

SMS SPAM CLASSIFIER

MAJOR PROJECT SYNOPSIS

Submitted to
Ms. Anjali Yadav

Submitted By:
Aniket Kumar Singh (19CS04)

in Partial Fulfillment for the Award of the Degree

of

B.Tech

in

COMPUTER SCIENCE



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Lingaya's Vidyapeeth
(Deemed to be University Under Section 3 of UGC Act, 1956)

Old Faridabad-Jasana Road, Nachauli, Faridabad

December 2022

INDEX

S.no	Title	Page Number
1	Abstract	1
2	Introduction	2
3	Scope andObjective	5
4	Methodology	6
5	Conclusions	8
6	Future Scope	9
7	References	10

ABSTRACT

The spam detection is a big issue in mobile message communication due to which mobile message communication is insecure. In order to tackle this problem, an accurate and precise method is needed to detect the spam in mobile message communication. We proposed the applications of the machine learning-based spam detection method for accurate detection. The SMS spam collection data set is used for testing the method. The dataset is split into two categories for training and testing the research. Automatic Text Classification is a machine learning technique. Document can be set to predefined categories based on textual content and extraction features. It has important applications in spam filtering and text mining. An analysis of SMS SPAM filtering classification model has also been done using Automatic Text Classification.

INTRODUCTION

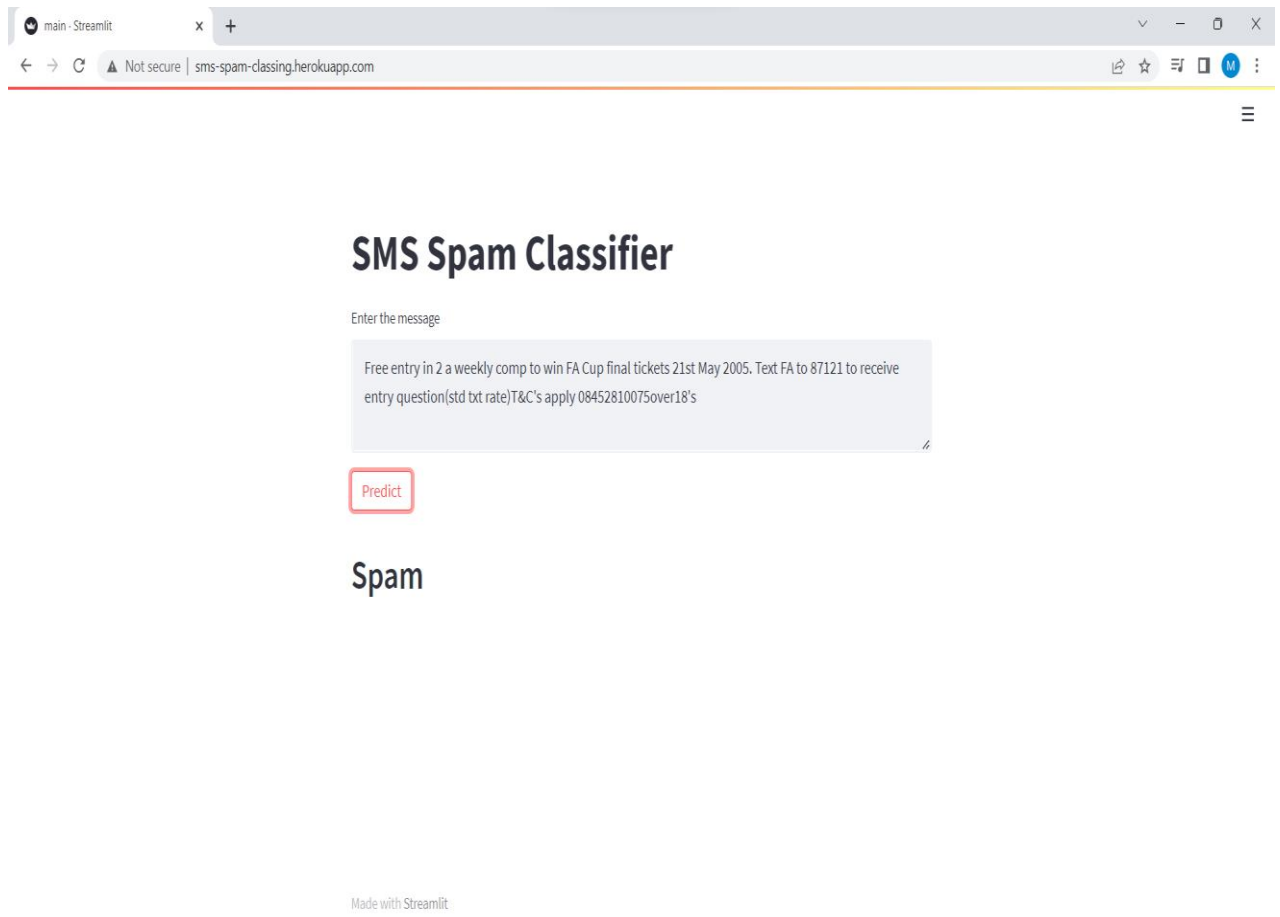
Mobile message is a way of communication among the people, and billions of mobile device users exchange numerous messages. However, such type of communication is insecure due to lack of proper message filtering mechanisms. One cause of such insecurity is spam, and it makes the mobile message communication insecure. Spam is considered to be one of the serious problems in e-mail and instance message services. Spam is a junk mail or message. Spam e-mails and messages are unwanted for receivers which are sent to the users without their prior permission. It contains different forms such as adult content, selling item or services, and so on. Due to these spam mails and messages, the values able e-mails and messages are affected because each user have limited Internet services, short time, and memory.

