A Survey on Enhanced Social Media Spamming Detection Framework Based Upon Activity and Text Analysis

Ramya Devi.K[1], Kameshwaran.T[2], Dinesh Kumar.P[3], Kalimudeen.S[4]

Assistant Professor, Dept of Computer Science and Engineering, S.A. Engineering College, Chennai, India[1]

U.G Student, Dept of Computer Science and Engineering, S.A. Engineering College, Chennai, India[234]

ABSTRACT: Netspam, an organized crime happening in social media is having a rapid scaling growth day by day. The freedom provided by various e-shopping sites has been an advantage for the people creating spam. Even a few spammed messages may create a huge disorder in the society. Normally social media is the major play ground for these spammers. It deals with the rumors spread by the spammers and some of the efficient methods to control them. The user log on to a social media and try to pick some friends from his/her own circle and sends spam messages. These messages get forwarded into groups which make the readers to believe in it. The Text analyzer engine checks whether the message is a spam or a true one. Once the message is found to be a spam a warning message is sent to the user who sent the message, if the user continues posting the spam messages, then he/she gets blocked.

KEYWORDS: Spamming, Activity, Text Analysis.

I.INTRODUCTION

Social media plays an important role in depicting the views of each and every people in the society. People have the freedom to post their views in the social platform, but the information posted by the people may or may not be true. If the veracity of the information is not right, then the information and the bearer of the information have to be penalized. The online users with any identity can leave comments as reviews, in decision making process there may be a positive or negative reviews according to the products. To evaluate these reviews we make use of activity and text analysis features.

II. RELATED WORK

In the previous years, comparing the performance machine learning algorithm became more popular to detect the performance and stability on large amount of data. It gave better scalability and performance in large scale parallel computing. Collection of data was one of the complex process. Researchers have proposed many solutions for detecting and filtering the SMS spam. A new technique named mitigation was proposed for detection of spam messages. The Bayesian network still exists even though many powerful algorithms are available. For detecting the spam tweets deep analysis on the statistical feature of million spam and non spam tweets were used.To classify more accurate spam tweet we have to eliminate the old spam tweets.The content-based model and the identity-based model are the two summarized approaches that are used in efficient spam detection.Even though unsupervised detection scheme has been proposed it does not work well for entire callers.An Unsupervised SPITters detection scheme is used which deals with the situation when the SPITters are significantly less than legitimate callers. The idea behind the scheme is to add artificial callers' data into inspected ones before clustering callers.Email spam image filtering is a problem where spammers modify by employing different techniques. The SVM classifier was used for minimizing false positives by

adjusting parameter of classifiers.Spammers share malicious link looking like a real one, develop malicious applications and sometimes fake accounts. The intruders make use of the portal for the purpose of spreading rumors. Readers are interested in reading curiously on topics, by creating unrelated comments the user may creates confusion. Two text mining approaches were used to measure relatedness between posts and comments.For analyses purpose we make use of two techniques namely String Similarity Indexes and Corpus based Indexes. Even though social networking sites has developed technology for detection of spam it is not possible to remove the spam completely from the sites.

III. EXISTING SYSTEM

Many research studies focus on the problem of detecting the spammers and spam reviews. The problem was challenging and was remained unsolved. The existing system was relied on the following approaches like Linguistic-based Methods, Behavior-based Methods and Graph-based Methods.

LIMITATIONS OF EXISTING SYSTEM:
- The Linguistic-based Method was not that much clear and distinct to implement for all the human languages that exists.
- The second approach Behavior-based Method also fails if the spammer learns the working logic of detection algorithm. It becomes easier to exploit the machine algorithm which is similar to the SEO(Search Engine Optimization) algorithm.
- Graph-based algorithms are costly to implement and takes high processing capacity.

IV. PROPOSED SYSTEM

We propose a NetSpamframework which is a network based approach where we make use of two main approaches such as activity and text analysis. The Combined Linguistics Behavioral Analysis algorithm is introduced that consists of many modules, but the text analyzer engine plays the major role in it. Whenever a user logininto a social media he/she sends messages which is analyzed a by text analyzer engine that uses a dictionary for checking whether the message is spam or not. A spam message can't be determined by a single message. According to the user's activity and the number of times he tries to send the repeated content makes the text analyzer engine to determine the spammer. After the message gets detected first a warning message is sent to the corresponding spammer. If the spammer tries to send the content again then he/she gets blockedfinally.

MODULES DESCRIPTION:
The project is divided into three modules as follows:
- ❖ Social Network Module
- ❖ Text Analysis and Malicious Post Detection Module
- ❖ Measures Module

SOCIAL NETWORK MODULE:
This is the major module of the project in which we develop a Social Networking Website as a model for real time Social Networking application. Provisions for a user to register with the application, such as new user creation, login, searching friends, sending friend request, sharing text messages etc. In addition to User Modules, we also develop admin module with the administrator privileges.

TEXT ANALYSIS AND MALICIOUS POST DETECTION MODULE:
In this module, we develop a new Text Analyzer Engine which analyzes not every message but only messages originating from high active users. And also, the engine considers the post history and then the actual content of the Message being post. To detect malicious activity, the application maintains a dictionary.

MEASURE MODULES:
In this module, we develop provisions for giving warning messages to the malicious post sender. If the User is not responding the application itself will block user.

