Harnessing Ai For SMS Security

[1.]G. Swathi M.Tech, Assistant Professor, Department of Computer Science and Engineering (Artificial Intelligence), Gates Institute of technology, Gooty, Andhra Pradesh,Email: swathi.ganta20@gmail.com
[2.]G.Madhurya,Student, Department of Computer Science and Engineering (Artificial Intelligence), Gates Institute of Technology-Gooty, Andhra Pradesh, Email: guduru.madhu9@gmail.com
[3.]G.Rakshitha,Student, Department of Computer Science and Engineering (Artificial Intelligence), Gates Institute of technology-Gooty, Andhra Pradesh, Email: rakshithagorantla@gmail.com
[4.]K.Usha Sree,Student, Department of Computer Science and Engineering (Artificial Intelligence), Gates Institute of technology-Gooty, Andhra Pradesh, Email: usha2002sree@gmail.com
[5.]M.Lakshmi Narayana Rao,Student, Department of Computer Science and Engineering (Artificial Intelligence),Gates Institute of Technology-Gooty, Andhra Pradesh,
Email: llakshminarayana870@gmail.com
[6.]J.Suresh,Student, Department of Computer Science and Engineering (Artificial Intelligence), Gates Institute of technology-Gooty, Andhra Pradesh, Email: sureshjambulapati34@gmail.com

Abstract

The current use of social media has created incomparable amounts of social data, as it is a cheap and popular information sharing communication platform. Nowadays, a hugepercentage of people depend on the accessible material on social networking in their choices (e.g. comments and suggestions about a subject or product). This feature on exchanging knowledge with a wide number of users has quickly prompted social spammers to exploit the network of confidence to distribute spam messages and support personal forums, advertising, phishing, scams and so on. Identifying these spammers and spammaterial is a hot subject of study, and while large amounts of experiments have recently been conducted to this end, so far the methodologies are only barely able to identify spam feedback, and none of them demonstrates the value of each derived function.

In this study,we have suggested a machine learning-based spam detection system that determines whether or not a specific message in the dataset is spam using a set of machine learning algorithms. Four main features have been used; including user-behavioral, user-linguistic, review- behavioral and review-linguistic, to improve the spam detection process and to gather reliable data.

Keywords: Spam Detection, Machine Learning, Random Forest algorithm, Reviews, Framework, Social Media.

I. INTRODUCTION

With the advent of technology and everything getting digitalized, we make some of our decisions based on the content of

information that we see available on the internetto make the wise or ideal decision to maximize the benefits obtainable when making a choice. From choosing electronic devices to even healthcare products and foods, we tend to check product reviews and pick the one that is most reliable and trustworthy according to the reviews from customers. This in most cases works for the best but there are cases where a fake review or a spam message tends to cheat or divert people away from valid products to potentially harmful or hazardous substances and in some cases even scam gullible people. Spam detection is done manually by designated staffs only when a review is reported as spam by the users of the platform.

This is good in terms of preventing a situation where the system detects the user authentic review in another language as spam and a situation where the system detects the user's authentic review in another language as spam ad deletes it

Some spam reviews are worded right to sound like a normal review but are used as a template to copy-paste everywhere

accordingly. This is done clearly to evade from possible reports from other reviewers hence avoiding the possibility of removal completely. Automation of spam detection using a well-defined machine learning framework can greatly help reduce spam reviews that are misleading or fake.

Our system uses Machine learning algorithms including Random forest, Bayes Network, Naïve Bayes, K-nearest neighbor and support vector machine combined with NLP techniques to detect and remove spam and to identify the spammer.

II. EXISTING SYSTEM

The current systems of spam detection are solely dependent on three main methods:-

A. Linguistic Based Methods

Humans can comprehend linguistic constructs and their interpretations, but machines can't, and so machines are taught some language in order to help them comprehend linguistic constructs. These techniques are used in search engines to determine the next term in an unfinished sentence. They are split into two Unigrams (Words one by one) and two Bigrams (Words two at a time). As every term has to be remembered, this approach is not as reliable and time intensive.

B. Behavior Based Methods

It is based on Metadata. This method requires users to create a set of laws, and users need to have extensive knowledge of such laws. It needs reformulation because the characteristics of spam shift overtime and the laws need tobe modified accordingly. As a consequence, it is mostlyuser-dependent and still human needs to examine more details.

