SMS SPAM DETECTION USING MACHINE LEARNING

K.SUPARNA[1], VUDDARAJU VENKATA TARUN SAI VARMA [2]

1 **Assistant Professor MSc (CS), DEPT,** Dantuluri Narayana Raju College, **Bhimavaram, Andhra Pradesh**
Email id:- suparnakalidindi@gmail.com
[2]PG Student of MSc Computer Science, Dantuluri Narayana Raju College, **Bhimavaram, Andhra Pradesh**
Email id : **:-** tarunsaivarmavuddaraju@gmail.com

ABSTRACT

The number of people using mobile devices increasing day by day. SMS (short message service) is a text message service available in smartphones as well as basic phones. So, the traffic of SMS increased drastically. The spam messages also increased. The hackers try to send spam messages for their financial or business benefits like market growth, lottery ticket information, credit card information, etc. So, spam classification has special attention. In this paper, we applied various machine learning and deep learning techniques for SMS spam detection. we used a dataset to train the machine learning and deep learning models like LSTM and NB. The SMS spam collection data set is used for testing the method. The dataset is split into two categories for training and testing the research. Our experimental results have shown that our NB model outperforms previous models in spam detection with an accuracy of good.

1 INTRODUCTION

The increasing mobile phones become one of the attached companions for many individuals. With the explosive penetration of mobile devices and millions of people sending messages every day, Short Message Service (SMS) has become a multi-million-dollar commercial industry with a value between 11.3 to 24.7 percent of the developing countries' Gross National Income (GNI) in the early year of 2013.

As the utilization of mobile phone devices has become commonplace, Short Message Service (SMS) has grown into a multi-billion dollars commercial industry [2]. SMS is a text communication platform that allows mobile phone users to exchange short text messages (usually less than 160 seven-bit characters). It is the most widely used data application with an estimated 3.5 billion active users, or about 80% of all mobile phone subscribers at the end of 2010 [3]. As the popularity of the platform has increased, we have seen a surge in the number of unsolicited commercial advertisements sent to mobile phones using text messaging. SMS spam is still not as common as email spam, where in 2010 around 90% of emails was spam, and in North America it is still not a major problem, contributing to less than 1% of text messages exchanged as of December 2012.

The spam increased in these days due more mobile devices deployed in environment for e-mail and message communication. Currently, 85% of mails and messages received by mobile users are spam. The cost of mails and messages are very low for senders but high for receipts of these messages. The cost paid some time by service providers and the cost of spam can be measured in the loss of human time and loss of important messages or mails. Due to these spam mails and messages, the values able e-mails and messages are affected because each user have limited Internet services, short time, and memory.

2. LITERATURE SURVEY AND RELATED WORK

Author: Pumrapee Poomka, Wattana Pongsena, Nittaya Kerdprasop, and Kittisak Kerdprasop
YEAR: - 2019
Abstract:

An SMS spam is the message that hackers develop and send to people via mobile devices targeting to get their important information. For people who are ignorant, if they follow the instruction in the message and fill their important information, such as internet banking account in a faked website or application, the hacker may get the information. This may lead to loss their wealth. The efficient spam detection is an important tool in order to help people to classify whether it is a spam SMS or not. In this research, we propose a novel SMS spam detection based on the case study of the SMS spams in English language using Natural Language Process and Deep Learning techniques. To prepare the data for our model development process, we use word tokenization, padding data, truncating data and word embedding to make more dimension in data. Then, this data is used to develop the model based on Long Short-Term Memory and Gated Recurrent Unit algorithms. The performance of the proposed models is compared to the models based on machine learning algorithms including Support Vector Machine and Naïve Bayes. The experimental results show that the model built from the Long Short-Term Memory technique provides the best overall accuracy as high as 98.18%. On accurately screening spam messages, this model shows the ability that it can detect spam messages with the 90.96% accuracy rate, while the error percentage that it misclassifies a normal message as a spam message is only 0.74%.

