An Efficient Email Spam Detection using Support Vector Machine

K sai Prasanthi, T Deepika, S Anudeep, M Sai Koushik

***Abstract:** This research paper proposes the electronics mail is small known as E-mail is used for communication between the people to person. E mail is providing as an necessary contribution for messaging by internet. Spam e mails are the unwanted messages that arise in high volume and are used by spammers for revealing users personal credentials. These e mails are regularly some sort of company/control announcement or viruses that the user receive without any notification. So as to defeat it, there need aid exactly existing frameworks that still don't keep them from striking. Therefore, there is a require should manufacture and proficient framework that adequately detects and more keeps the spam messages In those server utilizing the Naïve bayes classifier. Naïve bayes classifier is a mainstream statistical classifier utilized fundamentally for content arrangement.*

***Keywords:** Ham, SVM classifier, Naïve bayes classifier, Email, Spam*

I. INTRODUCTION

Email messages have now become a part of routine life with its increasing popularity and the flexibility it provides during communication. Earlier, emails were intended only for text messages, but now it permits us to send multimedia messages that include images, video, audio, etc. An email constitutes of 3 components: header, body and attachment. The header encompasses the sender address, recipient address and subject. The body consists of the message. The attachment may consist of documents, images, audio or video file. With the escalation of internet and vast use email there is an increase in the rate of spam messages. Spam is usually unwanted, uninvited or unprompted messages. Hackers, phishers and attackers usually try to send these messages in order to obtain the personal details of the users.

The details can include credit card number, passwords, account numbers and other private information that needs to be kept confidential. There are several existing techniques that checks whether the mail is spam or ham (dedicated message): black list/white list, Mail Header checking, Signatures. White list is a list that comprises of email address or domains that the user is aware of. An advantage is that it includes an automatic whitelist management tool which adds the addresses that the user knows into the list automatically. The blacklist is contradictory to white list. It is a list that comprises of addresses that is user is unaware of. These mails will be declared as junk mails and will be transferred to the spam folder. Mail Header Checking is the simple approach wherein the rules are specified. These rules are later matched with mail headers. In signature approach a hash value is generated that is unique for each spam email message that is later compared with the next incoming email values. These approaches do not correctly detect and filter spam mails and may leave residues that affect the users.

Email Filtering/Spam Filtering:

On recognize spontaneous and useless email and more stop the individual's useless messages from attainment on clients inbox is called spam filter. Those spam filter may be a project in different sorts from program project takes a gander for certain criteria for which it bases judgments.

The information from filtering email software product will be messages. Those message through unaltered for conveyance of the user's mail box will be the yield about email filter. A portion of the mail filters have the capacity will alter messages throughout preparing. Mail filters bring varying degrees about configurability. Distinctive times, key expressions in the message body need aid utilized, alternately perhaps the email location of the sender of the message. Exactly additional moved channels, particularly dangerous to spam mail. Picture filtering could similarly a chance to be used that use complex picture examination calculations will recognizing skin-tones and more specific figure shapes regularly associated with foul portraits. Mail filters can make presented by those client, whichever concerning illustration autonomous tasks (see interfaces underneath), alternately as a real perspective about their email one task (email client).On email programs, customers could aggravate individual, "manual" channels that at that point regularly channel mail as shown toward the picked criteria. Practically email tasks not withstanding similarly need a programmed spam dividing ability. Organize right suppliers can similarly present mail channels for their mail trade operators likewise a help of the more terrific and only their customers.

Naïve Bayes classifier is a simple and efficient method that requires fewer amounts of data sets for training the machine. A model has been proposed that classifies in the server machine, whether the incoming email is ham or spam before it reaches the client machine. The rest of the paper is organized as follows. In section II, we give a brief summary of various existing work done.

Revised Manuscript Received on December 30, 2019.
* Correspondence Author

K Sai Prasanthi*, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India.

T Deepika, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India.

S Anudeep, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India.

M Sai Koushik, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India.

In section III, different classifiers are discussed and the importance of NaïveBayes classifier is specified. In section IV, a model has been proposed that will detect and prevent the spam mails using the Naïve Bayes classifier. Each and every step involved in the system has been briefly explained here.

