# Machine Learning Project Report (SMS Spam Classifier)



Name: Irfan Arshad

**Reg# B21F0063AI019** 

**Instructor: Dr Arshad Iqbal** 

# **Department of ITCS**

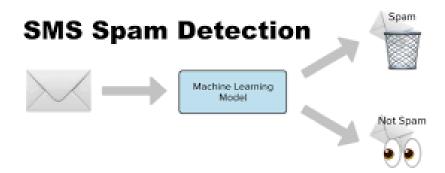
PAK-AUSTRIA FACHHOCHSCHULE:
INSTITUTE OF APPLIED SCIENCES AND
TECHNOLOGY

#### **ABSTRACT**

Over recent years, as the popularity of mobile phone devices has increased, Short Message Service (SMS) has grown into a multi-billion-dollar industry. At the same time, reducing the cost of messaging services has resulted in growth in unsolicited commercial advertisements (spam) being sent to mobile phones. In parts of Asia, up to 30% of text messages were spam in 2012. Lack of real databases for SMS spam, short length of messages limited features, and their informal language are the factors that may cause the established email filtering algorithms to underperform in their classification.

In this project, a database of real SMS Spam from the UCI Machine Learning repository is used, and after pre-processing and feature extraction, different machine learning techniques are applied to the database. Finally, the results are compared and the best algorithm for spam filtering for text messaging is introduced. Algorithms used in this technique are: Logistic regression (LR), K-nearest neighbor (K-NN), Random Forest Classifier (RFC), Naïve Baye's(NB), and Decision tree (DT) used for the classification of spam messages in mobile device communication. The SMS spam collection set is used for testing the method.

# **INTRODUCTION:**



Short Message Services (SMS) is far more than just a technology for a chat. SMS technology evolved out of the global system for mobile communications standard, an internationally accepted. Spam is the abuse of electronic messaging systems to send

unsolicited messages in bulk indiscriminately. While the most widely recognized form of spam is email spam, the term is applied to similar abuses in other media and mediums. SMS Spam in the context is very similar to email spams, typically, unsolicited bulk messaging with some business interest.

SMS spam is used for commercial advertising and spreading phishing links. Commercial spammers use malware to send SMS spam because sending SMS spam is illegal in most countries. Sending spam from a compromised machine reduces the risk to the spammer because it obscures the provenance of the spam. SMS can have a limited number of characters, which includes alphabets, numbers, and a few symbols. A look through the messages shows a clear pattern. Almost all of the spam messages ask the users to call a number, reply by SMS, or visit some URL. This pattern is observable in the results obtained by a simple SQL query on the spam. The low price and the high bandwidth of the SMS network have attracted a large amount of SMS spam. 3

Every time SMS spam arrives at a user's inbox, the mobile phone alerts the user to the incoming message. When the user realizes that the message is unwanted, he or she will be disappointed, and also SMS spam takes up some of the mobile phone's storage.



SMS spam detection is an important task where spam SMS messages are identified and filtered. As more significant numbers of SMS messages are communicated every day, it is challenging for a user to remember and correlate the newer SMS messages received in context to previously received SMS. Thus, using the knowledge of artificial intelligence with the amalgamation of machine learning, and data mining we will try to develop webbased SMS text spam or ham detector.

A number of major differences exist between spam-filtering in text messages and emails. Unlike emails, which have a variety of large datasets available, real databases for SMS spams are very limited. Additionally, due to the small length of text messages, the number of features that can be used for their classification is far smaller than the corresponding number in emails. Here, no header exists as well. Additionally, text messages are full of abbreviations and have much less formal language that what 4 one would expect from emails. All of these factors may result in serious degradation in performance of major email spam filtering algorithms applied to short text messages.

