ISSN No. 0976-5697

Volume 2, No. 5, Sept-Oct 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Filtering Spam Emails Based on User Behaviors

Mashael Alsowaiel* and Omar Batarfi
Department of Computer Science,
King Abdul-Aziz University,
Jeddah, Saudi Arabia
*Malsowaiel.cs@gmail.com
obatarfi@gmail.com

Abstract: Recently, more and more people are suffering from ever-increasing unwanted e-mails (named spam).It affects the cost of organizations and bothersome the email recipient. This paper will show an adaptive learning system that control spam emails by using user behaviour filtering. This filter can automatically adapt to the user interests, and it based on the action taken by the user by either delete or leaves the email. In addition to that the time taken for reading that email will be considered. This filter can recognize the meaning of each action has entered from the user and then it determines suspect rate for the filtered emails. Based on the rate that is given by the filter, the processed email will be considered either as spam or not. The results demonstrate that the technique has relatively lower false positives and false negatives. Also it is fast for adaptation to changing environment, show a good performance, and it is a good instant solution for spam filtering. So the users can reflect personality interest flow constantly by using this filter.

Keywords: spam email; Spam filter; Spam mail detection; behaviour recognition; user feedback, user action.

I. INTRODUCTION

With the development of Internet and the fast increase of network bandwidth, it has been clearly seen that Emails are one of the frequent used applications. Over the past few years, the propagation of bulk and unwanted emails, filled up email boxes of millions of people worldwide, these unwanted emails are known as spam or junk mails [4, 10]. Spam has caused some serious problems. Firstly, it wastes a gathering of network resources that are very important for network users. Secondly, it seriously influences the daily work of many users, especially those in enterprises or corporations [4].People has been stressed with spam for about 10 years. In 2002, an American person received 2200 spam mails on average and the amount increases 2% per month, causing up to 3600 pieces of spam mails in 2007. It causes the affected companies to have annual loss in proceeds [5]. Nowadays, more than 50% of emails received are spam on Internet [4].This trend is even worse in China and America. According to a major internet security company, increasing rate is 20% per year, 92.6% of total emails in last year were spam [1]. Moreover, the average number of spam emails received is continually increasing exponentially. Spam mail causes a huge problem to computer users today. People need to spend a lot of time to deal with spam every day. Even worse, many current spam emails would seriously fault the user's system by receive users unexpected malicious attachments.

The development method of anti-spam has been considered through three phases: content-based filter, statistic-based intelligent filter and behavior-based filter. With statistical analysis of behavior, spam has a high degree of distinction with normal message in behavioral characteristics [5]. Researches on behavioral characteristics regularly focus on incoming messages. This paper will discuss one phase which is behavior-based filter. Many studies have proposed regarding spam filtering have focused on studying the behavior of the sender or the receiver for incoming emails. For instance, typical normal user behavior will be recognized. Then the abnormal behavior will be detected and it suspicions to a spam behavior [2]. System of spam email filtering using different weight based on relationship between user action and time delay between actions [1].

This paper pays attention to another aspect in behaviour based spam detection. It will present an adaptive learning system that filter spam emails, each email will be given suspected rate by the filter system based on user's action pattern and time taken in reading a specific message after opening it. User's interest changes continuously, hence, filtering system is required to learn and reflect these changes in order to change the rate of the email depending on the interest of the user. In addition, the received emails from different people will be ordered in the inbox with respect to the rate given by the proposed system for each email. There is a significant concept is used in recognizing the changes and reflect them. This concept is known as "Concept Drift" or" Interest Drift" which mean that user interest regarding some topics and some suspicious emails spam may be changed from time to time [1,6].

This system for spam filtering standing at a unique point of view, which can effectively reduce the false positive (fp) and false negative (fn) .Additionally, it makes efforts to increase accuracy of detect spam email by analyze user's intention of each action more clearly and instantly. Therefore, from this paper of view, there is anticipation that the learning of detection spam emails will be improved accurately by adding additional actions and analyzing them clearly to reflect their rates precisely. The rest of this paper is structured as follows: In Section 2, we present the background studies. Section 3, we present related work. Section 4 describes proposed system; evaluation of experimental results is presented in Section 5. The Case study for the spam filter is presented in Section 6. Finally, we conclude our research work and future work in Section 7.