C. Graph Based Methods

In this approach, by integrating many, heterogeneous details into a single graphical representation, unusual patterns are detected in the data that shows spammer behaviors by

running graph-based anomaly detection algorithms for graphical representation. This approach is not reliable, so it is challenging to detect false opinions.

Feature engineering is not possible, spam features are not built-in, they are not statistically dependent they are mainly dependent on commercial attractiveness of words and are entirely content-oriented both of these aspects lead to a significant decline of this system.

III. PROPOSED SYSTEM

The system that is proposed on this paper combines random forest algorithm, which is a supervised classification algorithm with NLP concepts to categorize and detect spam reviews among all existing reviews on the TWITTER dataset. There are four major features used in the algorithm which includes 8 NLP concepts:-

A. Review-Behavioral(RB)Based Features

This type of functionality is metadata dependent and not the text of the review. There are two aspects to the RB category:-

- **Early Time Frame (ETF)**

Half of the spammers have a very short time span and 55% of the spammers publish all the reviews with a time difference of fewer than 10. That implies the spammersdelete their account instantly. Spammers tend to publishtheir reviews as early as possible, in order to hold their post among the top ratings that many users read first. It cantherefore be seen as a guideline for preventing spam.

- **Threshold Rating Deviation**

To determine a reviewer's rating deviation, it measures the total point discrepancy of a company rating point from a consumer ranking. Then we measure the average difference in score for the reviewer in all of his reviews. Spammers also appear to help the firms they have partnered with, so they reward certain organizations with high scores. As a consequence, various companies have a wide variability in their assigned scores which is the reason they have large variation and deviation.

B. Review-Linguistic (RL) Based Features

Features in this category are based on the review given by the user and precisely obtained from text. The RL category contains two features:-

- **Ratio of First Personal Pronouns (PP1) and Ratio of Exclamation Sentences (RES)**

Spammers use first personal pronouns and exclamation phrases as much as they can to maximize user's impressionsand to emphasize their reviews among others.

C. User-Behavioral (UB) Based Features

Such features are unique to each particular user and are determined by person, meaning that we can use such features to generalize all reviews posted by that same person. This category has two main features:-

Burstiness of reviews written by single user

Spammers usually publish their spam reviews in a limited amount of time for two

reasons: one because they intend to influence readers and other people, and the other as they are transient users, they have to write as soon as they can in a limited period of time. A spam may be detected with the aid of the number of comments at the same time.

Average of a user's negative ratio given to different businesses

Spammers prefer to write reviews that defame firms that compete with those they have partnered with, which may be achieved with negative feedback, or with rating those companies with low scores. Thus, the ratio of their scores appears to be small. This makes it easy to determine whetheror not a review is spam.

D. User-Linguistic (UL) Based Features

These features are taken from the user's language to demonstrate how customers view their thoughts or views on what they have encountered as a client of a specific company. We use this form of functionality to explain how a spammer interacts in terms of text. In this category there are some important feature:-

- **Average content similitude (ACS) and Maximumcontent similitude (MCS)**

Spammers usually publish their messages with the same template and tend not to spend their time writing the originalreview. As a result, they have similar reviews. By contrasting reviews that are similar, a single user can be detected as a bogus user and all of his feedback can be checked and classified as a spam or not.

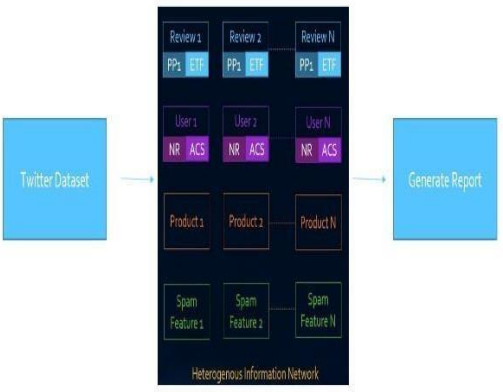

Fig. 1.System Architecture

The proposed framework is introduced with the aid of two key applications, one is anaconda prompt which is exactly similar to the usual command prompt and the other is Jupyter, an integrated python development environment. The anaconda prompt is used for running anaconda and conda commands without changing the directories and to access the local host by connecting the file folder to it and downloading and extracting packages to implement the framework.

Once all packages have been checked and handled, the local host is accessed with jupyter, which includes several code cells.

IV. MODULE DESCRIPTION

The proposed framework consists of a set of modules thatare implemented:

A. Dataset Extraction

First data is collected from the dataset, in our case which is Twitter messages. After collecting the data, it is cleansed by getting rid of extra spaces, removing duplicates and many more.

