Eshort Message Service Spam Detection and Filtering Using Machine Learning Approach

M. Arulprakash [a], K. R. Jansi [b]

[a,b] *Assistant Professor, Department ofCSE, SRM Institute of Science and Technology, Kattankulathur- 603203,India*

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 20 April 2021

Abstract: A robust and efficient spam filtering and detection system is important in today's ever changing and growing world. While basic filters and detector are there most of them are not efficient. There is a scope of further development in the systems used. Hence, we are doing our work in way to provide and design a system more efficient and user friendly according to user preferences. Most of the work that has been carried out in this field has been done on data-sets sourced from European countries and mostly on European language. We would be designing a SMS spam filter, which will be universal in nature.As well as our model would be smart enough to distinguish whether a SMS from an operator will be useful to the user or not and rank them accordingly.

Keywords: Spam, ham, Support Vector Machine (SVM), Naïve Bayes, Access Layer (AL), Service Provider layer (SPL), K-Nearest Neighbour (KNN).

1.Introduction

In this ever-growing age of information technology, the ways of harming the people using this technology has also diversified in time with the new technologies coming in the market the new ways of misusing them is also created. One of these technologies is the SMS. SMS represents short message service is a text messaging service which is part of most phone, Internet, and cell phone frameworks[1]. It utilizes normalized communication conventions that let cell phones trade short text messages.[2]As the number f mobile devices has grown exponentially in the past two decades the number of SMS users have also grown. With this ever-growing number the number of people exploiting this technology has grown with time.As the mobile devices are easy to carry around and has the access to internet most of the times the number of opportunities for the offenders has grown. [3]As the internet became popular so does the various methods used to harm others on internet. One such method is e-mail spamming.

[4]Now what is spamming, itis referred to when a violator or a spammer uses a messaging framework to send a large number of spontaneous random messages(spam) to the enormous number of users with the final goal of either to advertise their products, or harming the user data and device or any other false reasons (mostly false reasons for phishing.)

As the technology keep moving to the smaller footprint and more mobile in nature the communication has also taken mobile form. [5]Such as email is used for communication the SMS technology is used in mobile devices. Same as the email spamming the SMS technology has also been affected by the spamming attack. The spamming can be done in many ways some of which well known ways are appending, image spamming, internet spamming and blank spamming.

As the new types of attacks are formed the new ways to deal with attacks in efficient and secure manner are also devised accordingly. [6]The main area of problem in this situation is diversity of languages and the user preferences so keeping this in mind our prototype model main focus will be universal nature and to consider user preferences. [7]Most of the work related in this field is similar to that of email spamming but as due to the absence of proper form and formats in SMS the spamming issue raises the privacy and security concerns due to inefficiency. Hence, we will discuss the way to overcome some major shortcomings.

In the coming section we are going to review the related literature.

2.Related work

SMS spam detection is considered as a major tool to deal with security and privacy threats of the users. [8]As the technology has gone mobile more and more work of user can be done on mobile devices which carry most of the user's private data such as bank details and business details along with them. As the users become more expose to the various services the more vulnerable the user's private data become. [9]This vulnerable data can be attacked by the hackers or others by the spamming the user by either causing the problem in the user device with spamming or by getting information from the user through false messages. Most of the spam detectors these days are standard and provided by service providers which have very limited use and shortcomings. [10]Dealing with issues the Elsevier,Expert Systems with Applications have made the light on the weather context based or server-client based systems are better in this by gathering the data from various sources and recognized multilingual barrier as one of the major issues in this. The 2016 Advanced knowledge-basedsystem paper also discussed the

issue on the linguistics and the abbreviations and idioms used in the languages which cause the accuracy problems.

The study directed by the Bantukul and Marsico[11] regarding the various applications and techniques for the purpose of filtering and recognizing spontaneous promotion of the message or spam in telecom organization. The results obtained viewed that if the message manages to clear the screening, it would be conveyed to its destination without any changes. [12]Notwithstanding, the study focused mainly on the methods utilized for email spam recognition and prohibited different types of versatile SMS spam procedures like the artificial immune system.