Classification of SPAM/HAM SMS:

SPAM is the virus infected SMS which results malfunctioning of mobile. HAM is basics a virus free SMS. SPAM SMS can corrupt the operating system of the mobile. Mobile phone SPAM is originated from the text message and other communication services by mobile phones. Due to the extensive use of the mobile phones now a days advertisement through SMS has rapidly increased. For this reason the user cannot identify SPAM or HAM resulting the fall under the trap of fraudulent companies. A good text classifier is a classifier that efficiently categorizes large sets of text documents in a reasonable time frame and with acceptable accuracy, and that provides classification rules that are humanly readable for possible fine-tuning. If the training of the classifier is also quick, this could become in some application domains a good asset for the classifier. Many techniques and algorithms for automatic text categorization have been devised. The text classification task can be defined as assigning category labels to new documents based on the knowledge gained in a classification system at the training stage. In the training phase, we are given a set of documents with class labels attached, and a classification system is built using a learning method. Classification is an important task in both data mining and machine learning communities, however, most of the learning approaches in text categorization are coming from machine learning research.

SMS Spam Classifier:

<http://sms-spam-classing.herokuapp.com>



The screenshot shows a web browser window with a single tab titled 'main - Streamlit'. The address bar shows the URL 'sms-spam-classing.herokuapp.com' with a 'Not secure' warning. The page content features a title 'SMS Spam Classifier' in a large, bold font. Below the title is a text input field with the placeholder 'Enter the message'. The input field contains the text: 'Free entry in 2 a weekly comp to win FA Cup final tickets 21st May 2005. Text FA to 87121 to receive entry question(std txt rate)T&C's apply 08452810075over18's'. Below the input field is a red 'Predict' button. The output of the prediction is displayed as the word 'Spam' in a large, bold font. At the bottom of the page, there is a small text that reads 'Made with Streamlit'.

SMS Spam Classifier

Enter the message

Free entry in 2 a weekly comp to win FA Cup final tickets 21st May 2005. Text FA to 87121 to receive entry question(std txt rate)T&C's apply 08452810075over18's

Predict

Spam

Made with Streamlit

Algorithms used in SMS Spam Classifier:

- Multinomial Naive Bayes Classifier
- Random Forest

Python Libraries that are used in SMS Spam Classifier are:

- NLTK (Natural Language Toolkit)
- Scikit-Learn
- Pandas
- Numpy
- Seaborn
- Matplotlib, etc.

Stages to build SMS Spam Classifier:

1. Data Cleaning
2. EDA
3. Text Preprocessing
4. Model Building
5. Evaluation
6. Improvement
7. Website
8. Deploy

1) Data Cleaning

Data cleaning is one of the important parts of machine learning. It plays a significant part in building a model. However, the success or failure of a project relies on proper data cleaning. We will clean messages by removing the unnecessary things.

2) EDA

EDA stands for Exploratory Data Analysis. Exploratory Data Analysis (EDA) is an approach to analyze the data using visual techniques. It is used to discover trends, patterns, or to check assumptions with the help of statistical summary and graphical representations.

3) Text Preprocessing

Text preprocessing involves transforming text into a clean and consistent format that can then be fed into a model for further analysis and learning. Text preprocessing is a method to clean the text data and make it ready to feed data to the model. Text data contains noise in various forms like emotions, punctuation, text in a different case.

4) Model Building

Building an machine learning model requires splitting of data into 3 three sections which are 'Training data' , 'Validation data' and 'Testing data'. You train the classifier using 'training data set', tune the parameters using 'validation set' and then test the performance of your classifier on unseen 'test data set'.

