IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-11, Nov 2018 E-ISSN: 2347-2693

Effective E-mail Spam Filtering Using Origin Based Information

Pramod P. Ghogare[1*], Ajay U. Surwade[2], Manoj P. Patil[3]

[1]Dept. of Computer Science, KCES's Institute of Management and Research, Jalgaon (M.S.), India
[2,3]School of Computer Sciences, North Maharashtra University, Jalgaon (M.S.), India

[*]*Corresponding Author: pramod.ghogare@yahoo.com, Tel.: +91-9403634018*

Available online at: www.ijcseonline.org

Accepted: 27/Jul/2018, Published: 30/Nov/2018

Abstract - All over the world, Internet is a dominant communication tool. Internet not only provides different ways of communication, but also increases the misuse of strong communication tool for advertisement and other personal beneficial activities. Progress of unwanted emails has encouraged the development of numerous spam filtering techniques. Since spammers are devising fresh techniques every time, anti-spamming techniques fails to filter out spam emails. E-mail spam is a difficult for the sustainability of the internet and global business. Millions of e-mails sent by spammers for advertisement of products and services. This paper describes an experimental analysis of spam e-mail classification along with proposed framework for feature selection and spam classification. The experimental result signifies performance of algorithm for standard dataset Enron. Origin based information selected for classification.

Keywords – Spam, Spam Filter, Spam Detection.

I. INTRODUCTION

The Internet has grown as important way of communication. The long-lasting method of communication over the internet is an e-mail which also changing its forms. Currently users are able to send the e-mail with different type of attachments along with the text message. If spam grow at the current rate, the problem may become unmanageable in future [1]. Another use of e-mail address is in authentication or registration process on number of web services, which makes e-mail address as a resource to reach at customer. These customers gets spam e-mails in the form of advertisement, discount offers, product details. These spam emails are sent by using different spamming techniques which bypass spam filters on e-mail servers. Spam e-mails are very irritating stuffs, which not only distracts user but consumes many valuable resources that is why important to screen spam.

1.2 Spam e-mail

A spam email is one which user not intended to receive. "A spam is anonymous, unsolicited bulk e-mail". "Unsolicited, unwanted e-mail that was sent indiscriminately, directly or indirectly, by a sender having no current relationship with the user" [2]. A spam e-mail generally sent in bulk without user's permission. These spam e-mails can be an advertisement, product images, text in images, offers, discounts offers, asking for registration or donation, asking for debit card or bank details. "Real spam is that e-mail for advertising of product sent to list groups" [3].

1.3 Types of Spam

In the early days, spam directly sent to users that called as direct spam. Modem Pool is the type of spam in which dial-up connections were used as a source of distribution of spam, e-mails when overflowing open relay servers became less effective. Dial-up modems use a dynamic IP address that was the main advantage for spammers to use different IP address per session. In 2003 and 2004 Robot network were responsible for the majority of the spam being send. Trojan horses used for downloading malware and crippling viruses spread onto several machines through spam, which allows them to control system from a remote location [4]. Word obfuscation is the technique of spamming which changes the position of letters in a word makes it different than it is. For example, a word 'free' is easily traceable whereas 'f-r-e-e' is somewhat difficult to track but for a human it is readable [5]. Recently Image Spam is spreading rapidly because it is very complex to detect. It involves textual spam content implanted into images that are attached or inserted into e-mails [6].

Rest of the paper is organized as follows, Section II contain the related literature review, types of spam, spam filtering and Origin based spam, Section III contain the architecture and essential steps, Section IV showing details of dataset, Section V explain classification algorithm, Section VI contains discussion performance measurement, Section VII contain result and Section VIII concludes research work with future directions.

II. LITERATURE REVIEW

A spam not only irritates a user, but it degrades work efficiency by disturbing users continuously [7]. Sometimes genuine e-mail removed due to frustration by spam emails

