International Journal of Engineering & Technology
CENTRE OF PROFESSIONAL RESEARCH PUBLICATIONS
ISSN 2049-3444

International Journal of Engineering and Technology Volume 2 No. 10, October, 2012

Building a Spammer Monitoring System Using Heuristic Rule-Based Approach

[1]Adewole Kayode S., [2]Babatunde Ronke S., [2]Isiaka Rafiu M., [2]Abdulsalam Sulaiman O.
[1]Department of Computer Science, University of Ilorin, Ilorin.
[2]Department of Computer, Library and Information Science, Kwara State University, Malete.

ABSTRACT

Spam is a major problem of electronic mail system that has enjoyed extensive discourse. E-mail has been greatly abused by spammers to disseminate unwanted messages and spread malicious contents. Several anti-spam systems developed have been greatly abused and this is as evident in the proliferation of Spammer's activities. Observing this fact, a protective mechanism to countermeasure the ever-growing spam problem is indeed inevitable.

In this paper, a heuristic approach is proposed which employs a standard normalized Spammer's languages harvested from Google and Yahoo spam language data set to build the knowledge base. The spam languages were prioritized based on the frequency of occurrence in the two global data sets. A threshold of 5% was established for a user without spamming history while 3% was set for a suspected spammer. A platform independent system was designed and implemented to monitor users' mail in real time. As soon as the threshold is reached the user will be alerted and the suspected mail will be cancelled. The developed model was evaluated for accuracy and effectiveness using three composed email messages. It is recommended among others that this spam preventive model be incorporated in the architecture of every Internet Service Provider.

Keywords: *Electronic mail, spammer, anti-spam, heuristic, threshold, platform.*

1. INTRODUCTION

The Internet has become an integral part of everyday life and hence, e-mail has become a powerful tool which is intended to be a means of exchanging idea and information at low cost and guarantee of an efficient mail delivery [16]. It is a popular and preferred communication tool due to its availability, reliability and user friendliness [19]. Over the years, the problem of spam e-mail has being on the vast increase. Spam is unsolicited and unwanted e-mail from a stranger that is sent in bulk large mailing list usually with some commercial objective [18]. Spam waste time, storage space and communication bandwidth [24]. The categories of spam according to [9] are:

- Health; such as fake pharmaceuticals
- Promotional products; such as fake fashion items e.g. watches
- Adult content; such as pornography and prostitution
- Financial and refinancing; such as tax solution, loan package
- Phishing and other fraud; such as "Nigeria 419" and "Spanish Prisioner"
- Malware and Viruses; such as Trojan horses attempting to infect PC with malware.
- Education; such as online diploma.
- Marketing; such as direct marketing material, sexual enhancement product.
- Political; such as US presidential votes

The increasing volume of spam has become a serious threat not only to the Internet but also to the business sector, education and society at large. The issue of spam message filtering cannot be over emphasized and has to be addressed in a multilayered approach i.e. at the source, on the network and with the end user [16].

A vast number of researchers on spam filtering centers on classification of spam e-mail messages. In this approach a set of rules which are created either by the user of the filter or by some authority (e.g. the software company providing a rule base spam filtering) is specified and used to classify the e-mail to a spam or non-spam. This is called knowledge engineering approach to spam filtering. The problem of this method is that the rules must be constantly updated and maintained which de-regulates the system and waste time [2]. At present, machine learning for spam classification becomes paramount and as such many researchers continually explore learning algorithms for spam filtering [8].

In machine learning approach to spam filtering, a set of pre-classified e-mail messages are used as training samples. An algorithm is then used to learn the classification rules from the training samples [23].

Machine learning algorithms include; Artificial Immune system, K-Nearest neighbor, Neural Network, genetic algorithm, support vector machine and Naïve Bayes.

In this paper, a heuristic approach is proposed which employs a standard normalized Spammer's languages harvested from Google and Yahoo spam language data set to build the knowledge base for rule classification and spam filtering. A system was developed to effectively and efficiently monitor user's email language in real-time, it compares the statement with the database and compute for the threshold. The result of the activities on a network is used to allow the email or cause a suspension of the email.

2. REVIEW OF EXISTING METHODS FOR SPAM FILTERING

The increasing amount of unsolicited e-mails (junk e-mails or spam) that circulate over the internet has prompted research efforts aiming at building effective and efficient anti-spam filters [10]. Indeed, the online community appears quite united in its contempt for spam. In spite of the numerous attempts to regulate spam, the problem has not diminished. The spammers continue to win the war in spite of the Internet community's best efforts [7].

