Machine Learning-based spam detection using Naïve Bayes Classifier in comparison with Logistic Regression for improving accuracy

K. Varun Kumar¹, M. Ramamoorthy²

¹Research Scholar, Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical And Technical Sciences, Saveetha University, Chennai, TamilNadu, India, Pincode: 602105
²Project Guide, Corresponding Author, Department of Artificial Intelligence and Machine Learning, Saveetha School of Engineering, Saveetha Institute of Medical And Technical Sciences, Saveetha University, Chennai, TamilNadu, India, Pincode: 602105

Abstract

Aim: The aim of this research is to detect spam using machine learning with the Novel Naive Bayes Classifier (NB) and the Logistic Regression (LR). Material and Methods: For analyzing the spam, it needs two groups which consist of 40 samples. The two groups are group 1 which consists of Novel Naive Bayes Classifier (NB) with a sample size of 20 and group 2 which consists of Logistic Regression (LR) with a sample size of 20 and G-power (value = 0.8). Results: Novel Naive Bayes Classifier has an accuracy of 98.05% which is comparatively more than the Logistic Regression with an accuracy of 94.7%. The accuracy has a 2-tailed significant value of 0.012 (p<0.05) which is found in the Independent Sample T-Test analysis. Conclusion: The performance of the Novel Naive Bayes Classifier is more than the performance of Logistic Regression in terms of accuracy.

Keywords: Machine Learning, Supervised Learning, Spam detection, Ham, Novel Naive Bayes Classifier, Logistic Regression.

DOI: 10.47750/pnr.2022.13.S04.061

INTRODUCTION

Nowadays, email enables users to communicate faster with other users or with organizations and vice versa. In organizations, all the work details were shared through email only. So Spam mails or gratuitous emails cause a distraction to the users in the communication. The spam mails or gratuitous emails may contain an advertisement or unwanted information which may also include malicious code or malicious software which will help the hackers or the cyberpunks to sneak your information and make their business with our information (Trivedi 2016). A survey has reported that on average a person will receive 25-40 mails every day and 60-70% of business emails are spam mails only. Email spam is growing rapidly which causes inconvenience to users in the form of distraction, occupies more storage, wastes time and energy, increasing network traffic (Agarwal and Kumar 2018). There are a lot of tools and techniques to detect spam and to filter based on ham (consists of legitimate words) and spam (consists of gratuitous words) (Gibson et al. 2020). Spam detection is used in Google Mails, Microsoft Outlook, Yahoo mails, Internet Service Providers (ISPs), and Small-Medium sized Business organizations (SMBs) to safeguard their employee’s data and networks (Cichosz 2015).

Over the past 5 years, on spam detection using machine learning, 18,400 articles have been published in Google Scholar, 27 journal papers are available in IEEE Xplore, 1,773 articles are available in ScienceDirect. There are many machine learning methods used by researchers to get rid of spam. Some methods used are: using Logistic Regression, which is a supervised learning technique. It is used to predict discrete values such as True or False, 0 or 1. Logistic regression is used to measure the probability of occurrence of an event by squeezing it into the logistic function. It shows ‘0’ for ham and ‘1’ for the spam (Dedeturk and Akay 2020). Another method is by using Random Forest, which is a supervised learning technique. It consists of many individual decision trees, and each tree consists of votes which are given based on the overall classification of the set of data. This algorithm chooses the individual tree with the most votes. It is the superset of the Decision Tree (Devi 2018; Wang et al. 2015). Another method is by using KNN, which is a supervised learning technique. The K-Nearest Neighbor algorithm is the process of making clusters based on similar properties. The clusters are taken as classes and it defines the class as the yield or not yield. From the K classes of documents, it has to calculate the score. The
scores are taken into consideration only if they are greater than the threshold value following the statistical value of the class (Ren and Shi 2016; Laksono, Basuki, and Bachtiar 2020). Another method is by using the Decision Tree algorithm, which is a supervised learning technique. It works well for both categorical and continuous variables. It consists of the root node as an input variable. The recursive partitioning of subsets was done until the subset values matched the target variables (Chakraborty and Mondal 2012; Saini 2021).

