**OPTIMIZING SPAM FILTERING WITH MACHINE LEARNING USING PYTHON**

**TEAM LEADER: MENTOR:**

Shobana MDr. E. Elakkiya, M.Sc.,M.Phil.,Ph.D.,

**MEMBERS:**

Sindhu P

Snaha S

Sharmila N

**1. INTRODUCTION**

Short Messaging Service (SMS) is a significant kind of communication that people use in the world of wireless technology today. Its effects on the economy are significant both the user and the service provider. One issue in the world nowadays is spam SMS. To identify spam SMS, many different SMS spam filtering algorithms are utilized. The current study focuses on identifying spam SMS using machine learning, which is carried out using Python, an open source program. The experimental finding indicates that almost 98% of spam SMSs are recognized.

As the popularity of mobile phone devices has grown in recent years, Short Message Service (SMS) has grown into a multi-billion dollar industry. Simultaneously, as the cost of messaging services has decreased, the number of unsolicited commercial advertisements (spam) sent to mobile phones has increased. Spam SMS causes financial concerns for mobile service providers while also reducing calling time for subscribers. Unfortunately, if the user views such as Spam SMS, they may encounter a virus or malware issue. When SMS arrives on a mobile device, it disrupts the user’s privacy and concentration. It may lead to frustration for the user. As a result, spam SMS is a major issue in the wireless communication world as grow day by day.

Spam, known as Unsolicited Bulk message, Spam, or Unsolicited Commercial SMS, is the method of sending unsolicited SMS messages, frequently with commercial content, to a major corporation. SMS spam filtering is essentially instant messages SMS sent from just about any account or automated process. Spam refers to messages that the recipient does not need or want in their mailbox. The rules shared by many other SMS servers assist the spam filter in blocking more spam SMS than before.

* 1. **. OVERVIEW**

Short Messaging Service (SMS) is one of the simplest and most economical forms of communication in the wireless era. SMS has a high response rate, which makes it popular worldwide lowest price and secure, individualized service. However, adopting this SMS approach comes with several drawbacks, including Spam SMS. Spammers use the wireless world to their advantage to contact potential clients. Currently, the majority of SMS messages are spam messages with offers for credit cards, discounts, traffic plans, promotions, etc. Spam SMS causes both financial issues for mobile service providers and a reduction in call time for customers. Regrettably, the consumer may have malware or virus issues if they access such spam SMS. When an SMS message arrives, the phone will be disturbed user focus and confidentiality. That can make the user frustrated. Hence, spam SMS is a significant problem in the world of wireless communication and it becomes worse every day. People utilize white and black lists of numbers to avoid these spam SMSs. However, this method is insufficient to entirely prevent spam SMS. It is essential to employ a cleverer method that correctly distinguishes Spam SMS in order to address this issue. The text mining technique is helpful for identifying spam SMS. It examines text content to look for patterns that can be utilized to distinguish between spam and non-spam SMS. Spam SMS filtering is typically thought of as a text categorization approach. The maximum size of an SMS message is typically merely.