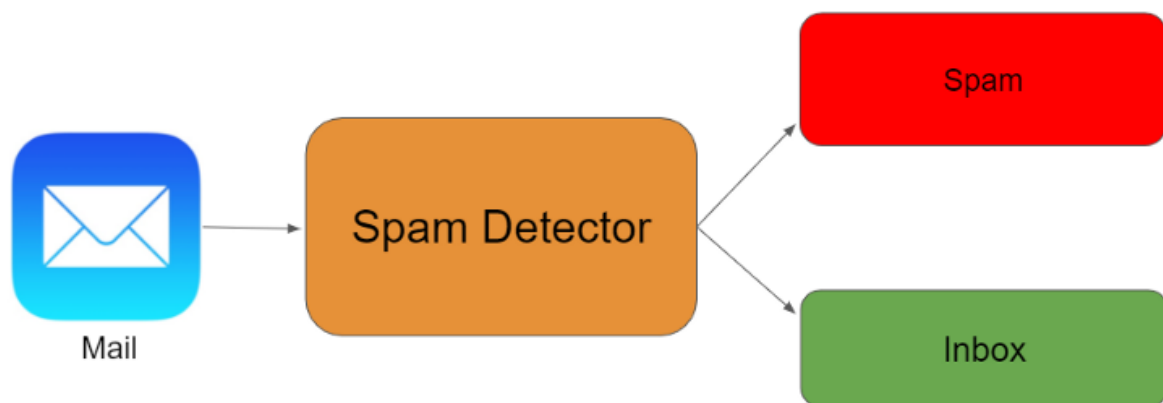
5) Evaluation

Model evaluation is the process of using different evaluation metrics to understand a machine learning model's performance, as well as its strengths and weaknesses. Model Evaluation is an integral part of the model development process. It helps to find the best model that represents our data and how well the chosen model will work in the future.

After evaluation we need to do some improvement if needed and then we will make a website and deployment of model shold be done. Heroku is a platform as a service (PaaS) that enables developers to build, run, and operate applications entirely in the cloud. Heroku is used to deploy our project of SMS Spam Classifier.

SCOPE & OBJECTIVE

Implementing spam filtering is extremely important for any organization. Not only does spam filtering help keep garbage out of email inboxes, it helps with the quality of life of business emails because they run smoothly and are only used for their desired purpose. Spam filtering is essentially an anti-malware tool, as many attacks through email are trying to trick users to click on a malicious attachment, asking them to supply their credentials, and much more. Understanding the problem is a crucial first step in solving any machine learning problem. We will explore and understand the process of classifying emails as spam or not spam. This is called Spam Detection, and it is a binary classification problem. The reason to do this is simple: by detecting unsolicited and unwanted emails, we can prevent spam messages from creeping into the user's inbox, thereby improving user experience.



Emails are sent through a spam detector. If an email is detected as spam, it is sent to the spam folder, else to the inbox.

METHODOLOGY

System Architecture:

The main objective of our approach is to classify the spam SMS messages as soon as it received on the mobile phone, regardless of newly created spam message (zero-hour attack). In this, we firstly collected dataset and finalized the features for our experiment. After finalizing features, we extracted the features from the messages (ham and spam) to create a feature vector.