II. LITERATURE SURVEY:

Web spam which will be a significant issue all around today's web quest tool; Thus it may be paramount for web crawlers with have the ability with identify web spam amid creeping. The order models are intended by machine learning in request algorithm.[2] Those you quit offering on that one machine learning in algorithm is Naïve bayesian classifier which is utilized for [1] with separate those spam and non-spam mails. Enormous information breaking down which is also framework to spam identification. Extricating that inclination starting with a message may be a technique to get that important information.

In machine learning in innovations can get starting with the preparation datasets moreover suspect the decision making schema subsequently they need aid comprehensively used likewise and only inclination request for the exceptionally precision for schema. [3].

Practically of the examination worth of effort need now been conveyed out looking into moving forward those effectiveness furthermore precision from the Naïve bayesian approach. Paul Graham’s Naïve bayesian machine taking in approach is used to move forward that effectiveness for bayesian methodology. The scrutinize worth of effort need additionally conveyed out to build the precision and accuracy and time efficiency about framework.

The most majority of the research work in need officially was conveyed crazy ahead enhancing the effectiveness and precision and accuracy Naïve bayesian methodology. Paul Graham’s Naïve bayesian machine taking in methodology will be used to enhance that effectiveness about bayesian approach. [1] For limitless dataset additionally utilizing that naïve bayesian calculation Furthermore augment those precision for NBC. [4] Those research worth of effort need additionally conveyed out for expansion those correctness also the long haul effectiveness for framework.

Sunil B. Rathod and Tareek M. Pattewar [1] [2] have used Bayesian classifier in order to separate legitimate message from spam messages. In paper [1] content of the email message is considered for implementation and works solely using Bayesian classifier. The performance of the system is assessed in terms of accuracy, error, recall, time and precision. In paper [2], a combinational approach is used to filter both spam mail and malicious URLs. Bayesian classifier is used to filter spam messages and Decision tree is used to prevent malicious URLs from attacking the users. Also the performance of this combination approach is compared with the existing system that filtered only spam email messages.

Savita Teli and SantoshkumarBiradar [4] have explored some methods for spam detection and the problems associated with it. The methods that are discussed include List based or rule based filters (like Blacklist, Whitelist, Black Holes and Greylist), Content based filter and Bayesian filter. The authors have justified that Bayesian classifier is more effective when compared to other methods as it considers the whole message into account and is constantly self adapting.

Rohit Giyanani and Mukti Desai [6] have given a model that uses statistical Natural Language Processing (NLP) for detecting the spam messages against legitimate messages. A threshold counter has been declared that overcomes the congestion, but creates overhead in the storage space. This approach blocks the incoming spam emails depending upon the sender and the body part of the email message.

Weimiao Feng et al., [3] have designed a support vector machine based naive Bayes filtering system (SVM-NB) that accurately classifies the message as spam or ham. The SVM-NB divides the training datasets based on the construction of the hyperplane that needs to be optimal. They have taken DATAMALL datasets for the experiment and have demonstrated that this approach gives higher accuracy and classifies at greater speed.

Nurul et al., [12] has done an analysis on Naive Bayes Classifier across different Datasets. The authors have incorporated SPAMBASE and Spam Data for their experiment using WEKA tool. Evaluation of performance (accuracy, recall, precision and F-measure) of Naive Bayesclassifier is made across multiple data sets. The result illustrates that the number of dataset instances and type of email has greater impact on the performance of the classifier.

III. ALGORITHMS:

1. Support Vector Machine Learning Algorithm Support Vector Machine is used for classification and also for regression problems where the datasets are used to train the SVM to classify any new data that it receives. It is a supervised machine learning algorithm that works by finding a hyperplane that classifies the dataset into different classes [8]. The SVM maximizes the distance between different classes because of the existence of many linear hyperplanes which is called as margin maximization.

2. K Means Clustering Algorithm It is an unsupervised machine learning algorithm that is used for efficient cluster analysis. It works by initially specifying the number of clusters (k) that needs to be formed. K-Means are a non-deterministic and iterative method. K clusters that form k different classes is the output of this algorithm.