**1.2 PURPOSE**

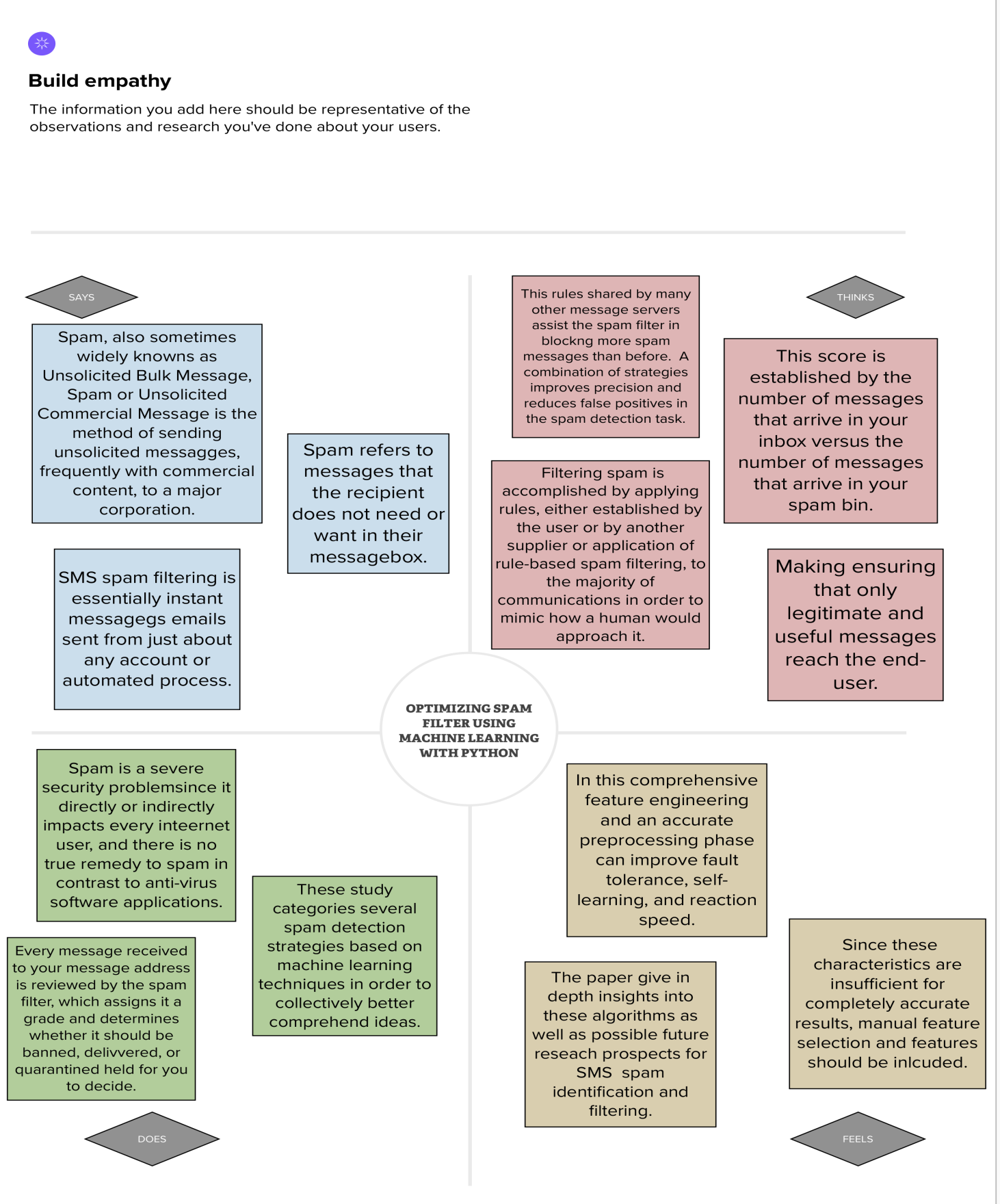
A program known as a spam filter is used to identify unwanted and unsolicited text messages and stop them from reaching a user's mobile device. A spam filter, like other types of filtering programs, searches for specific criteria before making a decision.

Spam SMS messages are on the rise as more people use cell phones. It can be challenging to deal with cell phone spam due to a number of factors, including the limitations of the spam filtering algorithms built into mobile devices and the low frequency of these types of communications.

