International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 3

A Survey: SMS Spam Filtering

Riya Mehta, Ankita Gandhi
Department of Computer Science & Engineering,
Parul Institute of Engineering & Technology, Vadodara, Gujarat, India

ABSTRACT

Now a days Short Message Service(SMS) is most popular way to communication for mobile user because it is cheapest mode or version for communication than other mode.SMS is used for transmitting short length msg of around 160 character to different devices such as smart phones, cellular phones, PDAs using standardized communication protocols. The amount of Short Message Service (SMS) spam is increasing. SMS spam should be put into the spam folder, not the inbox. The growth of the mobile phone users has led to a dramatic increase in SMS spam messages. To avoid this problem SMS filtering Techniques are used. Our proposed approach filters SMS spam on an independent mobile phone on a large dataset and acceptable processing time. There are different approaches able to automatically detect and remove most of these messages, and the best-known ones are based on Bayesian decision theory and Support Vector Machines.

Keywords: *SMS spam; Spam Filtering; style; Text classification; Naïve bayes ; SVM*

I. INTRODUCTION

In recent years, our era has witnessed a rapid development of mobile communications. The Short Message Service (SMS) has also become a popular communication service.[5]The term spam is generally used to denote an unsolicited commercial messages. The problem of spam can be quantified in economical terms since many hours are wasted everyday by workers. It is not just the time they waste reading the spam but also the time they spend deleting those messages. Almost 30 years ago, Denning stated that "Every inbox is accessible to any sender" This situation leads to electronic junk. The Short Message Services (SMS) is the most popular communication media because of its low price, convenient, mobility, personalization, and documentation. Spammers use SMS to send spam messages to users, since SMS provides more personal textual communication than email. According to the Korea Information Security Agency (KISA), the number of unwanted SMS and phone calls to mobiles surpasses that of email spam. [1] SMS is used as an alternate for voice calls in positions where voice communication is either not possible or not desired between the end phone users. Today's estimates signify that billions of SMS's are sent per day.[2]

Million of people Send the SMS for communication in daily life but the main Problem of user is Spam SMS. [6] The Definition of Spam SMS does not very much in Case of Emails or SMS Spam in simple word the it can be Describe as "Unsolicited Bulk Message" these are unwanted for the user Sent by Sander [6] due to low price the company and Spammer used this service for marketing and promotion. This message is not use full for user and its message is consume the networked bandwidth so it reduced networked Efficiency. So the main objective of the Spam SMS filtering to reduce or blocks the unwanted message Send by the Spammer. part of a larger collection of messages, all having substantially identical content. The purposes of SMS spam are advertisement and marketing of various products, sending political issues, spreading inappropriate adult content and internet offers. Spam SMS causes many issues for mobile users.. Users may accidentally call to premium rate numbers or call for expensive services by replying to these messages by mistake. They may

suffer financial loss from these messages by reacting to them. So, SMS Spam is some serious problem.

However, opening rates of SMS are higher than 90% and opened within 15 minutes of receipt whereas opening rate in email is only 20-25% within 24 hours of receipt. Thus, a proper SMS spam detection technique is very needful. There are several researches on email, twitter, web and social media spam detection techniques.

However, a very few researches have been conducted on SMS spam detection. Spam SMS detection is more challenging than email spam detection because of the restricted length of SMS, use of regional content and shortcut words and SMS contains less header information than an email. Proper SMS spam detection technique is needed to be identified. This is an open and comparatively new research field. There is a huge scope of research work in this field. A Systematic Literature Review (SLR) is necessary for starting any kind of research in any research field.

The communication service provider provides the service DND (do not disturb) which stops the unwanted spam messages .When DND service restrict the messages over mobile phones, some spammers send promotional messages by converting it tinto transactional messages and sent it to user. The advertiser comes with solution that send the promotional messages through the spammers mobile phone because there is not at all any restriction for messages sent through spammers mobile for communication.