Previous approach to spam filtering ranges from machine learning techniques such as Support Vector Machine (SVM), Naïve Bayes (NB), Artificial Neural Network (ANN), Artificial Immune System (AIS), Rough Set Classifier, and K-nearest neighbor, to Case-Based approach, White/Black list, and Legislation approach.

2.1 Machine Learning Spam Filtering Approach

Machine Learning is a scientific discipline which is concerned with the design and development of algorithms that enables adaptation of computers to behavior based on data. Machine Learning is a subfield from the broad field of Artificial Intelligence, that aims at making machines able to learn like human [3][19].

2.1.1 Support Vector Machine for Spam Filtering.

The Support Vector Machine (SVM) is a classification and regression algorithm. SVMs have worked well for the incremental model learning and have shown impressive performance in the active learning application for its nice properties of summarizing data in the form of support vectors [20]. The main idea of SVM is to construct a non linear kernel function to map the data from the input space into a possibly high dimensional feature space and then generalize the optimal hyper-plane with maximum margin between the two classes [5]. The search method of SVM aims to select the hyper plane that separate the training instances (messages) of the two categories with maximum distance [20]. [3] proposed a system that uses the SVM for classification. In their work, the system extract e-mail sender behavior data based on global sending distribution, analyze them and assign a value of trust to each IP address sending e-mail message. The experimental result shows that the SVM classifier is effective, accurate and faster compared to Random Forest Classifier.

2.1.2 Artificial Neural Network for Spam Filtering

Neural Network (NN) has been extensively used for text classification since its introduction by McCulloch and Pitts in 1943 [19]. NN is a computational model based on biological neural network. It is an adaptive system that changes its structure based on information that flows through the artificial network during a learning phase. It is based on the principle of learning. [14] in their work use perceptron algorithm to find a linear function of the feature vector $f(x) = w^T x + b$ such that $f(x) > 0$ for vectors of one class and $f(x) < 0$ for vectors of other class. The perceptron learning is done with an iterative algorithm that starts with arbitrarily chosen parameters (w_o, b_o) of the decision and updates them iteratively. A training sample (x,c) is chosen on the n-th iteration of the algorithm such that the current decision function does not classify it correctly. The parameters (w_n, b_n) are updated and the algorithm stops when a decision function is found that correctly classifies all the training samples. [6] classified spam using LINGER, a neural network-based system which uses a multilayer perceptron. It includes 2 feature selectors, information gain (IG) and variance (V). Their result shows that neural network based filters achieve better accuracy.

2.1.3 Naïve Bayes for Spam Filtering

The Naïve Bayes (NB) classifier for spam recognition was first proposed in 1998 by [17]. NB Classifier works on the dependent events and the probability of an event occurring in the future that can be detected from the previous occurring of the same event [2]. The NB technique can be used to classify spam e-mails in which words probability plays the main role. The Bayesian filter assign probability to every word in the spam or ham e-mail database and make filtering decision based on the score. There are only 2 categories. If the total of word probability exceeds a certain limit, the filter will mark the e-mail to either category [13]. [11] implemented a Bayesian filter that caught 99.5% of spam with 0.03% false positives.

[2] implemented a Rough Set based model to classify e-mails into 3 categories; Spam, non-spam and suspicious e-mails and compared it with NB classifier. The result shows that Rough Set classifier method has a better accuracy than Naïve Bayes.

2.2 Case Based Approach

The Case-Based spam filtering system uses the Mail User Agent (MUA) to Track Concept Drift which is extended to allow the user to label messages as spam and non-spam. There is also a CaseRetention Process that maintains a personalized Case-Base of spam. This involves selecting the appropriate features to represent spam and non-spam messages and selecting the cases that give the best coverage. Finally there is the spam classifier that intercepts the download of email and tags the spam. Cases need to be added to the Case-Base to cover new types of spam and cases need to be deleted as older types of spam disappear. [18] in his work proposed a case-based approach to spam filtering that can track concept drift. They carried out a preliminary evaluation of Case-Based approach to spam filtering and it was discovered to outperform Naïve Bayes. This is because spam is a disjoint concept. Case-Based classification works well for disjoint concepts whereas Naïve Bayes tries to learn a unified concept description.

