ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 15, March 2017

Identification of Unwanted Email Contents

Reshma Rajan
Computer Science Department
M A College of Engineering
India
reshmarajan6666@gmail.com

Rahul V Cheeran
Computer Science Department
M A College of Engineering
India
rahulcheeran@gmail.com

Dr. Surekha Mariam Varghese
Computer Science Department
M A College of Engineering
India
surekh.var@gmail.com

Abstract— Email or electronic mail is a digital mechanism for exchanging messages through Intranet or internet communication platforms. Email messages are comprised of message envelope, message header and message body. Like any other dynamic medium, it is also prone to misuse. In this work a new system is developed to analyse the email body content and to list out the offensive contents. The three main phases are content analysis, classification and objectionable content identification. At first, the contents are analyzed and based on this the category of email is identified as social, promotions and general. Then the content is checked to detect the presence of abusive words. Then all the abusive words which are present in the mail are identified and its different possible combinations are predicted using genetic algorithm.

Keywords— ***Electronic mail; Genetic Algorithm; Profanity Filter: Collaborative Filtering;***

I. INTRODUCTION

Electronic mail or email is one of the most commonly and widely used features of the internet. By using an email address we can send and receive messages from anywhere in the world. The main protocols used are SMTP, POP, IMAP and MIME. Like any other dynamic medium it is prone to misuse.

There may be many situations in which we have to deal with search queries and user inputs that contains profanity or undesirable language. This needs to be filtered out. Word filters are used commonly to censor language which are considered inappropriate by the operators of the forum or chat room. Expletives are typically partially replaced, completely replaced, or replaced by nonsense words. This relieves the users from dealing with offensive contents.

Usually in an email system we see normal spam filtering. A spam filter is a program that is used to detect unwanted and unsolicited email and prevent those types of messages from getting to a user's inbox. Usually a spam filter looks for certain criteria on which it bases judgments. For example, the simplest and earliest versions (such as the one available with Microsoft's Hotmail) are set to watch for particular words in the subject line of messages and to exclude these from the user's inbox. This method is not especially effective, too often omitting perfectly legitimate messages (these are called false positives) and letting actual spam through. More sophisticated programs, such as Bayesian filters or other heuristic filters, attempt to identify spam through suspicious word patterns or word frequency.

This existing approach simply removes the spam. It does not consider removing offensive content from all categories of mails. In this work a method is introduced to implement a profanity filter within the email system.

A word filter (sometimes referred to as just "filter" or "censor") is a script typically used on chat or Internet forums that automatically scans users' posts or comments when they are submitted and automatically changes or censors particular words or phrases. The main functions of a profanity filter include removal of vulgar language, cliché control, vandalism control etc. Here the profanity filter is implemented by using a collaborative filtering approach.

The rest of the paper is organized into four sections. Section II deals with the related works. Proposed System is discussed in section III. Section IV involves the results and discussions and the conclusion of the work is given in section V.

II. RELATED WORKS

(A)Email Classification Based on Structure and Content

In this paper they have proposed a novel approach that classifies the emails in a folder using structure as well as the content. This approach is based on the premise that representative - common and recurring structures/patterns can be extracted from a pre-classified email folder and the same can be used effectively for classifying incoming emails[6]. A number of factors that influence representative structure extraction and the classification are analyzed conceptually and also validated experimentally. In this approach, the notion of inexact graph match is leveraged for deriving structures that provide coverage for characterizing folder contents.

(B)Email Classification Based on Data Reduction Method

For anti-spam researchers, classifying user emails correctly from penetration of spam is an important research issue.In this paper, the authors proposed an effective and efficient email classification technique based on data filtering method[8]. They have introduced an innovative filtering technique using instance selection method (ISM) that reduce the pointless data instances from training model and then classify the test data. The objective of ISM is to identify which instances (examples, patterns) in email corpora ,without significant loss of information should be selected as representatives of the entire dataset. They have used WEKA interface in their integrated classification model and tested diverse classification algorithms. Their empirical studies show significant performance in terms of classification accuracy with reduction of false positive instances.

(C)Email Classification with Backpropagation Technique

This paper proposes a new email classification model using a teaching process of multi-layer neural network to implement back propagation algorithm. The major contributions in this paper are: the use of empirical analysis to select an optimum, novel collection of features of a user's email message content that enables the rapid detection of most important words, phrases in emails and a demonstration of the effectiveness of two equal sets of emails (training and testing data). [5] discussed about creating Obstacles to Screened networks. In today’s technological world, millions of individuals are subject to privacy threats. Companies are hired not only to watch what you visit online, but to infiltrate the information and send advertising based on your browsing history. People set up accounts for facebook, enter bank and credit card information to various websites. Those concerned about Internet privacy often cite a number of privacy risks events that can compromise privacy which may be encountered through Internet use. These methods of compromise can range from the gathering of statistics on users, to more malicious acts such as the spreading of spyware and various forms of bugs (software errors) exploitation.