For developing a SMS spam filtering system on mobile phone, with the following characteristics is important.

a) Independent: It does not need for a supporting computer system or server. Thus, training and updating the filtering system will be performed on mobile phone. It will reduce communication cost between mobile phone and server, hardware maintenance and infrastructure cost.

b) Private: The filtering system must be able to ensure user's privacy. The filtering system should not store user's SMS to anywhere. Storing SMS to the third party can raise privacy concerns, especially SMS ham, which may consists of private data.

c) Secure: In terms of security, spammer should not be able to access the filtering system because the spammer can create SMS spam that can fool the filtering system.

d) Personal: Each user has different perception of SMS spam Some users may say that a SMS is spam, the others may say not. Thus, users should have the chance to create their own filtering system by choosing the data set themselves.

e) Simple: The users cannot wait to start filtering SMS spam until they have a large amount of data for training data set. Thus, the filtering system must be able to start filtering SMS spam using small number of training data set. Simple also means that users does not have to configure connection between mobile phone and computer system.

f) Updatable: The filtering system must be able to adapt to new SMS characteristics by continuously updating the filtering system when receiving new incoming SMS.

Source of spam are Botnet, Directory harvest Attacks, Internet Hoaxes and chain process, Social Networking, Backscatter.

In this paper, we present an extended version of filtering techniques. We also present summary of currently available methods ,challenges and future research work and directions for SMS spam detection and filtering. First, it provides taxonomy of techniques: Second, it provides allover analysis of these techniques; Third, it examines all datasets which is available and then identifies limitations and do research work .In this paper, we use Naïve Bayes and SVM approach for this.

The remainder of the paper is organized as follows. Section II addresses related work .Section III determines more detail of our proposed technique: Naïve Bayes using Word Occurrences. Section IV focuses on implementation on the mobile phone and performance evaluation. The last section addresses our conclusions and future work.

In this section are examined similar surveys conducted by other researchers. These researches are mostly conducted after 2011. There are several established email spam detection techniques. SMS spam detection technique has some challenges over email spam detection such as restricted message size, use of regional and shortcut words and limited header information. These challenges need to be solved. There is scope of research in this field and some research works have been conducted on it.

M. Taufiq Nuruzzaman *et al* had done a good work to detect mobile phone spam. In this work,Text Classification techniques have gained maturity, but

feature extraction ,vector creation, such as character n-gram and word n-gram, are challenging. proposed to filter SMS spam on an independent mobile phone using Naïve Bayes and Word Occurrences table. This proposed approach does not depend on another computer system for support or a large amount of data in advance while obtaining reasonable accuracy, low storage consumption and acceptable processing time. ensures security and privacy because spammers do not have a chance to get the filtering system and users do not have to store SMS to anywhere. Abbreviations and Acronyms.

Tiago A. Almeida et al. showcased the particulars of a new authentic, open and non-encoded SMS spam compilation which constitutes of maximum number of messages. It is composed of 4,827 mobile ham messages and 747 mobile spams. Furthermore, the authors performed several established machine learning algorithms on their dataset and they came to the conclusion that according to them SVM is a better approach for advance evaluation.

Sakshi Agarwal *et al* had done inspiring work on the task of filtering mobile messages as Ham or Spam for the Indian Users by adding Indian messages to the worldwide available SMS dataset. The paper analyses different machine learning classifiers on large corpus of SMS messages for Indian people In this work, the first two well-known SMS spam datasets, namely, the Spanish and English test databases were proposed by the authors. A number of message portrayal methods and machine learning approaches were tested.

Cong-Jie Chen *et al* had done awesome work on analyses In spam SMS (Short Message Service) filtering system, key words frequencies are often used to measure the weights of key words. However, the behavior of this measurement is not very well. Therefore, they select the mutual information between the key word and the category, the length of it and the frequency of it as features of key words and figure out corresponding formula to measure the weights of key words. This method is applied tofiltering system based on the Naïve Bayes algorithm which is also improved by the Lidstone algorithm to solve the unseen feature words problem. The results of experiment based on the dataset built by ourselves show that the comprehensive evaluation index of our improved algorithm demonstrated a 19.61% increase in overall rating, compared to the filtering system using key words frequencies as feature

Nikunj Chaudhari *et al* had done awesome work on the various Spam SMS filtering techniques for Mobile Short message service. Most of the Naïve byes, Bayesian classifier and Support vector machine (SVM) techniques are more Accuracy for Spam SMS filtering compare to other. This paper Vector Space model based on Spam SMS filtering it addresses the particularly of Short message Service ,such as short ,vocal , domain related etc this technology Considers much about the particular and Apply much modification on the traditional VSM model. This technology has been deployed in Production environment of Dahan Tricom Corparation and results in Production Department turn out be Applied in SMS Commercial Companies.

