## Artificial Intelligence and Machine Learning

Project Report

Semester-IV (Batch-2022)

**SMS SPAM CLASSIFIER**

A red and white sign

Description automatically generated with low confidence

**Supervised By: Submitted By:**

Dr.Monica Dutta Monalika,2210990582(G11)

Navpreet,2210990601(G11)

Navya,2210990602(G11)

Neharika,2210990605(G11)

**Department of Computer Science and Engineering**

**Chitkara University Institute of Engineering & Technology,**

**Chitkara University, Punjab**

## ****ABSTRACT****

Our project has an approach for classifying Short Message Service (SMS) messages using machine learning techniques. With the exponential growth of SMS communication, the need for efficient message categorization has become paramount.

Our system aims to automatically categorize incoming SMS messages into predefined classes such as spam or not spam,facilitating better management and prioritization of messages by users.

The proposed system utilizes a supervised learning framework, where a diverse set of features extracted from the textual content of SMS messages are used to train a classifier. We experiment with various machine learning algorithms such as Support Vector Machines (SVM), Naive Bayes, Decision Trees, and Random Forests to determine the most suitable classifier for the task.

To evaluate the performance of the SMS classifier, we employ standard metrics such as accuracy, precision, recall, and F1-score. Additionally, we conduct cross-validation and use techniques like grid search for hyperparameter tuning to enhance the classifier's robustness and generalization ability.

Overall, our SMS classifier serves as a valuable tool for automating SMS message classification tasks, offering benefits such as time-savingimproved organization, and enhanced user privacy by filtering out unwanted messages effectively.

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| S.NO | Topic | Page-no. |
| 1. | Introduction  1.1 Background  1.2 Objectives  1.3 Significance | 1-5 |
| 2. | Problem Definition and Requirements  2.1 Problem Statement  2.2 Hardware Requirements  2.3 Dataset | 6-7 |
| 3. | Methodology  3.1 Problems Proposed  3.2 Algorithms Used | 8-9 |
| 4. | Results  4.1 Data cleaning  4.2 EDA  4.3 Data preprocessing | 10-25 |
| 5. | References | 26 |

**1.INTRODUCTION**

1. 1 Background

Short Message Service (SMS) has emerged as one of the most ubiquitous forms of communication in today's digital era. With the widespread adoption of mobile phones and the convenience of text-based communication, SMS has become integral to personal and business interactions alike. However, alongside its convenience, SMS also presents challenges related to managing the influx of messages, especially with the rise of spam and promotional content.

Machine learning (ML) techniques offer a promising avenue for addressing the complexities of SMS classification. By leveraging the power of ML algorithms, it becomes possible to automatically categorize incoming messages into different classes based on their content, thereby streamlining the process of message management for users.

The fundamental idea behind an SMS classifier is to train a model using labeled SMS data, where each message is associated with a predefined class (e.g., spam or not spam). The model learns to recognize patterns and features in the text that are indicative of each class, enabling it to make predictions on unseen messages.

1

* 1. Objectives

Objectives of SMS Spam Classifier in Machine Learning Project:

1. **Spam Detection**: The primary objective of the SMS spam classifier is to accurately identify and differentiate spam messages from legitimate ones. By effectively detecting spam, the classifier helps users avoid potential scams, phishing attempts, and unwanted promotional messages, thereby enhancing their overall messaging experience.
2. **Precision and Recall**: A key objective is to achieve high precision and recall rates in spam detection. High precision ensures that legitimate messages are not incorrectly classified as spam, minimizing false positives. Meanwhile, high recall ensures that the classifier correctly identifies a significant portion of actual spam messages, reducing false negatives.
3. **User Privacy and Security**: Another objective is to protect user privacy and security by filtering out malicious or unsolicited messages. By automatically detecting and segregating spam messages, the classifier helps users avoid potential threats such as malware, phishing links, or fraudulent schemes hidden within spam content.
4. **Efficiency and Scalability**: The classifier should be efficient and scalable, capable of handling large volumes of incoming messages in real-time. Efficient algorithms and optimized feature extraction techniques ensure that the classification process is fast and resource-efficient, enabling seamless integration into messaging applications and platforms.

2

1. **Adaptability and Robustness**: An important objective is to develop a classifier that is adaptable to evolving spamming techniques and robust against adversarial attacks. By continuously updating the classifier with new data and employing techniques such as retraining and model updating, it can adapt to changes in spam patterns and maintain its effectiveness over time.
2. **User Experience Improvement**: The classifier aims to improve the overall user experience by reducing clutter and noise in the messaging inbox. By automatically filtering out spam messages, the classifier enables users to focus on relevant and meaningful conversations, thereby enhancing productivity and satisfaction.

By addressing these objectives, the SMS spam classifier in the machine learning project aims to deliver a reliable, efficient, and user-friendly solution for effectively managing SMS communication and safeguarding users against spam and unwanted messages.

1.3 Significance

The significance of an SMS spam classifier in a machine learning project lies in its potential to address critical challenges and enhance various aspects of SMS communication:

1. **User Experience Improvement**: Spam messages inundate users' inboxes, causing annoyance and clutter. By accurately identifying and filtering out spam messages, the classifier significantly improves the user experience by ensuring that users only see relevant and legitimate messages.

3

2.**Protection Against Threats**: Spam messages often contain malicious links, phishing attempts, or fraudulent schemes, posing

security risks to users. The classifier helps protect users from these threats by automatically detecting and flagging suspicious messages, thereby safeguarding user privacy and security.

