Review on Various Spam Classification Techniques and its Limitations

Dharmendra Dewangan
Central College of Engineering and Management
Dept. of Computer Science and Engineering
Raipur, Chhattisgarh, India
akdewangan412@gmail.com

Poonam Gupta
Central College of Engineering and Management
Dept. of Computer Science and Engineering
Raipur, Chhattisgarh, India
poonamgupta.90@gmail.com

Abstract

Email is likely the most advantageous strategy for exchanging messages electronically starting with one individual then onto the next, rising up out of and heading off to any piece of the world. Essential highlights of E-mail, for example, its speed, dependability, productive capacity choices and a substantial number of included offices make it exceptionally famous among individuals from all parts of business and society. In any case, being to a great extent famous has its negative perspectives as well. Messages are the favored medium for countless over the web. The absolute most well-known assaults over the web incorporate spams. Hardly any strategies are quite location of spam related sends however they have higher false positives. An assortment of channels, for example, Bayesian channels, Checksum-based channels, machine learning based channels and memory-based channels are normally utilized as a part of request to distinguish spams. As spammers dependably endeavor to figure out how to dodge existing channels, new channels should be produced to get spam. This paper reviews various methods and techniques used for detection of e-mail spams and presents its advantages and limitations.

Keywords— *Email Spam, Data Mining, Email Classification, Spam Detection and Prevention.*

I. INTRODUCTION

Spam refers to unsolicited business email. Otherwise called junk mail, spam floods Internet client's electronic mail boxes. These junk mails can contain different sorts of messages, for example, commercial advertising, pornography, business promoting, doubtful product, infections or quasi legal services [1].

A. *Types of Spam*

Fundamentally, spam can be classified into the accompanying four types:

- Usenet Spam
- Texting Spam
- Mobile Spam
- E-mail Spam

Newsgroup spam is a sort of spam where the objectives are Usenet newsgroups. Usenet tradition characterizes spamming as "unreasonable different posting", that is, the rehashed posting of a message (or significantly comparable messages). Amid the mid 1990s there was significant contention among Usenet framework directors (news administrators) over the utilization of wipe out messages to control spam. A "wipe out message" is a mandate to news servers to erase a posting, making it be blocked off. Some viewed this as an awful point of reference, inclining towards oversight, while others thought of it as a legitimate utilization of the accessible devices to control the developing spam issue [2, 3].

Texting frameworks, for example, Telegram, WhatsApp, Twitter Direct Messaging, Kik, Skype and Snapchat are for the most part focuses for spammers. Numerous IM administrations are openly connected to online networking stages, which may incorporate data on the client, for example, age, sex, area and interests. Sponsors and tricksters can assemble this data, sign on to the administration, and send spontaneous messages which could contain trick joins, obscene material, malware or ransom ware. With most administrations clients can report and piece spam records, or set security settings so no one but contacts can get in touch with them.

Cell phone spam is a type of spam (spontaneous messages, particularly publicizing), coordinated at the content informing or different interchanges administrations of cell phones or cell phones. As the notoriety of cell phones surged in the mid 2000s, visit clients of content informing started to see an expansion in the quantity of spontaneous (and by and large

undesirable) business ads being sent to their phones through content informing. This can be especially irritating for the beneficiary on the grounds that, not at all like in email, a few beneficiaries might be charged an expense for each message got, including spam. Cell phone spam is by and large less inescapable than email spam, where in 2010 around 90% of email is spam. The measure of versatile spam changes generally from area to locale. In North America, versatile spam has consistently expanded from 2008 ed 2012, however stays beneath 1% as of December 2012. In parts of Asia up to 30% of messages were spam in 2012 [4].

Email spam, otherwise called garbage email, is a kind of electronic spam where spontaneous messages are sent by email. Spammers gather email addresses from chatrooms, sites, client records, newsgroups, and infections that reap clients' address books. These gathered email addresses are now and then additionally sold to different spammers. The extent of spam email was around 90% of email messages sent, toward the finish of 2014.

II. SPAM DETECTION TECHNIQUES

There are a few ways to deal with recognize approaching messages as spams seem to be, Whitelist/Blacklist, Bayesian examination, Mail header investigation, Keyword checking and so on some of them are characterized beneath [5]:

Whitelist/Blacklist: - These methodologies essentially make a rundown. A whitelist is a rundown which incorporates the email locations or whole spaces which the client knows. A programmed white rundown administration device is likewise utilized by client that aides in consequently adding known delivers to the whitelist. A boycott is the inverse of whitelist. In this rundown we include addresses that are destructive for clients.

Mail Header Checking: - This approach is exceptionally known approach. In this we just comprise of set of standards that we coordinate with mail headers. In the event that a mail header matches, at that point it triggers the server and return sends that have purge "From" field, that have an excessive number of digits in address that have distinctive locations in "To" field from same source and so on

Signature- This approach depends on creating a signature having extraordinary hash an incentive for each spam message. The channels look at the estimation of past put away esteems with approaching messages esteems. It is most likely inconceivable for honest to goodness message having same incentive with spam message esteem put away before.