Amit kumar *et al* had done awesome work on an anti spam filtering approach based on data mining techniques is proposed which classify the spam and ham emails. The effectiveness of proposed approach is experimentally evaluated on large corpus of simple text datasets as well as text embedded image datasets and comparisons between some classifiers such as Random Forest and Naive Bayes is done. Content based spam filtering is one of the most effective solutions to detect spam. It is based on features selection and text classification methods such as Naive Bayesian classifier, Random Forest and SVM etc.

Lutfun Nahar Lota *et al* had done milestone work on the search and selection procedure, their publication years and the journals and conferences where those studies were published. The results show the summary of the used techniques and advantages and disadvantages of the approaches. A performance comparison on the studied literature. In addition, they have found that none of the studies solve the challenges of use of regional contents and shortcut words. They have also discussed the problems of traditional machine learning algorithms. There is scope of further research in this filed .

Suraj J. Warade et al had done work on messages that sender will first unicast, multicast a text message which will land at mobile service provider server. Once the message is received by the server then server will send the sender and the receivers address to relationships analysis module which will give the concluded result in positive or the negative format. Here the relation analysis module will look in to and previous SMS log between the sender and receiver and also look for the direct or mutual relation between sender and receiver. System will also check for the

message replication or the individual message to different message and check for the content of the message. After the successful result from result analyzer system will apply and normal or spam as a tag to message and forward it to receiver or system can discard the message on the basis of configuration.

To address the limitations of the state of research on SMS spam detection, Amir Karani and Lina Zou propose a content-based method that leverages lexical semantics. Instead of relying on individual words, proposed method uses semantic categories of words as features, which allows us to handle variations in word choices by spammers. To address the limitations of the state of research on SMS spam detection, they propose a content based method that leverages lexical semantics. Instead of relying on individual words, their proposed method uses semantic categories of words as features, which allows us to handle variations in word choices by spammers. In addition, using categories of words as features also helps to reduce the feature space, which in turn improves the efficiency of spam detection that has significant implications for SMS users. An empirical evaluation of the proposed methods has shown promising results

III. PROPOSED APPROACH

Proposed working model is based on data mining approach for classify ham and spam emails separately to make more effective to content based spam filters at the user level. It has four major sections of data mining process as: data selection, data pre-processing, data classification and data evaluation. The effectiveness of proposed model is experimentally evaluated on simple text datasets as well text embedded image datasets of spam emails by detecting different features of spam emails. We can see the working of proposed model in "**Fig. 1**".

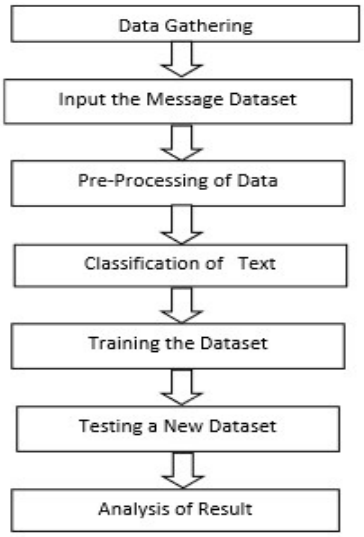

Figure 1 Process of data filtering

A. *DATA FILTERING PROCESS*

1) Data Selection: simple dataset is taken from some datset like british dictionary and iris.

2) Data Preprocessing: There are many data pre-processing techniques available as Data cleaning, Data integration, Data transformation and Data reduction.

3) Data Classification: Classification technique of data mining classifies the large data into separate classes by using different classifier. We are working with Naive Bayes and random forest classifier to classify ham and spam emails.We have compared the results after applying PCA and without applying PCA.

4) ***Data Analysis***: Data analysis is evaluation of results of different classifier applied on different datasets. It gives perfect accuracy and security.Various types of parameters can be taken which are as follows:

True Positive (TP): Correctly ham and spam detected rate that is actual ham and spam messages.

False Positive (FP): Incorrectly ham and spam detected rate that is not ham and spam messages.

Precision: Number of correctly classified instances of a class/number of instances classified as belonging to that class.

$$P = TP/TP + FP$$

Recall: Number of correctly classified instances of a class/number of instance in that class.