B. Collecting Metadata

The RB features are implemented with the cleaned dataset.First, the time frame of the message is identified. Afteridentifying the time frame, it is compared with the threshold rating deviation where the diversity and variance of the spammer is checked. Hence, the metadata is collected about the spam message and spammer.

C. Generalize Messages

All twitter messages are collected and generalized regardless of whether they are spam or not. By generalizing the messages a lot of time can be saved.

D. Implementing ML Algorithms

The ML algorithms are implemented in this stage by segregating the messages into spam content and original content. ML algorithms including Random forest, Bayes Network, Naïve Bayes, K-nearest neighbor and support vector machine is used.

In this stage of message segregation, a suite of machine learning (ML) algorithms is deployed to effectively distinguish between spam content and genuine messages. Among these algorithms are Random Forest, Bayes Network, Naïve Bayes, K-nearest neighbor, and Support Vector Machine (SVM).

Each algorithm brings its unique approach and strengths to the task, contributing to a robust and versatile spam detection system.

Random Forest, a powerful ensemble learning technique, constructs a multitude of decision trees during training and outputs the mode of the classes (spam or not spam) as the prediction. Its ability to handle large datasets and high dimensionality makes it a popular choice in spam detection scenarios.

Bayes Network, rooted in probabilistic reasoning, models the relationships between variables using a directed acyclic graph. By leveraging conditional probabilities, it evaluates the likelihood of a message being spam given its features, making it particularly adept at handling uncertain or incomplete data.

E . Generating Spam Text Data and information aboutthe Spammer

After the ML algorithms have been implemented the spammessages are identified and obtained, and the information about the spammer who has written the spam message will be collected. With the help of this information, thespammer’s entire history can be accessed and all his messages can be analyzed.

Once this data is collected, it undergoes rigorous analysis. Tools and techniques such as data mining, pattern recognition, and natural language processing come into play to extract insights from the spammer's entire history. This analysis aims to uncover recurring themes, linguistic patterns, targeted demographics

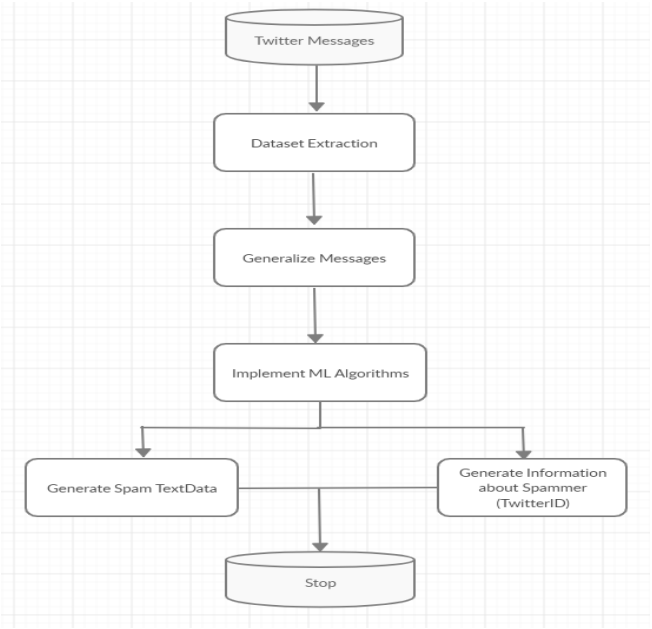

Fig. 3.Flow Diagram

The flow diagram shows the entire flow and steps of the framework.

The architecture of the proposed framework revolves around two key applications: Anaconda Prompt and Jupyter. Anaconda Prompt serves as a fundamental tool for managing dependencies and facilitating access to the local host environment. It streamlines the process of installing, updating, and configuring packages necessary for the framework's functionality. Additionally, Anaconda Prompt enables seamless interaction with the local host, allowing for efficient data handling and processing.

Complementing Anaconda Prompt, Jupyter provides an integrated Python development environment tailored to the needs of the framework. With its interactive and user-friendly interface, Jupyter facilitates code development, experimentation, and visualization.

V. ADVANTAGES

- Feature Engineering is available. Therefore, features of rawdata can be easily extracted with the help of data mining. It is used improve the performance of Machine learning algorithms.
  - Each and every data obtained is accurate.
  - Spam Features are as a built in function.
  - Less human interaction.
  - Real-time Monitoring
  - Scalability
  - It is statistics based approach.
  - Supports review centric spam detection.
  - Supports reviewer centric spam detection.