Bayesian Classifier: - There are specific words utilized as a part of spam messages and non-spam messages. These words have specific likelihood of happening in the two messages. The channels that we utilized don't have the foggiest idea about these probabilities ahead of time; we should prepare them first so it can develop them. In the wake of preparing the word probabilities are utilized to process the likelihood that an email having specific arrangement of words in it have a place with either spam or honest to goodness messages. Every specific word or just the most fascinating words add to email's spam likelihood. This commitment is known as the back likelihood and is registered utilizing Bayes' hypothesis. At that point, the messages spam likelihood is processed everywhere throughout the word in the messages. On the off chance that this aggregate esteem surpass over certain edge then the channels will check messages as spam.

Table I. Comparison of various Spam Detection Techniques

S.NO	Approach	Limitation
1	Whitelist / Blacklist	Spammer can easily penetrate through
2	Signatures	Unable to identify spam until email reported as spam & its hash distributed.
3	Mail Header Checking	High false positive rate
4	Bayesian Analysis	Replies on Naïve Bayes filtering technique which is not accurate

III. LITERATURE SURVEY

Izzat Alsmadi et al. 2015 [6], Information clients depend vigorously on messages' framework as one of the real wellsprings of correspondence. Its significance and

utilization are consistently developing in spite of the advancement of versatile applications, informal communities, and so on. Messages are utilized on both the individual and expert levels. They can be considered as official records in correspondence among clients. Messages' information mining and examination can be directed for a few purposes, for example, Spam location and arrangement, subject characterization, and so forth. In this paper, an extensive arrangement of individual messages is utilized with the end goal of envelope and subject orders. Calculations are produced to perform bunching and order for this vast content gathering. Order in light of NGram is appeared to be the best for such huge content accumulation particularly as content is Bi-dialect (i.e. with English and Arabic substance).

A.K.Sharma et al. 2015 [7], The nonstop development of email clients has brought about the expanding of spontaneous messages otherwise called Spam. In current, server side and customer side hostile to spam channels are presented for identifying diverse highlights of spam messages. Nonetheless, as of late spammers presented some powerful traps comprising of inserting spam substance into computerized picture, pdf and doc as connection which can make ineffectual to current procedures that depends on examination advanced content in the body and subject fields of email. A significant number of proposed working procedure gives an against spam separating approach that depends on information mining strategies which arrange the spam and ham messages. The viability of these methodologies is assessed on expansive corpus of basic content dataset and in addition content inserted picture dataset.

Idris I et al. 2015 [8], The expanded idea of email spam with the utilization of urge mailing instruments incite the requirement for locator age to counter the danger of unsolocited email. Locator age roused by the human insusceptible framework executes molecule swarm streamlining (PSO) to produce identifier in negative determination calculation (NSA). Exception indicators are remarkable highlights created by nearby anomaly factor (LOF). The neighborhood exception factor is executed as wellness capacity to decide the nearby best (Pbest) of every applicant identifier. Speed and position of molecule swarm improvement is utilized to help the development and new molecule position of every exception locator. The molecule swarm advancement (PSO) is actualized to enhance indicator age in negative choice calculation instead of the arbitrary age of identifiers. The model is called swarm negative determination calculation (SNSA). The trial result demonstrate that the proposed SNSA display performs superior to the standard NSA.

NADIR OMER et al. 2014 [9], pam messages are considered as a genuine infringement of protection. What's more, it has turned out to be exorbitant and undesirable correspondence. Despite the fact that, Support Vector Machine (SVM) has been broadly utilized as a part of email spam discovery, yet the issue of managing tremendous information is time and memory devouring and low precision. This investigation accelerates the computational time of SVM classifiers by decreasing the quantity of help vectors. This is finished by the K-implies SVM (KSVM) calculation proposed in this work. Moreover, this paper proposes a system for email spam identification in view of half breed of SVM and K-implies grouping and requires one more information parameter to be resolved: the quantity of bunches. The analysis of the proposed instrument was completed utilizing spam base standard dataset to assess the plausibility of the proposed technique. The consequence of this crossover technique prompted enhanced SVM classifier by lessening bolster vectors, expanding the precision and diminishing the season of email spam identification. Test comes about on spam base datasets demonstrated that the enhanced SVM (KSVM) fundamentally beats SVM and numerous other late spam identification techniques as far as order exactness (viability) and tedious (productivity).

