Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 9s (2025)

Email Spam Filtering Model with the Machine Learning Models

Dr Swapna Siddamsetti[1], Dr Purude Vaishali [2], K.J.Archana[3], Sure Mamatha[4], D Deepthi Reddy[5]

[1,2,3] Department of CSE, Neil Gogte Institute of Technology, Uppal, Hyderabad, Telangana 500039, India,

[4] Department of CSE, HITAM, Gowdavelly, Medchal-Malkajgiri (Dist.) – 501401. Telangana. India.

[5] Research scholar, Department of CSE, GITAM University, Hyderabad, Telangana 502329 , India.

Article History:

Received: 12-01-2025

Revised: 15-02-2025

Accepted: 01-03-2025

Abstract:

The increase in the volume of the unrequired emails which can be termed as the spam has started an issue for the development or implementation of the model for detecting the spam emails and named as the anti-spam filters. The various Machine learning models or the algorithms can be used for the success full detection of the spam emails. In this paper we will present the systematic approach of some of the best machine learning model based email spam filtering techniques. After implementing these models we will propose a bet model for the spam filtering as per the accuracy of the algorithm. We first discuss about the importance of the machine learning algorithms and various models suitable for the spam filtering. Then with the help of the dataset we will implement all the algorithms and finally proposed the best algorithm according to the results like high accuracy. Finally the results of all the suitable algorithms are presented in the paper. Then conclude and propose the best algorithm.

Keywords: Anti-Spam Filters, Machine Learning Models, Spam Filtering

1. Introduction

In our daily life due to the high usage of the technology and dependency on the network the chance of growing cyber-crimes can be considered as the borderless crimes. The different types of users over the internet like the government applications, different organizations, and the individuals are affected rigorously by this [1]. One of the problems faced was regarding the emailusers who receives different types of mails, which also includes the spam mails flooded into the inboxes.All the organizations and the individuals communicate through the electronic mails for various requirements and business communications. Now a days, the spam email became an issue for the email users and also attacks the system with the malicious links and data. Spam mails will be attractive and make the users to click on them to attack the systems,these may also include the commercial links of the famous websites [2]. Now the trend is only with the Machine learning as it plays an important role for avoiding the cybercrimes and provides the cyber security [3].It is one of the worldwide services linked problem connected to the email services. It consists of the unnecessary emails and does not have the required receiver, and generated due to many reasons, starting from the marketing to the scams which leads to the fraud [4,5]. As per the analysis in the year 2009, approximately 97% of the received and the sent emails have been categorized as spam mails. Therefore, in these modern era, the concentration have to be provided in this identification of the spam mails or emails have to be classified into the ham mails and spam mails.

Spam can be defined as the junk mail or the unwanted mail which has been sent to the user's inbox. This became the threat which has to be considered as the severe over the society and the internet [6]. These spam mails will cause the internet and the mail users to face various security problems and the improper, illegal issues. In additional to these issues, the valuable resources like productivity, network bandwidth, also the storage was wasted due to the spam mails [8]. Hence, there exists demand for the application of spam filtering model [7]. All the researchers are working for the generation of the accurate results for the spam detection but there was not an appropriate model for the spam detection. The spammers are sending many varieties of the messages without any costforthe specific botnets, malware which are harmful, and the various campaigns on spam mails [8,9]. Hence,the model for the detection is used for the identification of the fraudulent messages and the unsolicited mails which are affectingthe various benefits provided by the various emails.

The model for the Spam detection will consists of the comparison of the non-spam mails and the malicious spam mails, to stop receiving of the spam mails into the inbox of the email users which helps tostop theflow of the spam mail which are received by the user'sinbox [10,11]. The first phaseof this model is the filtering process in which the spam mails are detected to prevent the junk and unwanted mails from the inbox. These spam filters will recognize the spam emails by analysing the content of the data with the additional information about the mail [12]. In early stage, the spam filters will be implemented on the result of the blacklists which are recognized as the spammers, then the keyword filtering is implemented and the user-defined rules are grouped together to form the model which is based on the blacklists of the recognizedspammers, keyword-based filtering, and also with the user-defined rules of the group [13,14]. Furthermore, these specific methods have to be continuously updated and regular maintenance have to be monitored as these suffers from the ineffective and time-consuming problems.2.Proposed Model:

In the proposed model we will detect the mails with the help of different machine learning approaches and finally we will propose the machine algorithm whose accuracy is high and the detection of the spam mails are more. We will start the model by collecting the appropriate dataset for the spam detection and them we will implement the feature extraction through which we can remove the unwanted data like not related to the spam or ham mails. Then we can use different machine learning models for classifying the mails into spam mails or ham mails. Before that we will implement the label encoding for the mails with zero and one to train and test the dataset.