#### **Problem Statement:**

Short Message Service (SMS) is a popular mobile application used for personal and business communication worldwide. It has become a billion-dollar industry for text marketing, customer interaction, business updates, and reminders [1]. Along with these applications of short messages, there are many texts messaging mobile phone applications like WhatsApp, Telegram where people communicate daily, and nowadays many businesses are adopting these platforms to communicate with customers. Hence it is expected that this short message industry will grow enormously in the future. However, alongside legitimate SMSs, a significant number of spam messages flood in, serving various purposes, most of which are fraudulent. Filtering these spam SMS accurately is a challenging task that can benefit human lives both psychologically and financially.

### **Flow Chart:**

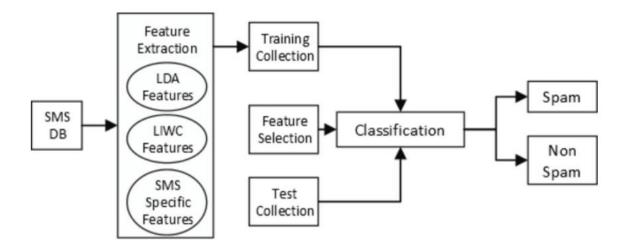


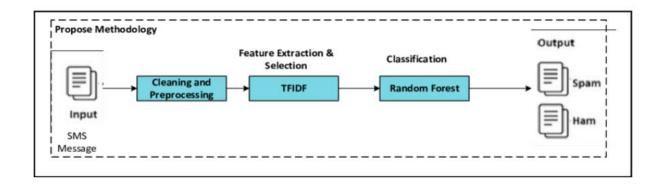
Fig-1.3 flow chart of sms spam detection

This is three parts of a bold series, where we will understand the in and out of spam or ham classifier from the aspect of Artificial Intelligence concepts, work with various classification algorithms in Jupyter Notebook, and select the one algorithm based on performance criteria. Then, we will develop the Python web-based SMS text spam or ham detector.

# **REQUIREMENTS:**

Anaconda Jupyter Notebook Anaconda3 Jupyter Notebook is used to write and execute the Python code using machine learning algorithms such as Naive Bayes Theorem, Logistic Regression, Decision Trees, K- Nearest Neighbors, and Random Forest.

# **METHODOLOGY:**



#### Dataset:

The dataset is collected from the UCI [20] or [21] and this dataset has 2 columns, a label, and an SMS. The label column says that SMS is either "spam" or "ham" (i.e., not spam). The SMS column has the raw text of the SMS and each row in the dataset contains the raw text of one SMS and its associated label. This dataset contains 5574 messages/rows.

Table 1. Detail Of The Dataset.

Source	Total Messages
The Grumbletext Web site	425
NUS SMS Corpus (NSC)	3375
Caroline Tag's Ph.D. Thesis	450
Spam Corpus v.0.1 Big	1324
Total	5574

The main reason for choosing this dataset is combined by randomly sampling from different resources hence it gives exposure to different scenarios of ham and spam SMSs. In statistics, it is proven that random sampling is the best.

# INTRODUCTION TO THE MACHINE LEARNING ALGORITHMS:

# • K-Nearest Neighbors:

k-nearest neighbor can be applied to classification problems as a simple instance-based learning algorithm. In this method, the label for a test sample is predicted based on the majority vote of its k nearest neighbors.

#### Random Forest:

Random forests is an averaging ensemble method for classification. The ensemble is a combination of decision trees built from a bootstrap sample from training set. Additionally, in building the decision tree, the split which is chosen when splitting

a node is the best split only among a random set of features. This will increase the bias of a single model, but the averaging reduces the variance and can compensate for the increase in bias too. Consequently, a better model is built. In this work, the implementation of random forests in the scikitlearn python library is used, which averages the probabilistic predictions. Two number of estimators are simulated for this method. With 10 estimators, the overall error is 2.16%, SC is 87.7 %, and BH is 0.73%. Using 100 estimators will result in overall error of 1.41 %, SC of 92.2 %, and BH of 0.51 %. We observe that comparing to the naive Bayes algorithm, although the complexity of the model is increased, yet the performance does not show any improvement.