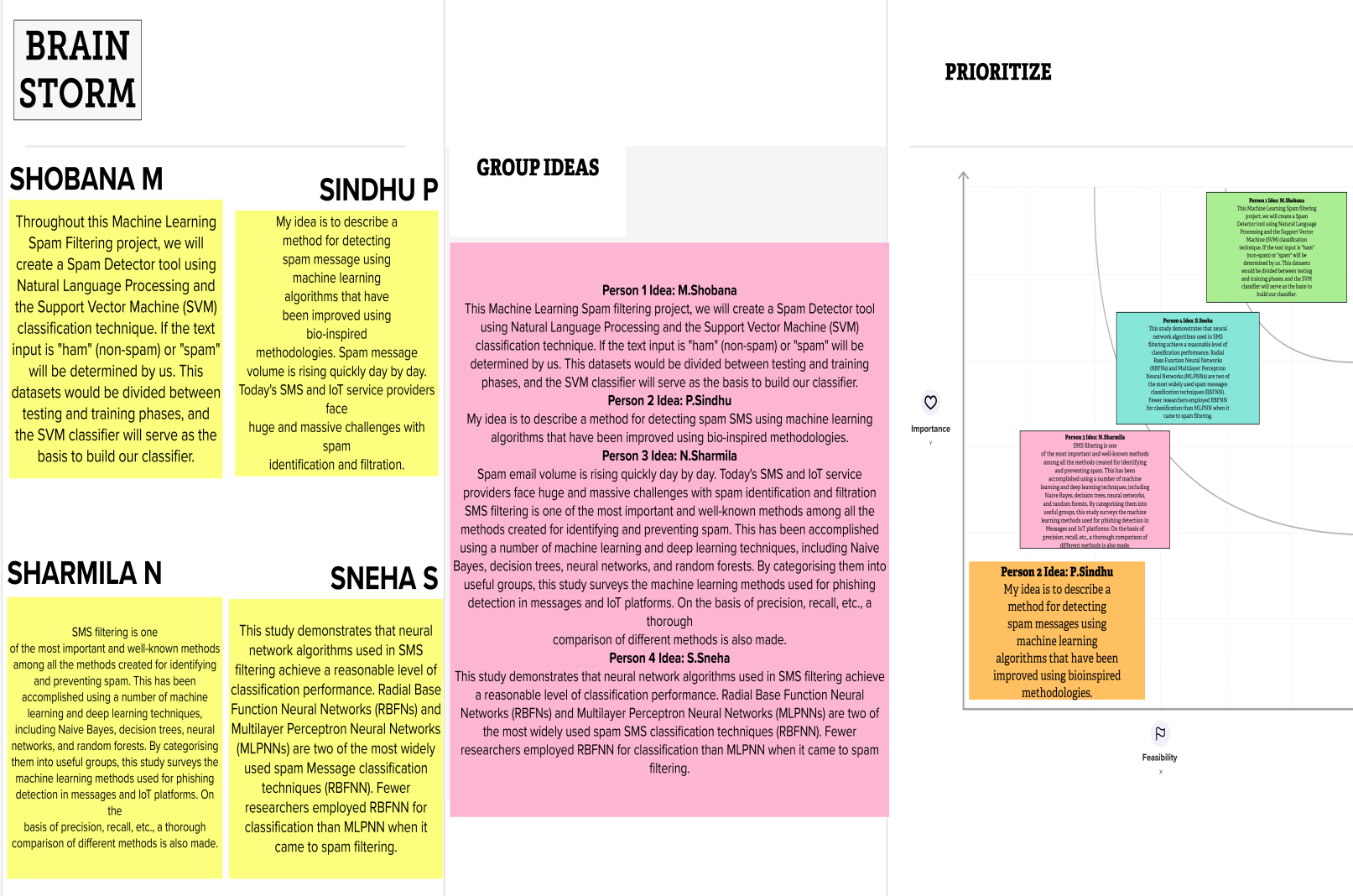
Spam is a widespread issue that everyone is aware with. Spam filtering employs a variety of techniques. Content-based filtering, which analyses the message's actual text to decide if it is spam or not, is the most often used filtering method. The information is really