3. Naïve Bayes Classifier Algorithm This classifier is a statistical classifier that will classify the email messages into spam or ham efficiently. It follows Bayesian team that employs the mathematical probability calculation for classification [2].

P (spam/word) = [P (word/spam) * P (spam)] / P (word)

Naïve Bayes Classifier takes a whole message and uses keywords for recognizing the ham and spam email messages. Initially the system is trained using sample data using this classifier. Later the new data is tested for spam or ham against the trained data set using the same classifier. This classifier is also self-adapting and requires a dataset less in number.

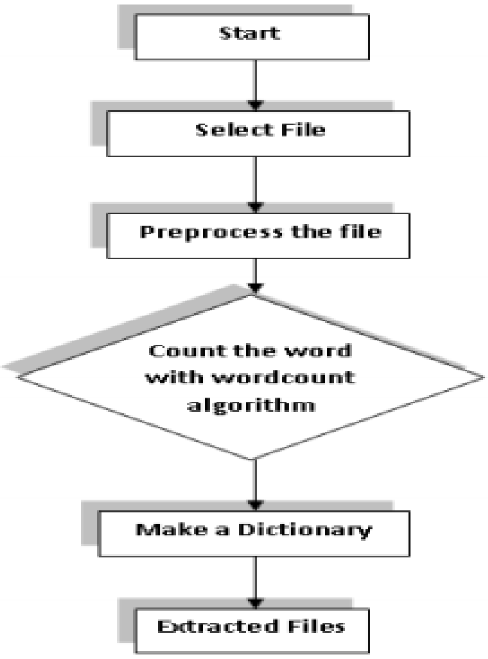
IV. IMPLEMENTATION:

Email spam classification needs significant issue over today's electronic world. Will unravel this issue those different spam arrangement techniques need aid utilized. Utilizing this spam identification method we might identifies those spam and more non-spam mails to our mail box. In this work would utilizing those Naïve bayesian classifier to email spam order. In this work in also use characteristic extraction systems for giving productive dataset. Those characteristic extraction systems need aid utilized at those data information will be excessively little also it may be excess to way thus characteristic is concentrated with get an exact come about. In this research we would utilizing the word-count algorithm for extracting characteristic from the dataset. Here we utilize the ling spam information situated which holds downright 960 mails done which 700 would prepare dataset and more 260 would test dataset. The train Also test information are further partitioned for two parts spam mails Furthermore non-spam i. E. Half from claiming train dataset would spam dataset and half need aid non-spam dataset as same to the test dataset.

Feature Extraction

Those word-count algorithm is precise basic should actualize all and more give a adaptable result. In this algorithm we pre-process those dataset also uproot those stop-words furthermore unique words over dataset. Et cetera it checks those downright amount from claiming exceptional saying crazy of the downright saying furthermore figures the recurrence for that saying in a specific report.

That fundamental relic around this algorithm may be will makes a dicti0nary. In that dictionary those way of the document will be saved which will be pre-processed. In this way those excess issue is evacuated. For numbering the expression and more stores the recurrence from claiming that expression may be extremely supportive will discover the unique word



.

Step1: choose the file from the data set

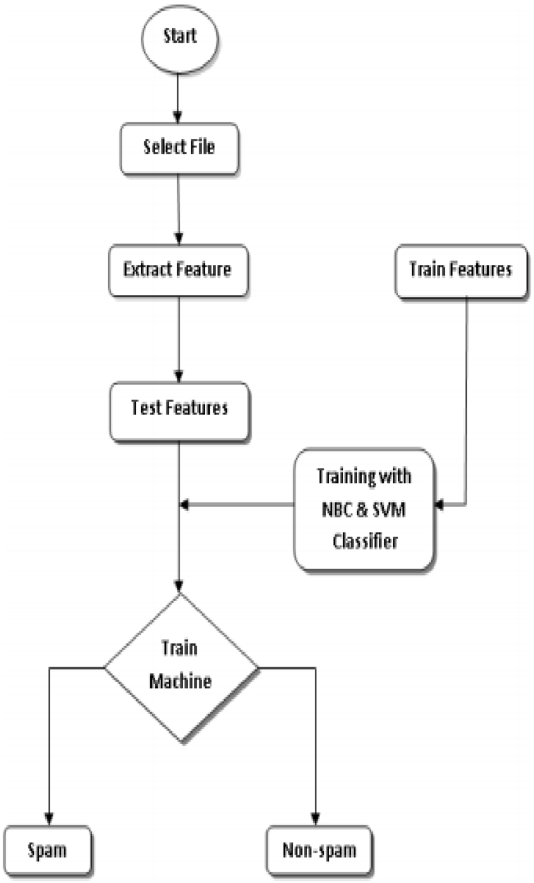
Step 2: Pre process the file and removing the stop word