© 2018, IJCSE All Rights Reserved

and that situation becomes very irritating. Email service users waste a lot of time in reading and deleting spam emails [8]. Spamming is banned in some countries due to its misuse but countries like Russia, where it is a legal task to increase turnover of an organization by sending e-mails related to electronics spare parts, cars, legal services, tourism, medicine, etc. Spam adverting is used to make the profit from the shares of listed companies. It is estimated that 58 billion junk e-mails will be send every day in the next coming years, it would cost annually $198 billion. Internet service provider, e-mail service provider, network administrator and users affected by increasing menace of spam. The amount of money, time and resources engaged by Spam are the main concern to stop Spamming. If spam filtered before entering into a network, it can save many resources to use, engaged or spoiled. Countries like the USA, Canada, and Pakistan has control of Electronic Crimes Ordinance, 2007, to regulate email spamming. India has no regulation to control bulk email advertising or spam emails. IT Act and Cyber law are still at a primary stage in India. In India very few precautions taken while using the internet as a communication channel, for example, VSNL does not contain spam mailbox, which makes very difficult to differentiate between legitimate and spam e-mail [9]. Today Indian cyber threat landscape, like other parts of the world, has seen a significant increase in spam & phishing activities. Computer infections spam and phishing activities rate in the country keep fluctuating, making India the active sources, as is seen in established economies with the high rate of IT usage.

2.1 Types of spam

Adult spam contains adult or pornographic content. Financial spams ask for details of bank account, debit or credit card. This information then used for making fraud transactions [10]. Health spam contains benefits of health products and offer of purchasing the same [11]. Email asking to buy shares, Market is down purchase share, these types of email are in the stock category of spam [11]. Advertisement of a political party, asking for VOTE in the election, demand for donation to a political party before an election is a type of political spam [12]. Phishing spam looks like official e-mails from a financial organization, e-commerce websites services. This makes people into giving away their sensitive information, which can use by the scammers for making fraud transactions from victim's account [12].

Table 1 Types of Spam

Type of Spam	Content / Description
Adult	Adult or pornographic content [11].
Financial	Bank account details, fake offers, debit or credit card details [10].
Health	Health products [11].
Stock	Share market [11].
Advertiseme nt	Products, offers on products, Discount offers [11].
Political	Vote, donation for political parties. [12]
Phishing	Looks like official e-mails, asking to share sensitive information like password, OTP [12]

2.2 Spam Filtering

Spam filtering is a classification technique; it classifies an email as spam or ham. Spam detection techniques detects spam e-mail based on features of an e-mail. The spam filtering techniques broadly classified in two type's origin based and content based.

2.2.1 Origin-Based

Origin-based filters are based on using network information to detect an e-mail message is spam or ham. The sender address is compared with the history of spam sender if the incoming mail is from one of spammer address then it is categorized as a spam [13]. The header of an e-mail has information like Sender IP, Precedence, Errors-To, Sender e-mail address, Sender, In-Reply-To, X-Spam Status, X-Spam Level, X-Mailer, X-Priority, X-Mime OLE, Content-Type, Message-ID, Delivered-To, Date, From, To, Received [14], [15]. This information can utilized to get sender information and metadata of an e-mail from which spam detection can made. Kulkarni et al. (2016) used the Decision tree, Bayes network, K-Nearest Neighbor, Random Forest and Bagging algorithms to test spam classification using e-mail header fields. The decision tree performs better than all remaining classifiers. K-nearest neighbor performs well but bagging and the random forest have not a good result. Using e-mail header e-mails can classified as spam and non-spam to the certain amount [16].

III. SYSTEM ARCHITECTURE

The objective of this paper is to describe and develop a classifier that can classify emails as spam and ham based on origin based filtering. Origin based information is taken for the classification of an email. An e-mail contains lots of information about the origin of an e-mail, Sender IP, Precedence, Errors-To, Sender, In-Reply-To, X-Spam Status, X-Spam Level, X-Mailer, X-Priority, X-Mime OLE, Content-Type, Message-ID, Delivered-To, Date, From, To, Received.

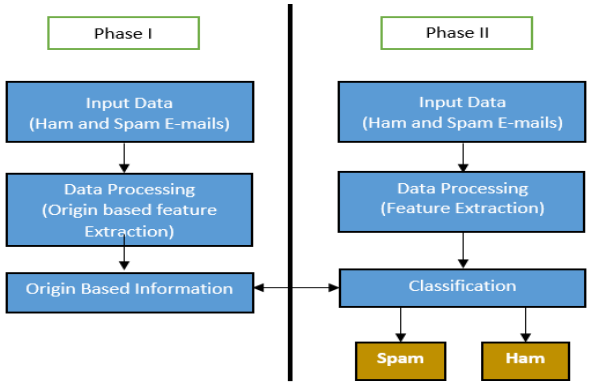

Figure 1 Proposed Framework for SPAM Filtering

© 2018, IJCSE All Rights Reserved

The framework is divide in two stages, In Phase I separate list of sender e-mail address for ham and spam e-mails are prepared from dataset. In Phase II, each e-mail sender's e-mail address extracted with the same procedure used in Phase I the extracted e-mail address will searched in spam and ham e-mail addresses list generated on Phase I. If the extracted e-mail address is present in list of spam then is marked as a spam e-mail address. If the extracted e-mail sender address is not present in spam list then it will search in ham list and if found in ham list then it will marked as ham e-mail address. If the extracted sender e-mail address is not present in both list then it will be treat as a ham email and can be keep under observation and called as Greylist email address.

