SMS SPAM DETECTION

INTERNSHIP PROJECT REPORT

SMART BRIDGE

**Presented by-**

Tariq Ahmed

Vamshi Kiran

Sai Seravan Bodipudi

Sushant Lenka

**CONTENTS**

Abstract

1.Introduction

2.Existing Problem

3.Proposed Solution

4.Related work

5.Proposed Methodology

5.1 Dataset collection

5.2 Flow chart

5.3 Feature extraction

5.4 Model building

5.5 Detection and Classification

5.6 Result

6.Applications

7.Advantages

8.Disadvantages

9.Conclusion

10.Future work

11.Bibliography

APPENDIX: Source Code

**ABSTRACT:** In modern years, the fame of cell phone gadgets has expanded; Short Message Service (SMS) has developed into a multi-billion dollars business. In the meantime, decrease in the cost of messaging services have brought about development in spontaneous business ads (spams) being sent to cell phones. SMS spams are one of the concerns and a lot of individuals do not like to accept them as they are annoying. Many SMS spam discovery techniques already exist and various classifiers like Support Vector machine, NaïveBayes and several other machine learning algorithms were utilized. The proposed framework classifies the SMS spam and ham by means of Artificial Neural Network (ANN) classifier using SMS Spams database from [www.kaggle.com](http://www.kaggle.com) . ( Keywords: SMS , Ham, Spam, Artificial Neural Network )

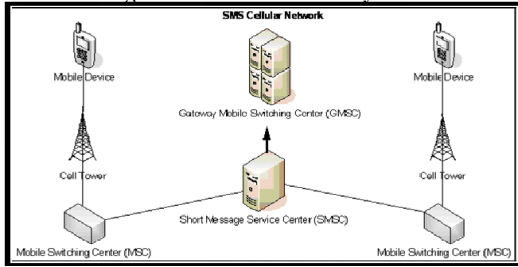
1.**INTRODUCTION :**

In recent years, a substantial growth has been experienced in the mobile phone market. A cumulative of 432.1 million mobile gadgets has delivered in the second quarter of 2013 with an increment of6.0% year over year . As the consumption of cellphone gadgets has turned out to be ordinary, Short Message Service(SMS) has developed into a multi-billion dollars‟ business . A rush in the quantity of unwanted business notices sent to cell phones utilizing text messages has additionally expanded due to the increased popularity of mobile platforms. One of the most prominent methods of communication between a huge numbers of individuals is SMS, where transmission of messages must happen as per the communication standard protocols. Consequently, there is a requirement for text categorization algorithms that can be utilized as a part of classifying the messages either to ham or spam messages. While spam messages are not alluring, ham messages are the one that is made by genuine users. Therefore spam messages must be identified and detached once they reach the mobile station, example of spam messages are the ones created by promotional companies. The additional consequences of the SMS spam are frustrating, they are also consuming more time, resources, money and network bandwidth, in any case the accessibility of spam filtering software for identifying SMS spam are limited. Moreover, there is an additional misclassification problem that may be arising when ham messages are eliminated and blocked as spam. In this paper we have proposed a system to develop a SMS spam detector using neural networks

**2. EXISTING PROBLEM:**

A recent report from Local Circles has surveyed more than 12,000 participants to get their opinion on spam SMS and how big an issue it is for them. The LocalCircles survey found that more than 78 percent of the respondents were getting four or more spam SMS every day. Which turns out to be 28 SMS on an average in a week and if 78 percent of 12,000 people are saying this, then telcos have a big problem on their hands. Speaking of telcos, 34 percent people said that at least a quarter of the unwanted SMS messages are coming from the service provider itself. This is where entities like the Telecom Regulatory Authority of India (TRAI) and Department of Telecom (DoT) need to intervene and ask telcos to stop with the spamming. Interestingly enough, TRAI had released a regulation to counter the spam SMS issue, but businesses have hardly adhered to it and the issues faced by consumers clearly show that. Text messaging has greatly increased in popularity in the past five years and the government is trying to keep up with rapidly changing technology. Although SMS spam is less prevalent than email spam, it still accounts for roughly 1% of texts sent in the United States and 30% of text messages sent in parts of Asia.