#### MultinomialNB:

Multinomial Naive Bayes (MultinomialNB) is a machine learning algorithm used for text classification tasks. It is based on the Bayes theorem and assumes that the features (words) in a document are conditionally independent given the class label. MultinomialNB works by computing the probability of each class label given the occurrence of the features (words) in the input document. It is particularly useful for text classification tasks because it can handle sparse data and works well with large feature spaces. It is commonly used for tasks such as spam filtering, sentiment analysis, and topic classification.

#### Decision Tree:

A decision tree is a machine-learning algorithm used for classification and regression. It works by recursively partitioning data into subsets based on a chosen feature and building a tree-like model of decisions until a stopping criterion is met. Each node represents a decision based on a feature and each branch represents a possible outcome. Decision trees are easy to interpret and handle categorical and numerical data. However, they can overfit and small changes in training data can lead to different structures. They are popular for tasks such as fraud detection, customer churn prediction, and medical diagnosis.

# • Logistic Regression:

Logistic Regression is a machine learning algorithm used for binary classification. It models the probability of an input belonging to a certain class using a sigmoid function applied to a linear combination of the input features. During training, it learns the coefficients that minimize the log-loss function. Logistic Regression is simple, efficient, and can handle both numerical and categorical input features. It is commonly used for tasks such as credit risk assessment, fraud detection, and medical diagnosis.

# **Data Preprocessing:**

Now that we have a basic understanding of what our dataset looks like, lets convert our labels to binary variables, 0 to represent 'ham' (i.e. not spam) and 1 to represent 'spam' for ease of computation. You might be wondering why do we need to do this step? The answer to this lies in how scikit-learn handles inputs. Scikit-learn only deals with numerical values and hence if we were to leave our label values as strings, scikit-learn would do the conversion internally (more specifically, the string labels will be cast to unknown float values). 12 Our model would still be able to make predictions if we left our labels as strings but we could have issues later when calculating performance metrics, for example when calculating our precision and recall scores. Hence, to avoid unexpected 'gotchas' later, it is good practice to have our categorical values be fed into our model as integers.

# **Bag of words:**

What we have here in our data set is a large collection of text data (5,572 rows of data). Most ML algorithms rely on numerical data to be fed into them as input, and email/sms messages are usually text-heavy. Here we'd like to introduce the Bag of Words (BOW) concept which is a term used to specify the problems that have a 'bag of words' or a collection of text data that needs to be worked with. The basic idea of BOW is to take a piece of text and count the frequency of the words in that text. It is important to note that the BOW concept treats each word individually and the order in which the words occur does not matter. Using a process which we will go through now, we can convert a collection of documents to a matrix, with each document being a row and each word(token) being the column, and the corresponding (row, column) values being the frequency of occurrence of each word or token in that document.

# Data preprocessing with CountVectorizer():

Some of the important parameters of CountVectorizer():

- 1. lowercase = True The lowercase parameter has a default value of True which converts all of our text to its lowercase form.
- 2. Token pattern = (? u) \b\w\w+\b The token pattern parameter has a default regular expression value of (?u)\b\w\w+\b which ignores all punctuation marks and treats them as delimiters, while accepting alphanumeric strings of length greater than or equal to 2, as individual tokens or words.
- 3. Stop words The stop words parameter, if set to English will remove all words from our document set that match a list of English stop words which is defined in scikitlearn. Considering the size of our dataset and the fact that we are dealing with SMS messages and not larger text sources like e-mail, we will not be setting this parameter value.

# **Training and testing sets:**

Now that we have understood how to deal with the Bag of Words problem we can get back to our dataset and proceed with our analysis. Our first step in this regard would be to split our dataset into a training and testing set so we can test our model later.

Instructions: Split the dataset into a training and testing set by using the train\_test\_split method in sklearn. Split the data using the following variables:

- X\_train is our training data for the 'sms\_message' column.
- Y\_train is our training data for the 'label' column
- X\_test is our testing data for the 'sms\_message' column.
- y\_test is our testing data for the 'label' column Print out the number of rows we have in each our training and testing data.