**2. PROBLEM DEFITION & DESIGN THINKING**

**2.1. EMPATHY MAP**

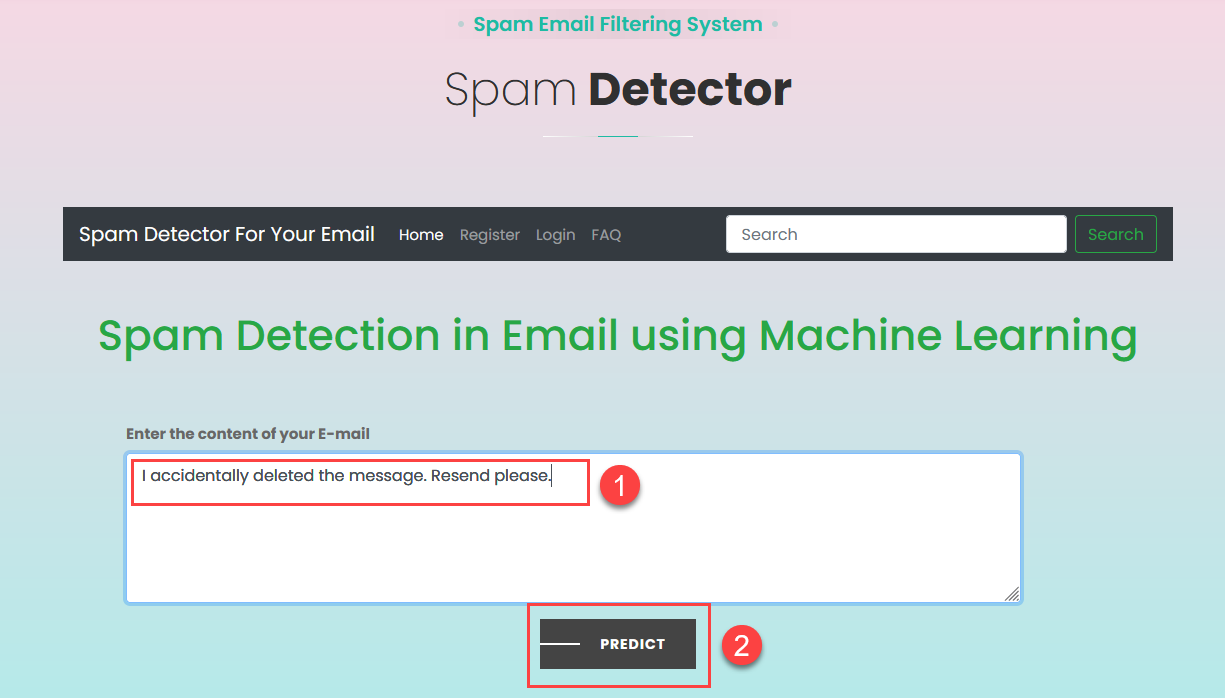
****

**2.2. BRAIN STORM**

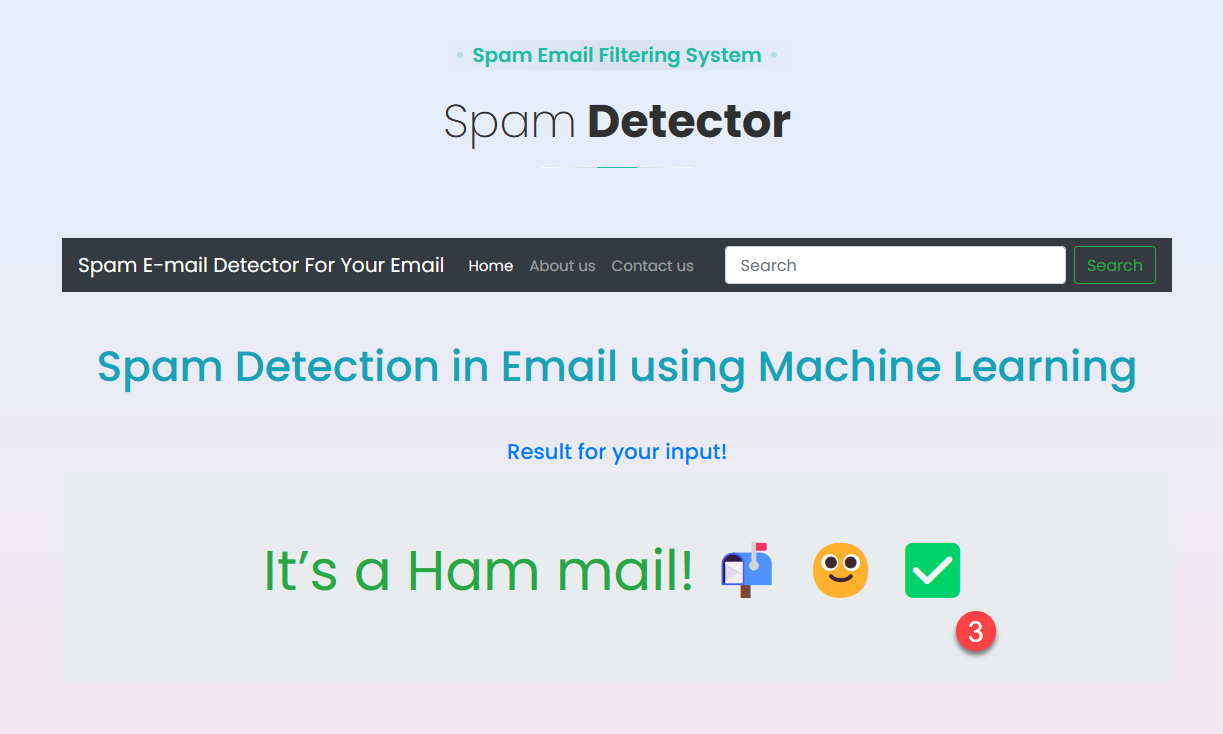
****

**3. RESULT**

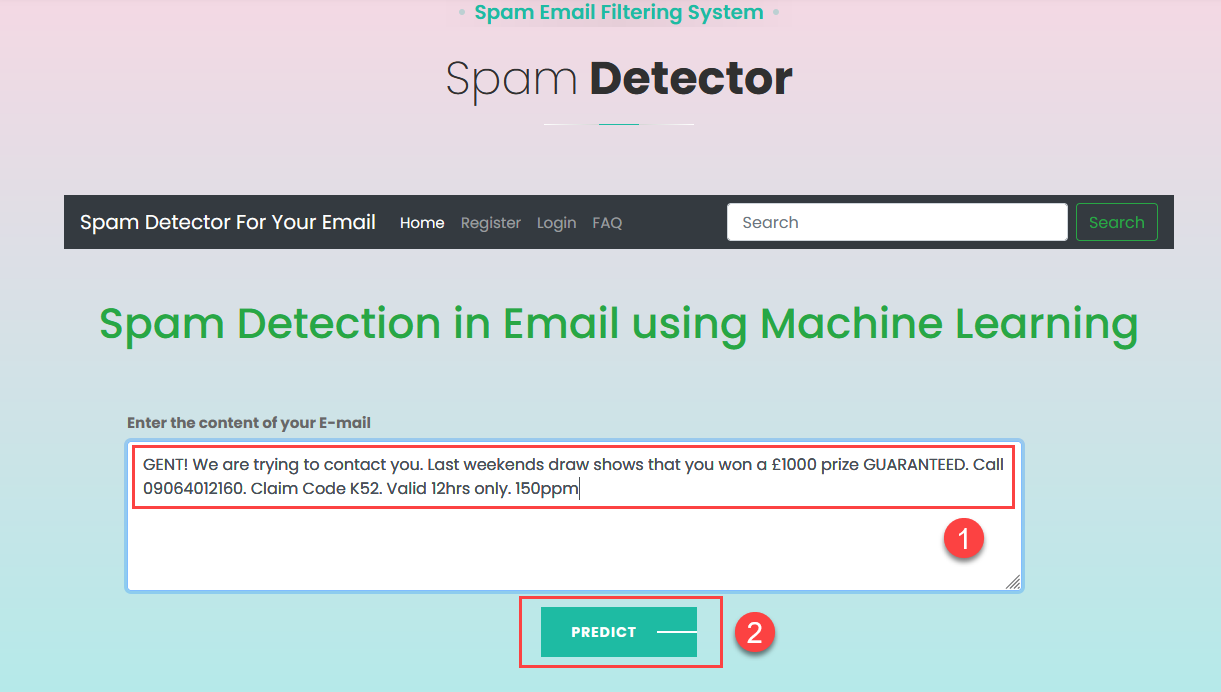
**A) HAM TEST 1:**

****

**B) HAM TEST 2:**

****

**C) SPAM TEST 1:**

****

**D) SPAM TEST 2:**

****

**4. ADVANTAGES & DISADVANTAGES**

|  |  |
| --- | --- |
| ADVANTAGES | DISADVANTAGES |
| Combination of machine learning algorithms with user generated features | Users need to select features manually |
| Classification based on two algorithms | No classification algorithm is used |
| Combination of client and server side algorithms | Threshold selection |
| Combination of client and server side algorithms | Challenge-response technique suffers from server side traffic and user interaction problems |
| Accurate as Naïve Bayesian with necessary feature extraction | Complex implementation |
| Incorporating Apriori Algorithm | Suffering from implementation complexity |
| Although SVM gives better results in Spam identification Bayesian is more feasible for mobile application. | Extensive feature engineering is needed for better accuracy. |

**5. APPLICATION**

We must accept that SMS messages do not have the same structure and properties as email messages because having a decent term representation is one of the most crucial components of getting a strong classifier. Although we have discussed methods for removing spam emails, we cannot guarantee that they will also be successful in removing SMS.

Email messages tend to be longer than SMS messages. There are just 160 characters in a conventional SMS text message, which may be problematic because there is less information available when fewer words are used. Due to the aforementioned restriction, people frequently use acronyms when sending SMS messages. Additionally, the abbreviations that SMS users use are not language-standard; rather, they are determined by the communities of users.

