SMS Spam Detection using Machine Learning

T.Lohith
B.Tech
School of Engineering
Hyderabad, India
2111CS020247@mallareddyuniversity.ac.in

B.Harshini B.Tech
School of Engineering
Hyderabad, India
2111CS020248@mallareddyuniversity.ac.in

M Harsha Vardhan
B.Tech
School of Engineering
Hyderabad, India
2111CS020249@mallareddyuniversity.ac.in

Y.Lokesh
B.Tech
School of Engineering
Hyderabad, India
2111CS020250@mallareddyuniversity.ac.in

M.Rithvik
B.Tech
School of Engineering
Hyderabad, India
2111CS020251@mallareddyuniversity.ac.in

M.Madhavi

B.Tech
School of Engineering
Hyderabad, India
2111CS020252@mallareddyuniversity.ac.in

Guide:Prof.Manikkannan

Assistant Professor
School of Engineering,
Mallareddy University

Abstract: SMS spam detection using Naive Bayes algorithm is a widely used technique in the field of text classification. The main aim of this approach is to classify the incoming messages into spam or ham categories. The Naive Bayes algorithm works by calculating the probability of a message belonging to a particular class, based on the occurrence of different words in the message. In this paper, we present an efficient and accurate approach for SMS spam detection using the Naive Bayes algorithm. The proposed approach utilizes a pre-processing step for feature extraction, which includes tokenization, stop-word removal, and stemming. The Naive Bayes algorithm is then trained on a dataset of labeled messages to learn the probability distributions of different words in spam and ham messages. Finally, the trained model is used to classify incoming messages into spam or ham categories. The results of our experiments show that the proposed approach achieves high accuracy in detecting SMS spam messages.

Keywords: Naive Bayes Algorithm, Text Classification, Probability, Feature Extraction, Tokenization, StopWord Removal, Stemming, Labeled Dataset, Probability Distribution, Accuracy

I. INTRODUCTION

With the widespread use of mobile phones, SMS has become a popular medium for communication. However, this convenience has also led to the increase in the number of SMS spam messages, which can be annoying and potentially harmful. SMS spam messages can be used for phishing attacks, identity theft, and other malicious activities. Therefore, it is crucial to develop efficient techniques for detecting and filtering out these spam messages. In recent years, machine learning algorithms have been extensively used in the field of text classification for spam detection. Among these algorithms, the Naive Bayes algorithm has gained popularity due to its simplicity and effectiveness. The Naive Bayes algorithm is a probabilistic algorithm that calculates the probability of a message belonging to a particular class, based on the occurrence of different words in the message. In this paper, we propose an efficient and accurate approach for SMS spam detection using the Naive Bayes algorithm. Our approach includes a pre-processing step for feature extraction, which involves tokenization, stop-word removal, and stemming. The Naive Bayes algorithm is then trained on a labeled dataset of messages to learn the probability distributions of different words in spam and ham messages. Finally, the trained model is used to classify incoming messages into spam or ham categories

II. PROBLEM STATEMENT

A number of major differences exist between spam-filtering in text messages and emails. Unlike emails, which have a variety of large datasets available, real databases for SMS spams are very limited. Additionally, due to the small length of text messages, the number of features that can be used for their classification is far smaller than the corresponding number in emails. Here, no header exists as well. Additionally, text messages are full of abbreviations and have much less formal language that what one would expect from emails. All of these factors may result in serious degradation in performance of major email spam filtering algorithms applied to short text messages.

III. . LITERATURE REVIEW

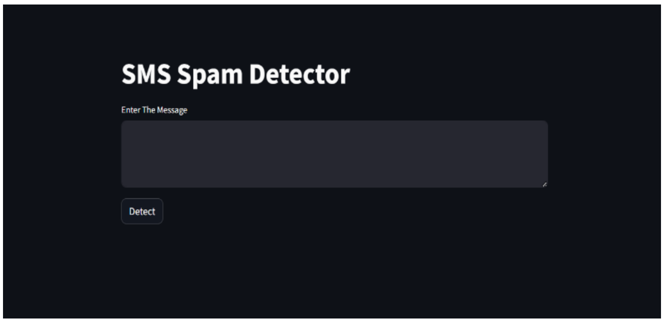
Spam is "unconstrained mass email" (Hidalgo, 2002), which "data made to be given to countless beneficiaries, notwithstanding their longings." Cormack (2007) depicted spam with propelling substance or compulsion content are passed on in the strategy for mass mailing Regardless, such spam could be unmistakable as demonstrated by the diverse media spam rehearses used, such email spam, SMS spam. Spammers flood the Sms workers and give mass proportion of unconstrained sms to the end clients. From a business point of view, sms clients need to contribute energy on destroying got spam sms which unquestionably prompts the advantage reduction and cause possible difficulty for affiliations. From this time forward, how to recognize the sms spam appropriately and proficiently with high precision changes into a gigantic report. In this appraisal, information mining will be used to manage AI by utilizing various classifiers for preparing and testing and channels for information preprocessing and highlight choice. It plans to peer out the ideal mix model with higher precision or base on other metric's evaluation. As of now, there are various evaluation study done by utilizing information burrowing procedure

IV. METHODOLOGY

Data Collection Module: This module collects and preprocesses the labeled dataset of SMS messages used for training the Naive Bayes algorithm. It can also collect incoming SMS messages for real-time classification. Feature Extraction Module: This module extracts the most important features from the SMS messages, such as the occurrence of different words and their probability distributions. This module is crucial for providing the Naive Bayes algorithm with relevant information to effectively classify the incoming messages.