# **Implementation of Machine Learning Algorithms:**

I will use sklearns sklearn.naive\_bayes method to make predictions on our dataset for SMS Spam Detection. Specifically, we will be using the multinomial Naive Bayes implementation. This particular classifier is suitable for classification with discrete features. It takes in integer word counts as its input.

# **Evaluating our model:**

#### • Evaluation Metrics:

In machine learning, a confusion matrix is a table used to evaluate the performance of a classification model. It is a matrix that summarizes the actual and predicted class labels for a set of test data. As shown in Figure 3, the confusion matrix shows the number of true positives, false positives, true negatives, and false negatives for each class. True positives (TP) are the number of correct predictions of the positive class, false positives (FP) are the number of incorrect predictions of the positive class, true negatives (TN) are the number of correct predictions of the negative class, and false negatives (FN) are the number of incorrect predictions of the negative class. A confusion matrix can be used to calculate various evaluation metrics such as accuracy, precision, recall, and F1 score.

Figure 4. Confusion Matrix Of Spam And Ham.

Confusion Matrix	Predicted HAM	Predicted SPAM
Actually HAM	TN (True Negative)	FP (False Positive)
Actually SPAM	FN (False Negative)	TP (True Positive)

To evaluate and compare different models, accuracy, precision, and recall are used as evaluation metrics in this research.

# Accuracy:

Accuracy measures the overall proportion of SMS messages that are correctly classified by the model, both spam and legitimate. While accuracy is an important metric, it is not as useful in SMS spam detection as it can be skewed by the high proportion of legitimate messages in the dataset. We can calculate accuracy using the formula below.

$$Accuracy = \frac{TP+TN}{TP+FP+FN+TN}$$

#### **Precision:**

Precision measures the proportion of SMS messages classified as spam that are actually spam. In other words, it measures how many true positives (spam

messages correctly classified as spam) there are relative to false positives (legitimate messages incorrectly classified as spam). In SMS spam detection, precision is an important metric as it ensures that users are not receiving too many false positives (legitimate messages incorrectly classified as spam) that could result in the loss of important messages. The precision of the model can be calculated using TP, and FP values given in the confusion matrix.

#### **Recall:**

Recall, on the other hand, measures the proportion of actual spam messages that were correctly classified as spam. In other words, it measures how many true positives (spam messages correctly classified as spam) there are relative to false negatives (spam messages incorrectly classified as legitimate). The recall is also an important metric in SMS spam detection, as it ensures that the model is able to capture all spam messages and not miss any that could result in users receiving unwanted messages. The formula of recall is shown below.

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

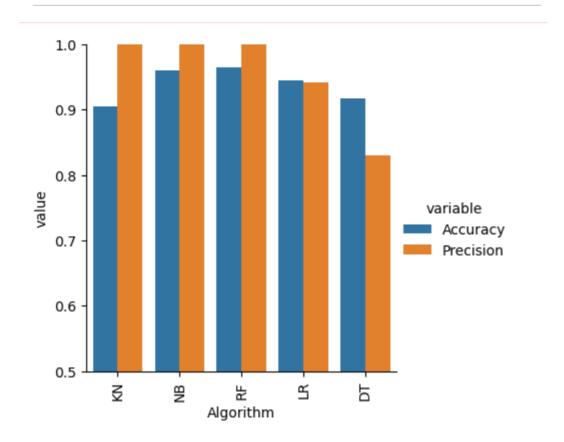
#### **Conclusion:**

One of the major advantages that Naive Bayes has over other classification algorithms is its ability to handle an extremely large number of features. In our case, each word is treated as a feature and there are thousands of different words. Also, it performs well even with the presence of irrelevant features and is relatively unaffected by them. The other major advantage it has is its relative simplicity. Naive Bayes' works well right out of the box and tuning its parameters is rarely ever necessary, except usually in cases where the distribution of the data is known. It rarely ever overfits the data. Another important advantage is that its model training and prediction times are very fast for data it can handle. All in all, Naive Bayes' is a gem of an algorithm!