Jindal and Liu [13] audited spam and spam acknowledgment on items promotion online journals. In any case, the survey just covered spams identified with item promotion sites and didn't cover any notice of SMS spam. Also, Web [14] assessed numerous algorithms for classification sceptical conduct over the time for decade and sorted dubious conduct into four categories traditional text spam, social text spam, link farming and fake reviews. In any case, this evaluation just considered email spams, counterfeit blogs surveys and web-media based spam and came up short on an inside and out investigation of SMS spam.

Rest most of the work done in this field is in form of experiment and talks several papers have done the work of and talked about using machine learning approach towards spam detection [15], they have performed and analysed the comparison done between various relevant models available for implementation. The models analysed used the techniquesNaive Bayes, Logistic regression, Decision tree, Random forest. The analysis made showed that a greater number of features can be added by refining and adding new data to the real-world dataset. SMS Assassination: A Crowd sourcing Driven Mobile-based System for SMS Spam Filtering [16] the main focus of this paper was to design prototype with the computationally less intensive real-time filter with the personalization, self-learning ad platform independency using Bayesian filter and Support vector machine (SVM) the issue raised was of low accuracy and problems with abbreviations. A Review on Mobile SMS Spam Filtering Techniques [17] provided taxonomic survey of SMS spamming techniques with the help of 11 different datasets used by researchers reaching a conclusion that SVM was not good for small datasets. Pacific Science review on Natural Science and Engineering [18] Proposed efficient algorithm to filter spam using Machine Learning Techniques by Set of rules to assign score to message for classification using multilayer perception Naïve bayes decision tree.

Next, we will discuss the issues and challenges of the system.

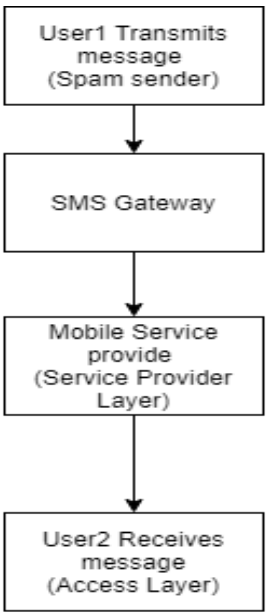
3.Issues and challenges in the system

The main and the most major issue in designing the filter is the limitation in the availability of universal data set for the research purpose and for the designing the new dataset for classification purpose on its bases. The ever changing data set according to time and regional bases causes the major issue in development. The shortcoming of SVM due to its proportionality to the size of data set is also a major issue. The Bayesian theorem is still in use due to its ability to handle the large amount of data sets in an efficient manner. But in upcoming as more work is being done in the field it is found that new efficient ways of AI can be used in the filter with, ore amount of research and work some of the methods that have been put into light after the research are "Artificial Bee Colony", "Bee" algorithm, "Fish swarm" can be used in more efficient manner with research. As for the data set new data set can be formed and refreshed by continuously refreshing the entities from self-learning and from the data aids by government authorities. The user preferences are different according to the regions and purpose and should not be mixed with the data on server side but a way should be devised for it to be dealt separately at the client side. At the present times and with the amount of research a better way to form a SMS spam detector is using a hybrid Naïve Bayes with multilayer structure for better filtering .In the future time with more amount of research and better techniques and data the more efficient and robust SMS spam filter can be formed. Currently most of the filters lack the functionality of the personalization of higher amounts according to the user and the ability to form a new data according to the personalization of the user.

The other major challenge is the type of spam attacks done out of which the criminal spam attacks possess the most amount if threat to the user's data and device functionality by stealing user's personal information.

4. Architecture of SMS spam Transmission

The architecture of SMS transmission is basically divided into two layers one is Access Layer (AL) other is Service provider Layer (SPL) the SMS spam detection filters and techniques are used in either of these two layers. The Access layer is the user-end layer and is mostly use for designing the software that are lightweight and can be used at user side for some light filtering. Most of the spamming techniques are designed by attackers to target on the user-end access layer and harm user device and private data others one is used to target SPL. As we have moved forward now we will look into the function of these layers and some of the techniques used in these.