II. THE BACKGROUND STUDIES

Email spam, also known as junk email or unsolicited bulk email (UBE), is a subset of spam that involves nearly identical messages sent to numerous recipients by email. Definitions of spam usually include the aspects that email is unsolicited and sent in bulk. One subset of UBE is UCE (unsolicited commercial email). The opposite of spam, email which one wants, is called "ham," usually when referring to a message's automated analysis (such as Bayesian filtering)[7,8,10].With respect to the definition of spam filter, is a piece of software that scans through a message to determine if it is spam or not. Most spam filters work in a very similar way, using a set of rules to try and work out what the message is about and whom it is from. Some are more successful than others. There are many types of spam filter, those types include: Content Based Filters, Challenge-Response; Rules based scans, White list/Blacklist Filters, Bayesian Analysis, Community Filters, and Filter Placement [8, 9]. Furthermore, the main terminology in spam filters False Positive this is where a spam filter identifies a message as spam when it is innocent. This is the worst kind of error for a spam filter to make. It is better to err on the side of false negatives. False Negative this is where a spam filter fails to identify a spam message as spam. A lesser problem than false positives, but still to be avoided [8].

Domain of spam change speedily, and user interests and concerns change with time also. So we need identify that change and reflect to learning. This is called Concept Drift or Interest Drift. Required concept of this need is Adaptive Learning. It means that learn user interest and feature of spam with track changing concepts. It reflects changing interests and features to learning in real time [1, 10].

III. RELATED WORK

Anti-spam technology has been developed to the third-generation technology [2]. There exist various forms of filters based on user behaviour. Most of these spam filtering based on rule or message is a method that identify spam features from email and make a decision whether the email were spam or not. This old approach is used by many filtering system because of its simplicity for implementation. But it has a limitation to update rule continuously every time features of spam change. The most representative method to solve this limitation is an adaptive learning system that filters spam emails based on user’s action pattern as time goes by. User interest change continuously, so filtering system is required to learn interest and reflect this.

So this system which based on the concept of "Concept Drift". Especially, base actions for emails is divided into six actions as ‘open’, ‘delete', 'save’, ‘reply’, ‘block’, ‘nothing'. Each action has a default weight and it is classified into positive category (non spam emails category), or negative category (spam emails category). Then the system calculates a final weight based on relationship between user’s actions. In other words, the overall actions have entered by the user for a particular email and the time has taken to do each action. So the system used weighting function to calculate final two weights of positive and negative category for email as follows: positive category weight that means a set of all non spam actins weight which known by the abbreviation (NW), and negative category weight that means a set of spam actions weight which known by the abbreviation (SW). And then the email will be classified to the category that has larger weight than the other category. Then, this email will be gained a new weight from the result of the following equation (NW - SW). There is a disadvantage in this system; it needs to increase the performance by analyzing relation between actions correctly. And also it needs to study the accurate method that reflects meaning of user action to the filtering system correctly [1].Many studies have focused on the detection of abnormal behaviour in the period of SMTP conversation. There is another study pays attention to a different aspect in behavior based spam detection. Outgoing behavior based on statistical analysis of email sending behavior is concerned.

The system can calculate the statistical characteristics and general features of incoming messages by observing outgoing traffic or behavior for that email. Then typical normal user behavior model will be built, and the histogram analysis is selected to model the behavior of the user. When the user behavior is distinct from the normal behavior by comparing their behavior patterns, the abnormal behavior will be detected .Therefore the behavior suspicions to spam. Behavior features of email include for example: number of email messages, size of email message, number of attachments, and number of recipients in a period of time.

Also other suitable features of single email message have been selected to observe the email sending behaviour. And most of spam is represented by hyperlink, some others with images, attachments, and so on [2]. There is a new anti-spam technique, which includes a user active feedback mechanism, and maximum entropy based spam filtering approach. It is a new technique to be discussed for spam filtering that focus mainly on server-side functions. In the period of mail training destined to the construction of classifier; any incoming email should be explicitly identified as spam or legitimate email by its corresponding user. Mail server will send the corresponding user a mail to ask whether the mail is spam or not. If the system cannot distinguish the incoming mail as spam or legitimate, the system sends a mail asking for the user feedback about whether it is spam or not. On receiving the feedback the system will timely update its corresponding classifier for user. When the same kind of mail enters the mail server again, the system will classify it independently [3].