2.3 White/Black List

These are earliest techniques for blocking spam messages. Whitelist is an MUA level rule-based filtering technique, where a whitelist is a register containing a collection of contacts from which e-mail messages can be accepted [16]. If an e-mail arrives but does not come from one of the contacts in the whitelist, then it is treated as spam and placed in the spam folder. While this technique is effective for some users, it has also drawbacks. Any email sent by a stranger will simply beincorrectly classified as false positive (FP). However there is a scheme that incorporates a challenge response mechanism to allow users to be added to a user's whitelist. Blacklists represent an online form of vigilantism with many side effects. Innocent parties often have their messages blocked, and there are few safeguards to make sure that parties are only being blacklisted for good cause [7].

A blacklist contains lists of known spammers. Essentially when a user gets spam, the user adds the senderof the spam to the blacklist. The entire domain of the sender of the spam can be added to the blacklist. Newly arrived e-mails are checked, and if the sender is on the blacklist, the e-mail is automatically classified as spam. As with the whitelist, there are flaws with blacklists too. The major problem stems from the fact that spammers tend to forge header information in their spam. The sender information is generally forged, meaning that perhaps innocent people are added to a blacklist but more importantly the effect which the blacklist will have, is diminished dramatically [24].

2.4 Legislation Approach

As the problem of spam has grown to 12.4 billion messages per day, Internet service providers ("ISPs"), and software developers have all tried various responses. Legislative responses have culminated in the Controlling the Assault of Non-Solicited Pornography and Marketing Act ("CAN-SPAM Act") of 2003 [7]. Numerous e-mail clients now include spam filters, and ISPs are using both technical and legal means to strike back at spammers. The recent CAN-SPAM Act in USA has had little effect. Legislative responses are limited by jurisdictional obstacles to enforcement and the technical measures taken by spammers to disguise their source and identity. According to [21], "*the goal of legislation is to create an enforceable law, which would make it illegal to send spam and impose heavy penalties for those caught doing so*". We consider legislation as an anti-spam solution because imposing legal consequences to spamming should discourage people from spamming and there are those who believe that no technological solution will solve the spam problem [15]. Despite the Legislative approach spammers routinely abuse the law and continue to deliver spam [22].

3. PROPOSED MODEL FOR SPAM FILTERING

The model below uses heuristic rule-based approach for spam filtering. It takes as an input a message sent from the user on a network. The message passed through filtering stage which also comprises classification and configuration modules. The configuration module is used to setup the collapsed spammers' words extracted from Google and Yahoo spam Language dataset to build the knowledge base. In the filtering stage, the user's history is first examined to determine if the current user has previous record of spammer or not. After the verification of the user's history, the input message will then pass through tokenization process where each word in the message is broken down for easy lemmatization. The words in the user's message are compared against the already stored spammers' languages in the knowledge base to set appropriate threshold for the current user. The resulting output is then subjected to classification process in order to determine if the user's message is a spam or legitimate message. The proposed model is shown in Figure1:

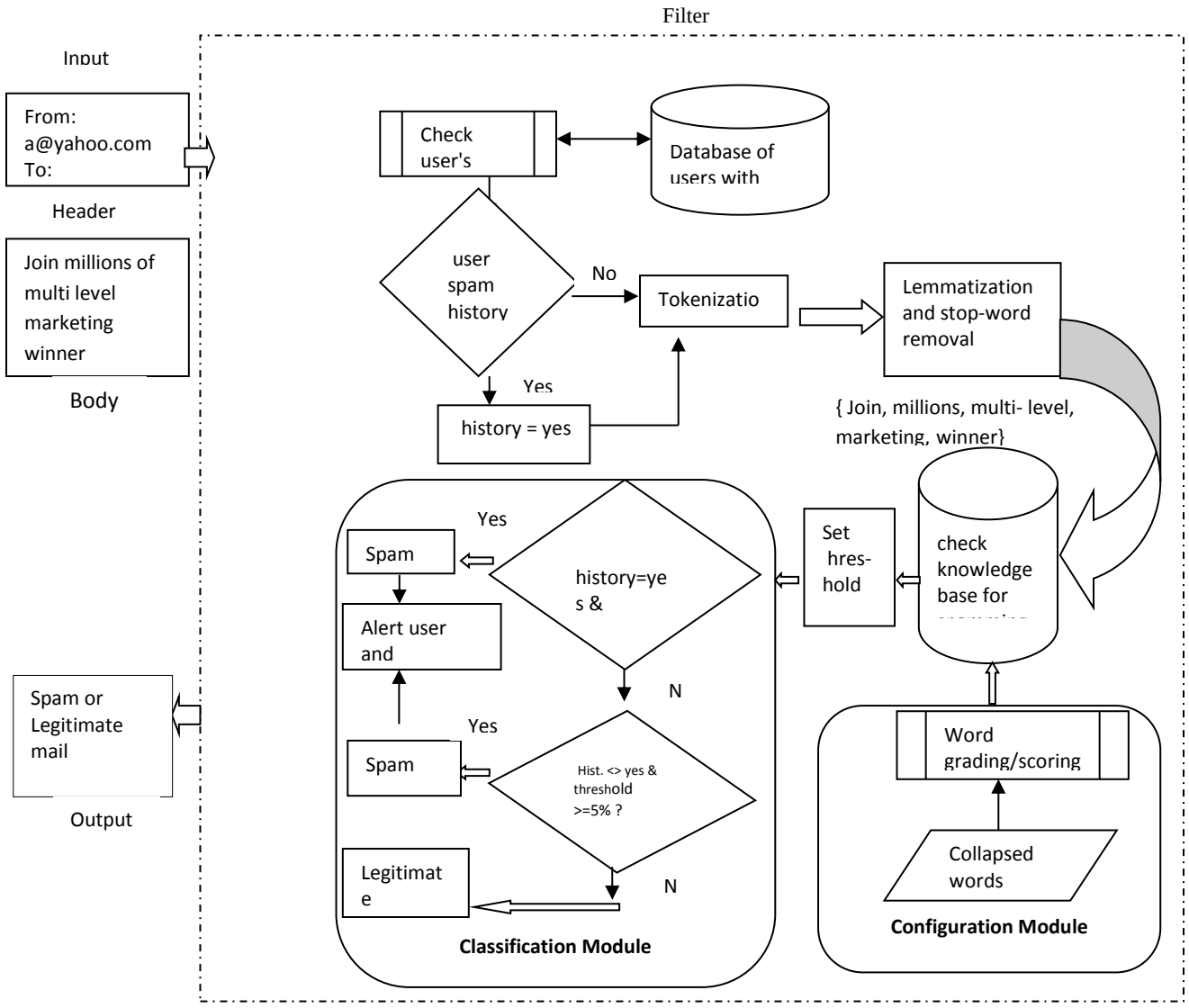

Figure 1: Structural Heuristic Approach Model for Spam Filtering

4. METHODOLOGY

4.1 Heuristic Approach

Heuristic filtering was developed in the late 1990s. This type of filtering uses a set of commonsense rules intended to identify specific characteristics of spam. These characteristics can include content or specific observations about particular constructions typical of spam. Unlike primitive filters, heuristic filters have rules to detect both spam and legitimate mail. Messages having somewhat spammy characteristics can quite possibly be delivered as legitimate mail if they also set off a number of alarms that the message is not spam[12].

Heuristic refers to the act or process of finding or discovering. In the computing context, it means proceeding to a solution by trial and error or by rules that are only loosely defined. The Merriam-Webster Dictionary as quoted in the work of [12] defines it as "*an aid to learning, discovery, or problem-solving by experimental and especially trial-and-error methods*" or in the context of computing "*relating to exploratory problem-solving techniques that utilize self-educating techniques as the evaluation of feedback to improve performance*" [4]. Heuristic programming is usually regarded as an application of artificial intelligence, and as a tool for problem solving. Heuristic programming, as used in expert systems, builds on rules drawn from experience, and the answers generated by such a system get better as the system learns by further experience, and augments its knowledge base [4].

However, this approach was employed in this research work for rule classification and spam filtering through the use of spammy characteristics extracted from different data sources.