Megha Rathi et al. 2013 [10], As web is extending step by step and individuals for the most part depend on web for correspondence so messages are the quickest method to send data starting with one place then onto the next. Presently a day's every one of the exchanges all the correspondence whether general or of business occurring through messages. Email is a viable apparatus for correspondence as it spares a great deal of time and cost. Be that as it may, messages are likewise influenced by assaults which incorporate Spam Mails. Spam is the utilization of electronic informing frameworks to send mass information. Spam is flooding the Internet with many duplicates of a similar message, trying to constrain the message on individuals who might not generally get it. In this investigation, we dissect different information mining way to deal with spam dataset keeping in mind

the end goal to discover the best classifier for email characterization. In this paper we break down the execution of different classifiers with highlight choice calculation and without include choice calculation. At first we explore different avenues regarding the whole dataset without choosing the highlights and apply classifiers one by one and check the outcomes. At that point we apply Best-First element determination calculation to choose the coveted highlights and after that apply different classifiers for characterization. In this investigation it has been discovered that outcomes are enhanced regarding exactness when we install include determination process in the analysis. At last we discovered Random Tree as best classifier for spam mail arrangement with exactness = 99.72%. Still none of the calculation accomplishes 100% precision in arranging spam messages yet Random Tree is close-by to that.

Table I. Shows comparisons of existing methods and its limitation

S. No.	Author	Year	Technique	Feature	Limitation
1	Alsmadi et al.	2015	Support Vector Machine and K-Means Clustering	Accuracy rates are improved as compared to existing method	For filtering, supervised mechanism is considered for pre-processing.
2	Idris et al.	2015	Particle swarm optimization and negative selection algorithm	Based on negative selection algorithm it selects or detects spams effectively	The main problem is with accuracy.
3	Sharma et al.	2015	Principal Component Analysis and Feature Selection	Feature selection and reduction techniques outperforms many other existing techniques while classifying email spam.	Only can be used at client side of detection of spam and ham emails.
4	Elssied et al.	2014	Support Vector Machine and K-Means Clustering	Improves accuracy by reducing the false positive rates and also enhance the cost in terms of time taken by classifier.	Do not does comparison with existing methods of k-means clustering algorithm hence the results got cannot be trusted.
5	Rathi et al.	2013	Support Vector Machine, Feature Selection, Random Trees, Naïve Bayes Theorem	Using feature selection and non-feature selection technique various classifiers are compared.	The classifiers results does not perform well without selection relevant features.

IV. TOOLS USED

There are many tools available for processing data and extracting user email information. Some of them are presented below.

a. Weka Tool used for simulating the email spams via classifiers.
b. MATLAB Data mining tool.

V. CONCLUSION

Email are utilized on both the individual as well as professional levels and it can likewise be considered as official records in correspondence between clients. Email information mining and analysis can be led for a few purposes, for example, spam location and grouping, subject characterization and so on.

This paper review some of the various existing techniques such as email spam detection, classification and also filtering techniques. The feature extraction are also covered a lot in this paper. Most of the existing approaches has certain limitation while selecting the features. This may be improved in future version of classifiers.

REFERENCES

[1] J. W. Yoon, H. Kim, and J. H. Huh, "Hybrid spam filtering for mobile communication," computers & security, vol. 29, no. 4, pp. 446–459, 2010.

[2] H. He and E. A. Garcia, "Learning from imbalanced data," IEEE Transactions on knowledge and data engineering, vol. 21, no. 9, pp. 1263–1284, 2009.

[3] S. Ruggieri, "Efficient c4. 5 [classification algorithm]," IEEE transactions on knowledge and data engineering, vol. 14, no. 2, pp. 438–444, 2002.

[4] B. Sch Ikopf, S. Mika, C. Burges et al., "Input space versus feature space in kernel-based method," IEEE Trans Neural Networks, pp. 1000–1017.

[5] N. Friedman, D. Geiger, and M. Goldszmidt, "Bayesian network classifiers," Machine learning, vol. 29, no. 2-3, pp. 131–163, 1997.

[6] Izzat Alsmadi, Ikdam Alhami, Clustering and classification of email contents, Journal of King Saud University - Computer and Information Sciences, Volume 27, Issue 1, 2015, Pages 46-57, ISSN 1319-1578

[7] A. K. Sharma and R. Yadav, "Spam Mails Filtering Using Different Classifiers with Feature Selection and Reduction Technique," 2015 Fifth International Conference on Communication Systems and Network Technologies, Gwalior, 2015, pp. 1089-1093.

[8] Idris I, Selamat A, A Swarm Negative Selection Algorithm for Email Spam Detection. J Comput Eng Inf Technol, 2015, 4:1. doi:10.4172/2324-9307.1000122

[9] NADIR OMER FADL ELSSIED, THMAN IBRAHIM, WAHEEB ABU-ULBEH, AN IMPROVED OF SPAM E-MAIL CLASSIFICATION MECHANISM USING K-MEANS CLUSTERING", Journal of Theoretical and Applied Information Technology 28th February 2014. Vol. 60 No.3

[10] Megha Rathi, Vikas Pareek, "Spam Mail Detection through Data Mining – A Comparative Performance Analysis", I.J. Modern Education and Computer Science, 2013, 12, 31-39.