Haslina Md Sarkan, Yazriwati Yahya, Suriani Mohd Sam, 2019,Abstract:The daily traffic of Short Message Service (SMS) keeps increasing. As a result, it leads to dramatic increase in mobile attacks such as spammers who plague the service with spam messages sent to the groups of recipients. Mobile spams are a growing problem as the number of spams keep increasing day by day even with the filtering systems. Spams are defined as unsolicited bulk messages in various forms such as unwanted advertisements, credit opportunities or fake lottery winner notifications. Spam classification has become more challenging due to complexities of the messages imposed by spammers. Hence, various methods have been developed in order to filter spams. In this study, methods of term frequency-inverse document frequency (TF-IDF) and Random Forest Algorithm will be applied on SMS spam message data collection. Based on the experiment, Random Forest algorithm outperforms other algorithms with an accuracy of 97.50%

Author: Shah Nazir,2 Habib Ullah Khan,3 and Amin Ul Haq YEAR: - 2020Abstract:The spam detection is a big issue in mobile message communication due to which mobile message communication is insecure. In order to tackle this problem, an accurate and precise method is needed to detect the spam in mobile message communication. We proposed the applications of the machine learning-based spam detection method for accurate detection. In this technique, machine learning classifiers such as Logistic regression (LR), K-nearest neighbor (K-NN), and decision tree (DT) are used for classification of ham and spam messages in mobile device communication. The SMS spam collection data set is used for testing the method. The dataset is split into two categories for training and testing the research. The results of the experiments demonstrated that the classification performance of LR is high as compared with K-NN and DT, and the LR achieved a high accuracy of 99%. Additionally, the proposed method performance is good as compared with the existing state-of-the-art methods.

Author: Sridevi GaddeYEAR: - 2021,Abstract:The number of people using mobile devices increasing day by day.SMS (short message service) is a text message service available in smartphones as well as basic phones. So, the traffic of SMS increased drastically. The spam messages also increased. The spammers try to send spam messages for their financial or business benefits like market growth, lottery ticket information, credit card information, etc. So, spam classification has special attention. In this paper, we applied various machine learning and deep learning techniques for SMS spam detection. we used a dataset from UCI build a spam detection model. Our experimental results have shown that our LSTM model outperforms previous models in spam detection with an accuracy of 98.5%. We used python for all implementations.

Author: Houshmand Shirani-Mehr, hshirani@stanford.eduYEAR: - 2019Abstract:Over recent years, as the popularity of mobile phone devices has increased, Short Message Service (SMS) has grown into a multi-billion dollars industry. At the same time, reduction in the cost of messaging services has resulted in growth in unsolicited commercial advertisements (spams) being sent to mobile phones. In parts of Asia, up to 30% of text messages were spam in 2012. Lack of real databases for SMS spams, short length of messages and limited features, and their informal language are the factors that may cause the established email filtering algorithms to underperform in their classification. In this project, a database of real SMS Spams from UCI Machine Learning repository is used, and after preprocessing and feature extraction, different machine learning techniques are applied to the database. Finally, the results are compared and the best algorithm for spam filtering for text messaging is introduced.

Final simulation results using 10-fold cross validation shows the best classifier in this work reduces the overall error rate of best model in original paper citing this dataset by more than half.

3 EXISTING SYSTEM

Random Forest (RF) algorithm will used for classification of ham or spam during this phase. RF is averaging ensemble learning method that can be used for classification problem. This algorithm combines various decision tree models in order to eliminate the over fitting problem in decision trees. In RF algorithm, each tree is capable in providing its own prediction results, different from each other. As a result, each tree gives different performances, in which the average of their performances will be generalized and calculated. During the training phase, a set of decision trees will be constructed before they can operate on randomly selected features. Regardless, RF can work well with a large dataset with a variety of feature types, similar to binary, categorical and numerical. The algorithm works as follows diagram: for each tree in the forest, a bootstrap sample is selected from S where S (i) represents the ith bootstrap. A decision-tree is then learn using a modified decision-tree learning algorithm.

Proposed system:

applying NB algorithm to the dataset using extracted features with different training set sizes. The performance in learning curve is evaluated by splitting the dataset into 70% training set and 30% test set. The NB algorithm shows good overall accuracy.

We notice that the length of the text message (number of characters used) is a very good feature for the classification of spams. Sorting features based on their mutual information (MI) criteria shows that this feature has the highest MI with target labels. Additionally, going through the misclassified samples, we notice that text messages with length below a certain threshold are usually hams, yet because of the tokens corresponding to the alphabetic words or numeric strings in the message they might be classified as spams.

By looking at the learning curve, we see that once the NB is trained on features extracted, the training set error and test set error are close to each other. Therefore, we do not have a problem of high variance, and gathering more data may not result in much improvement in the performance of the learning algorithm. As the result, we should try reducing bias to improve this classifier. This means adding more meaningful features to the list of tokens can decrease the error rate, and is the option that is explored next.

4 PROPOSED WORK AND ALGORITHM

- Complexity is less compared to previous process
- Ability to learn and extract complex features.
- Accuracy is good
- With its simplicity and fast processing time, the proposed algorithm gives better execution time.
- Both machine learning and deep learning technique is performed to predict the value effectively.
- Prediction is accurate.