Our team has extensive knowledge and research experience that has translate into high quality publications (Bhansali et al. 2021; Jayanth et al. 2021; Sudhakar, Ravel, and Perumal 2021; Sathiyamoorthi et al. 2021; Deepanraj et al. 2021; Raju et al. 2021; Arun Prakash et al. 2020; Kamath et al. 2020; Shanmugam et al. 2021; Rajasekaran et al. 2020; Adhinarayanan et al. 2020; Rajesh et al. 2020; Aurtherson et al. 2021). The lacuna in the existing system is accuracy. Due to less accuracy in the existing system, some spam emails or gratuitous emails are coming into the inbox of an email which causes distraction to the user. So it wants to improve the accuracy of the proposed system using machine learning. The aim of this research is to develop machine learning-based spam detection using the Novel Naive Bayes Classifier in comparison with the Logistic Regression to improve accuracy. The goal of this research is to increase accuracy in detecting spam.

Materials And Methods

The research work is accomplished in the Image Processing Lab, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences where the laboratory provides a high infrastructure system to obtain the experimental results. There are two groups required for this research and 20 samples are required for each group (Wei 2018). Group 1 consists of Novel Naive Bayes Classifier and group 2 consists of Logistic Regression. The calculation is performed utilizing G-power 80% (Gibson et al. 2020) with alpha worth 0.05 and beta worth is 0.95 with a confidence interval of 95%.

The dataset named spam is downloaded from the Kaggle website. The spam dataset is in the form of a CSV file with a size of 491 KB which consists of ham and spam words. The ham and spam words help us to decide whether the email is a ham(legitimate mail) or spam(gratuitous mail).

Google Colab is used as the implementation for this work. All my codes are executed in Google Colab only. Google Colab is used to execute all python codes with zero configuration and free access to GPUs. It is used to combine all the executable python codes and it is divided into cells. The hardware configuration used in this research was a system with 8 GB RAM and 1.8 TB ROM of a 64-bit operating system of Windows 10 with a processor of Intel(R) Core(TM) i5-7200U CPU @ 2.50GHz 2.70 GHz.

Novel Naive Bayes Classifier

The Novel Naive Bayes Classifier is a supervised learning algorithm. It uses the Bayes theorem to calculate the probability of an event. It follows the properties like strong independence, easily handles large datasets, and depends on probability distribution (Cichosz 2015; Pooja and Bhatia 2018). The Bayes theorem is used to calculate the probability distribution from the frequency of the dataset. From the probability distribution, the class having the highest posterior probability is chosen by the NB classifier. The posterior probability equation is as shown in equation (1) (Agarwal and Kumar 2018).

\[
P(B|A) = \frac{P(A|B) P(B)}{P(A)}
\]

Where

\(A=(a_1,a_2,a_3,....)\), \(B=(b_1,b_2,b_3,....)\)

\(P(A)\) is evidence probability,

\(P(B)\) is prior probability,

\(P(A|B)\) is a conditional probability,

\(P(B|A)\) is posterior probability.

Pseudocode

Input: Spam dataset
Output: Accuracy of spam detection

Step-1: Initially, all of us have to download and install all the packages and libraries.
Step-2: Import all packages that are downloaded.
Step-3: It needs to load the dataset and extract the ham and spam keywords.
Step-4: Clean the dataset which includes removing single letter words, truncating white spaces, tokenizing each and every message, deleting all punctuation, changing all the letters to lowercase, etc.
Step-5: Then split the dataset into test and train datasets.
   Train: X_train, Y_train.
Test: X_test, Y_test
Step-6: Train the machine which is spam and ham when they triggered the spam and ham words.
Step-7: Load the Novel Naive Bayes classifier and train the model with the training dataset.
   NB=NaiveBayesClassifier()
   NB.fit(X_train,Y_train)
Step-8: Calculate the probability distribution $P(B|A)$ for every class using the Bayes theorem.
Step-9: Calculate the confusion matrix and find the Accuracy.
   accuracy = sum(X_test.Label == Y_test.predicted)/len(X_test)

Logistic Regression
Logistic Regression is a supervised learning algorithm. It is used to calculate discrete values such as 0 or 1 and True or False. It is used to find the probability of occurrence of an event by squeezing it into the logistic function. It shows 0 for ham and 1 for spam (Gupta et al. 2018). The logistic function is an S-shaped curve which is a sigmoid curve, it is shown in equation (2).

$$f(x) = \frac{1}{1 + e^{-t(x-x_0)}} \forall x \in (-\infty, \infty)$$  \hspace{1cm} (2)

Where
M is the curve maximum value,
x, x_0 are the midpoints of the sigmoid curve,
t is the growth rate of the curve.