# **Compare Different ML and DL models:**

Below are different machine learning models compared.

Algorithm	Accuracy	Precision
KN	0.905314	1.000000
NB	0.960386	1.000000
RF	0.965217	1.000000
LR	0.944928	0.941748
DT	0.916908	0.829787
	KN NB RF LR	NB 0.960386 RF 0.965217 LR 0.944928



# Performance Measure Accuracy = True Positive + True Negetive Total Number of Test Data Spams caught (SC) = False negative cases Number of Spams Blocked hams (BH) = False Positive cases Number of Hams

#### **TESTING:**

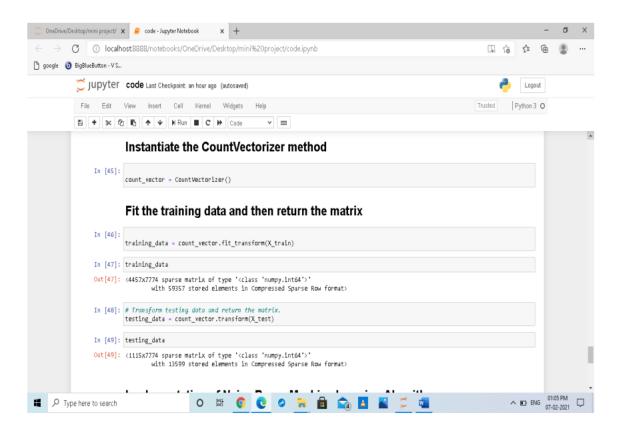


Fig.1 Testing the data.

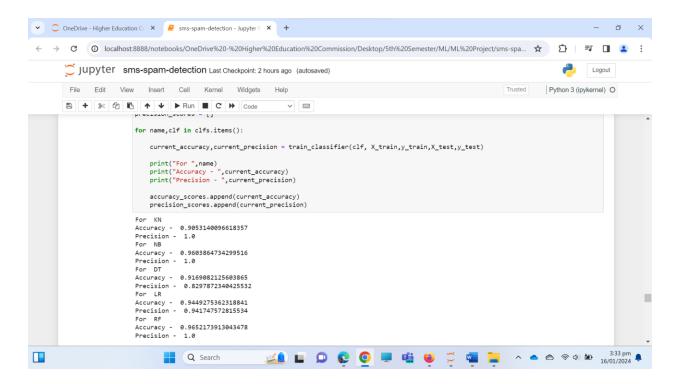
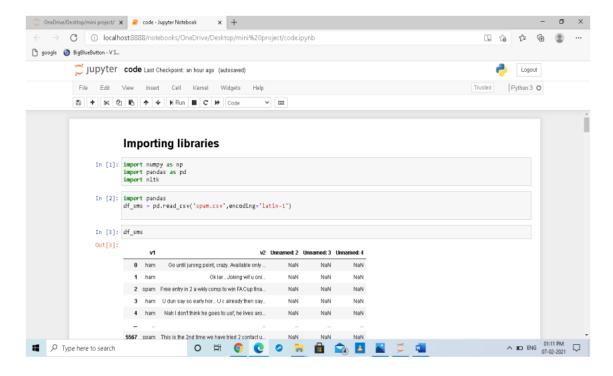
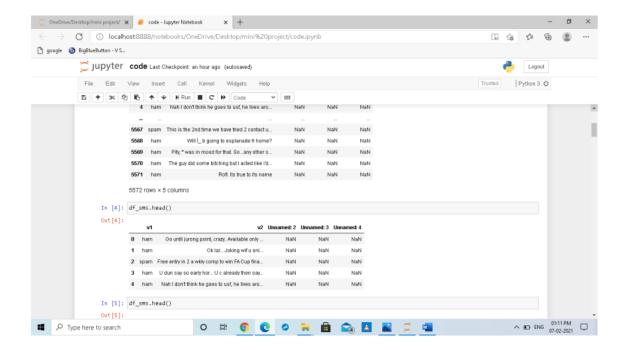


Fig.2 Evaluating the model.