1. **Time and Resource Savings**: Manual sorting through spam messages consumes valuable time and resources for users. By automating the spam detection process, the classifier saves users time and effort, allowing them to focus on important conversations and tasks.
2. **Enhanced Productivity**: Filtering out spam messages enhances user productivity by reducing distractions and interruptions caused by irrelevant messages. Users can allocate their attention more efficiently to meaningful conversations and tasks, thereby improving overall productivity.
3. **Trust and Confidence**: Providing users with an effective spam filtering mechanism instills trust and confidence in the messaging platform or application. Users are more likely to rely on and engage with platforms that offer reliable protection against spam, leading to increased user retention and satisfaction.
4. **Regulatory Compliance**: In many jurisdictions, there are regulations governing the transmission of unsolicited messages, including SMS spam. Implementing an SMS spam classifier helps organizations comply with these regulations by ensuring that only solicited messages are delivered to users.

4

1. **Business Reputation**: For businesses that use SMS for communication and marketing purposes, the presence of spam
2. messages can tarnish their reputation and brand image. By using an SMS spam classifier to deliver only relevant and requested messages to users, businesses can maintain a positive reputation and improve customer satisfaction.
3. **Adaptability to Evolving Threats**: Spamming techniques are constantly evolving, requiring adaptive solutions to combat new and emerging threats. A machine learning-based classifier can continuously learn from new data and adapt to changing spam patterns, ensuring ongoing effectiveness against evolving spamming tactics.

Overall, the significance of an SMS spam classifier in a machine learning project lies in its ability to enhance user experience, protect against threats, save time and resources, improve productivity, comply with regulations, maintain business reputation, and adapt to evolving threats, ultimately contributing to a safer, more efficient, and more enjoyable SMS communication experience.

Top of Form

5

**2.Problem Statement and Requirements**

2.1Problem Statement:

The problem statement for the SMS classifier in a machine learning project revolves around the need to effectively categorize incoming SMS messages into relevant classes such as spam, promotional, or personal.

Software Requirements:

1. **Python** : The primary programming language for implementing the object detection system and integrating necessary libraries and frameworks.
2. **Machine Learning Libraries**: Utilize machine learning libraries and frameworks such as Scikit-learn for developing and training the classifier. These libraries offer a wide range of algorithms and tools for building and evaluating machine learning models.
3. **Development Environment**: Set up a development environment with integrated development environment (IDE) such as Jupyter Notebook, PyCharm, or Visual Studio Code, along with necessary dependencies and packages installed.

6

2.2 Hardware Requirements

In terms of hardware, we require a computer with sufficient processing power and memory to support the computational demands of our algorithms. While the specific hardware specifications may vary depending on the scale of the project and the size of the dataset, a standard computer with a multi-core processor and ample RAM should suffice for development and testing purposes.

2.3 Dataset

Building an SMS classifier for machine learning typically requires labeled datasets containing examples of SMS messages categorized into different classes, such as spam and non-spam (ham). Here are some common datasets used for SMS classification projects:

1. **SMS Spam Collection Dataset**:
   * This dataset is one of the most widely used for SMS spam classification. It contains a collection of SMS messages labeled as spam or ham.
   * The dataset is available from various sources, including the UCI Machine Learning Repository and Kaggle.
   * It typically consists of thousands of SMS messages, with labels indicating whether each message is spam or ham.

Additionally, preprocessing steps such as text normalization, tokenization, and feature extraction may be necessary to prepare the data for training and evaluation.

7

**3.Proposed Design/Methodology**

3.1 Problems proposed

The objective of this project is to design and implement a machine learning-based classifier capable of accurately identifying and filtering out spam messages from legitimate ones in SMS communication. The classifier will be trained on a labeled dataset containing examples of SMS messages categorized as either spam or non-spam (ham).The goal is to develop a classifier that can automatically classify incoming SMS messages in real-time, thereby

enhancing users' messaging experience and reducing spam.

3.2 Algorithms used

1. Support Vector Machines (SVM):
   * SVM is a powerful supervised learning algorithm used for classification and regression tasks.
   * SVM constructs hyperplanes in a high-dimensional space to
   * It works well for binary classification tasks like spam vs. ham SMS classification and can handle high-dimensional feature spaces efficiently

8

2.Decision Trees:

* + Decision trees recursively partition the feature space into subsets based on the value of feature attributes, aiming to minimize impurity.
  + They are interpretable and can handle both numerical and categorical data.

3.Logistic Regression:

* + Logistic Regression is a linear classification algorithm used for binary classification tasks.
  + It models the probability of a sample belonging to a particular class using the logistic function.
  + Logistic Regression is simple, interpretable, and efficient for text classification tasks like SMS spam filtering.