Step3: Count the total word of the file and find the unique word of that file.

Step 4: calculate the frequency of words

Step 5: Make a dictionary and store the file path

Step 6: Extracted feature



Step 1: We have to select the file

Step 2: To extracting the feature with help of word count algorithm

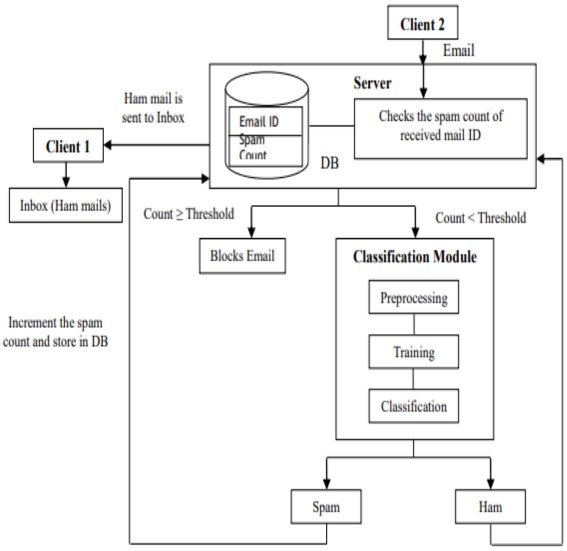
Step 3: Training the data set with the help of Naïve Bayesian classifier

Step 4: To find the probability of spam and non spam mails. Prob _spam = (sum(train_matrix(spam_indices,)) + 1) ./ (spam_WC+numtokens)

Step 5: "To testing the dataset log a = test_matrix*(log(prob_tokens_spam) + log(prob_spam)

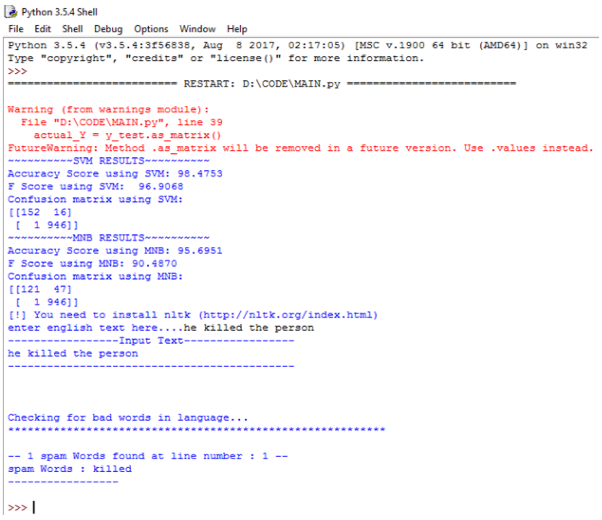
Step 6: To classify the spam and non spam mails. Fraction_wrong=numdocs_wrong/numtest_docs".