SMS Transmission process over Network Layers

Fig .1

4.1Access layer

Access layer is a user end layer with the light functioning capacity. The user receives a SMS over a network which passes through access layer for a integrity check and then made available to user to read. As the access layer is light function and at the user end it can be used to deal with the user personalization for spam detection and feedback. The size of data set for user personalization is comparatively small and can be handled with light techniques. Uysal et al. [10] recommended a k-closest neighbour (kNN) furthermore, Backing Vector Machine (SVM) classification of real-time portable application for Android based cell phones. Different blends of the Bag-of-Word (BoW) and Structural Features (SF) are dealt with into extensively used model arrangement estimations to arrange the SMS messages on the client's end.

Uysal et al. [11] additionally proposed a Bayesian-based filtering structure involving the functions got from the model based on BoW alongside with the grouping of SF express to spam. Exactly when another SMS spam message is detected, the recommended model chooses weather the message is spam or not. Right when it is distinguished as a real message, the message is moved into inbox from where the customer is frightened of a moving toward certified text. If not, the notification is turned off and the substance is unobtrusively moved into the 'Spam Box'. Regardless, the text containing spam can be followed back if fundamental. The introduction of the design is probably overviewed on a mass telecom service over the variety which consolidates spam and non-spam messages.

Many more techniques and researched and experimented in the field as it is more explored. Now moving on to the service provider layer, its function and some techniques.

4.2Service Provider Layer

Service provider layer is heavy function layers which regulates all the messages incoming and send them to the user. It deals with the gigantic amount of data and huge numbers of SMS all the time. As the data set is huge it can be used to identify broad type of SMS spams and filter them such as one containing viruses and malicious content for general user bases. Some of the work and research techniques experimented in this layer are as follows.

The method used by Joe and Shim for the filtering purpose of SMS spam was based on the SVM for a compact system by intelligence-based learning capacity of how to perceive spam SMSs. The SMS are used to mine out the text from them while going through the word reference and pre-processor. In the case when there is homogenised term is present in the component list, the stock of word is set to 0 and 1. The made vectors regards are utilized for the learning purpose of data for the changes in the SVM hyperplane. After each section vector is checked for 0 or 1, taking in cycle shut from the side-to-side SVM classifier. Taking kernel function as a base Gaussian Radial Basis Function (RBF) is utilized.

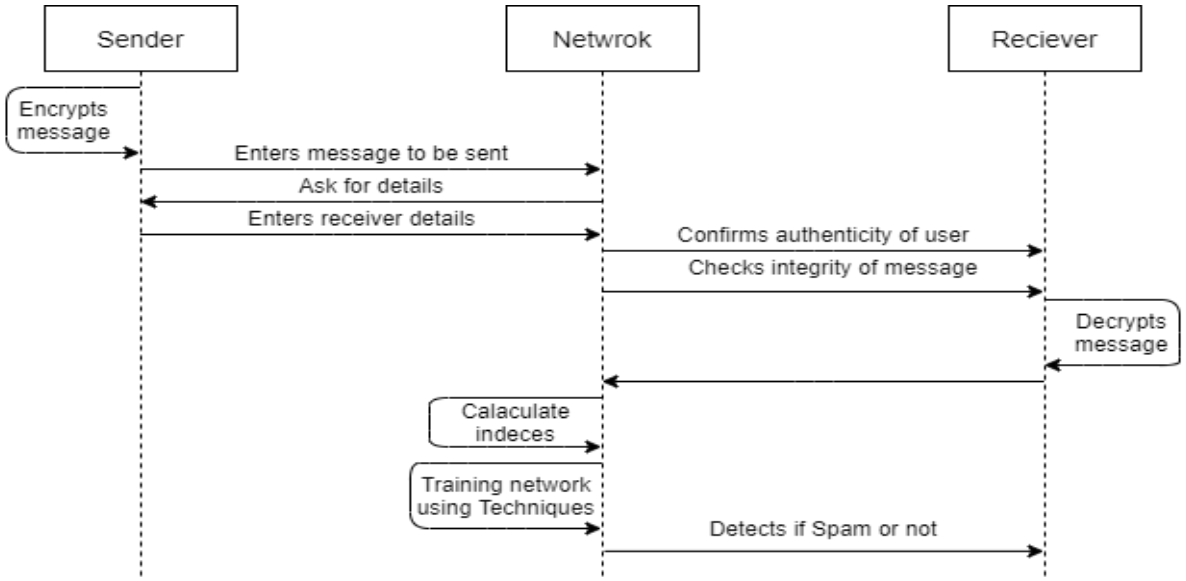
Mathew and Issacthought about the assortment of perceptiveBayesian classifier with other classification methods for portable spam filtering in versatile SMS. The WEKA doesn't understand strings and accordingly all strings are changed over into information as highlight vectors. This is accomplished by utilizing the Weka

'StringToWordVector' work for this change. The assortment of the Bayesian strategies ends up being very efficient with a triumph pace of about 98%.