A more sparse representation and more terminology or traits are offered by such linguistic diversity. We must determine whether the cutting-edge techniques used to extract phrases from email messages are equally appropriate for SMS texts.

**6. CONCLUSION**

It is reasonable to define a wide range of attribute types and allow the attribute selection using IG process to choose those most promising for classification, given the short size of messages and the literature on spam email filtering, according to this series of experiments. However, even if it appears to be correlated with the spam messages, the amount of selected qualities cannot be determined in advance. Testing different features, such as encrypting all numbers or marking phone numbers, could be useful.

After careful consideration, Support Vector Machines are determined to be the best learning method for a prototype. Our earlier work—as well as that of others—in text classification and spam email detection supports this.

The most suitable learning algorithm for a prototype is, after in-depth evaluation, Support Vector Machines. This is supported by our and other’s previous work in spam message detection and in text classification. Also, although we have not demonstrated this empirically, the running time of learning with Support Vector Machine has been comparable to Naïve Bayes, and much smaller than the running time for learning rules or decisions trees.

**7. FUTURE SCOPE**

It gives the client sensitivity and is ideally suited to upcoming spam tactics. When it comes to its organization, it takes into account the whole message rather than just a few phrases. It enhances Control and Security. It lowers the expense of IT administration. It also lowers the cost of network resources.