3.Related Work

Classification:

The important part of our proposed work is the Classification module. In this module we will use the four different classifiers likeNaïve Bayes Algorithm [15], Random Forest Algorithm [16], Decision Tress Classifier and the K-Nearest Neighbour algorithm which are used to classify all the available emails into the spam mails or the ham mails. The selected dataset will be split into two parts like 80% for training which can be named as thetraining dataset and the another 20% for testing which can be named as the testing dataset. The Classification algorithms likeNaïve Bayes Algorithm, Random Forest Algorithm, Decision Tress Classifier and K-Nearest Neighbour algorithmare built for the dataset training.

4. Implementation and Experimental Study

The basic performance of all the above mentioned classification algorithms will be computed with the various parameters and metrics like precision value, recall value, F-score value and the support. Finally, the Confusion matrix will be used for compute all the required measures. The four values likethe True Positive value, the True Negative value, the False Negative value and the False Positive value can be defined as below which can be helpful to generate the Confusion matrix.

TN (True Negative) will specifythe count of the specified ham emails which have beencorrectly classified as the ham mails.

TP (True Positive) will specify thecount of the specified spam emails which have beencorrectly classified as the spam mails.

FN (False Negative) will specify thecount of the specified spam emails which have been classified as the ham mails.

FP (False Positive) will specifythe count of the specified ham emails which have beenclassified as the spam mails.

Precision value will specify the relationship among the true positivesvalue,the predicted positivesvalue whereas the recall valuewill define the ratio calculated from the derived true positive values over the completepositive values. The value for Precision will determines the accuratepercentage value of the spam emails which are actually predicted as the spam mails among all the predicted positive values. Recall valuewill determine the percentage of the spam emails which are actually predicted as the spam mails among the total number of the spam emails which are predicted as the ham and the spam.

Precision value = count of spam emails which are classified as spam / total count of positive predictions.

Recall value = count of spam emails which are classified as spam / sum of True Positive and The False Negative.

Precision value and the Recall value are the important measure for the classification algorithm. But the Accuracy value may not be always suitable for measuring the email dataset when the dataset belongs to skewed.[16]

The dataset was taken from the email which consists of 3002 emails with four attributes. Then the Unnecessary columns were removed. Thenall the labels of the “spam” and the “ham” are named as 1,0 respectively. The Pre-processing methods are implemented to remove the special characters, the stop words, the numerals. Then the classification algorithms are implemented.[18]

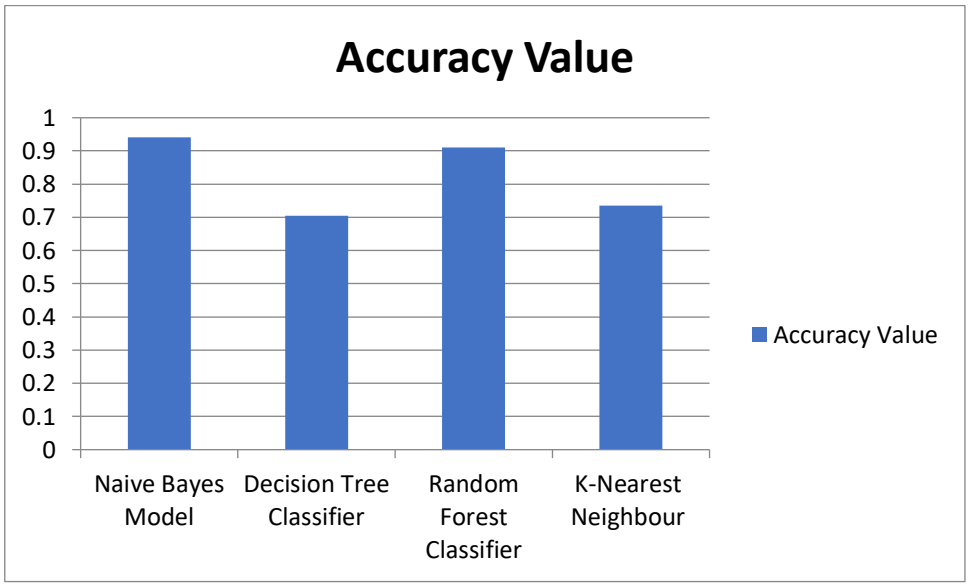
5. Results and Discussions

In the first experiment we have used the Naive Bayes Classifier for the spam detection and calculated the accuracy, then we implemented with Random forest classifier algorithm which resulted in the better performance compared to the Naïve Bayes Classifier, and also implemented with the other algorithms like K-Nearest Neighbour algorithm and Decision Tree Classifier .

The results are depicted in the below table:

S.No	Name of the Algorithm	Accuracy Value
1	Naive Bayes Model	0.941
2	Decision Tree Classifier Algorithm	0.705
3	Random Forest Classifier Algorithm	0.911
4	K-Nearest Neighbour Algorithm	0.735

According to the above table we can conclude that the Naïve Bayes algorithm will be better model for the spam detection as the accuracy of this algorithm is high compared to the other implemented algorithms.