5. Working sequence of SMS spam detector

Now let see the working sequence of the SMS spam detection. The sender or the spammer creates a message which is then encrypted and then the encrypted message is entered to be sent over a network. On the network the essential details for the transmission of the messageare entered and the verified. Once the detail of the sender and receiver has been verified the authenticity of the user is checked. In the next step over the network the integrity of the message is checked weather it is tampered or not. Then sent over to the user. Oncethe user receives the message it is decrypted and then checked for the spam.

Calculations done on the bases of various techniques are performed and the message is given a score. Then the training of the data set is done over network where further process involved identification of score provided to mark message as a spam or not.



Sequence of SMS spam detector

Fig .2

6. Classification techniques and accuracy measures

The dataset utilized for order should have events and two credits v1 and v2. The v2 contains the information messages which are either spam or ham. The expected imprint v1 contains two classes: 0 = ham and 1 spam.

6.1The techniques that are considered are as follows:

6.1.1Decision Tree

A DT is a regulated AI calculation [14, 15]. Its shape resembles a tree wherein every node is a choice node or leaf. This procedure of DT is effectively justifiable and basic for settling on the choices. A DT contains outside and interior nodes having interlinking with one another. Choices are conceded and made depending on the child nodes and inner nodes to get to the former node. There is no offspring of the leaf node and is connected with a label.

6.1.2 K-Nearest Neighbour

K-NN is a classification supervised learning algorithm [14]. Its purpose is to predict the mark of class as a new info and uses something similar to its contributions to the preparation set. The presentation of K-NN isn't sufficient acceptable. Let (x, y) be the preparation perception and the learning capacity h: $X \longrightarrow Y$, so a perception x, h (x) can set up 'y' esteem.

6.1.3 Naïve Bayes

FP-growth in affiliation is used for mining continuous example on SMS and Naive Bayes Classifier is utilized to group whether the message is spam or not [16]. The feedback from the recently ordered informational collection is utilized. The outcome of using composed exertion of Naive Bayes and FP-Growth plays out the most raised ordinary precision of 98. 506% and 0.025% better than when not using the FP Growth for the purpose of SMS Spam dataset Collection v.1, and boost the accuracy score; thusly, the course of action outcome is more exact.

6.2Performance measures

To measure the performance of the classifier we use the marks into the considerations such as accuracy, specificity,execution time and sensitivity which are expressed in equations.The calculations are done on the outcome of the results yielded and compared to actual results which are True-Positive (TP), True-Negative (TN), False-Positive (FN), False-Negative (FN).

The formulation measures are as follows:

1. Accuracy = $\frac{TN+TP}{TP+TN+FP+FN} \times 100\%$ ..... (1)

2. Sensitivity = $\frac{TP}{TP+FN} \times 100\%$ ..... (2)

3. Specificity = $\frac{TP}{TN+FP} \times 100\%$ ..... (3)

7.Discussions and Results

The work of SMS spam detection and filtering. It will take into account user preferences and would rank the same based on the preferences. On the basis of the research, we have reached on the conclusion of using hybrid Naïve bayes Classifier filtering method in order to classify the SMS as spam or ham. Most of the work that has been carried out in this field has been done ondata-sets sourced from European countries and mostly on European language. So, keeping this shortcoming in mind the goal is to design a SMS spam filter, which will be universal in nature, and which will filter transliterated scripts i.e., messages of one language semi-converted to another also by making new dataset by user preferences to make it more robust and universal. As well as the modelshould be smart enough todistinguish whether a SMS from an operator will be useful to the user or not.The idea proposed is to create or use a data set for our messages filtering which have the frequency of words or messages that are considered as spam and then use it to filter and block the unnecessary spam messages using hybrid techniques.

Following the discussions, we experimented the techniques which landed us on the following results.