4.2 Experimental Setup

This section of the research outlines and examines the proper experimentation that was carried out on the spammer's languages harvested from the two datasets. These languages were collapsed using Microsoft Office Excel and a total of 324 languages were recorded. A PivotTable feature of MS Excel was used to get the total number of unique languages as well as the number of duplicate languages in the two datasets. The result of the experiment gives 295 unique languages and a total of 29 duplicates as shown in table 1 below:

Table 1: Collapsed spammer's languages with rank

S/N	Spammers' Languages	Rank
1	% off!	1
2	4U	1
3	Accept credit cards	1
4	Act Now!	2
5	Additional income	1
6	Addresses on CD	1
7	All Natural	2
8	All New	1
9	Amazing	2
10	Apply Online	1
11	As Seen On	2
12	Auto email removal	1
13	Avoid Bankruptcy	2
14	Be amazed	1
15	Be your own boss	1
16	Being a member	1
17	Big bucks	1
18	Bill 1618	1
19	Billing address	1
20	Billion dollars	1
21	Brand new pager	1
22	Bulk email	1
23	Buy Direct	2
24	Buying judgments	1
25	Cable converter	1
26	Call free	1
27	Call now	2
28	Calling creditors	1
29	Can't live without	1
30	Cancel at any time	1
31	Cannot be combined with any other offer	1
32	Cash	1
33	Cash Bonus	2
34	Cashcashcash	1
35	Casino	2
36	Cell phone cancer scam	1
37	Cents on the dollar	1
38	Check or money order	1
39	Claims not to be selling anything	1
40	Claims to be in accordance with some spam law	1
41	Claims to be legal	1
42	Claims you are a winner	1
43	Claims you registered with some kind of partner	1
44	Click below	1
45	Click Here	1
46	Click here link	1
47	Click to remove	1
48	Click to remove mailto	1
49	Collect	1
50	Compare	1
51	Compare rates	1
52	Compete for your business	1
53	Confidentially on all orders	1
54	Congratulations	1
55	Consolidate debt and credit	1
56	Consolidate Your Debt	1
57	Copy accurately	1
58	Copy DVDs	1
59	Credit	1
60	Credit bureaus	1
61	Credit card offers	1
62	Cures baldness	1
63	Dear email	1
64	Dear friend	1
65	Dear somebody	1
66	Different reply to	1
67	Dig up dirt on friends	1
68	Direct email	1
69	Direct marketing	1
70	Discount!	1
71	Discusses search engine listings	1
72	Do it today	1
73	Don't delete	1
74	Don't hesitate!	1
75	Don't Delete	1
76	Double your income	1
77	Drastically reduced	1
78	Earn $	1
79	Earn per week	1
80	Easy Terms	2
81	Eliminate bad credit	1
82	Eliminate Debt	1
83	Email harvest	1
84	Email marketing	1
85	Expect to earn	1
86	Fantastic deal	1
87	Fast Viagra delivery	1
88	Financial freedom	1
89	Find out anything	1

90	For free	1
91	For instant access	1
92	For just $ (some amt)	1
93	Free access	1
94	Free cell phone	1
95	Free consultation	1
96	Free DVD	1
97	Free grant money	1
98	Free hosting	1
99	Free installation	1
100	Free investment	1
101	Free leads	1
102	Free membership	1
103	Free money	1
104	Free offer	1
105	Free preview	1
106	Free priority mail	1
107	Free quote	1
108	Free sample	1
109	Free trial	1
110	Free website	1
111	Free!	1
112	Full refund	1
113	get it now	1
114	Get Paid	2
115	Get started now	1
116	Gift certificate	1
117	Give it away	1
118	Giving it away	1
119	Great Offer	2
120	Guarantee	1
121	Guarantee or Guaranteed	1
122	Have you been turned down?	1
123	Hidden	1
124	Hidden assets	1
125	Home employment	1
126	Human growth hormone	1
127	If only it were that easy	1
128	In accordance with laws	1
129	Increase sales	1
130	Increase traffic	1
131	Information you requested	1
132	Insurance	1
133	Investment decision	1
134	It's effective	1
135	Join millions	1
136	Join millions of Americans	1
137	Laser printer	1
138	Limited time only	1
139	Loans	1
140	Long distance phone offer	1
141	Lose Weight	1
142	Lose weight spam	1
143	Lower interest rates	1
144	Lower monthly payment	1
145	Lowest price	1
146	Luxury car	1
147	Mail in order form	1
148	Marketing solutions	1
149	Mass email	1
150	Meet Singles	2
151	Member stuff	1
152	Message contains disclaimer	1
153	Million Dollars	1
154	MLM	1
155	Money back	1
156	Money making	1
157	Month trial offer	1
158	More Internet traffic	1
159	Mortgage rates	1
160	Multi level Marketing	2
161	Name brand	1
162	New customers only	1
163	New domain extensions	1
164	Nigerian	1
165	No age restrictions	1
166	No catch	1
167	No claim forms	1
168	No cost	2
169	No credit check	1
170	No disappointment	1
171	No experience	1
172	No fees	2
173	No gimmick	1
174	No inventory	1
175	No investment	1
176	No medical exams	1
177	No middleman	1
178	No obligation	1
179	No purchase necessary	1
180	No questions asked	1
181	No selling	1
182	No strings attached	1
183	Not intended	1
184	Off shore	1
185	Offer	1
186	Offer expires	1
187	Offers coupon	1
188	Offers extra cash	1
189	Offers free (often stolen) passwords	1
190	Once in lifetime	1
191	One hundred percent free	1
192	One hundred percent guaranteed	1
193	One time	1
194	One time mailing	1
195	Online biz opportunity	1
196	Online marketing	1
197	Online pharmacy	2
198	Only $	1
199	Opportunity	2
200	Opt in	1
201	Order Now	2
202	Order status	1
203	Orders shipped by priority mail	1
204	Outstanding values	1
205	Pennies a day	1