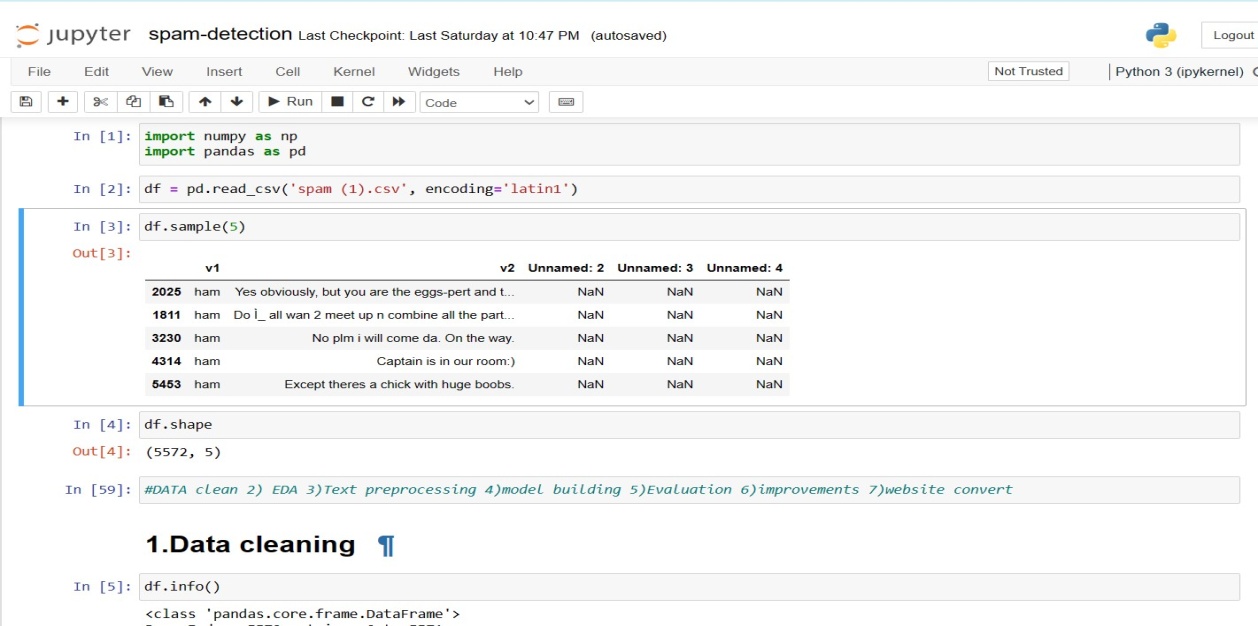
9

**4. Results**

4.1 Data cleaning

Data cleaning is a crucial step in building any machine learning model, including a spam classifier for SMS messages. Here's a general outline of how you might approach data cleaning for an SMS spam classifier:

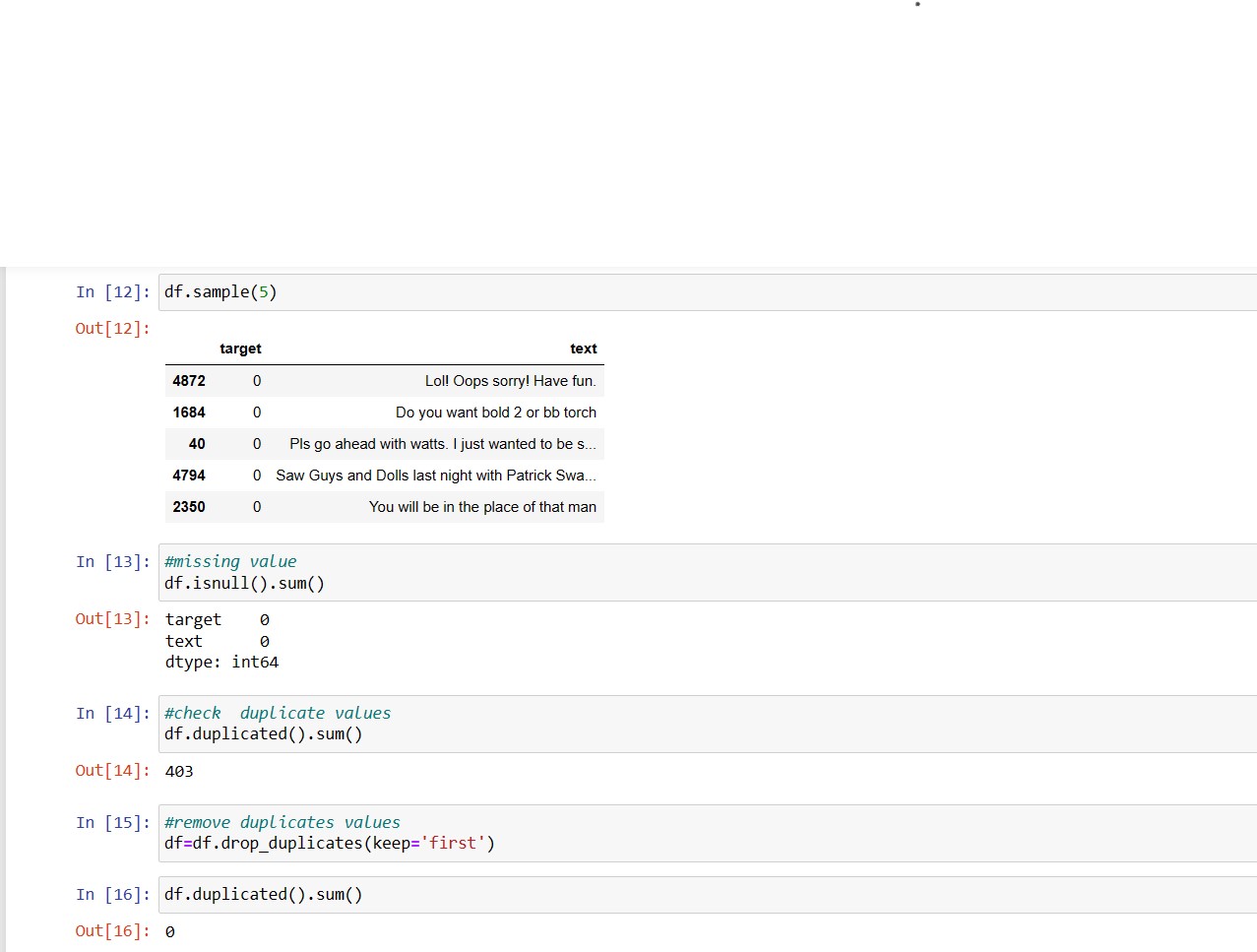
1.Remove duplicates:



Figure

Sometimes, you might have duplicate SMS messages in your dataset. Removing duplicates ensures that each message is unique and prevents bias in your model.