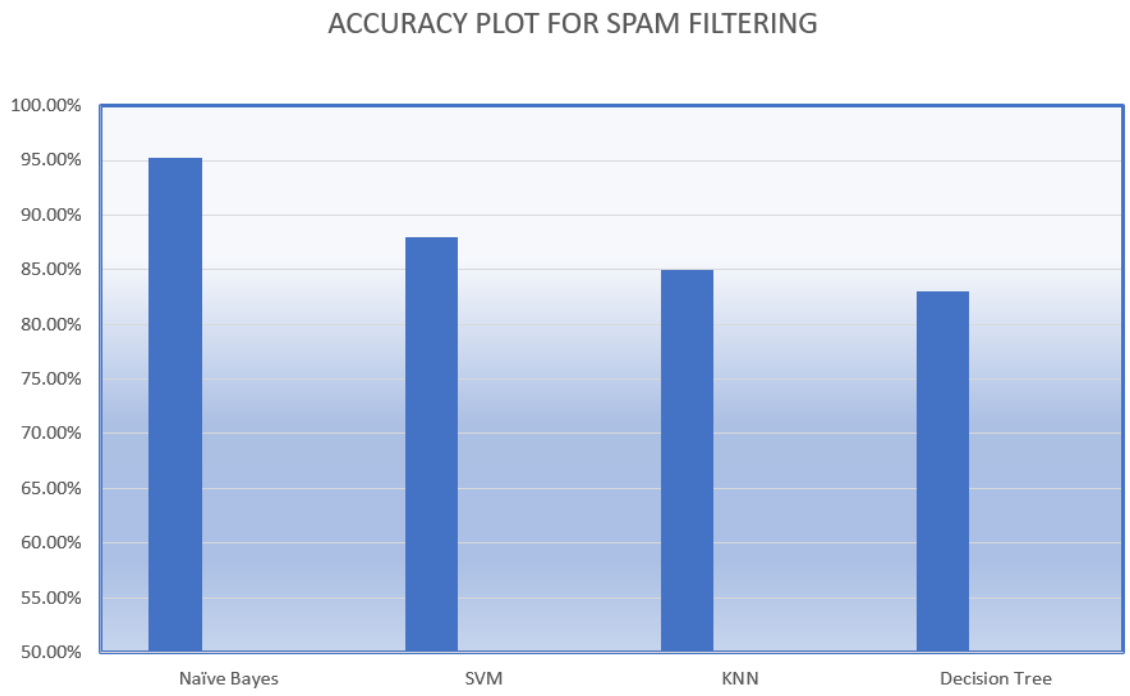


Fig .3

As observed from the Bar/column chart, Naïve Bayes algorithm gives the most elevated precision as far as grouping ham and spam messages and afterward being trailed by different techniques, for example, SVM, KNN, Decision tree.

Accordingly, we can securely reason that building SMS Spam filter utilizing hybrid Naïve Bayes algorithm that gives us the best outcomes coming about up to a precision of 95.2% making it more achievable to use for a large dataset

.

8. Conclusion

We have summarised the research along with the advancement in the technology and the limitations of them. Our related literature review discloses that most of the work in this field is done with the Support Vector Machine (SVM) and Naïve bayes theorem. With the better scope of developing a better efficient robust system with new bio-inspired algorithms techniques of AI, but for that deeper research and work is still lacking in both terms of prototype and datasets availability for their functionality. Due to these the Better option at the current stage which is viable with soma advancements and research in already done work is to design and test a new prototype using a hybrid Naïve Bayes theorem in a multilayer structure for better filtration results along with some development in the personalization side of the user in client-side layer to build a better classifier.

