Data Analytics and Artificial Intelligence
Vol: 2(5), 2022
REST Publisher; ISBN: 978-81-948459-4-2
Website: http://restpublisher.com/book-series/data-analytics-and-artificial-intelligence/

Spam Detection in SMS Using Naïve Bayes in Machine Learning

*Kokila. M, Amalredge .G
St.Joseph's College of Arts and Science for Women, Hosur, TamilNadu, India.
*Corresponding author Email:kokila2259@gmail.com

Abstract. The term SMS stands for short message service. It is a message networking method that uses smartphones and cellphones. It is a text messaging system that lets smart phones to communicate with one another. The development of the cell phone clients has prompted a sensational increment in SMS spam messages. Despite the fact that in many parts of the world, versatile informing channel is right now viewed as "spotless" and trusted, on the complexity ongoing reports obviously show that the volume of cell phone spam is drastically expanding step by step. In recent times, the increment of mobile phone usage has resulted in a huge number of spam messages. Spammers continuously apply more and more new tricks that cause managing or preventing spam messages a challenging task. The aim of this study is to detect spam message to prevent different cybercrimes as spam messages have become a security threat nowadays. In this paper, we contributed to previous studies on SMS spam problems to perform a better accuracy using several different techniques such as Support Vector Machine, K Nearest Neighbor, Naïve Bayes, Random Forest, Logistic Regression and some more. If some adjustments are needed to identify a new scam, they were made manually, either by applying changes to current algorithms or by inventing new algorithms. In this method, as the quantity of clients and data grows, so does the amount of human work, which may also effectively separate spam text messages and ham SMS messages. The random forest classification method, we proposed, is the methodology that produced 99.9% accuracy.
Keywords: Spam, Ham, Classifier, Accuracy, Security, Text Mining, SMS, Spam Detection.

1. Introduction

A message is transmitted digitally via the short messaging service (SMS), which which is one of the most widely used communication services. One of the most widely use Telecommunication firm's have cut the price of SMS services, which has resulted in increasing SMS usage. These increases recruited hackers, resulting in an SMS spam problem. Any unsolicited message sent from a user's device is referred to as spam.At present, spam channels are comprised of various modules which dissect diverse highlights of messages (to be specific sender address, header, content, and so on.People prefer SMS messages to emails for communication because delivering SMS messages requires no Internet connection and is convenient and easy. The increased usage of text messaging and the issue of spam are becoming more prevalent. There seems to be a lot of security solutions available to mitigate the issue of SMS spam, although they are not yet developed. Many android applications exist on the play store to stop spam texts; however, due to lack of awareness, most people are unaware of them. Apart from applications, the existing monitoring solutions mostly concentrate on spam messages, as email is among the biggest problems, but even with the rise in the use of android platforms, SMS spam has become a big concern.

Because mobile phones hold sensitive personal information such as card details, usernames, and passwords, SMS has been one of the cheapest ways to communicate and may be regarded as the easiest way to conduct phishing scams. Hackers are devising new ways of obtaining this data from smart phones, with SMS being one of the most straightforward. Type of phishing attack, or SMS-based hacking, is becoming increasingly prevalent these days. Phishing through SMS is becoming more common around the world, in which a person provides a malicious Web site by SMS and urges the recipient to click it, stealing important information from the recipient's smart phone. For identifying mobile fraud, there seems to be a variety of screening methods available, including smartcards, machine learning, finger prints, and matrix code scanner based, academic objectives, and identification based. MS Fraud Detection Using Machine Learning techniques to identify spam and ham SMS.Machine learning techniques for eliminating Ham and Spam messages, including the naive Bayes Technique, support vector machines approach, and maximum entropy method.

2. Related Work

Spam refer to the term, which is related to undesired content with low quality information. Spam referred to the major drawback of mobile business. When comes to the spam detection in campus network they done the analysis using Incremental Learning. For Collecting Spam detection on web pages Moreover Sending out a Spam messages was also analyzed under Data Collection was done privately by a limited company. From the data Collection. There also antispam filter system was evolved. Many parallel and distributed computing system has also processed this spam system. Machine learning algorithm provides accurate result. Text mining analysis done separates ham and spam separately.

Copyright@ 2022 REST Publisher

3. Design & Methodology

Text Mining: Text mining, conjointly spoken as text data processing, roughly corresponding to text analytics, is that the method of account high- quality data from text. High-quality data is often derived through the fashioning of patterns and trends through suggests that like applied mathematics pattern learning. 'High quality' in text mining sometimes refers to some combination of connection, novelty, and powerfulness .Typical text mining tasks include text categorization, text clustering, concept/entity extraction,production of granular taxonomies, sentiment analysis, document summarization, and entity relation modeling (i.e., learning relations between named entities).