IV. DATASET

Enron e-mail dataset [17] used, which has collection of spam and ham e-mails. Details of original Enron dataset files is given in Table 2.

Table 2 Details of Enron Dataset

Ham		Spam	
Directory	**Number of files**	**Directory**	**Number of files**
BG	10000	beck-s	1967
GP	13719	farmer-d	3669
SH	9269	kaminski-v	4363
		kitchen-l	4012
		lokay-m	2364
		ams-w3	2714

From Enron dataset 20457 spam e-mails and 26475 ham e-mails selected as per Table 3. For Phase I, 13238 ham e-mails and 10227 spam e-mails and for Phase II that is testing phase, 10230 spam e-mails and 13237 ham e-mails were selected. In both phases, only e-mail address of sender taken as a feature for classification.

Table 3 Dataset for Experiment

Type of E-mail	Phase I	Phase II	Sub Total
Spam	10227	10230	20457
Ham	13238	13237	26475
Total			46932

V. CLASSIFICATION ALGORITHM

The classification will done in two phases as follows.

Phase - I

I. Sender's e-mail address extracted from each e-mail present in selected dataset.

II. The unnecessary information from sender's e-mail address Truncated.

III. Extracted sender's e-mail address added in respective list of e-mail addresses that are spam and ham e-mail addresses.

Phase - II

I. Comparing extracted sender e-mail address with generated lists of spam and ham e-mails.

i. Sender e-mail address compared with each e-mail address present in the list of spam e-mail addresses.

ii. **If** the sender address of email is present in the blacklist addresses then it is emails declared as SPAM.

iii. **Else,** compare extracted sender's e-mail address with each address present in the list of Whitelist address of ham emails.

iv. **If** the e-mail sender address is present in the list of ham e-mail addresses then declare it as HAM.

v. **Else** add it in Greylist and declare it as HAM.

VI. PERFORMANCE MEASUREMENT

Performance is measure in terms of accuracy. Accuracy is define as the ratio between number of correctly classified spam and ham emails to the total emails used for testing i.e. all emails that are correctly classified by the classifier as given in "(1)". The objective is to classify the spam correctly into the real class, which means development of a classifier that can differentiate spam from ham. Finally, the focus is to reduce the false positive rate of the classifier i.e. if an e-mail is spam, it should detected as spam. The performance parameter for the system are as per Table 4.

Table 4 Performance Parameters

Classifier	Spam	Ham
Spam	Spam e-mails classified as Spam (True-Positive)	Spam e-mails classified as Ham (False-Negative)
Ham	Ham e-mails classified as Spam (False-Positive)	Ham e-mails classified as Ham (True-Negative)

$$\text{Accuracy} = \frac{(\text{Ham} \rightarrow \text{Ham}) + (\text{Spam} \rightarrow \text{Spam})}{\text{Total (Ham + Spam)}} \times 100\%$$

VII. RESULTS

Standard dataset Enron is used for experiment. The proposed technique extract the feature that is e-mail address of sender and used it for classification of e-mails.

Table 5 Confusion Matrix for Classification

Results	Spam	Ham	Total
Spam	6352	3878	10230
Ham	19	13218	13237

© 2018, IJCSE All Rights Reserved

Table 5 shows results of classification on testing dataset selected from standard Enron dataset.

$$\text{Accuracy} = \frac{13218 + 6352}{23467} \times 100\ \%$$

Accuracy = 83.39 %

The result obtained from the proposed system shows the accuracy of 83.39 % considering the True-Positive and True-Negative results. The results from the system are better while considering sender e-mail address as feature for classification.

VIII. CONCLUSION

This paper describes the origin based filtering. The experimental work carried out given accuracy 83.39 % when executed on standard dataset such as Enron. The aspects of this work is to increase the performance of the proposed algorithm.