The below figure shows travel map of an SMS among two parties:



**3. PROPOSED SOLUTION:**

There are many methods to build a SMS spam classifier. Some of them include using SVM based algorithms , Naïve Bayes Technique , Neural Networks, Evolutionary Algorithms, etc… . In this paper , we use Binary classification via Artificial Neural Networks to classify the given message as “ham” or “spam” and later develop a web application in order to test whether a given input message is a spam or not.

**4. RELATED WORK:**

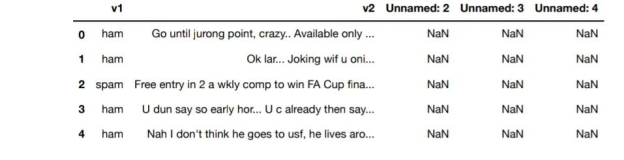
The issues of mobile SMS spam is addressed utilizing filtering system; however the execution of spam discovery is imperative and must achieve sufficient level by making certain adjustment on filtering strategies. Gordon V. Cormacket. altried to expand the execution of SMS spam discovery by applying the similar filter utilized as an email spam filters which accomplished the most elevated execution . For testing two datasets were utilized, one for English and another for Spanish. English dataset comprises of 1002 hams and 82 spams, while Spanish holds 1157 genuine and 199 spams. The greater part of machine learning calculations that were connected in vector interpretation of messages utilized for certain features, for example, words, bigram and trigram of characters, words bigrams and lowercase words. Email filtering algorithms has becoming failed to meet expectations when utilized with SMS spam, the reasons of this mentions to various reasons: messages with restricted set of features, there was no genuine database for SMS spam, the casual dialect of the messages and its short length. Consequently, a genuine database of SMS spams was made in 2011 UCI Machine Learning repository, this database was made and was made openly accessible . Therefore, many investigations were made in this dataset and examinations between various machine learning calculations occur in . In the beginning two tokenizers were utilized, the first tokenizer was used to divide the words in patterns containing colons, dots or commas, at the interior such as email, and the other one focuses on the splitted sequence of characters separated by commas, blanks, dots and others In any case, no pre-preparing was utilized, for example, stop word elimination or stemming since numerous scientists found that such pre-processing may influence the precision. Then again, correlations between numerous classifiers were made and all outcomes demonstrated that linear Support Vector Machine is the best. Additionally, as no stemming was utilized, while uncommon characters were evacuated and dataset was split into tokens: the quantity of numeric strings, number of dollar signs ($) and the length of the message, uncommon characters, for example, "://" and "@" are essential to arrange messages. Accordingly, the investigation demonstrated that the message length considered as a good measure to identify spams. Binary classification has been used with Artificial Neural Networks to classify a message as ham or spam and a web application has been developed for the neural network code.

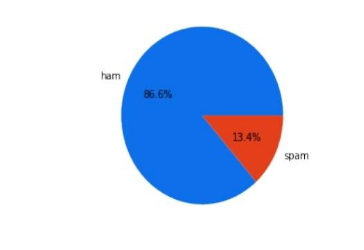
**5. PROPOSED METHODOLOGY:**

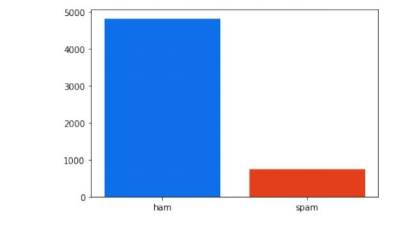
Theoverall system design of the proposed method is shown in Fig. 1. Dataset collectionphaseincludes the collection of spam and ham messages. Feature extraction phase includes pre-processing and normalization. Feature selection and pre-training of the selected features are performed using neural networks. Finally, ANN classifier is used in the binary classification of SMS data samples**.**

**5.1. Dataset Collection:**

The ham and spam SMS messages are gathered from UCI Machine Learning warehouse which was assembled in 2012 . The dataset comprises of 5574 wording messages classified as ham and spam messages, the quantity of spam messages is 13.4% while the quantity of ham messages is 86.6%. The dataset is saved in a text file where each line represents one message; the line consists of label of a message and text string. Table below displays examples of messages in dataset