IV. PROPOSED SYSTEM

Fig.1. shows a system layout proposed in this paper. The system assign the email with Rate calculated by user action type and time elapsed for each emails. Action recognizer method saves email ID, action type, start time and end time to action profile when user performs an action for email message. Then a system gives a rate to each email in the profile. The system permits a re-classification for email to update a rate as new action is added to that email. So the rate of each email can be updated continuously. At the test phase, email is finished filtered.

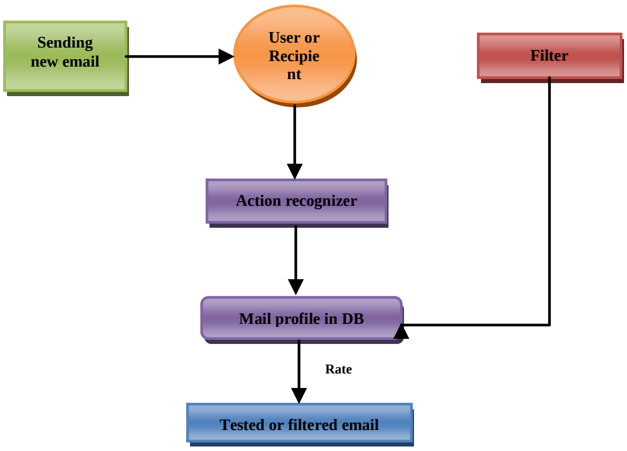


Figure.1. System Architecture

A. *Spam filters system work flow:*

The filter must be checked on state of email in two ways:

a. It will be checked the state of email at the time of arrival, If this email is new (just received) or not.

i. If the incoming email is new

It is forwarded automatically to inbox folder of mail, and the filter will assign the rate10 to it.

ii. If the incoming email is not new, the filter will be checked on the previous email rate in data base.

a. If the rate of previous email is from 2-10

i. The incoming email is forwarded automatically to inbox, and it takes the same previous email rate.

a. If the rate of previous email is 1.

i. The incoming email is forwarded automatically to spam, and it takes the same previous email rate.

b. It will be checked the state of the email at the time of opening, if this email is opened before or not.

i. If this email has not opened before

ii. Any actions from user on this email will be taken by the filter, and it affect on the rate.

ii. If this email has opened before

iii. Any actions from user on this email will be not taken (ignore) by the filter, and it do not affect on the rate at all.

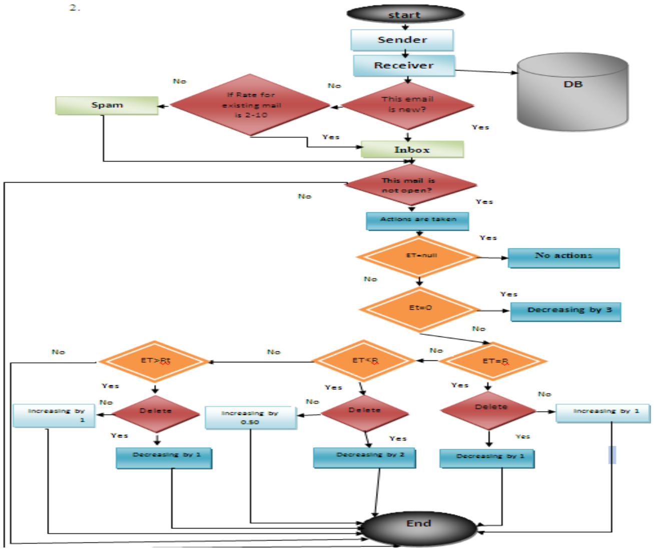


Figure.2. Flow chart for the spam filter system

B. *Email rating schema:*

While the filter in receiver side will use the rate from 1-10 for received email in this filter: 1 2 3 4 5 6 7 8 9 10, where 10 is higher or pure legal and it assigned to each new incoming email, and 1 is pure spam. This filter must calculate two times because it will be compare these time foe each user email.

First: Calculate the real time of reading email we denote it as RT: which indicates the actual required time to reed numbers of words in email. RT is computed as following:

a. Calculate the number of words in each email by counter.

b. Calculate the required time for reading one word which it is calculated as:

i. Most adults read at a rate of about 200 - 300 wpm, and we will use the average rate for speed reading of human is 250[10, 11, 12].

ii. The time required to read one word is 60/250 seconds=0.24 from second.

c. TR= the required time for reading one word* number of words in email.

Second: Calculate he elapsed time of reading email we denote it as ET: which indicates spent time in reading the specific message from opening the email to delete it or close it.