Pseudocode
Input: Spam dataset
Output: Accuracy of spam detection

Step-1: Download and install all the libraries required for this model.
Step-2: Import all the libraries.
Step-3: Load the dataset and extract the ham and spam keywords.
Step-4: Now clean the dataset, it includes removing all the white spaces, tokenizing each and every message, removing all punctuations, lower case every one of the letters, truncating all the single letter words(‘a’, ‘i’), etc.
Step-5: Encode the ham as ‘0’ and spam as ‘1’.
Step-6: Now divide the dataset into a test and train dataset.
   Train: P, Q.  
   Test: P_Test, Q_Test.  
Step-7: Load the Logistic Regression model and train the model with a training dataset.
   LR= LogisticRegression()  
   LR.fit(P.iloc[:,6:],Q)
Step-8: Calculate the confusion matrix for the training dataset.
   confusion_matrix(Q,LR.predict(P.iloc[:,6:]))
Step-9: Finally, calculate the confusion matrix for the test dataset.
   confusion_matrix(Q_Test,LR.predict(P_Test.iloc[:,6:]))
Step-10: Predict the accuracy from the confusion matrix of the test dataset.
   LR.score(P_Test.iloc[:,6:], Q_Test)

Statistical Analysis
The IBM SPSS Version 28 software is used to calculate the statistical variables like mean, standard deviation, standard error mean, mean difference, sig, and F value. The Independent Sample T-Test analysis is carried out in this research. The spam dataset with 4862 ham words and 728 spam words is used to detect spam. The dependent variables are spam and ham. The independent variables are accuracy and count of words (Udge et al. 2019).

Results
The accuracy is taken as a measurement for comparing the Novel Naive Bayes Classifier and Logistic Regression. The spam dataset is required for both comparing and analyzing the models. From the results, it is clearly shown that the novel Naive Bayes Classifier has more accuracy than Logistic Regression. The Mean accuracy for the Novel Naive Bayes Classifier is 98.05% and the Mean Accuracy for Logistic Regression is 94.7%.
Table 1 represents the statistical variables like Mean, Standard Deviation, and Standard Error Mean are measured for both the Novel Naive Bayes Classifier and the Logistic Regression. The Mean Accuracy of the Novel Naive Bayes Classifier is 98.05% which is greater than the Mean accuracy of Logistic Regression with 94.7%. The Standard Deviation of the Novel Naive Bayes Classifier(0.759) is slightly less than the Standard Deviation of Logistic Regression(0.801).

Table 2 represents the Independent Sample T-Test which consists of Mean Difference and Standard Error Difference calculated for both the Novel Naive Bayes Classifier and the Logistic Regression with Confidence Interval of 95%. The 2-tailed significant value of accuracy for both models is 0.012 (p<0.05).

Fig 1 depicts the Bar graph for comparing the Mean Accuracy of the Novel Naive Bayes Classifier and Logistic Regression along with error bars of Confidence intervals of 95% and SD. The X-axis consists of groups(NB, LR) and the Y-axis consists of Mean Accuracy. The Mean Accuracy of the Novel Naive Bayes Classifier is 98.05% which is slightly greater than the Mean Accuracy of Logistic Regression with 94.7%.

Discussion

The data is evaluated in IBM SPSS software with version 28 and an Independent Sample T-Test is carried out. From the results, it is clearly observed that the Novel Naive Bayes Classifier has more accuracy than the Logistic Regression. The Mean Accuracy of the Novel Naive Bayes Classifier is 98.05% which is slightly greater than the Mean Accuracy of Logistic Regression with 94.7%.