REFERENCES

[1] D. Mallampati, "An Efficient Spam Filtering using Supervised Machine Learning Techniques," International Journal of Scientific Research in Computer Science and Engineering, vol. 6, no. 2, pp. 33-37, April 2018.

[2] G. V. Cormack and T. Lynam, "Spam Corpus Creation for TREC," in Second Conference on Email and Anti-Spam, California, USA, 2005.

[3] N. Advilkar, P. Mane and D. Walunj, "SPAM MAIL FILTERING," International Journal of Advanced Research in Computer Engineering & Technology, vol. 5, no. 1, pp. 99-104, 01 2016.

[4] D. Wang, D. Irani and C. Pu, "A Study on Evolution of Email Spam Over Fifteen Years," in 9th International Conference on Collborative COmputing: Networking, Application and Worksharing, Austin, TX, USA, 2013.

[5] A. Bhowmick and S. M. Hazarika, "Machine Learning for E-mail Spam Filtering: Review,Techniques and Trends," in Advances in Electronics, Communication and Computing, 2016, pp. 583-590.

[6] B. Biggio, G. Fumera, I. Pillai and F. Roli, "A survey and experimental evaluation of image spam filtering techniques," Pattern Recognition Letters, July 2011.

[7] M. Siponen and C. Stucke, "Effective antispam strategies in companies: An international study," in International Conference on System Sciences, Kauia, HI, USA, 2006.

[8] Namrata and Suman, "Review Paper on Spam Detection Antiphishing Techniques," International Journal of Computer Sciences and Engineering, vol. 6, no. 5, pp. 1156-1161, 2018.

[9] S. N. Raj , "Evaluation Of Cybercrime Growth And Its Challenges As Per Indian Scenario," International Journal of Informative & Futuristic Research, vol. 2, no. 9, pp. 3120-3128, May 2015.

[10] E. Blanzieri and A. Bryl, "A survey of learning-based techniques of email spam filtering," in Artificial Intelligence Review, 2009, pp. 63-92.

[11] E. P. Sanz, J. C. Cortizo Pérez and J. M. GOMEZ HIDALGO, "Email Spam Filtering," in Advances in Computers, vol. 74, 2008, pp. 45-114.

[12] P. G. Juneja and R. K. Pateriya, "A Survey on Email Spam Types and Spam Filtering Techniques," International Journal of Engineering Research & Technology (IJERT), vol. 3, no. 3, pp. 2309-2314, March 2014.

[13] N. Agrawal and S. Singh, "Origin (Dynamic Blacklisting) Based Spammer Detection and Spam Mail Filtering Approch," International Conference on Digital Information Processing, Data Mining, and Wireless Communications, pp. 99-104, 6-8 july 2016.

[14] H. Guo, B. Jin and W. Qian , "Analysis of Email Header for Forensics Purpose," in International Conference on Communication Systems and Network Technologies, Gwalior, India, 2013.

[15] Rekha and S. Negi, "A Review on Different Spam Detection Approaches," International Journal of Engineering Trends and Technology (IJETT), vol. 11, no. 6, pp. 315-318, May 2014.

[16] P. Kulkarni and H. Acharya, "Comparative analysis of classifiers for header based emails classification using supervised learning," International Research Journal of Engineering and Technology, vol. 3, no. 3, March 2016.

[17] Enron-Spam datasets, Mountain View, CA, 2006.

Authors Profile

Pramod P. Ghogare received MCA degree from North Maharashtra University, Jalgaon, India in 2008. He is currently pursuing Ph.D. in North Maharashtra University, Jalgaon and working as Assistant Professor in Department of Computer Science, KCES's Institute of Management and Research, Jalgaon. His research work focuses on Network Security, SPAM detection.

Ajay U. Surwade received the MCA degree in 2000 and Doctoral degree in Computer Science in 2016 from North Maharashtra University, Jalgaon, India. He is Assistant Professor in School of Computer Sciences, North Maharashtra University, Jalgaon. His area of research is Distributed Computing and Network Security.

Manoj P. Patil received the M.Sc. degree in computer science from North Maharashtra University, Jalgaon, India, in 2001 and Ph.D. in Computer Science in 2014. He is currently working as Assistant Professor in the School of Computer Sciences, North Maharashtra University, Jalgaon. His research interests include digital image processing and machine learning. He is a Life Member of Indian Science Congress Association.

© 2018, IJCSE All Rights Reserved