VI.ARCHITECTURE DIAGRAM
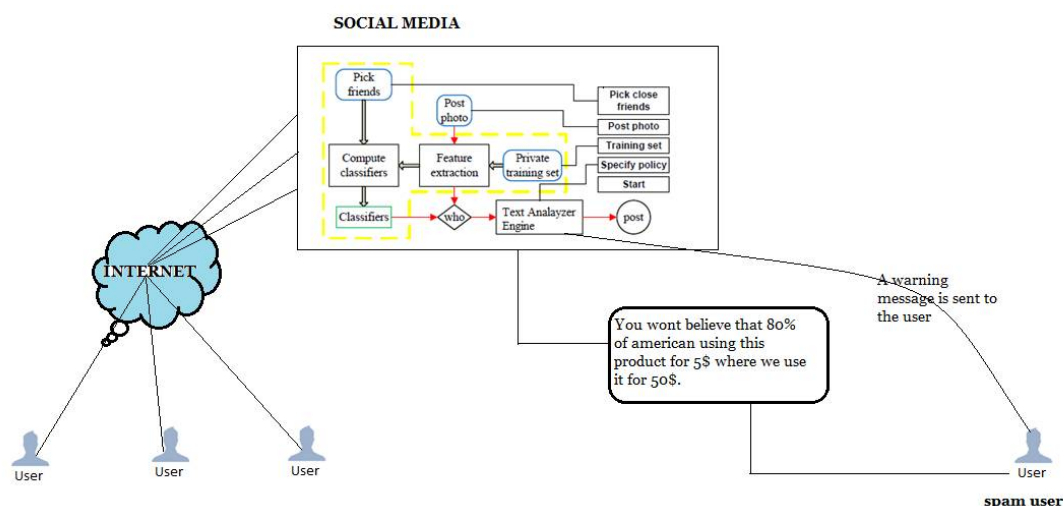
VII.CONCLUSION AND FUTURE WORK

We make use of spamming detection framework based on the activity and text analysis. The performance of the proposed framework is better than that of the existing methods. The existing system made use of many methods for the detection of spammers and spam reviews. Instead of those approaches we made use of two main approaches namely activity and text analysis. The Combined Linguistic Behavioral Analysis algorithm is used in our system which is one of the machine learning algorithms.
For the future work, the machine learning algorithm must be extended. The algorithm that we use can only be applicable for the English language, but in future an algorithm can be implemented for detecting the spammers not only in English language but also for all the other languages present in the world. The algorithm and the framework must be highly secured so that any of the spammers can't exploit or identify the algorithm which is used for the detection spammers and spam reviews posted by them.

REFERENCES

[1]guanjun lin1, nan sun1, surya nepal2, jun zhang1, (member, ieee), yang xiang3, (senior member, ieee), and houcine hassan4, (member, ieee), **"**Statistical Twitter Spam Detection Demystified: Performance, Stability and Scalability**"**Received April 1, 2017, accepted May 15, 2017, date of publication June 1, 2017, date of current version July 3, 2017.

[2] shafi'imuhammad abdulhamid1, (member, ieee), muhammadshafie abdullatiff2, haruna chiroma3, (member, ieee), oluwafemi osho1, gaddafi abdul-salaam5, adamui. abubakar6, (member, ieee), and tutut herawan4, "A Review On Mobile sms Spam Filtering Techniques" Received January 11, 2017, accepted February 7, 2017, date of publication February 13, 2017, date of current version August 22, 2017.

[3]chaochen, yuwang, junzhang, yang xiang, wanleizhou, senior member, ieee, and geyong min, "Statistical features-based real-time detection of drifted twitter spam"ieee transactions on information forensics and security, vol. 12, no. 4, april 2017.

[4]girisha khurana1, mrmarish kumar2   1student, 2assistant professor, department of computer science gnimullanakurushetra university, "Review: Efficient Spam Detection On Social Network"Vol 3 issue vi,rjune 2015 ic value: 13.98 issn:2321-9653

[5] kentaroh toyoda1,2, (member, ieee), mirang park1, naonobu okazaki3, and tomoaki ohtsuki2, (senior member, ieee), "Novel Unsupervised Spitters Detection Scheme By Automatically Solving Unbalanced Situation" received october 9, 2016; accepted december 14, 2016, date of publication december 21, 2016, date of current version june 7, 2017.

[6] boguo, haowang and zhaojunyu business intelligence department meizuinc, "Detecting Spammers In E-commerce Website Via Spectrum Features Of User Relation Graph"2017 Fifth International Conference on Advanced Cloud and Big Data.

[7] basheer al-duwairi∗, ismailkhater† and omar al-jarrah, "Texture Analysis-Based Image Spam Filtering" [6th] International Conference on Internet Technology and Secured Transactions, 11-14 December 2011, Abu Dhabi, United Arab Emirates.

[8]HimanshiAgrawal, RishabhKaushal Department of Information Technology Indira Gandhi Delhi Technical University for Women Delhi, India. "Analysis Of Text Mining Techniques Over Public Pages Of Facebook"2016 ieee 6th international Conference on Advanced Computing.

[9] CristinaRădulescu, MihaelaDinsoreanu, RodicaPotolea Technical University of Cluj-Napoca, Romania. "Identification Of Spam Comments Using Natural Language Processing Techniques".

[10]Amit Kumar Sharma Assistant Professor Department of Computer Science & Engineering The ICFAI University Jaipur, Rajasthan, India. RenukaYadav Associate System Engineer IBM India Pvt. Ltd. Pune, Maharashtra, India."Spam Mails Filtering Using Different Classifiers With Feature Selection And Reduction Techniques", 2015 Fifth International Conference on Communication Systems and Network Technologies.