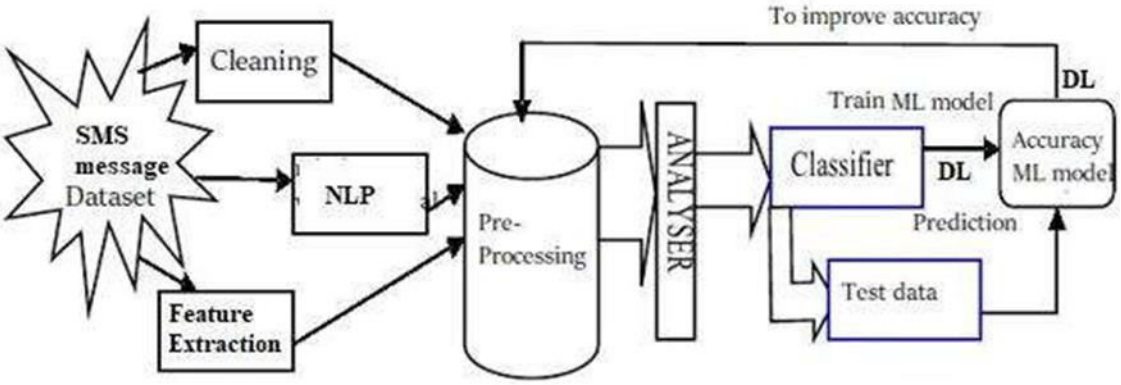

FIG 1: SYSTEM ARCHITECTURE

5 METHODOLOGIES

MODULES

There are various machine learning models you can use to build a spam SMS detector. Here's a simplified outline of the process:

Data Collection: Gather a dataset of SMS messages labeled as either spam or not spam (ham).

Data Preprocessing: Clean and preprocess the text data, which may involve tasks like tokenization, lowercasing, and removing punctuation.

Feature Extraction: Convert text data into numerical features. Common techniques include TF-IDF (Term Frequency-Inverse Document Frequency) and word embeddings like Word2Vec or GloVe.

Model Selection:

Naive Bayes: A simple and effective algorithm for text classification.

Support Vector Machines (SVM): Can be used with various kernel functions.

Random Forest: An ensemble method that can handle a wide range of features.

Neural Networks: You can use deep learning modelslike Recurrent Neural Networks (RNNs) or Convolutional Neural Networks (CNNs) for more complex patterns.

Model Training: Split your dataset into training and testing sets. Train your chosen model(s) on the training data.

Model Evaluation: Evaluate your model's performance using metrics like accuracy, precision, recall, F1-score, and ROC-AUC on the testing data.

Hyperparameter Tuning: Fine-tune your model by adjusting hyperparameters like learning rate, regularization strength, and model architecture.

Deployment: Once satisfied with the performance, deploy your model to detect spam SMS messages in real-time.

Continuous Improvement: Monitor the model's performance and update it as needed to adapt to changing spam patterns.

Remember that the choice of model and preprocessing techniques may vary based on your specific dataset and requirements. Additionally, you might consider using a combination of models or ensemble methods for improved accuracy.