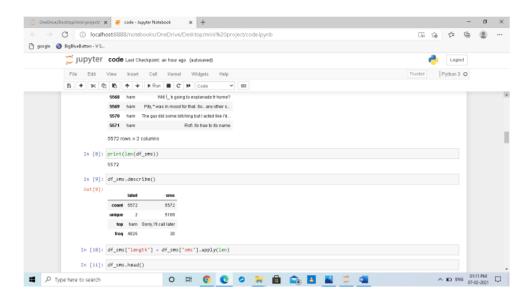
# **OUTPUT SCREENS:**



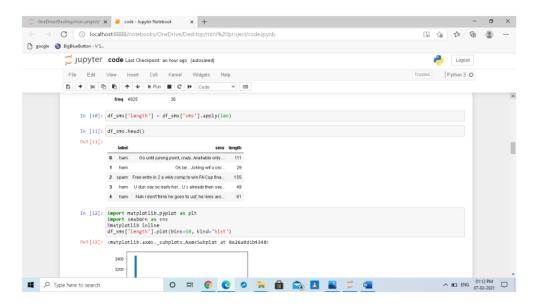
Importing libraries



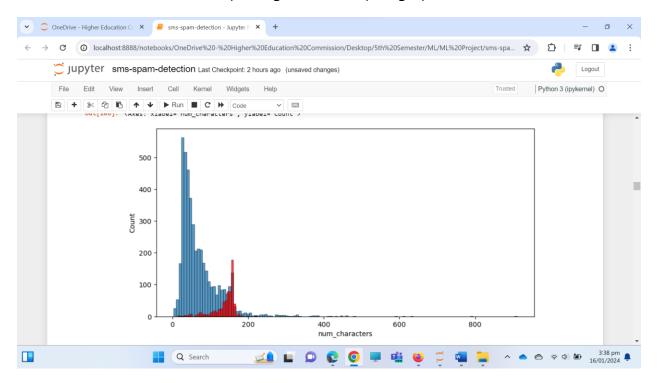
Viewing the Data

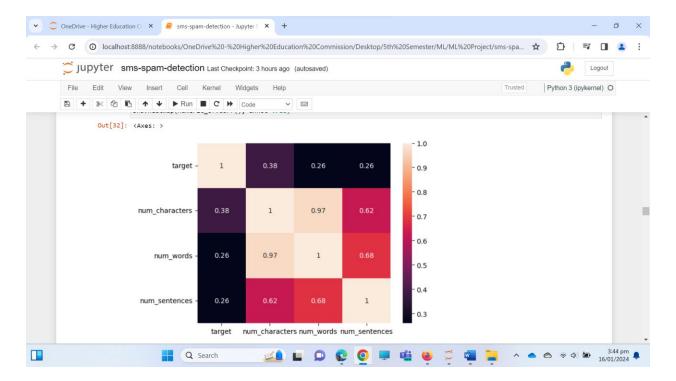


Viewing the Unique Data

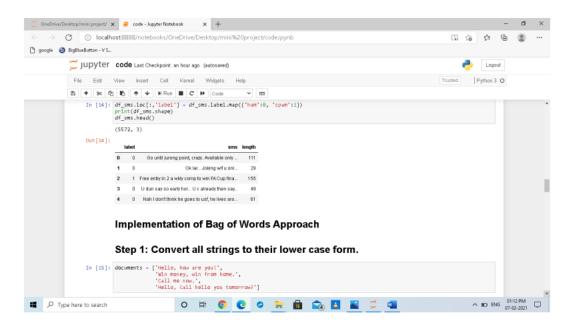


# Importing libraries to plot graphs

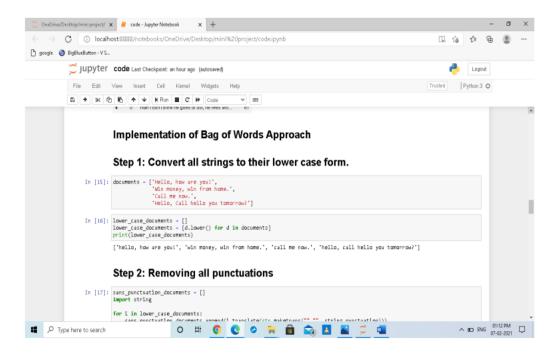




