Spam Email Classifier with Voice Notes

N Pavitha, Darshan Bachhav, Amrut Bhagwat, Ankit Singh and Aditya Kirar

June 4, 2022

Spam Email Classifier with Voice Notes

Pavitha. N, Darshan Bachhav, Amrut Bhagwat, Ankit Singh, Aditya Kirar

Vishwakarma Institute of Technology, Pune, Maharashtra, India

Abstract— **A large portion of the population nowadays relies on readily available email or texts from strangers. Because anyone can send an email or leave a note, spammers have a perfect opportunity to write spam messages concerning our various interests. Spam clogs up your inbox with a barrage of absurd emails. Degrades our internet speed significantly. Takes vital information, such as our contact information from our contact list. Identifying these spammers, as well as the spam content, maybe a time-consuming and difficult operation. Spam email is a method of sending messages in mass through email. Because the recipient bears the majority of the cost of the spam, it is postage owing to advertising. Spam email has become a type of business communication.**

Keywords— Naïve Bayes, machine learning, python frame,sci-kit learn, pandas, NumPy.

I. *INTRODUCTION*

Since the last decade or so, emails have been the primary way of communication especially among professionals and for job-related communication and interactions. The importance of emails in everyone's daily lives is something that can't be ignored now. One of the main problems with email communication is spam emails or unsolicited emails that have no relevance to professional, well-kept emails[2]. They often flood the inboxes and can cause a lot of problems including clogging of emails and human errors such as missing important emails between all the spam that inboxes receive. Hence it is quite essential to be able to classify between spam emails and actual relevant emails and segregate them accordingly to help maintain professionalism as well as increase the efficiency of communication through emails especially when it's being done on such a large scale[1]. Let's have a brief look at what exactly is meant by spam and ham mail. Spam emails are generally the malicious emails that are sent in bulk through mailing lists, newsletters etc that are generally sent with a commercial nature. Along with that, it can also be personalised emails that are sent about job offers, education offers etc. There is no clear definition as such of spam emails and hence it is also quite hard to accurately classify between the mail is spam or ham.

After the classification of the emails, the ones that are positively spam are to be segregated. This can be done in two ways[1]. The first one is at the individual user level and is probably better in terms of quality but worse in terms of efficiency. This can be done by making software that can be installed on the user's computer and will then interface with the mail service being used and then carry out the segregation of spam and not spam from the inbox.

The other way is it can be done at an enterprise level. This is the opposite of the first in terms of efficiency and quality[8]. We say it's lower in quality as the system needs to be generalised a lot so that it is widely applicable and hence there is no room for personalisation. The software should be installed on the mail servers themselves, then it will interface with the system and classify emails as they are received.

For the model to work properly it needs to be trained with proper data sets of spam as well as legitimate emails and then based on the scoring of the model, further classify the test sets and check whether they are properly being classified[6]. For the scoring, different machine learning algorithms can be used with the support vector machine being the most dominant one in this case.

To implement a machine learning classification model using python and its libraries. This model will differentiate whether the message is spam or not and will tell us in the form of voice commands[3]. The use of various algorithms is made while implementing this project model.

II. *LITERATURE REVIEW*

[1] M.RAZA, N. D.Jayasinghe and M. M. A. Muslam, This paper is a survey paper or a kind of review paper on the subject of spam email classification. It explains the various machine learning algorithms that are s used to achieve the same as well as gives a broad overview of the topic and the classification algorithms used to sort the unsolicited spam emails that are received. Mainly it goes in-depth in support vector machines further in the paper as it is the most relevant and useful tool to classify the emails.

[2] N. H. Marza, M. E. Manaa and H. A. Lafta. This paper is the implementation of the email classifier using deep learning instead of machine learning. This is not entirely relevant to the scope of this project but it was still quite interesting and informative to refer to as the fundamentals of the project are still the same.

[3] Clement, J. This is a citation from the company Statista. Statista is a database company and has all various forms of data stored, collected and processed to conclude it. This is about the total email traffic all around the world. It judges the total amount of spam based on some of the sample data collected and that survey estimation is considered here and cited in the introduction.

[4] Saad, Omar, Ashraf Darwish, and Ramadan Faraj. This paper is similar to most of its others but it does bring up some unique and really good points such as the fact that the spam emails subject is always changing and hence it needs to be a dynamic system that changes and can catch all the spam emails no matter how much its contents change. Another interesting point is that the algorithms used can not give any false positives. This is because a lot of important communication is done through emails and any false positives can lead to the loss of important emails and can have severe consequences. This is mainly about the OCR based spam classification systems and hence also specifies some specific problems pertaining only to such systems.

[5] Sathya, Ramadass, and Annamma Abraham. This paper is about the differences between supervised and unsupervised machine learning algorithms and specifically, their use in pattern recognition and classification. Spam email classification is also essentially a kind of pattern classification and hence it is relevant.