2.Handle missing values:



Figure

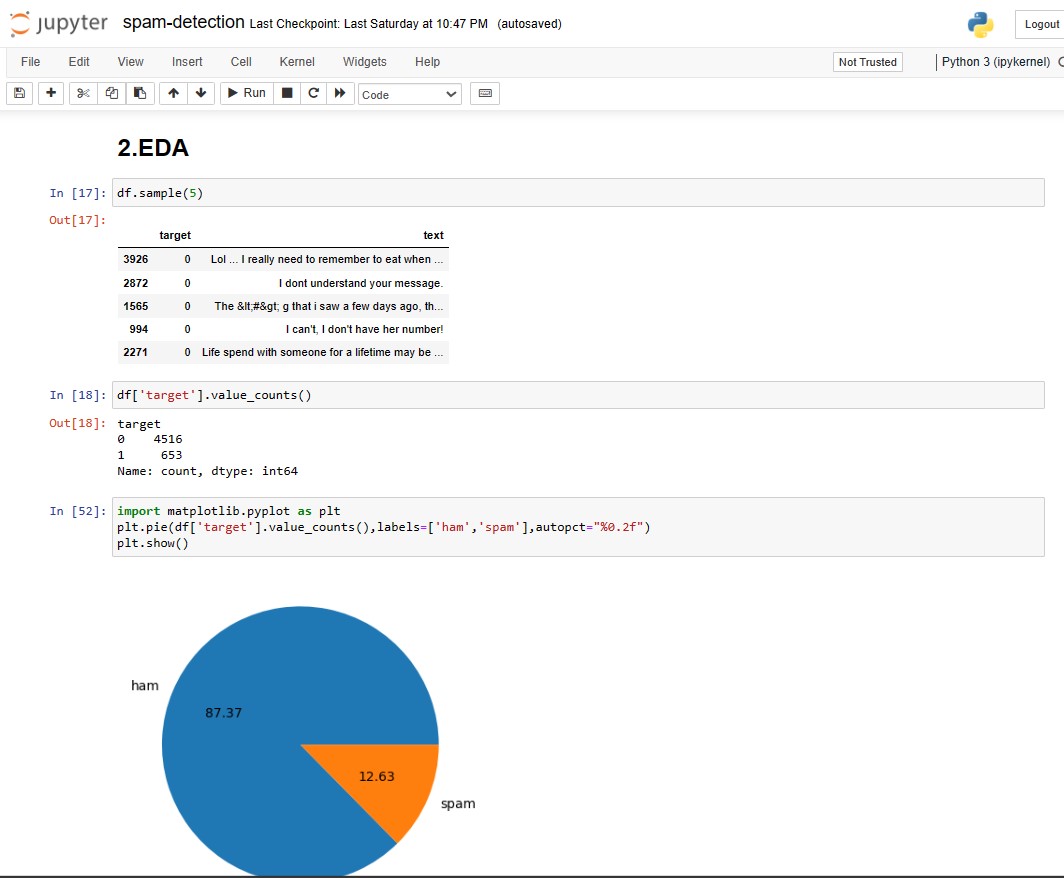
Check if there are any missing values in your dataset and decide how to handle them. You might choose to drop rows with missing values or impute them using methods like mean imputation or using more advanced techniques like predictive imputation.

11

4.2 EDA

Exploratory Data Analysis (EDA) is a crucial step in understanding your dataset before building a machine learning model. Here's how you can perform EDA for an SMS spam classifier:

**4.2.1.Basic statistics:**

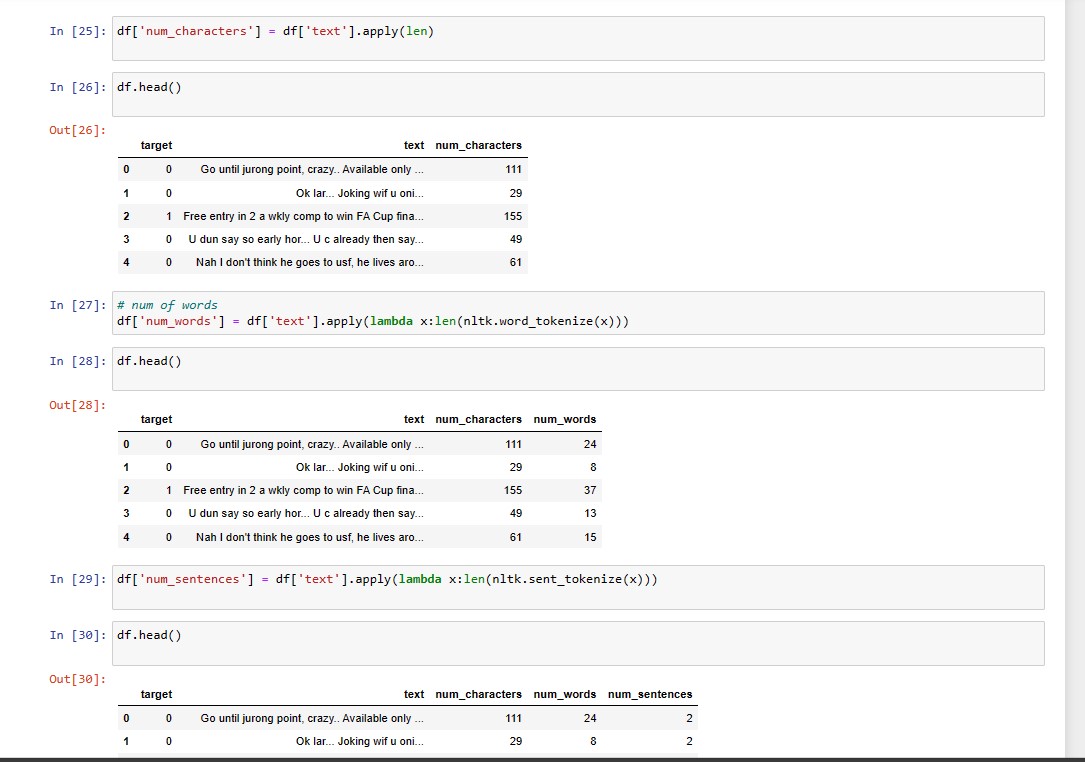


Figure

Calculate basic statistics such as the number of messages, the distribution of spam vs. non-spam messages, average message length, etc.