REFERENCES

1. SMS spam filtering: Methods and data, 2012, Elsevier, Expert Systems with Applications.
2. Text normalization and semantic indexing to enhance Instant Messaging and SMS spam filtering-2016 Knowledge Based Systems.
3. Bantukul and P. J. Marsico, “Methods, systems, and computer programproducts for short message service (SMS) spam filtering using E-mailspamfiltering resources," U.S. Patent 7 751 836 B2, Jul. 6, 2010.
4. N. Jindal and B. Liu, ``Review spam detection," in Proc. 16th Int. Conf. World Wide Web, 2007, pp. 1189_1190.
5. M. Jiang, P. Cui, and C. Faloutsos, ``Suspicious behavior detection: Current trends and future directions," IEEE Intell. Syst., vol. 31, no. 1,pp. 31_39, Jan./Feb. 2016.
6. Vengatesan, K., Kumar, A., Chavan, V., Wani, S., Singhal, A., & Sayyad, S. (2019). Simple Task Implementation of Swarm Robotics in Underwater. In International Conference on Emerging Current Trends in Computing and Expert Technology (pp. 1138–1145)
7. Towards Filtering of SMS Spam Messages Using Machine Learning Based Technique, July 2017 DOI: 10.1007/978-981-10-5780-9_2.
8. SMS Assassin: Crowd sourcing Driven Mobile-based System for SMS Spam Filtering, March 2011 DOI: 10.1145/2184489.2184491.
9. Abdulhamid, Shafi’I, Shafie, Abd Latiff, Latiff, Abd, Chiroma, Haruna, Osho, Oluwafemi, Abdul-Salaam, Gaddafi, Abubakar, Adamu, Herawan, Tutut, “A Review on Mobile SMS Spam Filtering Techniques”, IEEE Access, 2017.
10. Proposed efficient algorithm to filter spam using Machine Learning Techniques— 2016Pacific Science Review A: Natural Science and Engineering.
11. K. Uysal, S. Gunal, S. Ergin, and E. S. Gunal, ``The impact of feature extraction and selection on SMS spam filtering,"Elektron. Elektrotechn., vol. 19, no. 5, pp. 67_72, 2012.
12. A. K. Uysal, S. Gunal, S. Ergin, and E. S. Gunal, ``A novel framework for SMS spam filtering," in Proc. Int. Symp. Innov. Intell. Syst. Appl. (INISTA), Jul. 2012, pp. 1_4.
13. VENGATESAN, K., KUMAR, E., YUVARAJ, S., TANESH, P., & KUMAR, A. (2020). An Approach for Remove Missing Values in Numerical and Categorical Values Using Two Way Table Marginal Joint ProbabilityInternational Journal of Advanced Science and Technology, 29(5), 2745–2756
14. I. Joe and H. Shim, ``An SMS spam filtering system using support vector machine," in Future Generation Information Technology. Berlin, Germany: Springer, 2010, pp. 577_584.
15. A. Kumar, A. Singhal, K. Vengatesan and D. K. Verma, "Study and Research of 3D Animation Courseware Development," 2018 International Conference on Recent Innovations in Electrical, Electronics & Communication Engineering (ICRIEECE), Bhubaneswar, India, 2018, pp. 2514-2516, doi:10.1109/ICRIEECE44171.2018.9008670.
16. K. Mathew and B. Issac, ``Intelligent spam classi_cation for mobile textmessage," in Proc. Int. Conf. Comput. Sci. Netw. Technol. (ICCSNT),Dec. 2011, pp. 101_105.
17. X. Wu, V. Kumar, J. Ross Quinlan et al., “Top 10 algorithms in data mining,” Knowledge and Information Systems, vol. 14, no. 1, pp. 1–37, 2008.
18. A. U. Haq, “A hybrid intelligent system framework for the prediction of heart disease using machine learning algorithms,” Mobile Information Systems, vol. 2018, Article ID 3860146, 2018.
19. A. Kumar, K. Vengatesan, A. Singhal and D. K. Verma, "3D Lighting Courseware development for 3D Motion Picture Science," 2018 International Conference on Recent Innovations in Electrical, Electronics & Communication Engineering (ICRIEECE), Bhubaneswar, India, 2018, pp. 2321-2323, doi: 10.1109/ICRIEECE44171.2018.9009258.
20. Enhancing spam detection on mobile phone SMS performance using FP-growth and Naïve Bayes Classifier, 2016 IEEE Asia Pacific Conference on Wireless and Mobile.

21. K. R. Jansi and S.V.Kasmir Raja, "A survey on Privacy Preserving Data Aggregation Schemes in People Centric Sensing Systems and Wireless Domains",Indian journal of science and technology,Vol 9,2016.
22. K. R. Jansi and S.V.Kasmir Raja, "Design Perspectives of People Centric Sensing Systems",Indian journal of Science and Technology,Vol 9(37), 2016.