

# SPAM SMS DETECTION USING MACHINE LEARNING

## 1. Introduction

Spam SMS messages are unsolicited messages sent in bulk, often for advertising or fraudulent purposes. With the increasing use of mobile communication, detecting spam messages has become essential to protect users from scams and unwanted content. Machine learning provides an efficient way to automatically classify SMS messages as spam or legitimate (ham).

## 2. Objective

The objective of this project is to build a machine learning model that can accurately classify SMS messages as spam or ham using natural language processing techniques.

## 3. Dataset Description

The project uses the SMS Spam Collection dataset. The dataset contains two main columns: **label**: Indicates whether the message is spam or ham **message**: The actual SMS text The dataset includes a balanced mix of spam and non-spam messages suitable for text classification.

## 4. Data Preprocessing

The following preprocessing steps were applied: Removal of unnecessary columns Label encoding (ham → 0, spam → 1) Text vectorization using TF-IDF These steps converted raw text data into numerical features suitable for machine learning models.

## 5. Feature Extraction

TF-IDF (Term Frequency–Inverse Document Frequency) was used to transform SMS text into numerical feature vectors. This technique highlights important words while reducing the impact of common terms.

## 6. Model Selection

The Multinomial Naive Bayes classifier was selected due to its effectiveness in text classification problems and its computational efficiency.

## 7. Model Training

The model was trained on the processed dataset and learned patterns that differentiate spam messages from legitimate messages.

## 8. Model Evaluation

The model was evaluated using accuracy and classification metrics. It achieved high accuracy in distinguishing spam messages from ham messages, demonstrating strong performance.

## 9. Results

The trained model successfully classified SMS messages with high accuracy and minimal misclassification. Custom message testing further confirmed the model's reliability.

## 10. Conclusion

This project demonstrates that machine learning combined with natural language processing techniques can effectively detect spam SMS messages. The Naive Bayes model provides a simple yet powerful solution for spam detection tasks.

## 11. Future Improvements

Use advanced NLP models such as word embeddings or deep learning Improve text preprocessing techniques Deploy the model as a real-time spam detection system

## 12. Tools & Technologies Used

Python, Jupyter Notebook, Pandas, Scikit-learn, TF-IDF, Matplotlib, Seaborn.

## 13. Final Outcome

The project successfully fulfills the requirements of Task 4 of the CODSOFT Machine Learning Internship.