[6] M. A. Hassan and N. Mtetwa. This paper is also similar to other papers mentioned but it also focuses on feature extraction along with the classification of spam emails.

[7] Alamlahi, Yahya, and Abdulrahman Muthana. It focuses mainly on the implementation of neural networks for the implementation of the spam classifier, It is quite extensive and an excellent in-depth review on the subject.

[8] F.Wei, H.Qin, S.Ye and H. Zhao. This paper focuses on the text classification in a specific document. This is also the main tool that we are going to implement in our project hence this was an excellent paper to refer to and gave a lot of insight on the stuff that is and is not possible using text-based classification.

III. *Methodology/Implementation*

This project is implemented using Various Machine Learning Concepts and libraries like sci-kit-learn, pandas, and NumPy are used. win32com library is one of the APIs available in python. It provides various methods and one of them is the Dispatch method. It when passed with the argument of SAPI.SpVoice. The dataset here used is taken from Kaggle, this dataset contains spam and ham messages. Firstly the data set is trained and the accuracy we got is 97%. For the voice notes, the above-mentioned libraries and arguments are used, they tell us whether the message is spam or not through voice notes. The classification model is predicted using the Naive Bayes algorithm classifier which is one of the significant machine learning algorithms.

For the frontend, part python frame is used. In that frame, various geometrical attributes are used for the layout and designing the frame.

Machine Learning Techniques

Naïve Bayes Algorithm

The Naïve Bayes technique/algorithm depends on the Bayes theorem. Probability distribution,Strong independence, and the ability to handle enormous datasets are all aspects of the statistical machine learning-based technique. The probability distribution is calculated in NB using the dataset's frequency distribution. The Bayes decision rule is used to assign a class in the classification problem. The classifier selects the class with the highest posterior probability number, according to the Bayes decision rule. It is possible to calculate the posterior probability by using

$$P(Y \mid X) = \frac{P(X \mid Y)\, P(Y)}{P(X)}$$

Here X represents any feature vector set (X1, X2, X3,....Xn) and y represents a class variable with m potential results (Y1, Y2, Y3,……..Yn). P(Y | X) is the posterior probability, and the term P(X| Y) is the class on which the term P(Y | X) depends. The value of P(X) depends on the known feature variables and the P(Y) is the probability value.

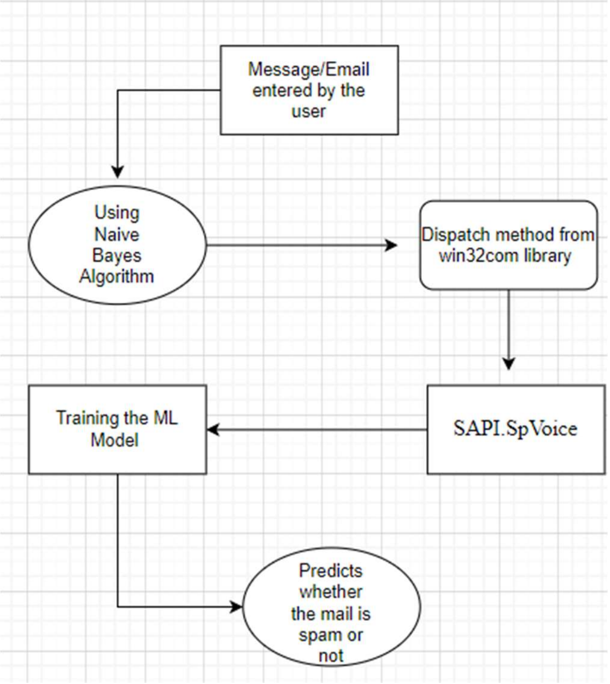
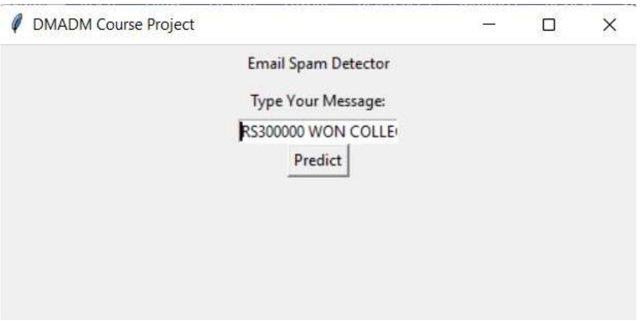

Message/Email entered by the user
Using Naive Bayes Algorithm
Dispatch method from win32com library
SAPI.SpVoice
Training the ML Model
Predicts whether the mail is spam or not

Fig 1: Flow of the project

V. Result and Discussion

1] User can see whether the message/email is spam or ham with a single click.
2] Generally spam mail classifiers don't have a voice feature in it but in this project, we have added this feature too which makes it unique.
3]Accuracy of the model came out to be 97%.