Step we need aid calculate the word which need aid wrongly ordered the classifier What's more ascertain exactness of the classifier furthermore likewise figure the lapse rate from claiming classifier by figuring those portion about saying which is wrongly arranged also aggregate amount for words in document



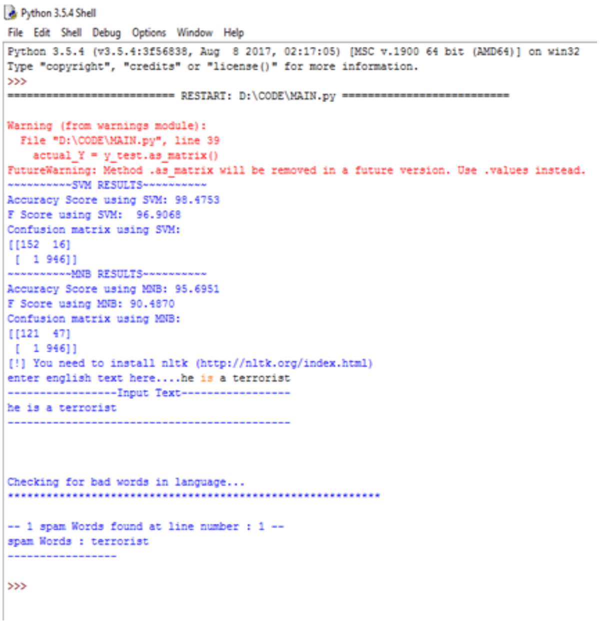
V. RESULTS

Displaying result of spam words found (1)



```
Python 3.5.4 (v3.5.4:3f56838, Aug  8 2017, 02:17:05) [MSC v.1900 64 bit (AMD64)] on win32
Type "copyright", "credits" or "license()" for more information.
>>>
========================== RESTART: D:\CODE\MAIN.py ==========================

Warning (from warnings module):
  File "D:\CODE\MAIN.py", line 39
    actual_Y = y_test.as_matrix()
FutureWarning: Method .as_matrix will be removed in a future version. Use .values instead.
~~~~~~~~~~SVM RESULTS~~~~~~~~~~
Accuracy Score using SVM: 98.4753
F Score using SVM:  96.9068
Confusion matrix using SVM:
[[152  16]
 [  1 946]]
~~~~~~~~~~MNB RESULTS~~~~~~~~~~
Accuracy Score using MNB: 95.6951
F Score using MNB: 90.4870
Confusion matrix using MNB:
[[121  47]
 [  1 946]]
[!] You need to install nltk (http://nltk.org/index.html)
enter english text here....he killed the person
-----------------Input Text-----------------
he killed the person
--------------------------------------------



Checking for bad words in language...
***********************************************************

-- 1 spam Words found at line number : 1 --
spam Words : killed
-----------------

>>> |
```

Displaying result of spam words found (2)



```
Python 3.5.4 (v3.5.4:3f56838, Aug  8 2017, 02:17:05) [MSC v.1900 64 bit (AMD64)] on win32
Type "copyright", "credits" or "license()" for more information.
>>>
========================== RESTART: D:\CODE\MAIN.py ==========================

Warning (from warnings module):
  File "D:\CODE\MAIN.py", line 39
    actual_Y = y_test.as_matrix()
FutureWarning: Method .as_matrix will be removed in a future version. Use .values instead.
~~~~~~~~~~SVM RESULTS~~~~~~~~~~
Accuracy Score using SVM: 98.4753
F Score using SVM:  96.9068
Confusion matrix using SVM:
[[152  16]
 [  1 946]]
~~~~~~~~~~MNB RESULTS~~~~~~~~~~
Accuracy Score using MNB: 95.6951
F Score using MNB: 90.4870
Confusion matrix using MNB:
[[121  47]
 [  1 946]]
[!] You need to install nltk (http://nltk.org/index.html)
enter english text here....he is a terrorist
-----------------Input Text-----------------
he is a terrorist
--------------------------------------------



Checking for bad words in language...
***********************************************************

-- 1 spam Words found at line number : 1 --
spam Words : terrorist
-----------------

>>>
```

Displaying result of ham words found

VI. CONCLUSION

Once the system is trained a set of mail datasets can be tested for spam or ham mails. Naive Bayes Classifier is used for classification which is based on Bayesian theorem. Bayesian classifier is a theorem that is based on an assumption that is conditionally independent. Based on the probability it correctly classifies the message as either spam or ham. If the message is spam then it respected spam counter is incremented in the database. Otherwise, the message is sent to the dedicated client. The performance of the system is the main criteria that need to be evaluated to check whether the system works efficiently or not. There are several measures available for measuring the performance. Some are: accuracy, precision, recall and F-measure. Accuracy refers to the percentage of correctly classified spam and ham messages. Precision refers to percentage of correct spam email. Recall refers to the percentage of spam messages can be blocked and F-measure refers to average of recall and precision.

