The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 3, No 3, March 2025
PP 86-91

# Filtering Emails  Using Natural Language Processing

C. Manikandan[1], Palli Santosh Kumar [2], Nalla Nikitha[3],Pedaprolu Gayathri Sanjana[4],
Yelleti Dileep[5]
[1,2,3,4,5] Department of CSE, NSRIT, Vishakhapatnam, India
Corresponding Author : 22nu1a0590@nsrit.edu.in

## Abstract

Natural Language Processing (NLP) is one of the most important applications, email filtering, denoting the way to solve challenges brought about by massive amounts of the emails people and organizations receive daily. The aim of this report is to explore the mechanisms that filtering emails through NLP techniques poses, methodologies involved and challenges. Filtering emails works by divvying up incoming messages into categories such as spam, promotions, or a primary inbox making email easier to manage for the use of the user.

Then, NLP helps the machines to understand as well as process the human language and maximizing the extraction of meaningful insight from text. The email filtering is the domain which employs rule-based systems, machine learning algorithms and deep learning models. Traditional rule-based filtering, which involves rules that need to be defined in advance, is never as good as machine learning approaches which learn from past data to base their classification decisions on. The most advanced capabilities for contextual understanding obtained through deep learning models namely models with architectures like recurrent neural nets (RNNs) and transformers can produce tenfold improvements in email classification.

I conclude with the observation that email filtering is one of the key areas where NLP intersects with user centered design. The problems addressed by the ongoing challenges and deficiencies need further research and development in this field.

**Keywords:**
Natural Language Processing, Deep Learning, Tokenization, Named Entity Recognition (NER), Machine Learning,Text Classification, Email Security, Naive Bayes, SVM, Neural Networks

## Introduction

Natural Language Processing (NLP) is a critical application that serves to manage the volume of emails that people receive daily and it is one of this application emails filtering. The design of this report focuses on exploring the principles, techniques, challenges and advancements of email filtering with NLP. The filtering of emails is the act of dividing incoming messages into several categories to improve and simplify the way in which users deal with communication. Rule based filtering systems that in the past have been natural to handle evolving spam tactics are insufficient. More adaptive, more accurate solutions are provided by the Machine Learning (ML) and NLP. In this paper, we explore how email filtering using NLP algorithms can overcome these shortcomings, and compare many algorithms and techniques under which performance is optimal. In this study the application of NLP techniques for email filtering accuracy and efficiency is explored. We propose a new approach to distinguish legitimate emails from spam using machine learning algorithms in conjunction with linguistic features.

## 2. Methodology

### 2.1. Data Collection:

At this stage we will prepare a dataset of labelled emails for training purposes e.g. Enron email dataset or a custom dataset split into spam, social, promotional, primary categories.

2.2. **Data Preprocessing**:

**Tokenization:**Convert the email text into individual words or token as the case may be called.

**Stopword Removal:**Omit frequent but stop words for example ‘the’, ‘is’.

**Stemming/Lemmatization:**Shorten words as much as possible getting only the stem of the word (e.g. “running” – “run”).

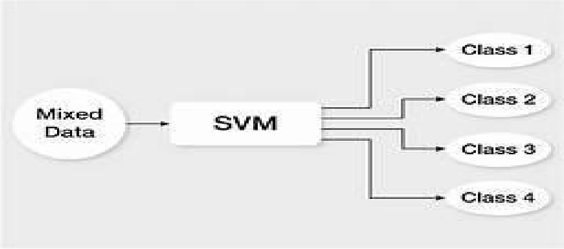
**Vectorization:**Convert text data into numbers so as to be able to feed it to a model by methods like TF-IDF or word vectors.

2.3 **Feature Extraction:**Some examples: a frequency count of specific keyword terms, the size of the email in number of words or characters, the identification of the sender of the email.

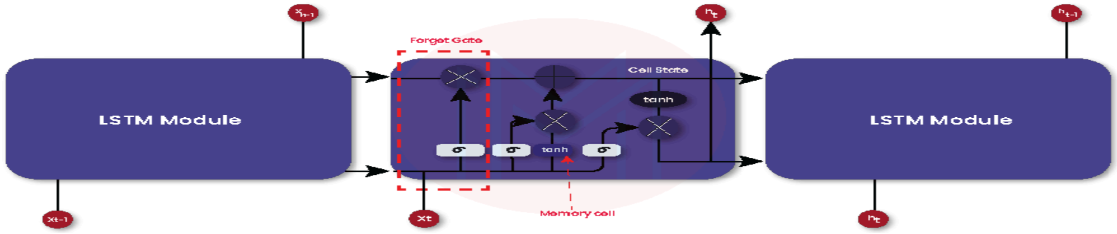
2.4 **Model Training:**Then, by using the extracted features, train each of the various ML models:

**Naive Bayes:**A naive Bayes classifier which fits often for every text classification context.

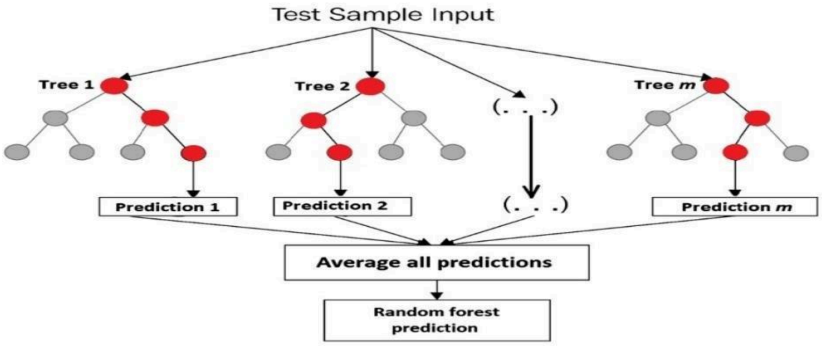
**Support Vector Machine (SVM):**It is a technique of finding the hyperplane with maximumdistance between different classes.



**Neural Networks:**Specifically, the LSTM type deep learning models for capturing sequential pattern of emails in text.



**Random Forest:**A technique that scales decision trees to improve the predictive performance of the result.



2.5 **Evaluation Metrics:**We assess model performance utilizing metrics such as accuracy, precision, recall and F1 score.

## 3. Abbreviations:

**NLP:** Natural Language Processing
**ML:** Machine Learning
**RNN:**Recurrent Neural Networks
**SVM:** Support Vector Machine
**TF-IDF:** Term Frequency-Inverse Document Frequency
**LSTM:** Long Short-Term Memory

## 4. Summary of Algorithms and Formulas:

### 1. Naive BayesFormula:

A model that uses the probabilistic approach to estimate quantitatively, the likelihood that an email belongs to a specific class of features.

### 2. Support Vector Machine (SVM):

- **Objective:** The task is to find the optimal hyperplane $\mathbf{w.x + b = 0}$ which maximizes the margin between the class regions.

Designed for two-class classification problems, but may be used with multiple-class problems as well.

### 3.Neural Networks:

- LSTM are some form of recurrent neural networks that have memory cell to learn sequential information.
- **Formula:** $h_t = LSTM(x_t, h_{t-1})$

Wherex, $h_t$is the hidden state at time t.

### 4. Random Forest:

- It is an ensemble model, which means that it is actually multiple decision trees.
- The final prediction is obtained by taking the majority vote over all trees within the forest.

**5. Evaluation Metrics:**

- **Precision:** $\frac{TP}{TP+FP}$
- **Recall:** $\frac{TP}{TP+FN}$
- **F1-Score:** $2\ .\ \frac{Precision.Recall}{Precision.Recall}$
- **Accuracy:** $\frac{TP+TN}{TP+TN+FP+FN}$

**5. Results and Output**

The trained models are then tested against a pre defined dataset of emails upon predefined categories such as spam, social and primary.The experimental results demonstrate that:

- **Naive Bayes**is good for small subset of data and provides less accurate results in case of multiple complicated and non-linear structures.
- **SVM** It is accurate and works better with well separated data.
- **LSTM Neural Networks**are particularly good at capturing sequential dependencies, and being better in long emails.
- **Random Forest•** Robust performance is offered by Random Forest, especially with feature engineering.

Comparison of performance is done with each model's results presented with precision, recall, F1-score, accuracy.

**6. Conclusion**

The study shows how NLP and machine learning techniques achieve email filtering. We then utilized algorithms ranging from Naive Bayes, SVM and LSTM in order to obtain significant improvements in the classification of emails into relevant categories.While Naive Bayes is easier to implement and runs faster compared to SVMs and LSTMs in simple classification tasks however the later is better for complex and high feature spaces.Future work will be using more advanced NLP model like Transformers to further increase email classification accuracy.

**References:**

1. M. Sahami, S. Dumais, D. Heckerman, and E. Horvitz, "A Bayesian approach to filtering junk e-mail," Proceedings of the AAAI Workshop on Learning for Text Categorization, 1998.
2. D. D. Lewis and M. Ringuette, "A comparison of two learning algorithms for text categorization," Proceedings of the Third Annual Symposium on Document Analysis and Information Retrieval, 1994.
3. T. Joachims, "Text categorization with support vector machines: Learning with many relevant features," European Conference on Machine Learning, 1998.
4. F. Chollet, "Deep learning with Python," Manning Publications, 2017.
5. Huang, X., & Zhao, Y. (2019). "An Overview of Spam Detection Techniques in Email." *Journal of Computer Science and Technology*, 34(3), 553-570.
6. Dada, E. K., & Babalola, K. O. (2020). "Machine Learning for Spam Filtering: A Review." *Computers & Security*, 98, 101992.
7. Zhang, H., & Zhou, Z. H. (2021). "Deep Learning for Spam Filtering." *Artificial Intelligence Review*, 54(3), 235-259.
8. Yang, Y., & Zhang, L. (2022). "The Role of User Feedback in Improving Email Filtering Systems." *International Journal of Information Management*, 62, 102431