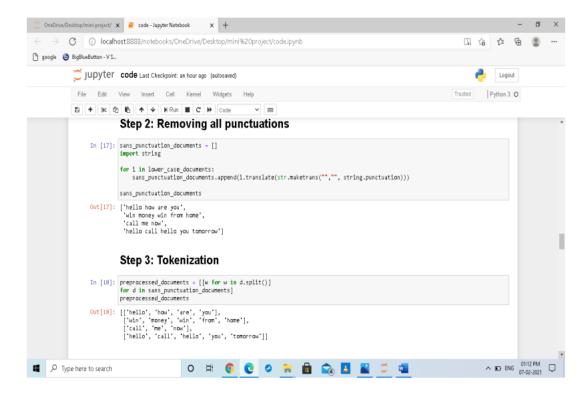
#### Correlation Matrix



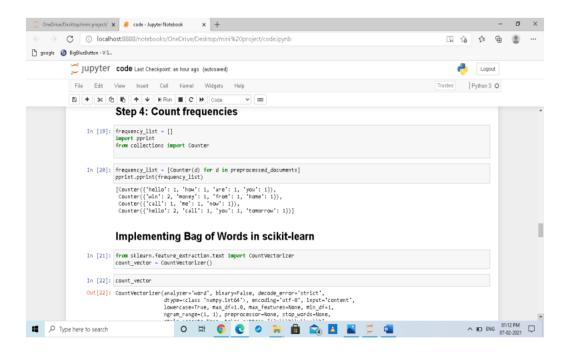
Converting all Strings to their lower Form



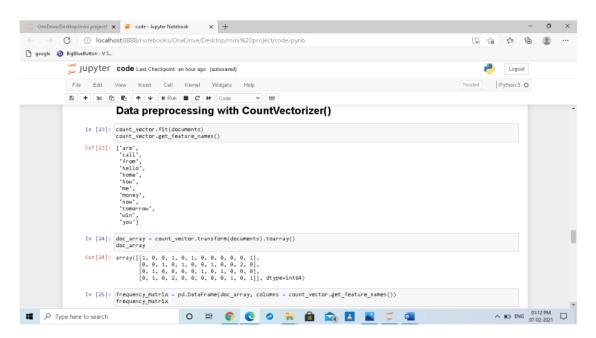
# Removing all punctuation



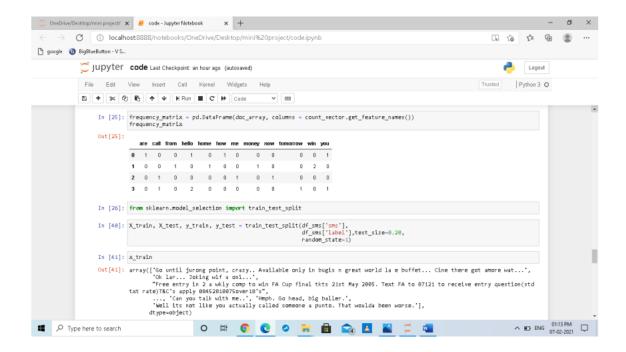
**Tokenization** 



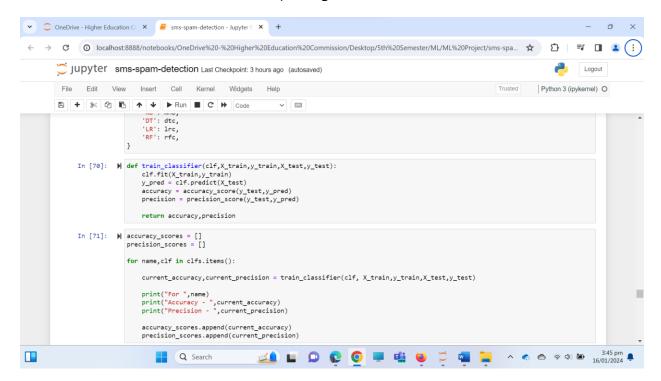
Counting frequencies and implementing bag of words in scikit-learn