C. *Rating Action Patterns for Rating:*

This filter can automatically adapt to the user interests and behaviour with each incoming email, it based on the action taken by the user by either delete or leaves the email and the time taken for reading that email after opening it.

This filter can recognize the meaning of each action on specific email, and then it determines suspect rate for that email. The rate of the email in this system will be changed according the user action every time. Email messages from a sender will be handled based on the action taken on his/her previous email messages and classified those messages depending on whether it is spam emails or not. Furthermore, the email messages will be sorted with respect to their rates given by our proposed system. The actions that are considered in this filter included; 'open', 'not open', 'delete', and 'not delete or leave message'. And in this filter, the action delete is worst action and more affect negatively to the rate of email. Therefore it leads the email into spam quickly. The rate of email gradually decreases by the negative gradient of the case. Listen Read phonetically

Each arrived email will have eight cases, and it based on two important factors:

a) The delete action.

b) Reading time for the email.

a. The eight cases are as the following:

a. When the user open and read received email:

i. Elapsed time equals real time which means that the user reads the email in time = the required time for read this email.

Case1: ET=RT and action=leave message; (this email is kept in the inbox). In this case, the rate of email will be increased by 1 (Rate +1).

Case2: ET=RT and action=delete message, (this email is deleted from the inbox). In this case, the rate of email will be decreased by 1 (Rate-1).

ii. Elapsed time less than the real time which means that the user reads email in time < the required time for read this email.

Case3: ET<RT and action=leave message. In this case, the rate of email will be increased by 0.50 (Rate+0.50)

Case4: ET<RT and action=delete message. In this case, the rate of email will be decreased by2 (R-2)

iii. Elapsed time more than the real time which means that the user reads email in time > the required time for read this email.

C ase5: ET>RT and action=leave message. In this case, the rate email will be increased by1 (R+1)

Case6: ET>RT and action=delete message. In this case, the rate of email will be decreased by1 (R-1).

b. When the user does not open the received email:

Case7: ET=0 and action=delete message. In this case, the rate of email will be decreased by3 (R-3)

Case8: ET=null, do not take any action after received the email. (This email is kept in the inbox).In this case, the rate of email will be not changed.

Note:

a. The rate for any new email is started with 10 as initial value. And any actions applied on the message will change the rate to new value that is based on previous rate for that email.

b. In case the email's rate is 10, the rate will not be changed for any positive action.

c. In case the email's rate is 1, the rate will not be changed for any negative action.

d. The email which is considered as spam and exists in the spam folder can be retrieved to the inbox as non spam email if the user only applies to it some actions that increase the rate.

e. Each time the emails in inbox will be sorted based on its rate value. And if the different account of emails has the same rate, then they will be ordered base on date and time for these emails.

D. Handling the personalization and email rate with DB:

We have created three tables in data base for this system:

a. Info table contains: the main Email ID (prime key) for email, counters, and rate.

b. mail_box table contains: the secondary Email ID (foreign key).

c. spam_box table contains: the secondary Email ID (foreign key).

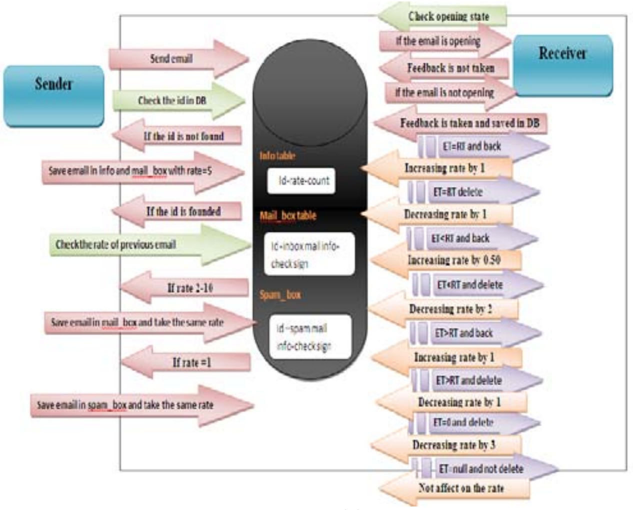


Figure.3. the process of filter with DB

V. EVALUATION OF EXPERIMENTAL RESULTS

From the results are obtained after testing we have a good instant detection system for spam emails by using the user behavior. This filtering system can recognize user actions on each email and detects spam email vastly and accurately. This system cans adaptation to changing environment. So the rate of any new email will be updated according to the changes of user's action every time.