Visualize these statistics using histograms, bar plots or pie-chart to get a quick overview of the dataset.

**4.2.2 Word frequency analysis:**



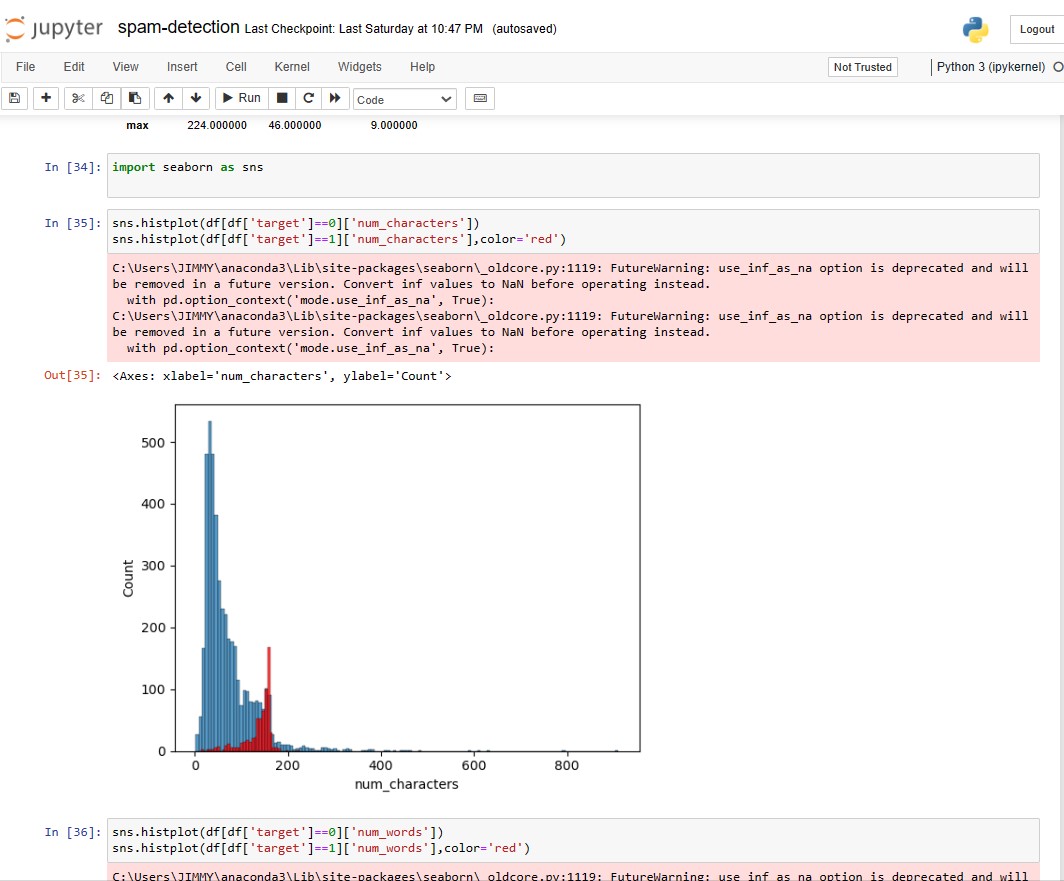
Figure

Analyze the frequency of words in both spam and non-spam messages separately.

Create word clouds or bar plots to visualize the most common words in each category.

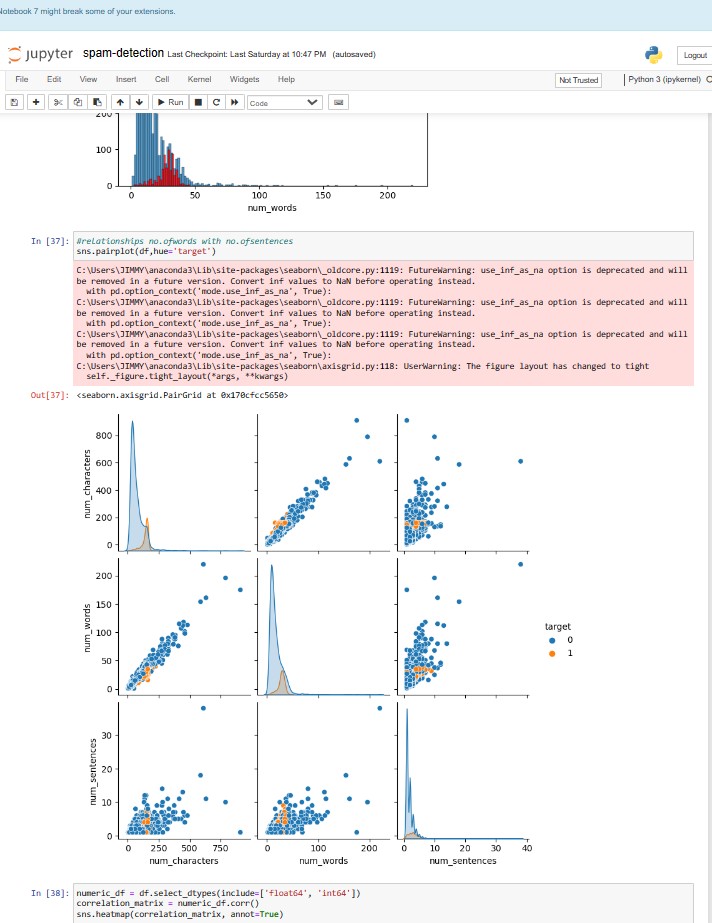
Identify stopwords (common words like "and", "the", "is") and consider removing them from further analysis.