**5.2 Flow Chart:**

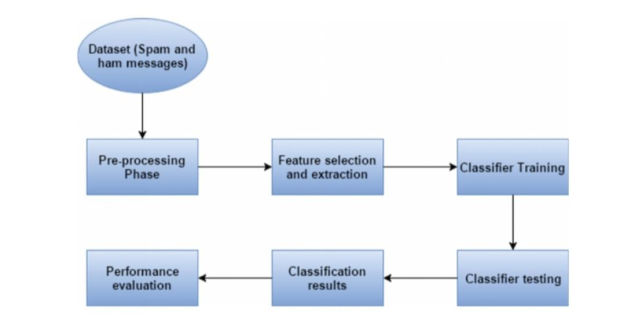


Fig 1: System architecture

**5.3 Feature Extraction:**

In this section , we discuss about changes made to the dataset parameters which have been removed from the dataset that are un-necessary for the prediction of a spam SMS.

1. Removal of numbers and digits in the messages
2. Removal of null columns in the dataset
3. Removal of special characters such as @,$,&,#,etc…
4. Converting each alphabet into lower case so that the model can consider words like “They” and “they” as same words.
5. Removal of punctuations such as ! , . ? < > { } [ ] etc…

**5.4 Model Building:**

After feature extraction, we further proceed towards model building. The following steps have been involved in model building:

1. At first we import count vectorizer from sklearn.feature\_extraction library followed by splitting of the data into X train and Y train and X test and Y test
2. Obtain the shape of splitted data
3. With keras , import prerequisites and build Artificial Nueral Network
4. Train the model built
5. Test the model and deploy it

**5.5 Detection And Classification:**

The pre-trained data is divided into training data (80%) and testing data (20%) before providing it to Artificial Neural Network (ANN) classifier. The training data is fed into the ANN classifier and the network is trained in order to detect the spam & ham SMS messages. The trained ANN classifier is used to predict the SMS in the testing data. ANN performs a binary classification to identify whether the SMS is spam or ham messages

**5.6 RESULT:**

The proposed work is developed in “Jupyter notebook” in python using machine with the configuration,16 GB RAM memory and Intel(R) Core(TM) i7 1.80 GHz processor. The accuracy of this ANN based SMS spam detector turned out to be : 97.7%

**6. APPLICATIONS:**

At the very least, spam SMS or email is a nuisance that will clog up your employees’ inboxes and overload your servers. Spam is also dangerous — the entry point for serious attacks that could damage your computers or mobiles, your computer network, your bottom line, and even your company’s reputation. Yes, you need a spam filter solution as the key first line of defense.

When you decide to invest or upgrade your spam filter solution, know that there are countless spam filter programs out there and it will take time to figure out which one works best for your business.

Here are a few key things to look for:

1. At a minimum, the solution you choose must block spam. This might sound like a given, but not all spam filter software is up to the job (or doesn’t keep up to date with the evolving world of spam attacks).
2. The solution you choose must provide the security you need for your network, but not stop the legitimate emails your employees need to conduct their business.

Administrators must have the ability to edit and create rules over and above predefined rule settings so that the solution meets your organizational needs. This customization should be easy, even for unsophisticated computer users.

**7. ADVANTAGES OF SMS SPAM FILTERING:**

To increase efficiency and safeguard your business or personal data from potential risk, it is essential to take advantage of various spam filtering services available. Following are some of the important benefits of spam filtering :

1. **PROTECTION AGAINST VIRUS:**

Spam emails are not just innocent marketing tools they can be carriers of dangerous computer viruses. Just one click on the wrong SMS/ email can debilitate your network. Filters can provide a great firewall.

1. **KEEPING HACKERS AT BAY:**

In addition to dangerous viruses, hackers can also gain access to your device through a benign looking email. A filter that blocks spam SMS/ emails from reaching your message inbox can save your important data.

1. **SAVING TIME:**

Spam filtering can save time. Business employees do not have to go through numerous SMS/emails to decide which ones are spams, as sometimes that can be hard to decide. The time saved can be used to increase productivity.

1. **KEEPING YOUR REPUTATION INTACT:**

Spam filters can help keep a company maintains its reputation. They can block viruses from reaching consumers data and prevent any spam sms/mail accidentally being forwarded to consumers.