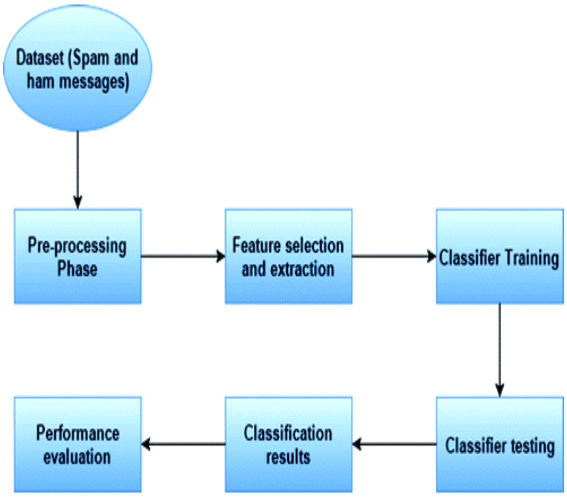

FIGURE 1. Design & Methodology

Identification of fine feature that may expeditiously filter spam. SMS messages could be a difficult task. Moreover , we have a tendency to study the characteristics of spam messages exhaustive and notice some options, that area unit helpful within the economical detection of spam SMS.

4. Background

- SMS Spam messages are any type of unwanted or harmful messages, such as advertisements, frauds, business services, etc.
- They annoy end users, consume the resource of mobile devices including memory spaces, and lead to overloading SMS channels.
- A spam SMS often contains some special keywords, such as “free” or “winner,” it might include extensive use of punctuation marks and capital letters, such as “BUY!!” or “MONEY” or it includes phones numbers and personal information equests.

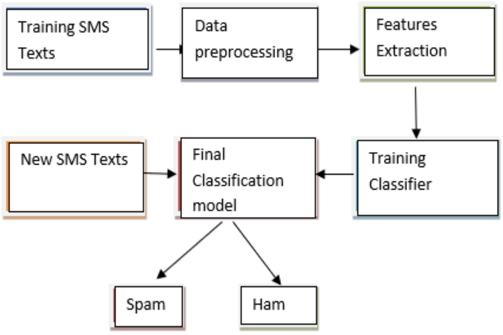

FIGURE 2. SMS

5. Data Collection

- Our utilized data in this study was collected from UCI repository that contains 4,827 legitimate messages and 747 mobile spam messages, a total of 5,574 short messages.
- To the best of our knowledge, it is the largest available SMS spam corpus that currently exists.
- The following table shows the basic description of the collected data.

Copyright@ REST Publisher

Many SMS Spam messages detection techniques are available these days to block spam messages and filter them. The most famous machine learning algorithm used in spam filtering are the following:

Naive Bayes (NB): it is considered one of the simplest classification methods. It got its name from the famous Bayes theorem and it works by learning from observing each feature individually.

Random Forests: A random forest is just a composition of grouped trees. The way random forest algorithm works is that each branch of tree can produce predictions that are somehow different from other trees. That difference can give us a better generalization of the results by averaging them.

Logistic regression: This type of algorithm best suits binary classification. The goal of logistic regression is to find the best fitting that describe the relationship between dichotomous features. In other algorithm, our goal is to select parameters that minimize the sum of squared errors like in Naïve Bayes.

Support Vector Machine (SVM): the principle view of SVM is to find an "Optimal" hyperplane that best classify the learning data. The optimal solution produced by SVM are characterized by having the maximum margins from the input data. The simplest formulation of SVM is a linear one.

Example, suggesting new products for customers Unsupervised ML algorithms has evolved and caught the attention of researcher all around the world because of it strong ability to learn on completely strange environments. Some of its applications are:

- Data clustering: grouping data points based on how much are they similar to each other. The process should be mutually exclusive meaning a data point should not belong to two groups at the same time.
- Dimensionality reduction: this type of application reduces the number of features in among the data sets because real life data usually contain massive number of dimensions (features).
- Feature learning: this application preserves the common behavior patterns to form certain rules on what should go next on the pattern. This type works best in shopping experience to follow customers preferences.
- Anomaly detection: this type of applicationfocus on defining the outliers among data points. This type of application suits the best real-life problems that includes fault and virus detection.
- Naïve Bayes algorithm is a supervised learning algorithm, which is based on Bayes theorem and used for solving classification problems.
- It is mainly used in *text* classification that includes a high-dimensional training dataset.
- Naïve Bayes Classifier is one of the simple and most effective Classification algorithms which helps in building the fast machine learning models that can make quick predictions.
- It is a probabilistic classifier, which means it predicts on the basis of the probability of an object.
- Some popular examples of Naïve Bayes Algorithm are spam filtration, Sentimental analysis, and classifying articles.

Bayes' Theorem: Bayes' theorem is also known as Bayes' Rule or Bayes' law, which is used to determine the probability of a hypothesis with prior knowledge. It depends on the conditional probability. The formula for Bayes' theorem is given as:

P(A|B) = P(B|A) P(A)

P(B)

Where, (A|B) is Posterior probability: Probability of hypothesis A on the observed event B. P (B|A)is Likelihood probability: Probability of the evidence given that the probability of a hypothesis is true.