REFERENCES

1. Sunil B. Rathod, Tareek M. Pattewar, “A Comparative Performance Evaluation of Content Based Spam and Malicious URL Detection in E-mail”, IEEE CGVIS 2015, pp: 49-54.
2. Weimiao Feng, Jianguo Sun, Liguo Zhang, Cuiling Cao, Qing Yang, “A Support Vector Machine based Naive Bayes Algorithm for Spam Filtering”, IEEE 2016.
3. Savita Teli, SantoshkumarBiradar, “Effective Spam Detection Method for Email”, IOSR Journal of Computer Science, pp: 68-75.
4. Rohit Giyanani, Mukti Desai, “Spam Detection using Natural Language Processing”, IOSR Journal of Computer Engineering, ISSN: 2278-0661, Volume 16, Issue 5, Sept-Oct 2014.
5. Priyanka Sao, Kare Prashanthi, “Email Spam Classification Using Naive Bayesian Classifier”, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET),Volume 4, Issue 6, June 2015.
6. Omar Saad, Ashraf Darwish and Ramadan Faraj, “A Survey of Machine Learning Techniques for Spam Filtering”, IJCSNS International Journal of Computer Science and Network Security, Volume 12, February 2012.
7. Akash Iyengar, G. Kalpana, Kalyankumar S., S. GunaNanshini, “Integrated Spam Detection for Multilingual Emails”, International Conference of Information, Communication & Embedded System, IEEE 2017.
8. S. Roy, A. Patra, S. Sau, K. Mandal, S. Kunar, “An Efficient Spam Filtering Techniques for Email Account”, American Journal of engineering Research (AJER), ISSN: 2320-0847, Volume 02, Issue 10, pp: 63-73, 2013.
9. Rekha, Sandeep Negi, “A Review on Different Spam Detection Approaches”, International Journal of Engineering Trends and Technology, Volume 11, May 2014.
10. Nurul F. R, Norfaradilla W., Shahreen K., Hanayanti H, “Analysis of Naive Bayes Algorithm for Email spam Filtering across Multiple Datasets”, International Research and Innovation Summit, 2017.
11. W. A. Awad and S. M. Elseuofi, “Machine Learning Methods for Spam E-mail Classification”, International Journal of Computer Science and Information Technology, Volume 3, February 2011.
12. Kavitha, M., Manideep, Y., Vamsi Krishna, M., & Prabhuram, P. (2018). Speech controlled home mechanization framework using android gadgets. International Journal of Engineering and Technology(UAE), 7(1.1), 655-659.
13. Modepalli Kavitha, Singaraju Srinivasulu, Kancharla Savitri, P. Sameera Afroze, P. Akhil Venkata Sai, S. Asrith l. (2019). "Garbage bin monitoring and management system using GSM." International Journal of Innovative and Exploring Engineering 8(7),pp. 2632-2636.

Retrieval Number: B9001129219/2019©BEIESP
DOI: 10.35940/ijitee.B9001.129219
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

14. M. Kavitha, K Anvesh, P Arun Kumar, P Sravani . (2019). "IoT based home intrusion detection system." International Journal of Recent Technology and Engineering 7(6),pp. 694-698.
15. Kavitha, M., et al. "Wireless Sensor Enabled Breast Self-Examination Assistance to Detect Abnormality." 2018 International Conference on Computer, Information and Telecommunication Systems (CITS). IEEE, 2018.
16. Kavitha, Modepalli, P. Venkata Krishna, and V. Saritha. "Role of Imaging Modality in Premature Detection of Bosom Irregularity." Internet of Things and Personalized Healthcare Systems. Springer, Singapore, 2019. 81-92.
17. Hybrid approach for securing the IoT devices published in IJITEE .Sai Prasanthi ,Volume 8, Issue 4, 2019, Pages 147-151,ISSN: 22783075 ,CSE, Koneru Lakshmaiah Education Foundation, Guntur, India