(D)Email Classification Using Semantic Feature Space

This paper proposes a new email classification model using a linear neural network trained by perceptron learning algorithm (PLA) and a nonlinear neural network trained by back propagation neural network (BPNN). A semantic feature space (SFS) method has been introduced in this classification model[7]. The bag of word based email classification system has the problems of large number of features and ambiguity in the meaning of the terms. It will cause sparse and noisy feature space. We use the semantic feature space to address these problems.It converses the original sparse and noisy feature space to semantic-richer feature space.It also helps to accelerate the training speed. Experimental results show that the use of semantic feature space can greatly reduce the feature dimensionality and improve the classification performance.

III. PROPOSED SYSTEM

In this approach, initially the message body and header is read. Based on this content, the category to which the mail belongs is identified. Then the identified categories will be listed out. Then the system checks for the presence of abusive words. If an abusive word is identified then the mail is listed to have an abusive word. Then the identified abusive word is given to the genetic algorithm to generate the possible future combinations. The concept of collaborative filtering is used here. Then the training is performed using neural network. The entire email content is considered as the training set. From this the weightage of each word is calculated and the most appropriate word at that particular instant is found out.

A. Content Analysis

Content analysis is the first step performed. In this the content of email body is read and identified[3]. This phase finds out the possible categories that email can belong to based on the content

B. Promotional Mails

If the mail contains promotional words like flipkart, myntra, jabong etc then it is included in promotional mail.

C. Social Mails

If social words like Facebook, twitter, Gmail etc are identified then the mail is included in social category.

D. General Mails

If the mail contains general matters other than social and promotional matter then the mail is classified as general.

E. Detection of Abusive Words

Once the mail category is identified then it is checked to see whether it contains any abusive word. This is done by using a collaborative filtering approach. The original mail content is matched with the set of listed abusive words and if any match is found then the mail is listed to have abusive content.

F. Collaborative Filtering

Collaborative filtering is the process of filtering for patterns or informations using techniques involving collaboration among multiple viewpoints, agents and data sources. Applications typically involve very large datasets[1]. Collaborative filtering has two senses, a narrow one and a more general one[2]. Collaborative filtering methods have been applied to many different kinds of data including: sensing and monitoring data, such as in mineral exploration, environmental sensing over large areas or multiple sensors; financial data, such as financial service institutions that integrate many financial sources; or in electronic commerce and web applications where the focus is on user data, etc. Here this is used to identify the offensive or abusive content.

G. Genetic Algorithm

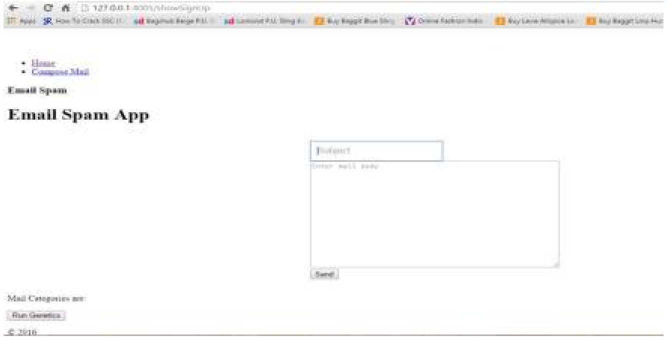
Genetic algorithm (GA) is a search heuristic that mimics the process of natural selection. This is used to generate useful solutions to optimization and search problems[4]. Genetic algorithms belongs to the larger class of evolutionary algorithms (EA), which usually generate solutions to optimization problems using techniques inspired by natural evolution, such as mutation, inheritance, selection and crossover. These techniques are termed as genetic operators. In this work GA is used to predict the possible combinations of the detected abusive word. This is based on the assumption that the words generated using an abusive word may turn abusive in future.

H. Training Using Neural Network

Artificial neural networks are generally presented as systems of interconnected "neurons" which exchange messages between each other. They are a family of models inspired by biological neural networks (the central nervous systems of animals, in particular the brain) which are used to approximate or estimate functions that can depend on a large number of inputs and are generally unknown.