Actions or feedback				Affect on the rate	
Read email	Time	back	delete	Count	Rate
Read email	ET=RT	✓	☒	☒	Increasing by 1
Read email	ET=RT	☒	✓		Decreasing by 1
Read email	ET<RT	✓	☒		Increasing by 0.50
Read email	ET<RT	☒	✓		Decreasing by 2
Read email	ET>RT	✓	☒		Increasing by 1
Read email	ET>RT	☒	✓		Decreasing by 3
Not read	ET=0	☒	✓	☒	Decreasing by 3
Not read	ET=nu	☒	☒	☒	No affect on rate

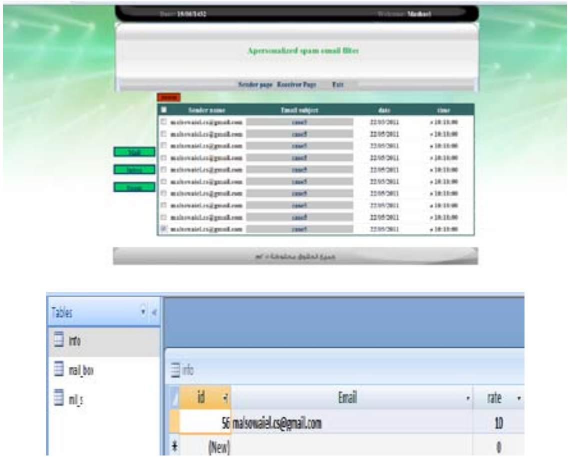
Table no.1 summarizes the experimental results of the prototype, and it show summary the user feedback and affect these feedback on the rate

We have been confirmed the validity of our hypothesis which is written for this research paper. Because we proved that we can make a personalized email spam filter with a fast and highly accurate metric. It can automatically adapt to the user interests and his/her behavior with each incoming email. And then inferring rate for each email based on user action. As shown in table1. So the real and spam email not be permanently fixed in their place, but they are variable depending on the behavior of user on email message in every time. Then we have relatively lower false positives and false negatives. Therefore, the number of permissible messages from unknown and trust people can receive high rate and constantly classified as real. Also the number of unwanted messages constantly classified as spam respectively.

VI. SPAM EMAIL FILTER CASE STUDY

According to the techniques discussed above, we implemented a prototype mail server system. We created this web application to simulate the real system by using VB.NET, and we used Access 2007 to create the data base for these filter.

Figure 4.1 the home page to welcome the users and log in to my system.

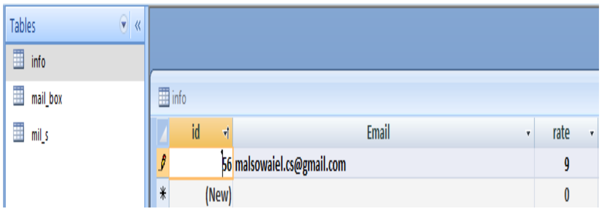

Apersonalized spam email filter
Sender page Receiver Page Exit
Sender name
Email subject
date
time
Tables
info
mail_box
mil_s
info

id	Email	rate
56	malsowaiel.cs@gmail.com	10
(New)		0

Figure 4.2 the filter will assign the value 10 as the initial rate for the received emails in inbox folder.

a. When the receiver opens the email. And he reads it in time equal the real time for this email, then he click on back .The filter will be increase the rate automatically by 1.But here the rate for email already is 10,therefore the rate will be stay =10 .As shown in figure 4.2

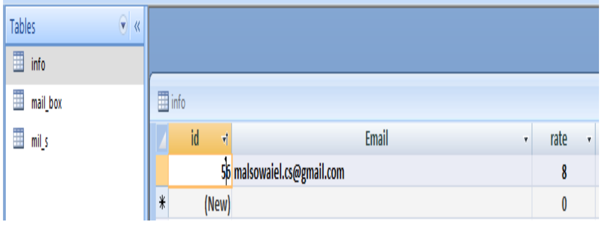
b. When the receiver opens the email. And he reads it in time equal the real time for this email. Then he clicks on delete. The filter will be decrease the rate of the email by 1, and it becomes 9. As shown in figure 4.3