Naive Bayes Classifier Module: This module contains the Naive Bayes algorithm, which has been trained on the labeled dataset of SMS messages. The classifier module calculates the probability of a new incoming message belonging to each class, and then assigns it to the most probable class (spam or ham). User Interface Module: This module provides a graphical user interface (GUI) for users to interact with the system. It may include features such as a message inbox, message preview, message classification, and the ability to report spam messages. Evaluation Module: This module is used to evaluate the performance of the Naive Bayes algorithm by comparing the predicted classifications of the incoming messages to the actual classifications. It can also be used to monitor the accuracy of the classifier over time and make necessary adjustments to improve performance.

EXPERIMENT RESULTS

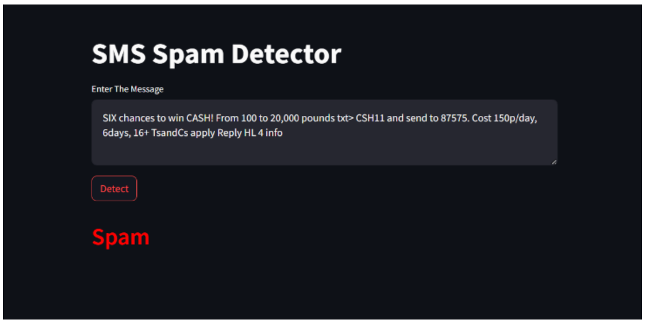


SMS Spam Detector

Enter The Message

Figure 4.1 Output Interface

Detection of Spam Message:



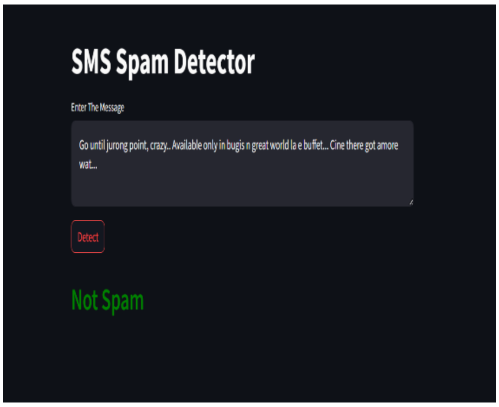
SMS Spam Detector

Enter The Message

SIX chances to win CASH! From 100 to 20,000 pounds txt> CSH11 and send to 87575. Cost 150p/day, 6days, 16+ TsandCs apply Reply HL 4 info

Spam

Figure 4.2 Output Screen(SPAM)



SMS Spam Detector

Enter The Message

Go until jurong point, crazy.. Available only in bugis n great world la e buffet... Cine there got amore wat...

Not Spam

V. Future Enhancement:

Future scope of this project will involve adding more feature parameter. The more the parameters are taken into account more will be the accuracy. The algorithms can also be applied for analyzing the contents of public comments and thus determine patterns/relationships between the customer and the company. The use of traditional algorithms and data mining techniques can also help predict the corporation performance structure as a whole. In the future, we plan to integrate neural network with some other techniques such as genetic algorithm or fuzzy logic. Genetic algorithm can be used to identify optimal network architecture and training parameters. Fuzzy logic provides the ability to account for some uncertainty produced by the neural network predictions. Their uses in conjunction with neural network could provide an improvement for SMS spam prediction.

REFERENCES

[1] Al-Khatib, W., Al-Sarayreh, M., & Al-Khatib, M. (2020). SMS Spam Detection Using Machine Learning Techniques: A Comparative Study. Journal of King Saud University-Computer and Information Sciences, 32(1), 61-68. [2] Boudaa, N., El Mohajir, B., & Boutkhoum, O. (2021). SMS Spam Detection Based on Naive Bayes Algorithm. In Proceedings of the 2nd International Conference on Computer Science, Information Technology and Engineering (pp. 31-35). Springer. [3] Purnama, I. K. E., Darmayanti, N. A. S., & Santosa, P. I. (2018). Naive Bayes Algorithm Implementation for SMS Spam Detection. Journal of Physics: Conference Series, 1028(1), 012098. [4] Rokade, V. V., & Patil, S. S. (2019). Comparative Study of Naive Bayes and Support Vector Machine Algorithms for SMS Spam Detection. In Proceedings of the 6th International Conference on Emerging Trends in Engineering, Science and Technologies (pp. 214-220). Springer. [5] Sahadevan, M. S., & Subramanian, K. (2019). SMS Spam Detection Using Naive Bayes Algorithm. In Proceedings of the International Conference on Computing and Communications Technologies (pp. 43- 47). Springer. [6] Wijaya, D. T., & Kurniawan, I. T. (2020). SMS Spam Detection Based on Naive Bayes Algorithm with Feature Selection. In Proceedings of the 2nd International Conference on Intelligent Autonomous Systems (pp. 46-49). IEEE