ISSN No:-2456-2165

SMS Spam Classifier Using Machine Learning

Shaniya Chauhan
Department of Computer Applications

Abstract:- The purpose of this research paper is to examine how machine learning techniques are used to identify whether a SMS is spam or not. The growth of mobile users has led to a dramatic increase in SMS and messages. Despite the fact that our idea of information channels are currently seen as spotless and reliable in many parts of the world on going data clearly demonstrates that the amount of cell phones Spam is dramatically increasing overtime. It is a growing catastrophe, especially in the middle East and Asia.

Separating SMS spam is a similarly lead task to solve this problem. It games several concerns and practical fixes from SMS spam separation in any case, it brings up it's own unique problems.

Keywords – *Machine Learning, Spam Separation.*

I. INTRODUCTION

The bulk delivery of unscheduled messages, primarily of a business nature but also containing offensive content, has become a major problem for SMS service for internet service providers, businesses,and individual customers in the last 10 years due to the spam phenomenon's steady growth. Recent analysis show that more than 60% of all messages are spam. Spam puts excessive strain on sms frameworks ability to make data quickly and store data on servers, increasing annual costs for partnership by more than several billion dollars.

II. LITERATURE REVIEW

The expression 'cybercrime' is a product of the expansion in communications technology which has accelerated over the last twenty five years.

Cyber Crime is a term that encompasses a variety of offences associated with the use of information and communication technology. The internet was born around

1960’s where its access was limited to few scientist, researchers and the defense only.

Internet user base have evolved exponentially. Initially the computer crime was only confined to making a physical damage to the computer and related infrastructure.

Around 1980’s the trend changed from causing the physical damaging to computers to making a computer malfunction using a malicious code called virus.

Till then the effect was not so widespread because internet was only confined to defense setups, large international companies and research communities.

In 1996, when internet was launched for the public, it immediately became popular among the masses and they slowly became dependent on it to an extent that it have changed their lifestyle. As on April 2018, the number of mobile broadband subscribers in India reached 401.41 million. Overall, the number of broadband subscribers, including wired, in India reached 419.79 million by the end of April 2018.

III. METHODOLOGY

The terms "Spam" refers to unwanted content with questionable information. The data set consists of a randomly choseniction of plain text emails that have been classified as either SPAM or HAM. The model for categorising emails as ham and spam is developed using the training data. The model created using the training data is examined using the test data for accuracy.The system is shown as a block diagram in Fig.1.

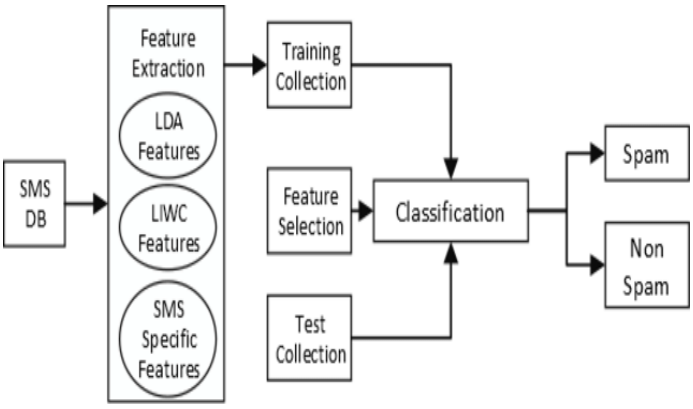

Fig. 1 System Block Diagram

Data cleaning-One of the crucial components of machine learning is data cleaning, it is crucial to the process of creating a model. There are no hidden twist or secrets to discover, but it is also not the most fancy aspect of machine learning.

Exploratory Data Analysis-Data analysis utilizing visual methods is called exploratory data analysis. With the use of statistical summaries and graphical representations, it is used to identify trends, patterns, or to verify assumptions.

ISSN No:-2456-2165

Data pre-processing-The learning data's emails are in plain text format. The simple text must be transformed into characteristics that can represent emails. We may then apply a learning algorithm to the emails using these features. First and for most certain preposition procedures are carried out.
Model building-The last step is model building where we finalize everything and build a precise model.

IV. DATASET AND FEATURES

The dataset used was picked up from Kaggle. This dataset was first thoroughly examined and then data cleaning and data analysis was performed. Further Exploratory data analysis was done for this dataset. The data pre-processing includes the removal of stop words, stemming, tokenization and removal of special characters and punctuation marks.

V. RESULT

We tested different algorithms for the dataset for the best precision score and accuracy.

Typically, the performance of an SMS spam classifier is evaluated using metrics such as precision, recall, and F1 score. Precision is the fraction of spam messages correctly identified as spam, while recall is the fraction of all spam messages that are correctly identified by the classifier. The F1 score is the harmonic mean of precision and recall, which provides an overall measure of the classifier's performance.

Multinomial Naive Bayes is a popular machine learning algorithm used for text classification tasks, including SMS spam classification. The algorithm works by modeling the probability distribution of words in a text message and calculating the likelihood that a message is spam or not based on these probabilities.

The performance of a Multinomial Naive Bayes SMS spam classifier can be evaluated using metrics such as accuracy, precision, recall, and F1 score. The highest precision achieved is 1.0 and accuracy is about 97 percent.

VI. CONCLUSION & FUTURE WORK

This projects goal and objectives were established at the very very of the process and were accomplished throughout . The research process involves a detailed analysis of the various filtering algorithms and available anti-spam technologies in order to gather all the information.

The projects work was inspired in part by the large scale research articles and existing software packages mentioned above. The entire project was broken up into various iterations.Each iteration was finished by walking through the different phases.

There are still certain areas that can be improved, such as by incorporating more filtering methods or altering certain features of the ones that already exist. Changes like increasing or decreasing the message's intriguing word count and rearranging the formula for determining the interesting rate can be made at a later time.

We intend to tackle more difficult issue in the future, like the analysis and administration of report data stored in SMS spam filters.Future work will additionally concentrate on finding a solution to this issue.

REFERENCES

[1]. https://www.youtube.com/watch?v=YncZ0WwxyzU
[2]. Swayam
[3]. 3.https://www.researchgate.net/publication/349799157_SMS_Spam_Detection_Using_Machine_Learning
[4]. https://ieeexplore.ieee.org/document/9441783