VI. RESULTS AND ANALYSIS

	TwittID	TextData	TweetCreatedAt	RetweetCount	TweetFavouriteCount	TweetSource	UserID	UserScreenName	UserName
11	1239487501414219777	Here's something for all the young ones out th...	2020-03-16 09:43:43	17	46	Twitter for iPhone	1239448814689218560	TSEduDept	Telangana State Education Department
12	1239471638111899648	Happy to note, the majority of the educational...	2020-03-16 08:40:41	12	23	Twitter Web App	1239448814689218560	TSEduDept	Telangana State Education Department
13	1239471481236512769	In view of the #CoronaVirus threat, the Telang...	2020-03-16 08:40:04	16	48	Twitter Web App	1239448814689218560	TSEduDept	Telangana State Education Department
14	1239463906588392448	Greetings!\n\nTelangana State Education Depar...	2020-03-16 08:09:58	82	329	Twitter Web App	1239448814689218560	TSEduDept	Telangana State Education Department

Fig. 4.Spammer Information

The Fig. 4 shows entire data about the spammer including TwitterID, TextData, TweetCreatedAt, RetweetCount,TweetFavouriteCount,TweetSource ,UserID, UserScreenName and UserName. This information can inturn help in identifying more spammers with way the text data has been written.

Vll. CONCLUSION

In this paper, we identified the spams and spammers present in a twitter dataset with the help of machine learning algorithms and NLP concept determining other spams, spammers and their way of writing messages. We considered two attribute sets which includes content and user behavior, the content is determined with the help of average content similitude, maximum content similitude, ratio of exclamation sentences and the ratio of first personalpronouns. The user behavior is determined with the help of properties such as reviews written and an average of negative ratio given. Thus, making it a very effective and accurate spam detection framework.

REFERENCES

1. Nurul Fitriah Rusland, Norfaradilla Wahid, Shahreen Kasim, Hanayanti Hafit, “Analysis of Naive Bayes Algorithm for Email Spam Filtering across Multiple Datasets”.
2. J. Rout, S. Singh, S. Jena, and S. Bakshi, “Deceptive Review Detection Using Labeled and Unlabeled Data”.
3. Feng Qian, Abhinav Pathak, Y. Charlie Hu, Z. Morley Mao, and Yinglian Xie, “A Case for Unsupervised-Learning-based Spam Filtering”.
4. Shrawan Kumar Trivedi, “A Study of Machine Learning Classifiers for Spam Detection”.
5. W.A. Awad, S.M. ELseuofi, “Machine Learning Methods for Spam E-mail Classification”
6. S. Gharge, and M. Chavan``An integrated approach for malicious tweets detection using NLP," in *Proc. Int. Conf. Inventive Commun. Comput.Technol. (ICICCT)*, Mar. 2017, pp. 435_438.
7. T. Wu, S. Wen, Y. Xiang, and W. Zhou, ``Twitter spam detection: Survey of new approaches and comparative study," *Comput. Secur.*, vol. 76, pp. 265_284, Jul. 2018.
8. M. Mateen, M. A. Iqbal, M. Aleem, and M. A. Islam, ``A hybrid approach for spam detection for Twitter," in *Proc. 14th Int. Bhurban Conf. Appl. Sci.Technol. (IBCAST)*, Jan. 2017, pp. 466_471.
9. F. Fathaliani and M. Bouguessa, ``A model-based approach for identifying spammers in social networks," in *Proc. IEEE Int. Conf. Data Sci. Adv.Anal. (DSAA)*, Oct. 2015, pp. 1_9.
10. Saeedreza Shehnepoor, Mostafa Salehi*, Reza Farahbakhsh, Noel Crespi, “NetSpam: a Network-based Spam Detection Framework for Reviews in Online Social Media “
11. G. Jain, M. Sharma, and B. Agarwal, ``Spam detection in socialmedia using convolutional and long short term memory neural network," *Ann. Math. Artif. Intell.*, vol. 85, no. 1, pp. 21_44, Jan. 2019.
12. C. Meda, F. Bisio, P. Gastaldo, and R. Zunino, ``A machine learning approach for Twitter spammers detection," in *Proc. Int. Carnahan Conf.Secur. Technol. (ICCST)*, Oct. 2014, pp. 1_6