id	Email	rate
56	malsowaiel.cs@gmail.com	9
(New)		0

Figure 4.3 the filter will be decrease the rate of the deleted email by 1

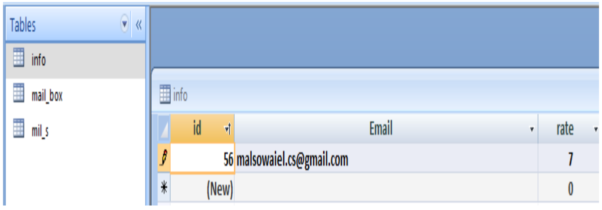
c. When the receiver opens the email .And he reads it in time less than the real time for this email. Then click on delete. The filter will be decrease the rate of the email by 2, and it becomes 8. As shown in Figure 4.4



id	Email	rate
56	malsowaiel.cs@gmail.com	8
(New)		0

Figure 4.4 the filter will be decrease the rate of the deleted email by 2.

d. When the receiver does not opens the incoming email. And then he clicks on delete. The filter will be decrease the rate of the email by 3**,** and it becomes 7. As shown in Figure 4.5



id	Email	rate
56	malsowaiel.cs@gmail.com	7
(New)		0

Figure 4.5 the filter will be decrease the rate of the deleted email by 3.

VII. CONCLUSION AND FUTURE WORK

In this paper we proposed a system to control the spam email by using user behavior filtering. This filter based on the action taken by the user by either delete or leaves the email and the time taken for reading that email. Then it is inferring differentiated ratings between emails. This work proved the rate of any new email will be updated according to the changes of user's action every time. The real benefit from our system is that fast and highly accurate metric is obtained to do the spam email filtering. And it shows a good performance. Also this paper deals with a personalization feature. So users can give more correct and accurate rates to emails by their interest .And they can reflect personality interest flow constantly. There are more idea can be applied in the future work, and these include,

a. We need to make the optional for user to choose the state or type of this filter. If he wants that state is strong, medium or poor. This is achieved by choose the value of rate. So it makes this value variable to change every time by user. This value put it in settings of email interface to allow the users to choice the value which they wanted.

b. We will study more actions are taken by user on the email .So that we can give more correct and accurate weights to emails by their interest, and can reflect individual interest flow constantly.

VIII. REFERENCES

[1]. A.Han1,j.Hyun,I.Ha1,G.Jo2,"Semantic Analysis of User Behaviors for Detecting Spam Mail", 1 Intelligent E-Commerce Systems Lab., Inha University, Incheon, School of Computer Science & Engineering, Inha University, Incheon, Korea,2010.

[2]. M.Wang,Z.Li, L. Xiao, Y. Zhang, "Research on Behavior Statistic Based Spam Filter", School of Computer Science & Technology Huazhong University of Science & Technology Wuhan, China,2009

[3]. S. Zhong, H. Huang, L. Pan," An Effective Spam Filtering Technique Based on Active Feedback and Maximum Entropy", Computer and Information Engineering College, Central South University of Forestry &Technology Changsha, Hunan, 410004, China,2010

[4]. Y. Li1,2, B.Fang1, L.Guo1, S. Wang1,2," Research of a Novel Anti-Spam Technique Based on Users' Feedback and Improved Naïve Bayesian Approach", 1Software Division, Institute of Computing Technology, Chinese Academy of Sciences, 100080,Beijing, China,2006

[5]. S. Naksomboon1, C. Charnsripinyo2 and N. Wattanapongsakorn1, "Considering Behavior of Sender in Spam Mail Detection", Computer Engineering Department, King Mongkut's University of Technology Thonburi, 2009

[6]. M. MORITA, Y. SHINODA,"Information Filtering Based on User BehaviorAnalysis and Best Match Text Retrieval",School of Information Science Japan Advanced Institute of Science and Technology.2009

[7]. P. Cortez, C. Lopes, P. Sousa, M. Rocha, M.Rio," Symbiotic Data Mining for Personalized Spam

Filtering",Dep. of Information Systems/Algorithmic University of Minho,4800-058 Guim. Portugal, 2009.

[8]. http://www.clearmymail.com/guides/spam_filter_types.aspx

[9]. http://www.whichspamfilter.com/TypesOfFilters.htm

[10]. http://en.wikipedia.org/wiki/E-mail_spam

[11]. http://www.ehow.com/how_7923940_read-very-fast.html

[12]. http://keirkei.com/blog/personaldevelopment/whats-the-average-reading-speed-and-the-best-rate-of-reading