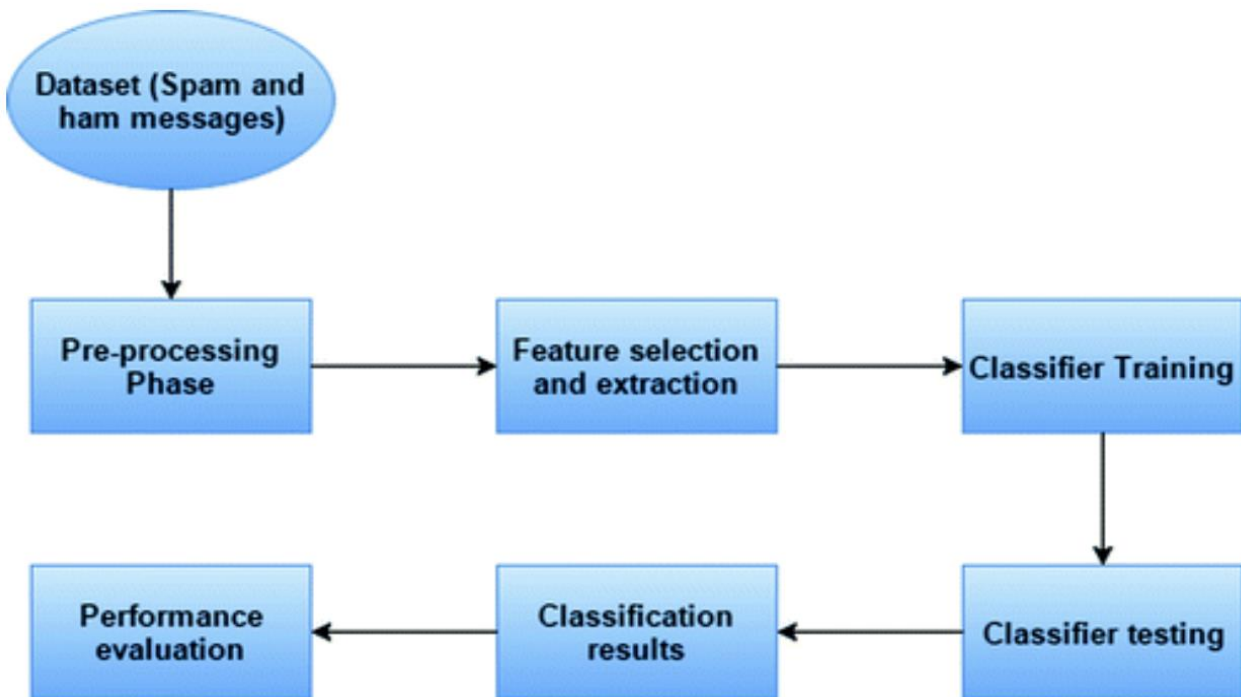


Fig.1 System Architecture

Figure1 shows the system architecture of our proposed approach. In the coaching section, a binary classifier is generated by applying the feature vectors of spam and ham messages. In the testing section, the classifier determines whether or not a replacement message may be a spam or not. At the end we get classification results for different machine learning algorithms and performance is evaluated for each machine learning algorithm such that we can get the best algorithm for our proposed

approach. Feature choice may be a vital task for the SMS Spam filtering. Selected options ought to be correlate to the message sort specified accuracy for detection of spam message are often enlarged. There is a length limit for SMS message and it contains solely text (i.e.no file attachments, graphics, etc.) while in the email, there is no text limit and it contains attachments, graphics, etc. SMS message is usually of two types i.e. ham (legitimate) message and spam message. Fig 1.System Architecture Identification of fine feature that may expeditiously filter spam. SMS messages could be a difficult task. Moreover, we have a tendency to study the characteristics of spam messages exhaustive and notice some options, that area unit helpful within the economical detection of spam SMS.

CONCLUSION

Detection of spam is important for securing message and e-mail communication. The accurate detection of spam is a big issue, and many detection methods have been proposed by various researchers. However, these methods have a lack of capability to detect the spam accurately and efficiently.

To solve this issue, we have proposed a method for spam detection using machine learning predictive models. The method is applied for the purpose of detection of spam. The experimental results obtained show that the proposed method has a high capability to detect spam. The proposed method achieved 99% accuracy which is high as compared with the other existing methods. Thus, the results suggest that the proposed method is more reliable for accurate and on-time detection of spam, and it will secure the communication systems of messages and e-mails. The whole project was divided into several iterations.

Each iteration was completed by completing four phases: inception, where the idea of work was identified; elaboration, where architecture of the part of the system is designed; construction, where existing code is implemented; transition, where the developed part of the project is validated.

FUTURE SCOPE

In the future, we plan to deal with more challenging problems such as the analysis and management of report in spam SMS filters storing. Solution for this problem is another focus of work in the future.

However, there are still some parts that can be improved: for example, adding additional filtering techniques or changing aspects of the existing ones. The changes such as incrementing or decrementing the number of interesting words of the message and reorganizing the formula for calculating interesting rate can be done later.

We introduced Machine Learning concepts for prediction of spam based on the content data like only message content. In future work we can elaborate this topic to prediction by using content and context data like Host address of the SMS, sender, number of times received, URL's in the messages etc.

REFERENCES

- ❖ SMS Spam Collection Data Set from UCI Machine Learning Repository, <http://archive.ics.uci.edu/ml/datasets/SMS+Spam+Collection>.
- ❖ SMS, “Spam collection dataset,” 2019, <https://www.kaggle.com/datasets>.
- ❖ <https://www.ijstr.org/final-print/feb2020/Spam-Detection-In-Sms-Using-Machine-Learning-Through-Text-Mining.pdf>
- ❖ <https://www.ijcsmc.com/docs/papers/June2021/V10I6202102.pdf>
- ❖ <https://ieeexplore.ieee.org/document/9734128/>
- ❖ <https://www.hindawi.com/journals/scn/2020/8873639/>
- ❖ <https://towardsdatascience.com/spam-detection-in-emails-de0398ea3b48>
- ❖ <https://www.kaggle.com/datasets/uciml/sms-spam-collection-dataset>
- ❖ <https://medium.com/analytics-vidhya/sms-spam-classifier-natural-language-processing-1751e2b324ed>
- ❖ https://www.researchgate.net/publication/340607093_An_Effective_Model_for_SMS_Spam_Detection_Using_Content-based_Features_and_Averaged_Neural-Network