Our project has a large number of potential improvements. The following improvements are possible, on the basis of its contents, spam can be filtered. The spam SMS classification is crucial for classifying SMS and identifying spam from non\_spam SMS. Large organizations can use this strategy to discriminate between good SMS and SMS that they do not want to receive.

The algorithms developed so far have not been able to remove the requirement of manual checking of the reviews. Hence there is scope for complete automation of spam detection systems with maximum efficiency.

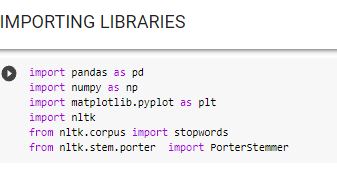
It has a broadcasted, rather than targeted, message and suits the purposes of the sender rather than the receiver. Most important, the message is distributed without the explicit permission of the recipients.

Generally, a 90% spam catch rate and a false positive rate of less than 1% is considered good. Not only does spam filtering help keep garbage out of message inboxes, it helps with the quality of life of business messages because they run smoothly and are only used for their desired purpose.

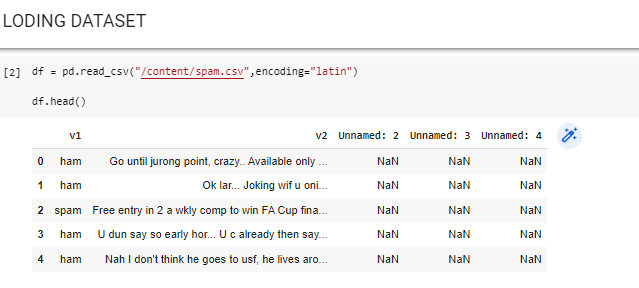
**8. APPENDIX**

**A. SOURCE CODE**

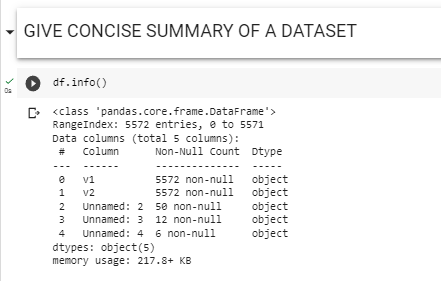
Importing the libraries in google colabs

****

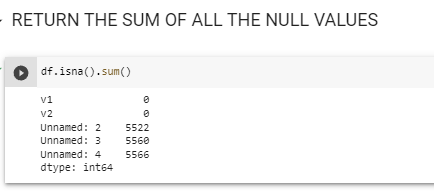
Loading the dataset

****

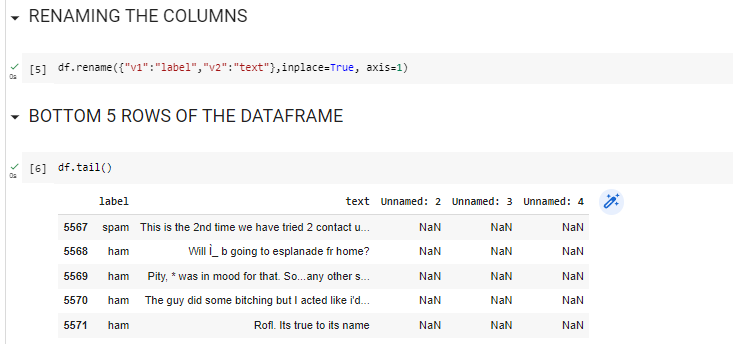
Summary of the Dataset

****

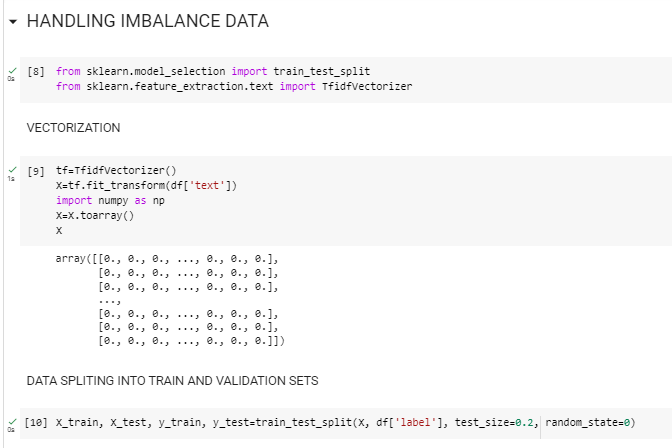
Sum of all the NULL values into the dataset