The above results can be represented as the graph which depicts that the accuracy of the Naïve Bayes Model was optimum.

6.Conclusion and Future Scope

After analysing the results we can conclude the best machine learning algorithm for the spam detection was Naïve Bayes Classification algorithm. The further research can be implementation of the spam detection within the images, as there may be the images in the spam mails. This will be useful for providing the security for the mail users by detecting any type of the messages which are harmful to the user.

7.References

[1] V. Krishnamurthy, Internet spam threats and email exploitation – A scuffle with inbox attack.
[2] K. Renuka and T. Hamsapriya, Email classification for spam detection using word stemming, Int J Compute Appl 5(5) ,(2010), 45–47.

[3] S. Mali Patil, V. Maheshwari and M.B. Chandra, Area optimization of CMOS full adder design using 3T XOR, in:2020 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET) IEEE, 2020, pp. 192–194. doi:10.1109/WiSPNET48689.2020.9198627
[4] W.A. Awad and S.M. ELseuofi, Machine Learning Methods for Spam E-Mail Classification.
[5] E. Ezpeleta, U. Zurutuza and J.M.G. Hidalgo, A study of the personalization of spam content using Facebook publicinformation, Logic Journal of the IGPL 25(1) (2017), 30–41. doi:10.1093/jigpal/jzw040.
[6]A.M. Al-Zoubi, H. Faris, M.A. Hassonah et al., Evolving support vector machines using whale optimization algorithmfor spam profiles detection on online social networks in different lingual contexts, Knowledge-Based Systems 153 (2018),91–104. doi: 10.1016/j.knosys.2018.04.025.
[7]S. Günal, S. Ergin, M.B, Gülmezoglu and Ö.N. Gerek, On feature extraction for spam E-mail detection, in: ˇ International Workshop on Multimedia Content Representation, Classification and Security, 2006, pp. 635–642. doi:10.1007/11848035_84.
[8] A. HamdanMohammad and R. AbuZitar, Application of genetic optimized artificial immune system and neural networksin spam detection, Applied Soft Computing 11(4) (2011), 3827–3845. doi: 10.1016/j.asoc.2011.02.021.
[9] W.Z. Khan, M.K. Khan, F.T. Bin Muhaya, M.Y. Aalsalem and H. Chao, A comprehensive study of email spam botnetdetection, IEEE Communications Surveys & Tutorials 17(4) (2015), 2271–2295. doi:10.1109/COMST.2015.2459015.
[10] G. Jain, M. Sharma and B. Agarwal, Spam detection in social media using convolutional and long short-term memoryneural network, Annals of Mathematics and Artificial Intelligence 85 (2019), 21–44. doi:10.1007/s10472-018-9612-z.
[11]V. Patidar, D. Singh and A. Singh, A novel technique of email classification for spam detection, International Journal ofApplied Information Systems 5(10) (2013), 15–19. doi:10.5120/ijais13-450976.
[12]T.S. Guzella and W.M. Caminhas, A review of machine learning approaches to spam filtering, Expert Systems with Applications 36(7) (2009), 10206–10222. doi:10.1016/j.eswa.2009.02.037.
[13]G. Mujtaba, L. Shuib, R.G. Raj, N. Majeed and M.A. Al-Garadi, Email classication research trends: Review and openissues, IEEE Access 5 (2017), 9044–9064. doi:10.1109/ACCESS.2017.2702187.
[14] H. Shen and Z. Li, Leveraging social networks for effective spam filtering, IEEE Transactions on Computers 63(11)(2014), 2743–2759. doi:10.1109/TC.2013.152.
[15]Eman M.Bahgat Sherine Rady Walaa GadIbrahim F.Moawad "Efficient email classification approach based on semantic methods" 2018 Ain Shans Engineering Journal.
[16]Deepika, M., Hegde, N.P. (2022). Efficient Email Classification Algorithm for Better Customer Support. In: Satapathy, S.C., Bhateja, V., Favorskaya, M.N., Adilakshmi, T. (eds) Smart Intelligent Computing and Applications, Volume 2. Smart Innovation, Systems and Technologies, vol 283. Springer, Singapore. https://doi.org/10.1007/978-981-16-9705-0_22
[17]Rathod, Sunil &Pattewar, Tareek. (2015). Content based spam detection in email using Bayesian classifier. 1257-1261. 10.1109/ICCSP.2015.7322709.
[18]Deepika, M., Hegde, N.P. (2021). Framework for Spam Detection Using Multi-Objective Optimization Algorithm. In: Satapathy, S.C., Bhateja, V., Favorskaya, M.N., Adilakshmi, T. (eds) Smart Computing Techniques and Applications. Smart Innovation, Systems and Technologies, vol 225. Springer, Singapore. https://doi.org/10.1007/978-981-16-0878-0_34