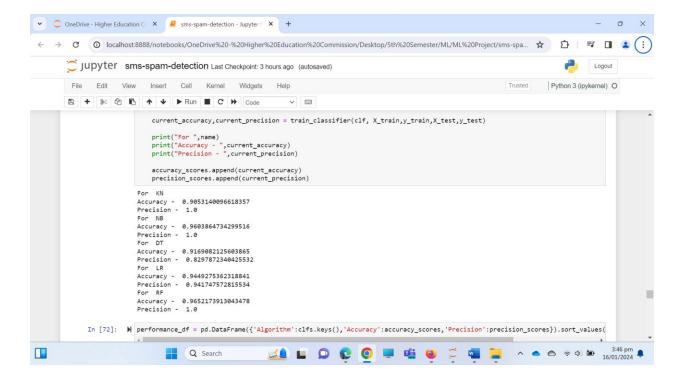
Data Preprocessing with CountVectorizator()



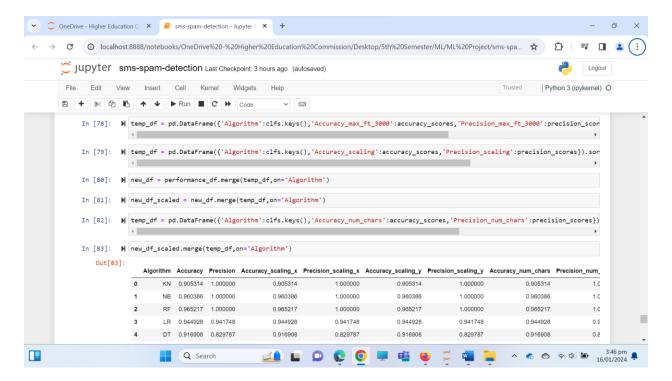
# Splitting the data

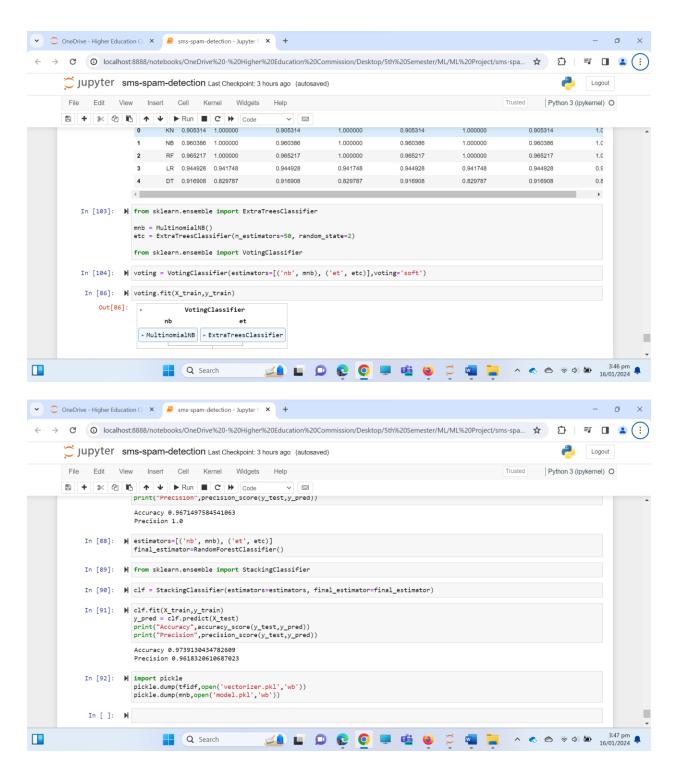


Fitting Models on the Data



#### Model Evaluation Result





Models Improvements