****

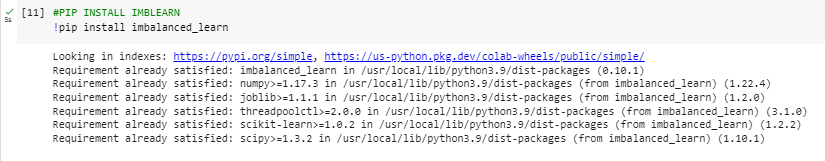
Renaming the column v1 and v2 as respectively ‘label’ and ‘text’

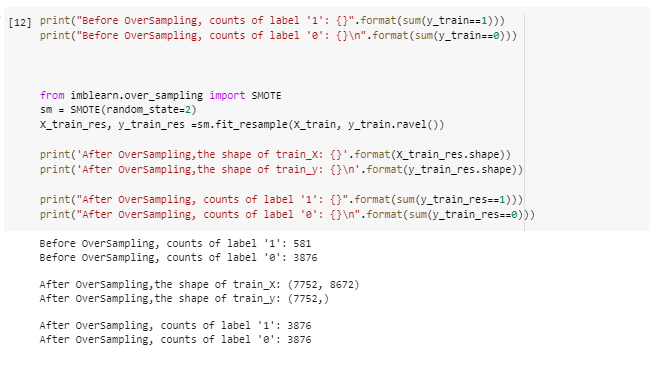
****

Handling the imbalanced data into the dataset

****

Install the library as pip install imblearn

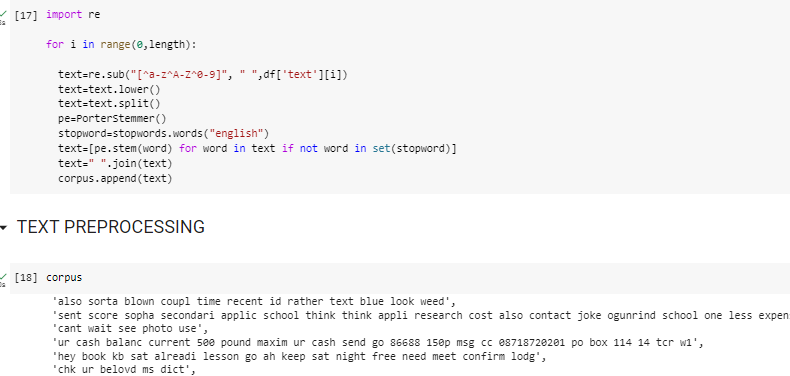
****

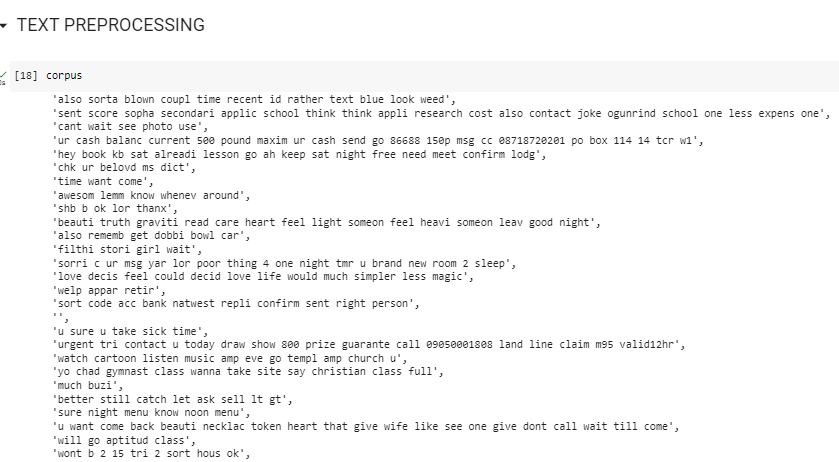
****

Cleaning the Dataset

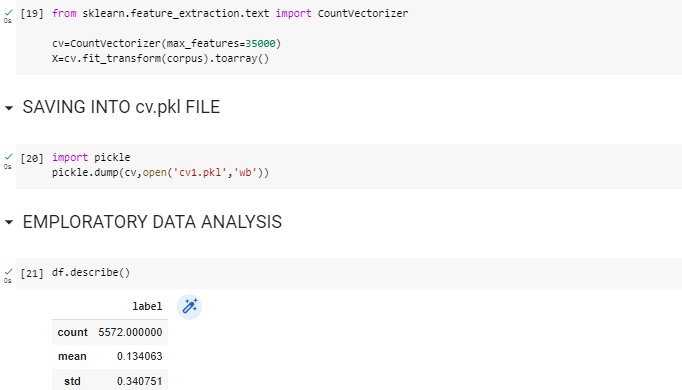
****

Data Preprocessing

