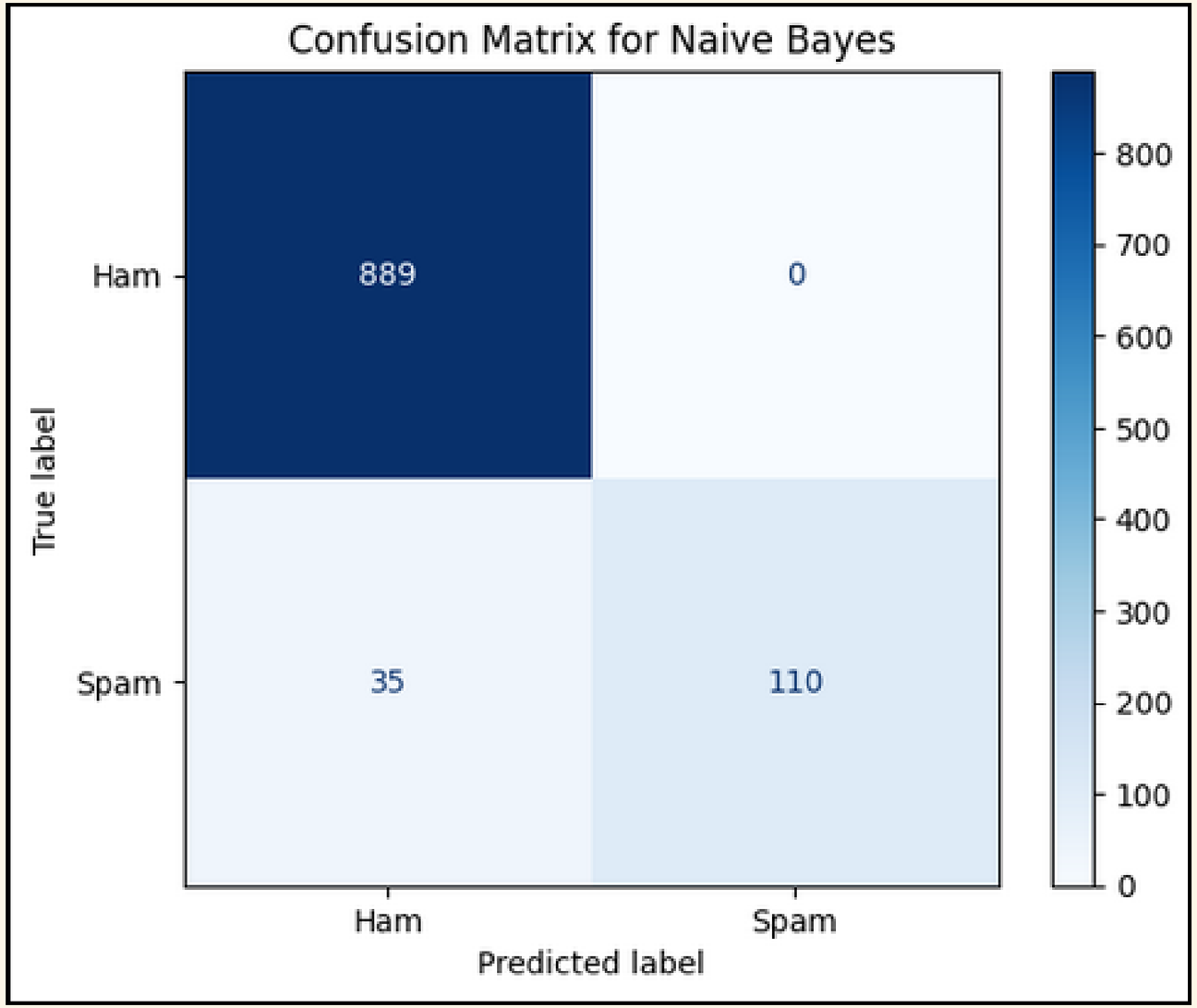
Multi-Layer Perceptron

Testing Phase Result



Naive Bayes

Testing Phase Result



Comparison with Existing Model

Model	Accuracy	Precision	Recall	F1 Score
Support Vector Machine	0.95	0.96	0.94	0.94
Decision Tree	0.90	0.91	0.89	0.90
Random Forest	0.92	0.93	0.91	0.92