**4.2.3. Message length distribution:**



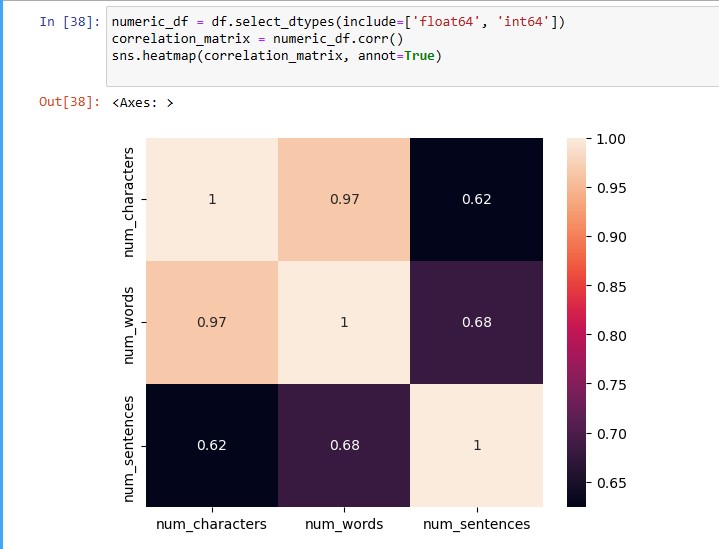
Figure

Explore the distribution of message lengths for both spam and non-spam messages.



Figure

17



Figure

18

4.3 Data Preprocessing

1.Lowercasing: Convert all text to lowercase to ensure consistency (e.g., "Hello" and "hello" are treated the same).

2.Tokenization: Split each SMS message into individual words or tokens. This step is essential for further text processing.

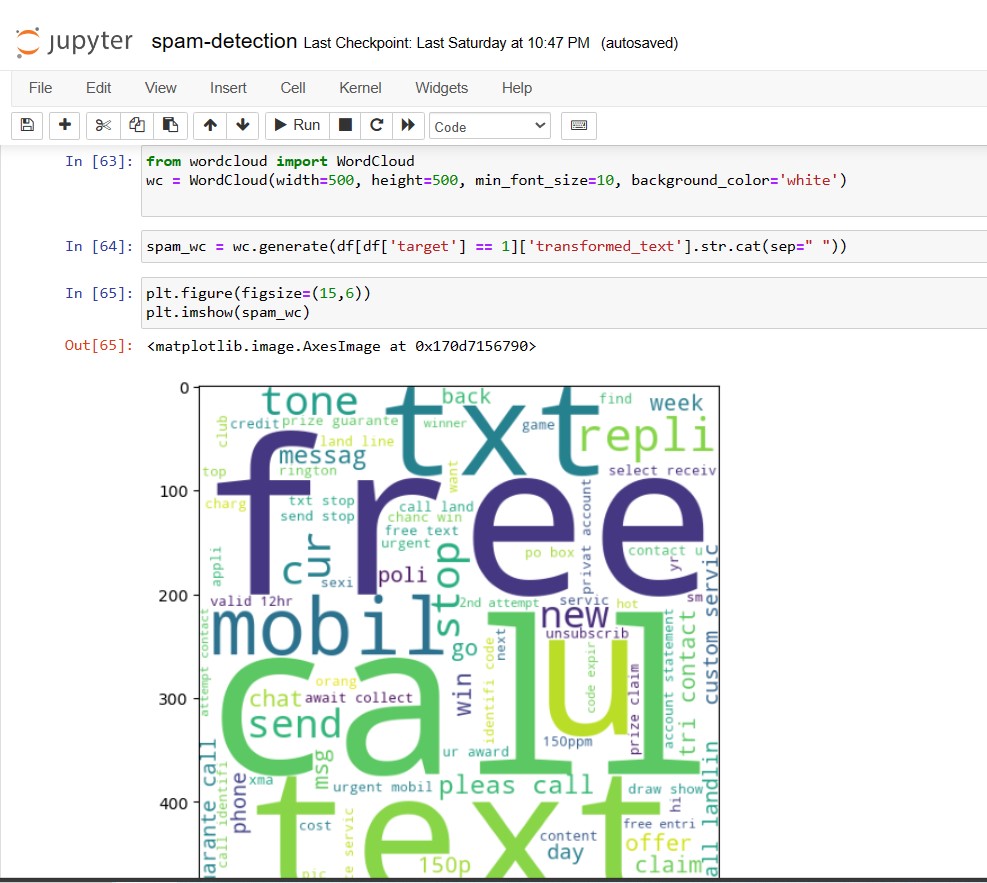
3.Removing punctuation: Remove any punctuation marks from the text as they usually don't carry much meaning for spam classification.

4.Removing stop words: Stop words like "and", "the", "is", etc., are common words that often don't carry much information for spam classification. Removing them can help reduce the dimensionality of the data and improve model performance.

5.Stemming : Reduce words to their base or root form (e.g., "running" becomes "run") to consolidate similar words and reduce the feature space.

6.Handling special characters and numbers: Depending on your specific task, you might want to handle special characters and numbers differently. For example, you might choose to remove them entirely, replace them with a special token, or keep them if they convey important information..