B.CLASSIFIERS

1)Naive Bayes:Naïve bayes is a probabilistic classifier so that the probability of each word will be calculated from the number of words in all SMS ham or SMS spam.so we don't need to know the number of words in each SMS.Thus, vector table can be replaced by word occurance table.We have 2 sms spam: **" buy free chocolate"** and **"free SMS"** SMS ham: **"buy tea"**

SMS ID	Type	Word Attributes				
		Buy	chocolate	free	tea	SMS
SMS 1	Spam	1	1	1	0	0
SMS 2	Spam	0	0	1	0	1
SMS 3	Ham	1	0	0	1	0

TABLE I. Vector table

TABLE II. WORD OCCURRENCES TABLE

Word Attributes	**Ham Occurances**	**Spam Occurances**
Buy	**1**	**1**
Chocolate	**0**	**1**
Free	**0**	**2**
Tea	**0**	**0**
SMS	**1**	**1**
Ns	**2**	**5**

Once the word occurrences table is built, we can apply the Naïve Bayes approach to filter unknown incoming SMS.. From these three SMSs, we can get:

• Prior probability of ham P(ham) = 1/3 = 0.33

• Prior probability of spam P(spam) = 2/3 = 0.67

From the Table II, we can obtain the following information:

• Number of vocabulary |v| = 5

• Number of ham words Nham = 2

• Number of spam words Nspam = 5

We can classify the unknown SMS "buy me the tea!" using these data. After feature extraction, we can get four words "buy", "me", "the" and "tea". Since the words "me" and "the" do not exist in the word occurrences table, the words will not be processed. Naïve Bayes classifies SMS based on the probability of each word in SMS for each class, in this case SMS ham and SMS spam. Therefore,toclassify C(buy, tea) the SMS, we can saythat:

$$C(buy,tea) = \begin{cases} \text{ham if } P(\text{ham} \mid \text{buy, tea}) \geq P(\text{spam} \mid \text{buy , tea}) \\ \text{Spam otherwise} \end{cases}$$

We already know P(ham) and P(spam); now we must get the probability of "buy" and "tea" for both SMS ham and SMS spam. The probability of word "buy" as SMS ham is the number of word "buy" in SMS ham compared to the number of all words in SMS ham.

P(buy|ham)=1/2=0.5

P(tea|ham)=1/2=0.5

P(buy|spam)=1/5=0.2

P(tea|spam)=0/5=0.0

Now, the probabilities will be:

P(buy|ham)= (1+1)/(2+|v|) = 2/(2+5) = 2/7 = 0.29

P(tea|ham)=(1+1)/(2+|v|)=2/(2+5)=2/7=0.29

P(buy|spam)=(1+1)/(5+|v|)=2/(5+5)=2/10=0.20

P(tea|spam)= (0+1)/(5+|v|)=1/(5+5)12/10=0.10

So, final probaility will be:

P(ham|buy,tea)= 0.33 × 0.29 × 0.29 =0.0278

P(spam|buy,tea)= 0.67 × 0.20 × 0.10 =0.0134

2) ***SVM:*** Support vector machine (SVM) is one of the most recent techniques used in text classification. In this method a data point is viewed as a p-dimensional vector and the approach aims to separate such points with a (p − 1)-dimensional hyperplane. This is called a linear classifier. There are many hyperplanes that might classify the data. One reasonable choice as the best hyperplane is the one that represents the largest separation, or margin, between the two classes. Therefore, SVM chooses the hyperplane so that the distance from it to the nearest data point on each side is maximized. If such a hyperplane exists, it is known as the maximum-margin hyperplane Figure2 of proposed work is as follows:

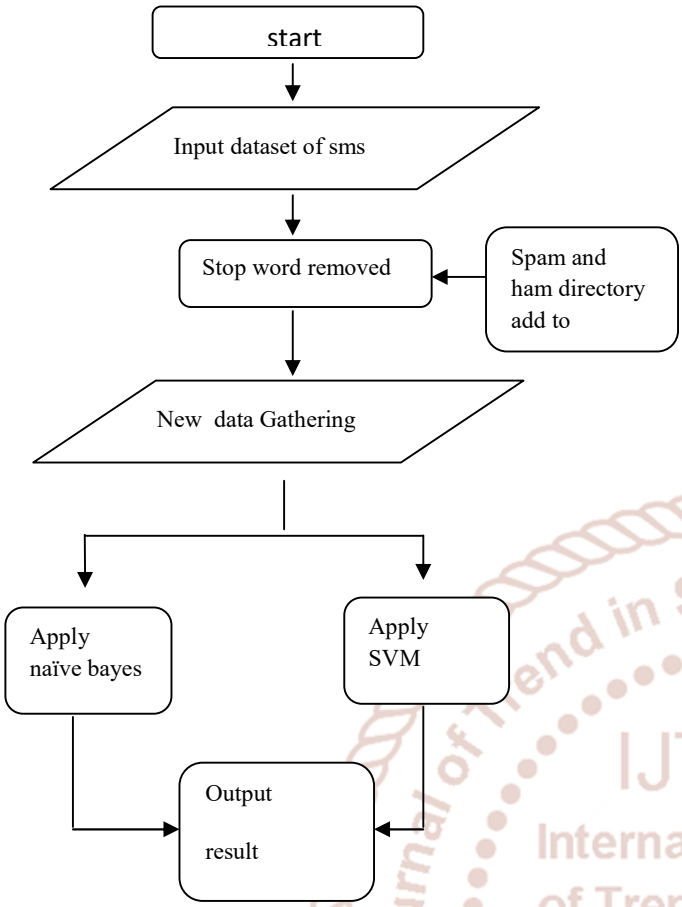

Figure. 2 proposed model of sms spam filtering

IV. CONCLUSION

This review has encountered a number of feature types in SMS spam filtering which have resulted at a different level of accuracy. It is also found that the spam filter for email is less practical for SMS messages. Even though there are al- ready available researches on this subject, a comparative study would be beneficial to the real world application and substantiate the earlier findings. A proof of performance testing has been conducted to have a better perspective of spam words influ- ence in recognizing spam messages. Presented approach have been successfully applied on both simple text dataset as well as image text dataset. We have compared its performance with the Naive Bayes And SVM classifiers. We have also compared the performance and accuracy with the using PCA and without using PCA. Our proposed approach does not depend on another computer system for support or a large amount of data in advance while obtaining reasonable accuracy, low storage consumption and acceptable processing time. Our proposed approach ensures security and privacy because spammers do not have a chance to get the filtering system and users do not have to store SMS to anywhere.

V. REFERENCES

1) M. Nuruzzaman, C. Lee, D. Choi "Independent and Personal SMS Spam Filtering" In:11th IEEE International Conference on Computer and Information Technology,IEEE 2011,doi: 10.1109/CIT.2011.23
2) S. Agarwal, S. Kaur , S.garhwal, "SMS Spam Detection for Indian Messages",In:1st International Conference on Next Generation Computing Technologies (NGCT-2015) Dehradun(2015),IEEE, doi:978-1-4673-6809-4/15/$31.00
3) T. Almeida, A.Yamakami "Content-Based Spam Filtering" IEEE(2012),doi: 978-1-4244-8126-2/10/$26.00
4) C.Chen , Y.Cui , T. Xie "Study of Spam Short Message Filtering Based on Features Selection of Key Words", In: Beijing University of Posts and Telecommunications, pp. 646–654, (2012).
5) N. Chaudhari , Prof. Jayvala , Prof. Vinitashah "Survey on Spam SMS filtering using Data mining Techniques" IJARCCE ,vol. 5, no. 11,2016,doi: 10.17148/IJARCCE.2016.51141
6) A. Kumar Sharma, P. Kaur and S. Kumar Anand "Evaluation of Content Based Spam Filtering Using Data Mining Approach Applied on Text and Image Corpus" In: Proceesings of the Third International Conference on Soft Computing for Problem Solving, doi: 10.1007/978-81-322-1771-8_50, Springer (2014),pp. 561-577
7) L. Lota, B M Mainul Hossain "A Systematic Literature Review on SMS Spam Detection Techniques" In: MECS((http://www.mecspress.org/),doi:10.5815/ijitcs.2017.07.05(2017)
8) S. Warade, P. Tijare, S. Sawalkar "An Approach for SMS Spam Detection" International Journal of Research in Advent Technology, Vol.2, No.12, December2014 E-ISSN: 2321-9637