6 RESULTS AND DISCUSSION SCREENSHOTS

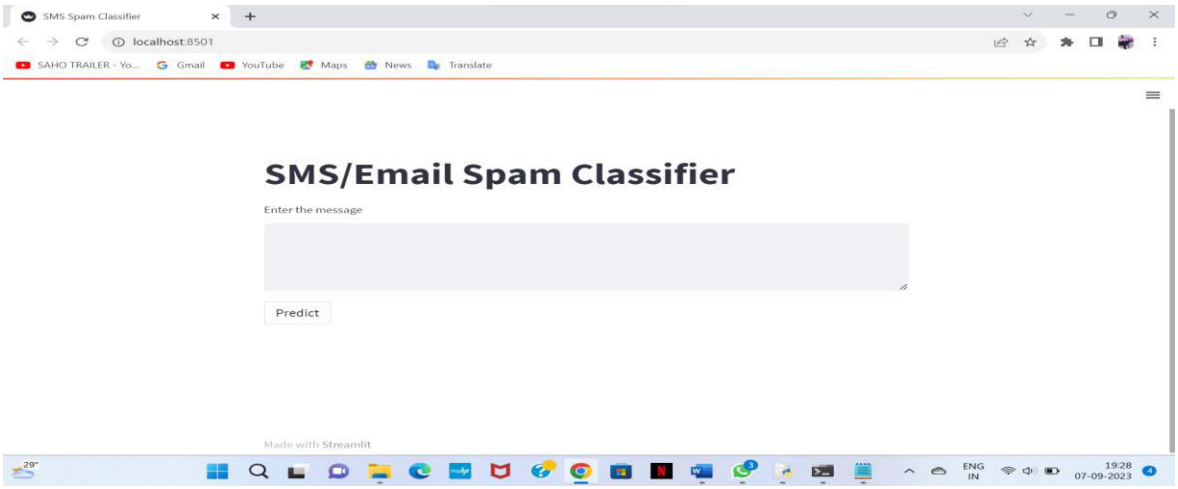

Fig2: Home Page

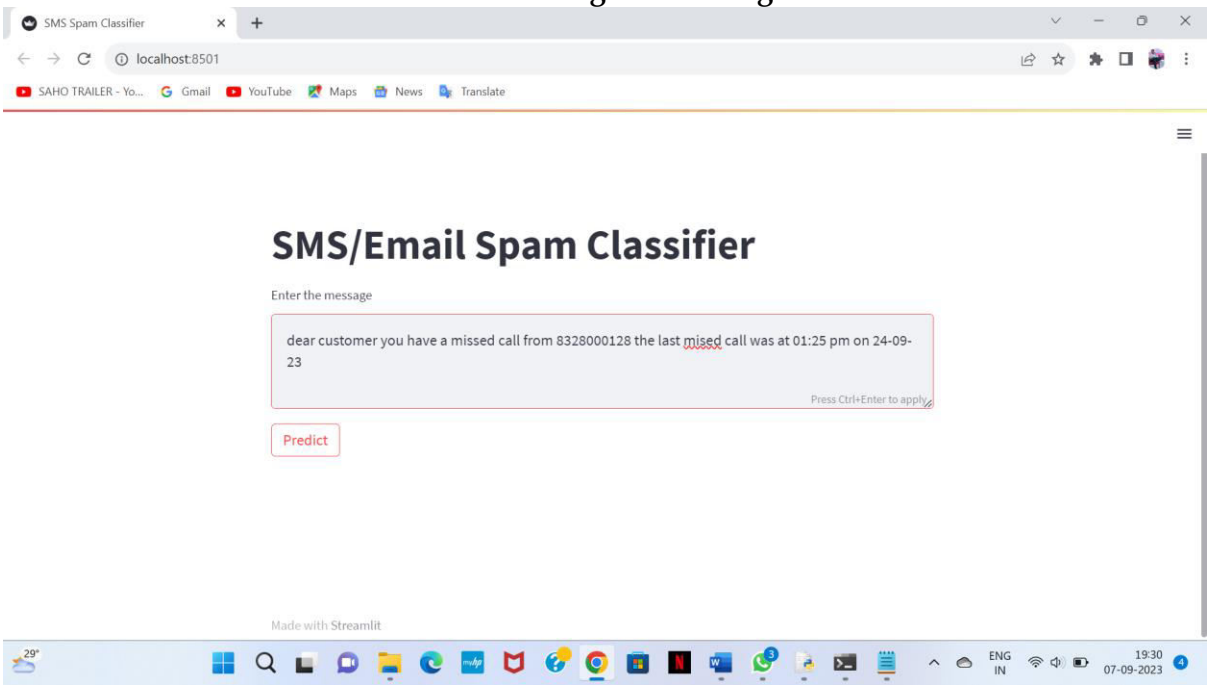

Fig3 : User Input Text

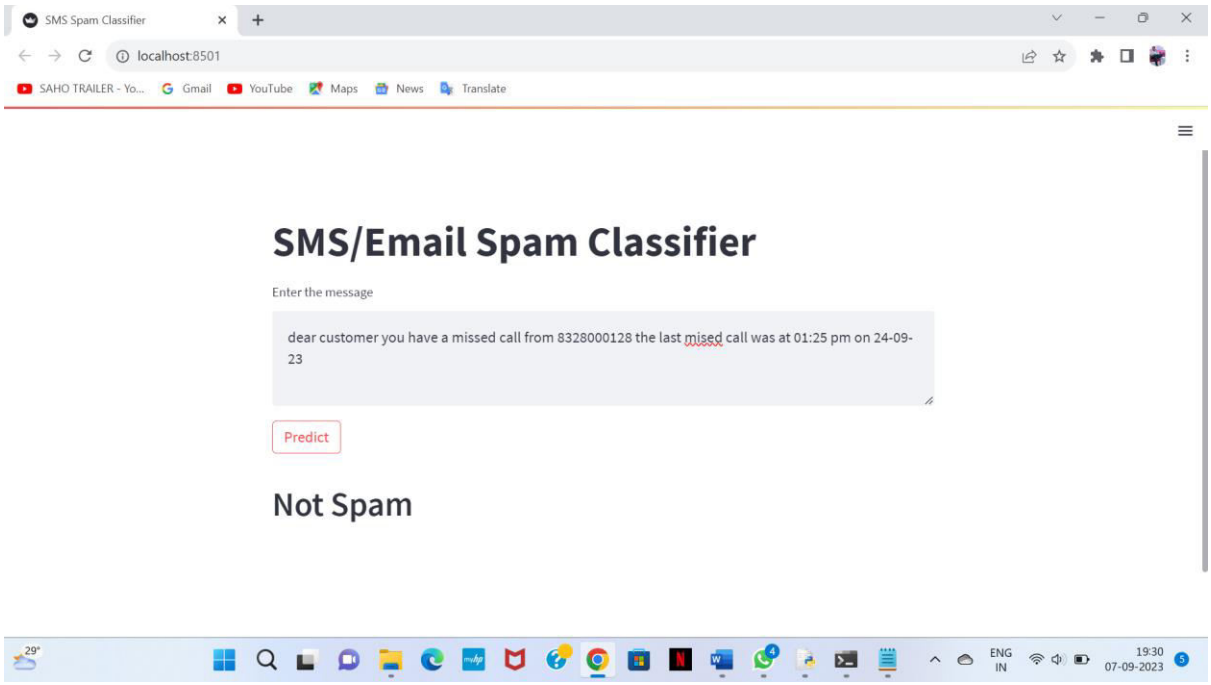

Fig4 : PREDICTED RESULT

6.CONCLUSION AND FUTURE SCOPE

The SMS spam message problem is plaguing almost every country and keeps increasing without a sign of slowing down as the number of mobile users increase in addition to cheap rates of SMS services. Therefore, this paper presents the spam filtering technique using various machine learning algorithms. Based on the experiment, TF-IDF with Nave bayes classification algorithm outperforms good compare to other algorithm like LSTM in terms of accuracy percentage. However, it is not enough to evaluate the performance based on the accuracy alone since the dataset is imbalanced. After some examinations, NB algorithm still manages to provide good precision and f- measure with 0.98 of precision while 0.97 for f-measure. Different algorithms will provide different performances and results based on the features used. For future works, adding more features such as message lengths might help the classifiers to train data better and give better performance.It would be great to perform a comparative study between the Machine learning classifiers and Deep learning models.

Future scope:

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.

7 REFERENCES