In this system the entire email content is considered as the training set. From this the most appropriate word at that instant is found by calculating the weightage of each word. So this word will be the most significant word and turns out that there is no chance for this word to be abusive. So this is added to a good list of words. Genetic algorithm generates or predicts different combinations of abusive words. So these words can be cross checked with the words in the good list. If the predicted list matches with any word in the generated good list then this word can be easily eliminated from the abusive list because it was once found as the most appropriate word in some context. This further adds the overall efficiency of the system.

IV. RESULTS AND DISCUSSIONS



Email Spam

Email Spam App

Mail Categories are:

© 2016

Figure 1.Interface for composing email

On clicking “Compose email” button we are able to compose the email. On clicking the “Send” button the mail content is checked by the system. Then the possible categories are listed. On clicking the “Run Genetics” button the different possible combinations of detected abusive words are generated and displayed.

VI.CONCLUSION

A spam filter is a program that is used to detect unwanted and unsolicited email and prevent those types of messages from getting to a user's inbox. Usually a spam filter looks for certain criteria on which it bases judgments. For example, the simplest and earliest versions (such as the one available with Microsoft's Hotmail) are set to watch for particular words in the subject line of messages and to exclude these from the user's inbox. This method is not especially effective, too often omitting perfectly legitimate messages (these are called false positives) and letting actual spam through. More sophisticated programs, such as Bayesian filters or other heuristic filters, attempt to identify spam through suspicious word patterns or word frequency. But this does not guarantee the removal of offensive or abusive content.

References

[1] Fisher, D.; Hildrum, K.; Hong, J.; Newman, M.; Thomas,M.; and Vuduc, “A framework for collaborative filtering algorithm development and evaluation.", SIGIR 2000. Short paper, 2000.

[2] Popescul, A.; Ungar, L.; Pennock, D. M.; and Lawrence S., “Probabilistic models for unified collaborative and content-based recommendation in sparse-data environments,” InProceedings of the Seventeenth Conference on Uncertainity in Artificial Intelligence ,1998.

[3] Hammami, M., Chahir, Y., and Chen, L., “WebGuard: a Web filtering engine combining textual, structural, and visual content-based analysis,” IEEE Transactions on Knowledge and Data Engineering 18, (2006), 272-2844

[4] DUMAIS,S.T.,PLATT,J.,HECKERMAN,D.,ANDSAHAMI,M., “Inductive learning algorithms and representations for text categorization,” InProceedings of CIKM-98, 7th ACM International Conference on Information and Knowledge Management (Bethesda, MD, 1998), 148–155..

[5] Christo Ananth, P.Muppidathi, S.Muthuselvi, P.Mathumitha, M.Mohaideen Fathima, M.Muthulakshmi, “Creating Obstacles to Screened networks”, International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST), Volume 1,Issue 4,July 2015, pp:10-14

[6] M.AeryandS.Chakravarthy, “eMailSift:Email classification based on Structure and Content,” In Proceedings of Fifth IEEE International Conference in Data Mining[ICDM’05], 2005.

[7] Yun Fei Yi.;Cheng Hua Li.; and Wei Sing, “Email Classification using Semantic Feature Space,” Proceedings of ALPIT’08,International Conference on Advanced Language Processing and Web Information Technology., 2008.

[8] Rafiqul Islam.; and Yang Xiang, “Email Classification using Data Reduction Method,” Proceedings of Fifth Inernational ICST Conference on Communications and Networking in China [CHINACOM].,2010

AUTHOR PROFILE

Reshma Rajan is currently pursuing M.Tech in Computer Science and Engineering in Mar Athanasius College of Engineering, Kothamangalam.

Rahul V Cheeran is currently pursuing M.Tech in Computer Science and Engineering in Mar Athanasius College of Engineering, Kothamangalam.

Surekha Mariam Varghese is currently heading the Department of Computer Science and Engineering, M.A. College of Engineering, Kothamangalam, Kerala, India. She received her B-Tech Degree in Computer Science and Engineering in 1990 from College of Engineering, Trivandrum affiliated to Kerala University and M-Tech in Computer and Information Sciences from Cochin University of Science and Technology, Kochi in 1996. She obtained Ph.D in Computer Security from Cochin University of Science and Technology,Kochi in 2009. She has around 26 years of teaching and research experience in various institutions in India. Her research interests include Network Security, Database Management, Data Structures and Algorithms, Distributed Computing and Machine Learning. She has published 27 papers in international journals and international conference proceedings. She has served as reviewer, committee member and session chair for many international conferences and journals.