Similar findings related to the Novel Naive Bayes Classifier are (Cichosz 2015; Pooja and Bhatia 2018). In those articles, the spam dataset is selected. The dataset is cleaned and split into train and test datasets. Loading the model and training it with a training dataset. Then test the model with a test dataset and calculate the confusion matrix. The Naive Bayes Classifier offers certain advantages, such as the capacity to forecast class data fast and easily, the ability to cope with independent assumptions, and the ability to operate with categorical rather than numerical input elements (Cichosz 2015). The disadvantages are as follows: The Naive Bayes Classifier, which assumes all predictors are independent, faces the ‘zero-frequency problem,’ which allocates likelihood ‘0’ to categorical variables that are available in the test dataset but not in the training dataset (Trivedi 2016). Opposite findings for spam detection are (Singh, Pamula, and Shekhar 2018). This paper makes use of the spam dataset. The data was cleaned and subdivided into two categories: training and test datasets. In this example, they used the Support Vector Machine method, which is a sort of supervised learning technology. It shows the data as a point in n-dimensional space from the input. Each feature is a value for a certain coordinate. After that, the categorization is completed by creating a hyperplane with vectors that clearly identify the two classes. This model is loaded, trained, and tested using train and test datasets. The calculations for accuracy and the confusion matrix are done.

The limitations in spam detection are making a good text classification, link analysis will be done accurately, avoiding picking ham mail to the trash instead of spam, requiring more keywords, and providing data security to users. In the future, all of us will try to increase the detection of spam to greater than 99%, and also all of us will try to decrease the error rate to less than 1%. All of us will also try to implement this spam detection by using other Deep Learning algorithms.

Conclusion

This review shows that the accuracy of the Novel Naive Bayes classifier is more when compared to the Logistic Regression model in detecting spam. The accuracy of the Novel Naive Bayes Classifier is 98.05% which is comparatively more than the accuracy of the Logistic Regression model with 98.70%.

DECLARATION

Conflict of Interest

No conflict of interest in this manuscript.

Authors Contribution

Author KVK was involved in data collection, data analysis, and writing the manuscript. Author MR was involved in the conceptualization, data validation, and critical review of the manuscript.

Acknowledgments

The authors would like to express their gratitude towards Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences (formerly known as Saveetha University) for providing the necessary infrastructure to carry out this work successfully.

Funding

Personally thank the following organizations for providing financial support that enabled us to complete the study.
2. Saveetha University.
3. Saveetha Institute of Medical and Technical Sciences.
4. Saveetha School of Engineering.

References

https://doi.org/10.1109/gucon.2018.8674973.


ABLES AND FIGURES

Table 1. The statistical calculations for the Novel Naive Bayes Classifier and Logistic Regression are measured. The mean accuracy of the Novel Naive Bayes classifier is 98.05 and the Mean accuracy of Logistic Regression is 94.70. Standard Deviation for Novel Naive Bayes Classifier is 0.759 and Standard Deviation for Logistic Regression is 0.801.

<table>
<thead>
<tr>
<th>Groups</th>
<th>N</th>
<th>MEAN</th>
<th>Std. Deviation</th>
<th>Std. Error Mean</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accuracy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NB</td>
<td>20</td>
<td>98.05</td>
<td>0.75915</td>
<td>0.16975</td>
</tr>
<tr>
<td>LR</td>
<td>20</td>
<td>94.70</td>
<td>0.80131</td>
<td>0.17918</td>
</tr>
</tbody>
</table>

Table 2. Statistical Independent T-Test between Novel Naive Bayes Classifier and Logistic Regression with a confidence interval of 95%. The 2-tailed significant value of accuracy is 0.012 (p<0.05).

<table>
<thead>
<tr>
<th></th>
<th>Levene's Test for Equality of Variances</th>
<th>T-Test for Equality of Means</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>F</td>
<td>Sig.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Equal variances not assumed</td>
<td>13.573</td>
</tr>
</tbody>
</table>
K. Varun Kumar, et al.: Machine Learning-based spam detection using Naïve Bayes Classifier in comparison with Logistic Regression for improving accuracy

**Fig. 1.** Bar Graph for comparing the Novel Naive Bayes Classifier and the Logistic Regression with 95% confidence interval and with SD of +/- 2. The mean accuracy of the Novel Naive Bayes Classifier is slightly greater than the Logistic Regression. The X-axis consists of groups (NB, LR) and the Y-axis consists of Mean Accuracy.