206	People just leave money laying around	1
207	Please Read	2
208	Potential earnings	1
209	Print form signature	1
210	Print out and fax	1
211	Produced and sent out	1
212	Profits	1
213	Promise You	1
214	Promise you …!	1
215	Pure profit	1
216	Real thing	1
217	Refinance home	1
218	Removal instructions	1
219	Remove in quotes	1
220	Remove subject	1
221	Removes	1
222	Removes wrinkles	1
223	Reply remove subject	1
224	Requires initial investment	1
225	Reserves the right	1
226	Reverses Aging	2
227	Risk free	1
228	Round the world	1
229	S 1618	1
230	Safeguard notice	1
231	Satisfaction Guaranteed	2
232	Save $	1
233	Save big money	1
234	Save up to	2
235	Score with babes	1
236	Search Engine Listing	1
237	Section 301	1
238	See for yourself	1
239	Sent in compliance	1
240	Serious Cash	2
241	Serious only	1
242	Shopping spree	1
243	Sign up free today	1
244	Social security number	1
245	Special Promotion	2
246	Stainless steel	1
247	Stock alert	1
248	Stock disclaimer statement	1
249	Stock pick	1
250	Stop or Stops	1
251	Stop snoring	1
252	Strong buy	1
253	Stuff on sale	1
254	Subject to credit	1
255	Subscribe	1
256	Supplies are limited	1
257	Take action now	1
258	Talks about hidden charges	1
259	Talks about prizes	1
260	Tells you it's an ad	1
261	Terms and conditions	1
262	The best rates	1
263	The following form	1
264	They keep your money — no refund!	1
265	They're just giving it away	1
266	This isn't junk	1
267	This isn't spam	1
268	Time limited	1
269	University diplomas	1
270	Unlimited	1
271	Unsecured credit/debt	1
272	Unsecured debt or credit	1
273	Urgent	1
274	US dollars	1
275	Vacation	1
276	Vacation offers	1
277	Viagra	1
278	Viagra and other drugs	1
279	Wants credit card	1
280	We hate spam	1
281	We honor all	1
282	Weekend getaway	1
283	What are you waiting for?	1
284	While supplies last	2
285	While you sleep	1
286	Who really wins?	1
287	Why pay more?	2
288	Will not believe your eyes	1
289	Winner	2
290	Winning	1
291	Work at home	2
292	You have been selected	1
293	Your income	1
294	You're a Winner!	1
295	You've been selected	1

From the table, after collapsing, those languages with the rank of 1 appear only once while those with the rank of 2 appear twice in the two datasets collapsed. This means that those with the rank of 2 are phrases with a very high tendency of being classified as spammer languages while those with the rank of 1 have low tendency of being suspicious.