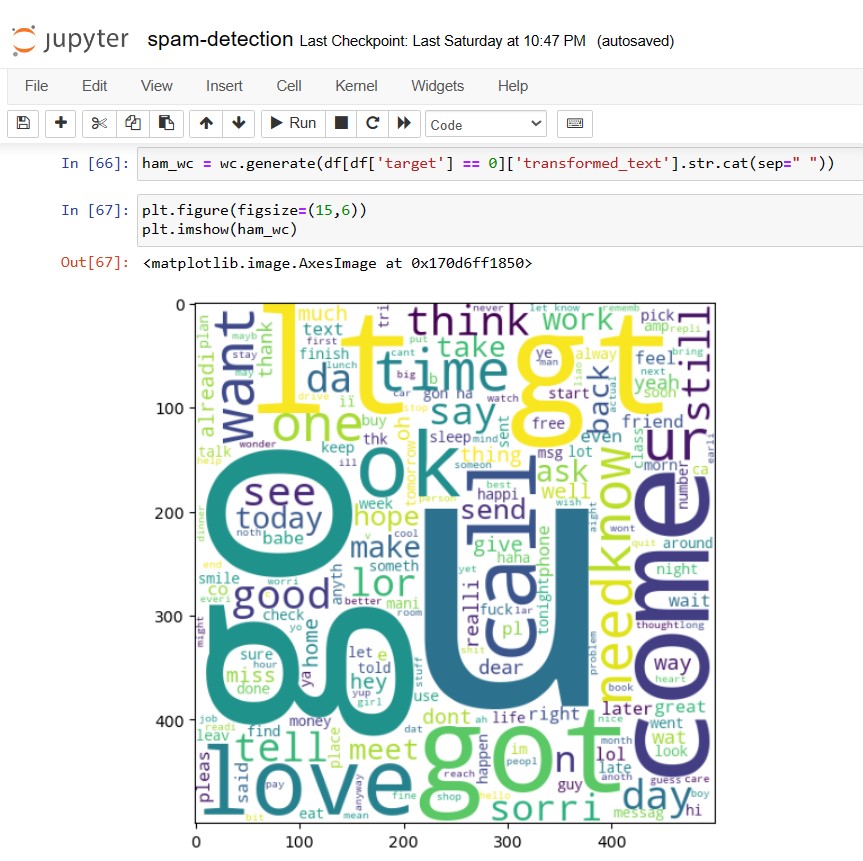
19



Figure

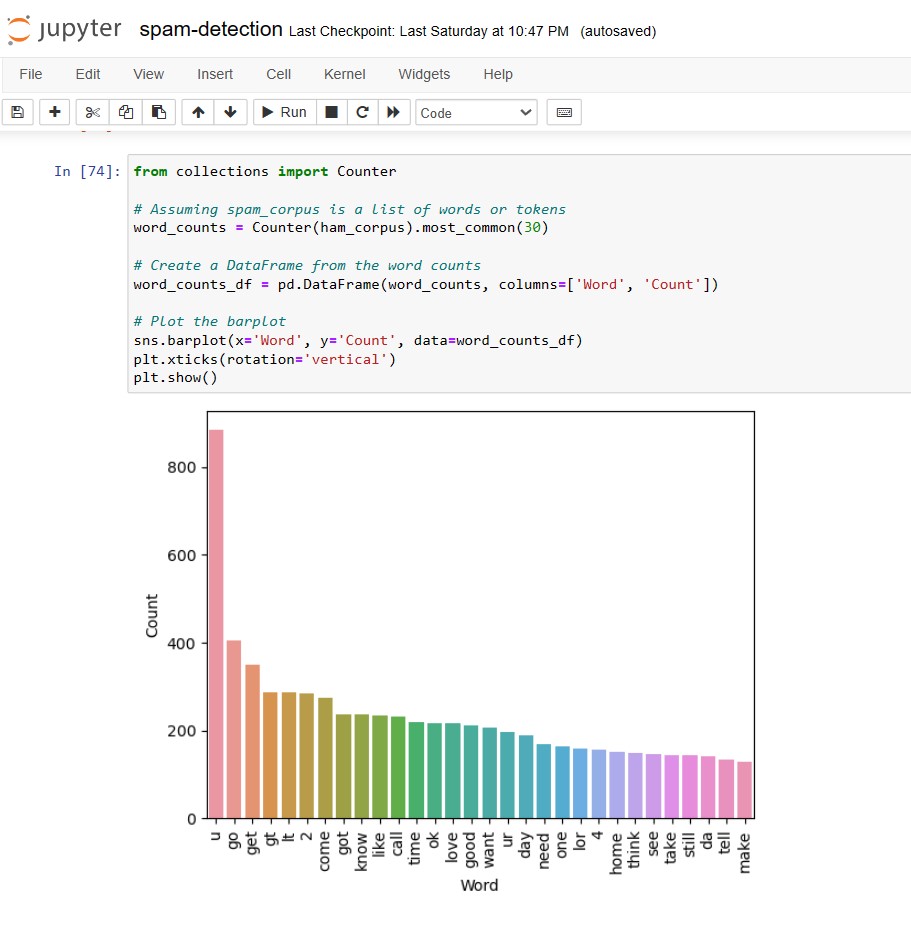
By using wordcloud,we will find top 30 words which are used in ham messages and which are used in spam messages,then we will make the bar plot of top 30 ham words and spam words.