Email Spam Detector

Type Your Message:

RS300000 WON COLLE

In future, we can deploy this model in many commercial industries where it will become easy to classify messages and filter them. Also, Gmail can add a voice feature into their system instead of a special spam folder. Users can be misguided which can turn into phishing. So these classification models should be deployed in sensitive and confidential systems which can prevent such malicious things.

Here, is the SAPI.SpVoice is combined with the machine learning prediction result to show the computerized voice output. CountVectorizer library of python is used to transform the given dataset into a vector which is stored in spam.pkl file and vectorizer.pkl.

VII.CONCLUSION

Due to rising cyberbullying, cybercrime and spammers, email spam has become one of the most serious commercial problems. To detect email spam, several authors have used different approaches with testing on different datasets. In the future, the Naive Bayes algorithm/classifier might be used with any other such algorithm as the ant colony optimization, artificial bee colony optimization algorithm, swarm optimization notion algorithm or the firefly algorithm. To improve the findings, even more, the Naive Bayes technique might be replaced with any alternative machine learning-based algorithm.

VI.REFERENCES

[1] V. S. Vinitha and D. K. Renuka, "Performance Analysis of E-Mail Spam Classification using different Machine Learning Techniques," 2019 International Conference on Advances in Computing and Communication Engineering (ICACCE), 2019, pp. 1-
[2] M. Singh, R. Pamula and S. k. Shekhar, "Email Spam Classification by Support Vector Machine," 2018 International Conference on Computing, Power and Communication Technologies (GUCON), 2018, pp. 878-882.

[3] M. RAZA, N. D. Jayasinghe and M. M. A. Muslam, "A Comprehensive Review on Email Spam Classification using Machine Learning Algorithms," *2021 International Conference on Information Networking (ICOIN)*, 2021, pp. 327-332.

[4] P. V. Raja, K. Sangeetha, G. SuganthaKumar, R. V. Madesh and N. K. K. Vimal Prakash, "Email Spam Classification Using Machine Learning Algorithms," *2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS)*, 2022, pp. 343-348.

[5] M. K. and R. Kumar, "Spam Mail Classification Using Combined Approach of Bayesian and Neural Network," *2010 International Conference on Computational Intelligence and Communication Networks*, 2010, pp. 145-149.

[6] G. Mujtaba, L. Shuib, R. G. Raj, N. Majeed and M. A. Al-Garadi, "Email Classification Research Trends: Review and Open Issues," in *IEEE Access*, vol. 5, pp. 9044-9064, 2017.

[7] N. Kumar, S. Sonowal and Nishant, "Email Spam Detection Using Machine Learning Algorithms," *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)*, 2020, pp. 108-113.

[8] S. K. Trivedi, "A study of machine learning classifiers for spam detection," *2016 4th International Symposium on Computational and Business Intelligence (ISCBI)*, 2016, pp. 176-180.

[9] P. V. Raja, K. Sangeetha, G. SuganthaKumaV.Madesh and N. K. K. Vimal Prakash, "Email Spam Classification Using Machine Learning Algorithms," *2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS)*, 2022, pp. 343-348.

[10] L. Duan, A. Li and L. Huang, "A New Spam Short Message Classification," *2009 First International Workshop on Education Technology and Computer Science*, 2009, pp. 168-171.

[11] D. K. Renuka, T. Hamsapriya, M. R. Chakkaravarthi and P. L. Surya, "Spam Classification Based on Supervised Learning Using Machine Learning Techniques," *2011 International Conference on Process Automation, Control and Computing*, 2011, pp. 1-7.

[12] N.Govil,K. Agarwal,A.Bansal and A. Varshney," A Machine Learning based Spam Detection Mechanism,"2020 *Fourth International Conference on Computing Methodologies and Communication (ICCMC)*,2020,pp. 954-957. *Methodologies and Communication (ICCMC)*,2020,pp. 954-957.

[13] M. V. C. Aragão, I. C. Ferreira, E. M. Oliveira, B. T. Kuehne, E. M. Moreira and O. A. S. Carpinteiro, "A Study and Evaluation of Classifiers for Anti-Spam Systems," in *IEEE Access*, vol. 9, pp. 157482-157498,2021.

[14] S. E. Rahman and S. Ullah, "Email Spam Detection using Bidirectional Long Short Term Memory with Convolutional Neural Network," *2020 IEEE Region 10 Symposium (TENSYMP)*, 2020, pp. 1307-1311.

[15] A. AlMahmoud, E. Damiani, H. Otrok and Y.Al-Ha-Mmadi, "Spamdoop: A Privacy-Preserving Big DataPlatform for collaborative Spam Detection," in *IEEETransactions on Big Data*, vol. 5, no.3,pp. 293-304,1 Sept. 2019.