[1] Modupe, A., O. O. Olugbara, and S. O. Ojo. (2014) ―Filtering of Mobile Short Messaging Communication Using Latent Dirichlet Allocation with Social Network Analysis‖, in Transactions on Engineering Technologies: Special Volume of the World Congress on Engineering 2013, G.-C. Yang, S.-I. Ao, and L. Gelman, Eds. Springer Science & Business. pp. 671–686.

[2] Shirani-Mehr, H. (2013) ―SMS Spam Detection using Machine Learning Approach.‖

[3] Abdulhamid, S. M. et al., (2017) ―A Review on Mobile SMS Spam Filtering Techniques.‖ IEEE Access 5: 15650–15666.

[4] Aski, A. S., and N. K. Sourati. (2016) ―Proposed Efficient Algorithm to Filter Spam Using Machine Learning Techniques.‖ Pac. Sci. Rev. Nat. Sci. Eng. 18 (2):145–149.

[5] Narayan, A., and P. Saxena. (2013) ―The Curse of 140 Characters: Evaluating The Efficacy of SMS Spam Detection on Android.‖ p. 33– 42.

[6] Almeida, T. A., J. M. Gómez, and A. Yamakami. (2011) ―Contributions to the Study of SMS Spam Filtering: New Collection and Results.‖ p. 4.

[7] Mujtaba, D. G., and M. Yasin. (2014) ―SMS Spam Detection Using Simple Message Content Features.‖ J. Basic Appl. Sci. Res. 4 (4): 5.

[8] Gudkova, D., M. Vergelis, T. Shcherbakova, and N. Demidova. (2017) ―Spam and Phishing in Q3 2017.‖ Securelist - Kaspersky Lab‘s Cyberthreat Research and Reports. Available from: https://securelist.com/spam-and-phishing-in-q3-2017/82901/. [Accessed: 10th April 2018].