1. **CUSTOMIZED SERVICES:**

Anti-spam software and programs can be tailored to your needs. You can create a blacklist of SMS/email addresses that often send you spam. A whitelist contains all the SMS/email addresses of your important associates. Many anti-spam filters offer the service of keeping the spam SMS/ emails saved for a few days. It allows you to make sure that no useful SMS emails are being deleted together with the junk sms.

These are some of the benefits of spam filtering .

**8. DISADVANTAGES OF USING SPAM FILTER:**

The biggest disadvantage of using an spam filter is that you may end up with messages being identified as being spam through a mistake of the algorithm that is used. According to many specialists across the globe, even with the very best spam filters on the market you can still end up with messages being improperly labelled.

While missing out on important emails is a nuisance, we need to think about the fact that you can also miss the same SMS/emails if you receive a lot of spam. How can you see that message from the boss if there are hundreds of

SMS/emails sent every single day? You can be highly attentive and still miss out on some SMS/emails.

**9. CONCLUSION :**

The proposed work demonstrates that deep learning method using ANN can be successfully applied in SMS spam detection and classification domain. This deep learning model not only learns high dimensional representations but also performs efficient classification tasks. The test comes about on SMS spam dataset demonstrates that ANN can learn a better generative model and perform well on SMS spam recognition task.

**10. FUTURE WORK:**

For future study, application a full‐featured hybrid implementation on a mobile phone and give it to many users. After several months, we can obtain the real performance for each real user. We also need to find better features for SMS classification to improve accuracy. Text Classification techniques have gained maturity, but feature extraction and vector creation, such as character *n* ‐gram and word *n* ‐gram, are still challenging. Another area for future research is stylistic features, such as special characters, for example, “:)” (smiling) or “T\_T” (crying)

**11.BIBLIOGRAPHY:**

**Dataset:**

<https://www.kaggle.com/uciml/sms-spam-collection-dataset>

**References:**

International Journal of Pure and Applied Mathematics Volume 119 No. 18 2018, 2425-2436

**APPENDIX:**

Source Code-

import pandas as pd   
import numpy as np  
import pickle  
dataset = pd.read\_csv('spam.csv', encoding = 'latin-1')  
dataset = dataset.iloc[:, :2]   
dataset.columns = ['Outcome', 'Message']   
from sklearn.preprocessing import LabelEncode  
le=LabelEncoder()   
dataset['Outcome']=le.fit\_transform(dataset['Outcome'])  
import matplotlib.pyplot plt   
plt.figure()  
plt.pie(dataset.Outcome.value\_counts() , labels = ['ham','spam'])  
plt.bar(['ham','spam'], dataset.Outcome.value\_counts())  
import re  
import nltk  
nltk.download('stopwords')  
from nltk.corpus import stopwords  
from nltk.stem.porter import PorterStemmer   
ps = PorterStemmer()  
data = []  
for i in range(len(dataset)):  
text = dataset['Message'][i]  
text = re.sub('[^a-zA-Z]',' ',text)  
text = text.lower()  
text = text.split()  
text = [ps.stem(word) for word in text if not word in set(stopword text = ' '.join(Text)  
data.append(text)  
from sklearn.feature\_extraction.text import CountVectorizer   
cv=CountVectorizer(max\_features=8000)   
x=cv.fit\_transform(data).toarray()  
with open('CountVectorizer','wb') as file:   
pickle.dump(cv,file)  
pickle.dump(cv,open('count\_vec.pkl','wb'))   
y=dataset.iloc[:,0].values  
from sklearn.model\_selection import train\_test\_split   
x\_train,x\_test,y\_train,y\_test = train\_test\_split(x, y, test\_size=0.2,random\_state=0)  
import keras  
from keras.models import Sequential   
from keras.models import load\_model   
from keras.layers import Dense  
model = Sequential()  
model.add(Dense(units = 6302, activation = 'relu',init = 'uniform' ))  
model.add(Dense(units = 5000, activation = 'relu',init = 'uniform' ))  
model.add(Dense(units = 1303, activation = 'relu',init = 'uniform' ))  
model.add(Dense(units = 1, activation = 'sigmoid',init = 'uniform' ))  
model.compile(optimizer = 'adam',loss = 'binary\_crossentropy',metrics = [‘accuracy’])  
model.fit(x\_train,y\_train,batch\_size =4459, epochs = 20)  
model.save('sms-model.h5')