20



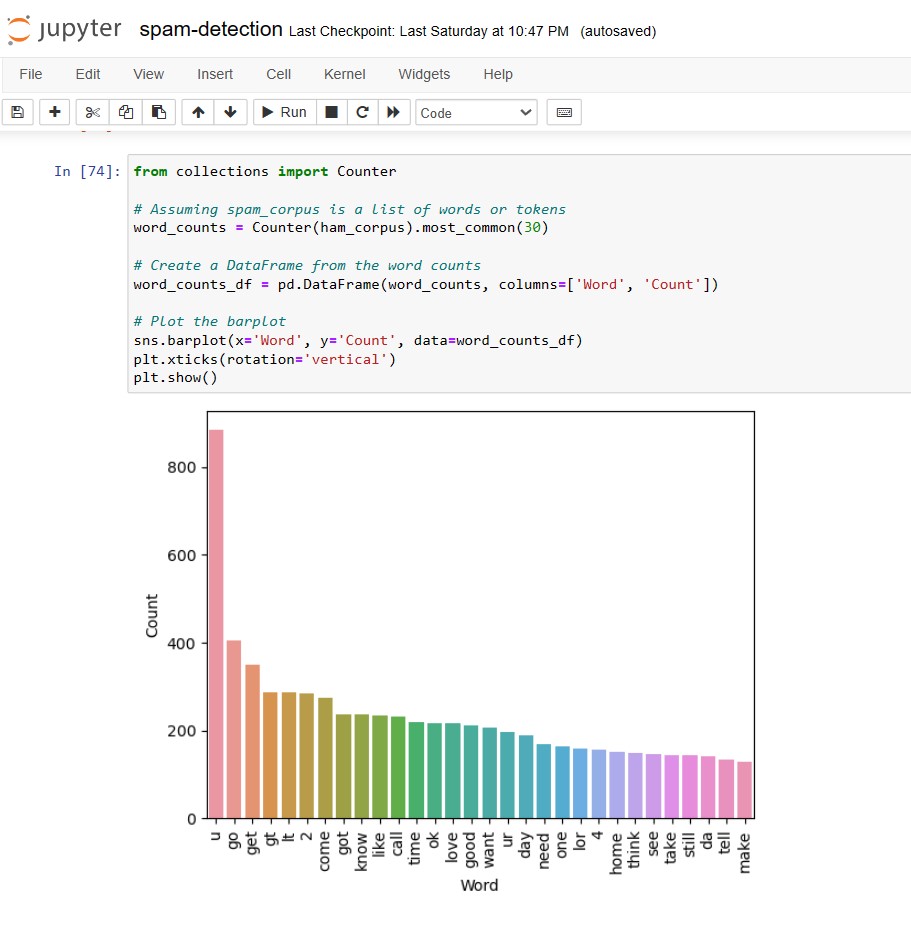
Figure

21



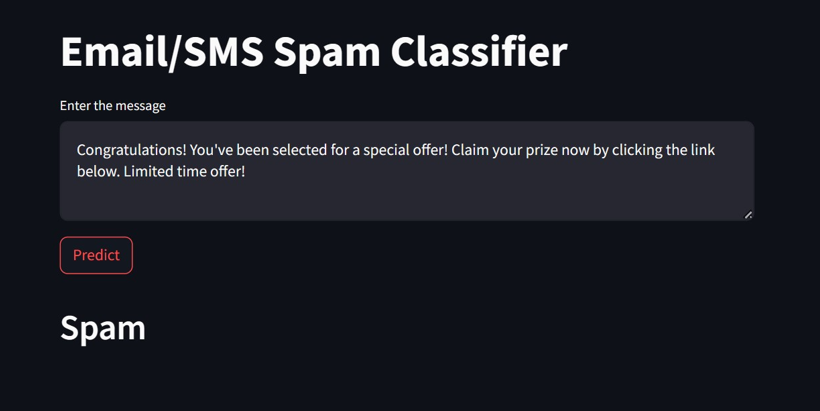
Figure

22



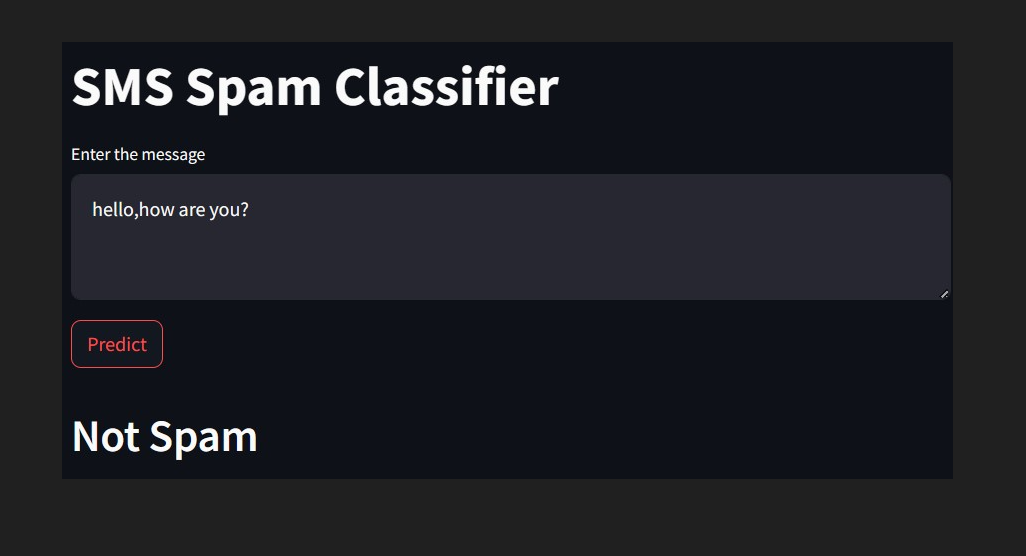
Figure

23

****

Figure

24



Figure

25

**5. References**

1. https://www.youtube.com/watch?v=FkF2jhaRJIs
2. https://www.kaggle.com/datasets/uciml/sms-spam-collection-dataset

26