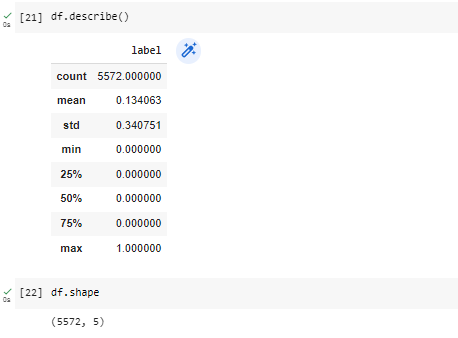


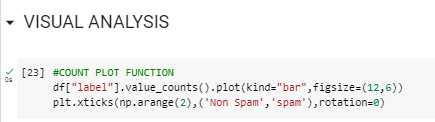


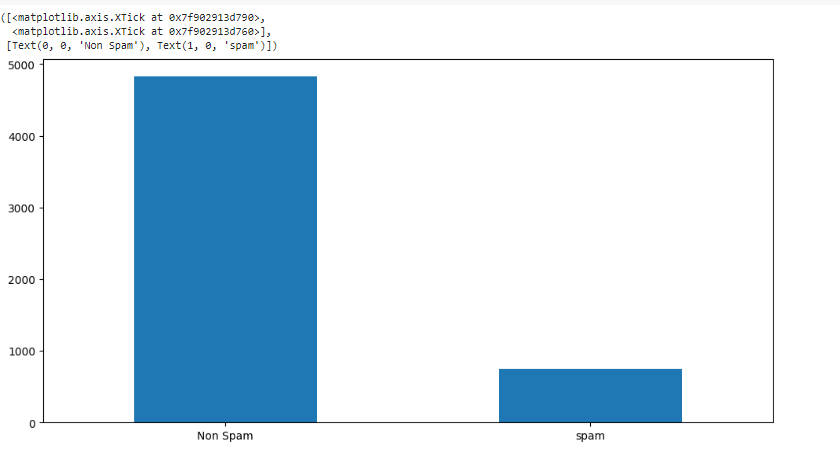
Saving the cv.pkl file



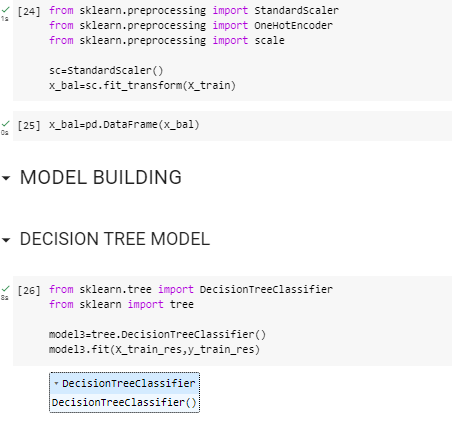
Visualizing the data

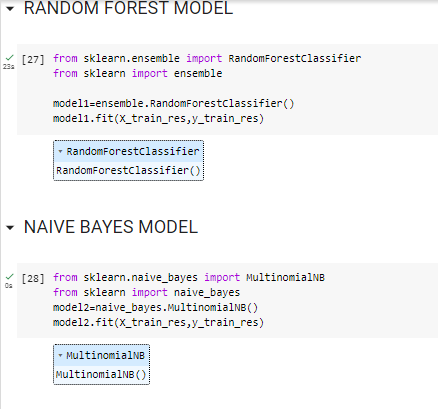




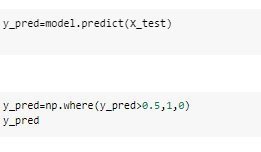


Model building using decision tree model, navie Bayes and ANN

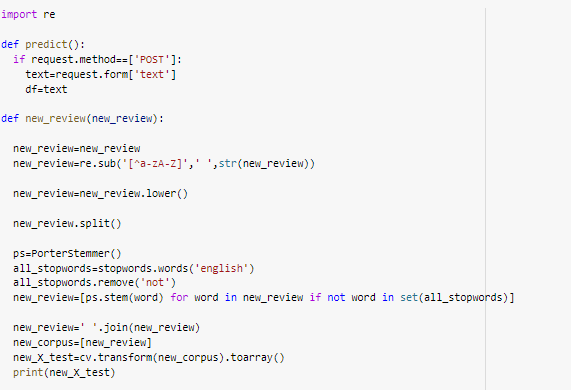








Loading the model





Saving our model as Spam.h5 format