Model	Accuracy	Precision	Recall	F1 Score
Logistic Regression	0.96	0.98	0.75	0.85
Multi-Layer Perceptron	0.98	0.96	0.88	0.92
Naive Bayes	0.96	1.0	0.75	0.86

Best Performance Model

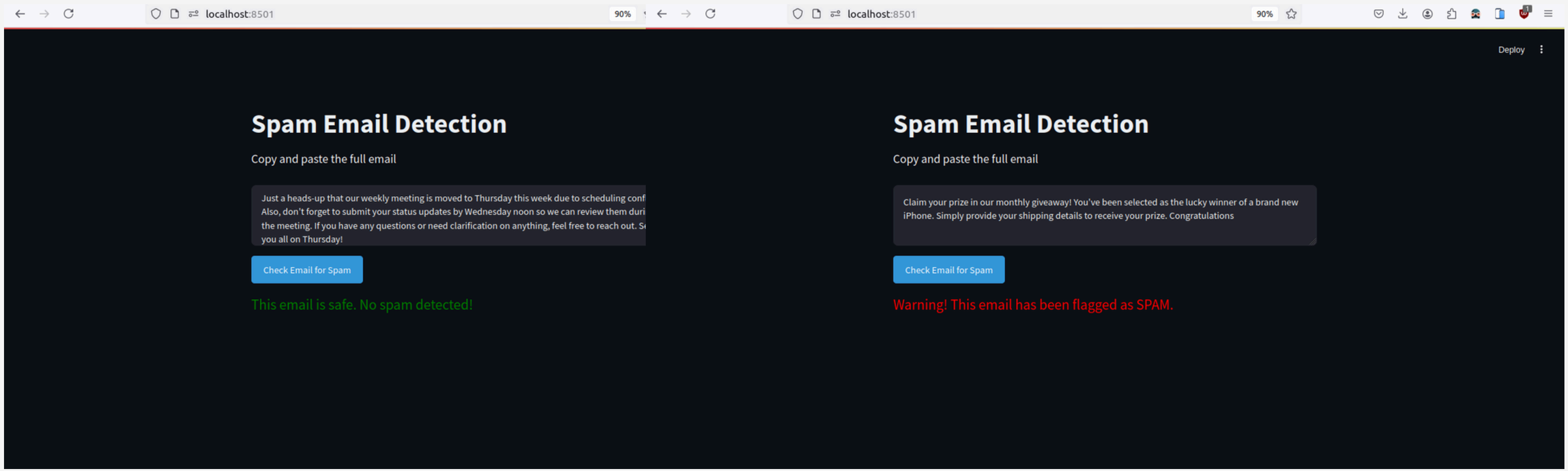
After evaluating all models, the Multi-Layer Perceptron (MLP) showed the highest accuracy and effectiveness in detecting spam emails

Multi - Layer Perceptron

Accuracy : 98%
Precision : 96%
Recall : 88%
F1 Score : 92%

Spam Detection Web Application

Demonstration of a web application designed to classify email messages as either spam or ham based on machine learning models.



Future Work

Advanced Machine Learning Models

Explore CNNs, RNNs and transformers. Use ensemble methods (stacking, boosting) for improved accuracy in spam detection.

Feature Engineering and Extraction

Use embeddings (Word2Vec, BERT) for better features. Include metadata and semantic analysis for richer classification context.

Real-time Spam Detection

Develop real-time systems for streaming data. Optimize models for fast, efficient deployment in real-time environments.

References

- *Logistic Regression : https://cse.iitkgp.ac.in/~adas/courses/dl_spr2020-slides/04_Logistic_Regression*
- *Spam Email Classification : R. Karthika, P. Visalakshi, A hybrid ACO based feature selection method for email spam classification, WSEAS Trans. Comput. 14 (2015) 171–177.*
- *Sigmoid Function : https://deepai.org/machine-learning-glossary-and-terms/sigmoid-function*
- *Loss function : https://medium.com/@deeksha.goplani/activation-functions-loss-functions-optimizers*
- *Spam Email Dataset : https://www.kaggle.com/datasets/uciml/sms-spam-collection-dataset*

Thank You