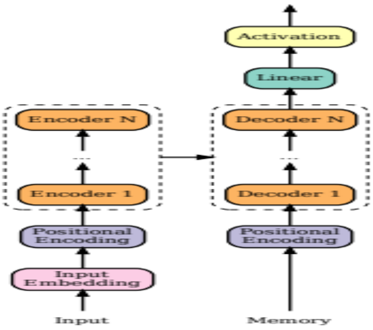

FIGURE 3. Data Collection

6. Architecture

Structure of proposed modified Transformer model for SMS spam detection. The input messages embeddings and memory (trainable parameters) are positional encoded, respectively. Then, the processed message vectors are passed to encoder layers, where the self-attention is performed. The results of encoder layers are passed to decoder layers. In decoder layers, the Multi-Head Attention is executed based on the results of encoder layers and the processed memory. Then, the decoded vectors are sent to some fully-connected linear layers, followed by a final activation function for classification layer in the original Transformer model is also removed since there are no target sequence texts anymore to be mapped to numeric vectors. Similar to the output sequence in the vanilla Transformer model, the positional information is injected into the memory at the positional encoding layer before being fed into decoders. During the training process, the parameters of memory are trained, and the memory matrix is expected to contain the important information that can help to predict whether or not a message is a spam.

7. Conclusion & Future Work

Since communication though mobile phones are increasingly becoming a necessity, subscribers became more demanding on having a safe mobile network. In this paper, different supervised ML classifiers has been tested based on performance and then tested by being a part of the final hybrid model. By comparing six different supervised model, SVM showed to have the highest precision with 0 false positive rate and KNN has the least performance among other classifiers. Then, after implementing different combination of hybrid models, merging K-means with SVM has stood out with the highest accuracy of 98.8%. So, even though overall, supervised algorithms have performed more accurately than unsupervised algorithm (k-mean), at the end hybrid system has achieved much better than a single classifier. So, we can conclude that using hybrid system best suits spam filtering system since it takes the advantage of both schemes of ML models and guarantee to deliver better classification results. At future development, more ML models can be tested and tried out to be part of the hybrid system. Furthermore, the results of can be brought up a little bit by adding more pre-processing steps such as including more Wight to $ sign in spam classification. Lastly, a real time application can be developed to interpret the suggested hybrid model and tested on real-time performancee.

Acknowledgment

I am delighted to express my heartfelt appreciation to our department's head and staff, as well as family and friends. This paper is made possible by their encouragement, assistance, and support.

References

[1]. P. Ghosh, S. Azam, K. M. Hasib, A. Karim, M. Jonkman and A. Anwar, "A Performance Based Study on Deep Learning Algorithms in the Effective Prediction of Breast Cancer," 2021 International Joint Conference on Neural Networks (IJCNN), 2021, pp. 1-8, doi: 10.1109/IJCNN52387.2021.9534293.

[2]. "statista," 2017. [Online]. Available: https://www.statista.com/statistics/483255/number-of mobile-messaging-users-worldwide/. [Accessed February 2019].

[3]. P. Sethi, V. Bhandari and B. Kohli, "SMS spam detection and comparison of various machine learning algorithms," in 2017 International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN), 2017.

[4]. D. D. Arifin, Shaufiah and M. A. Bijaksana, "Enhancing Spam Detection on Mobile Phone Short Message Service (SMS) Performance using FP Growth and Naive Bayes Classifier," in The 2016 IEEE Asia Pacific Conference on Wireless and Mobile (APWiMob), 2016.

[5]. K. Yadav, P. Kumaraguru, A. Goyal, A. Gupta and V. Naik, "SMSAssassin: crowdsourcing driven mobile based system for SMS spam filtering," in In Proceedings of the 12th Workshop on Mobile Computing Systems and Applications (pp. 1-6). ACM. 2011.

[6]. Han, Jiawei, M. Kamber and J. Pei, Data mining: concepts and techniques, 3rd Edition. Morgan, 2013.

[7]. M. Usama, J. Qadir, A. Raza, H. Arif, K.-L. Yau, Y. Elkhatib, A. Hussain and A. Al-Fuqaha, "Unsupervised Machine Learning for Networking: Techniques, Applications and Research Challenges," 2017.

[8]. Camponovo G, Cerutti D., “The spam issue in mobile business: A comparative regulatory overview”, Proc. 3rd Int. Conf. Mobile Bus., pp. 1-17.

[9]. Cleff E.B., “Privacy issues in mobile advertisin”’, Int. Rev. Law Comput.Technol., vol. 21, pp. 225-236.

[10]. Fu J, Lin P, Lee S. , “Detecting spamming activities in a campus network using incremental learning”, J. Netw. Comput. Appl., vol. 43, pp. 56-65.

[11]. Hua J, Huaxiang Z., “Analysis on the content features and their correlation of Web pages for spam detection”, China Commun., vol. 12, no. 3, pp. 84-94.

[12]. Dubey, Ratnesh& Mishra, Subha&Choubey, Dilip. “Recognizing Spam Emails/SMS Using Naive Bayes and Support Vector Machine.” Complex Systems and Complexity Science Journal, Vol.8 ISSN-NO 1672-3813, 2021.