4.2.1 Database Design Phase

In this experiment, we developed our database using MySQL and it contains three tables which are; history, message_log and rules tables. The 295 total collapsed languages from above were loaded into the rules table for use as shown in figure 2:

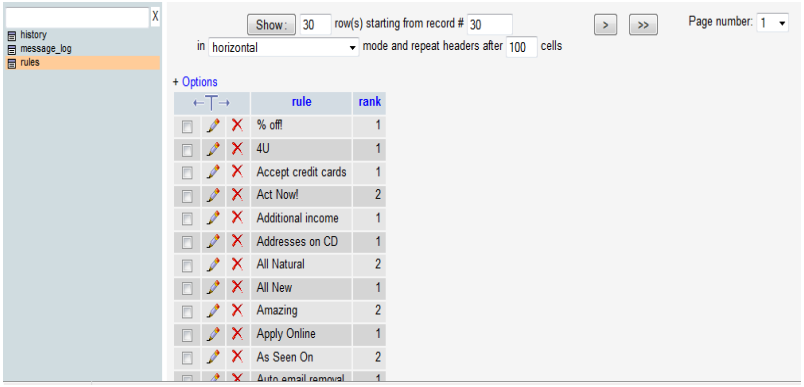

Figure 2: Collapsed languages in rules table

4.2.2 Interface Design

The proposed system will make use of a graphical user interface (GUI) for its implementation. The system was developed using Adobe Dreamweaver CS4, PHP, and MySQL. The prototype design for the interface screen is shown below.

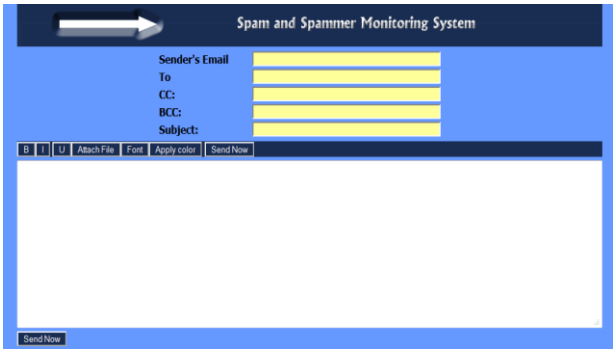

Figure 3: Application screen design

5. RESULTS AND DISCUSSION

The proposed system was tested using three e-mail messages in order to evaluate the performance of the system in classifying user's mail as either spam or legitimate. The threshold for the first time user was set to 5% while the threshold for users with previous spam record was set to 3%. The live running of the interface screens for the three tested e-mail messages are discussed below.

Figure 4 above shows a message being sent by a first time user of the proposed system. The sender's and receiver's email addresses are shola@yahoo.com and kolade_eniola@yahoo.com respectively. After composing the message, the sender attempts to send the mail to the receiver by clicking on "Send Now" button and the system calculates the threshold based on the contents of the mail and the user's history. Since the sender is a first time user with no spammy history, the system used 5% as the base threshold for classification. The contents of this mail resulted into a threshold of 9.49% and the system therefore, denies the user from sending the mail to the destination email through a message box shown in the figure. After the user discard the message, the system therefore, keeps the record of this attempt into the database.

Figure 5 shows a user with spammy history (shola@yahoo.com) attempting to send a message to the destination address (dele_jb@yahoo.com). After the user clicks on "Send Now" button, the system calculates the threshold of the mail contents as 4.07%. Since the sender has spammy history, a threshold of 3% was used by the system as the basis for classification without waiting for the threshold to reach 5% as in the case of a user without spammy history or first time user. The user's message was classified as being suspicious since a previous attempt of spamming is detected with the sender's email address. The figure also displayed message box that canceled the message from being sent to the destination. After the message is discarded, the profile of the sender is updated by the system for subsequent verification and auto-detection.

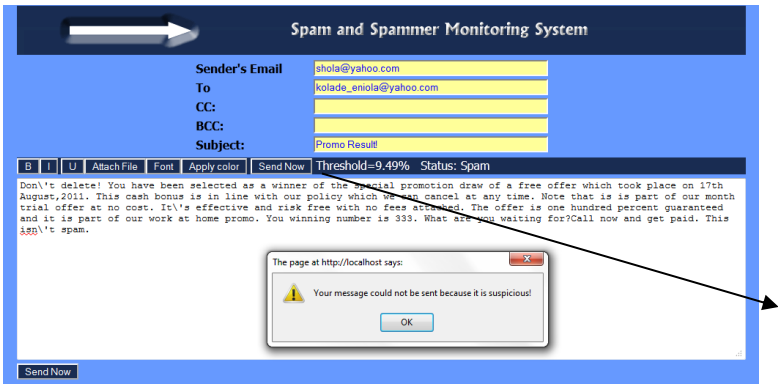

Figure 4: Spam message sent by first time user

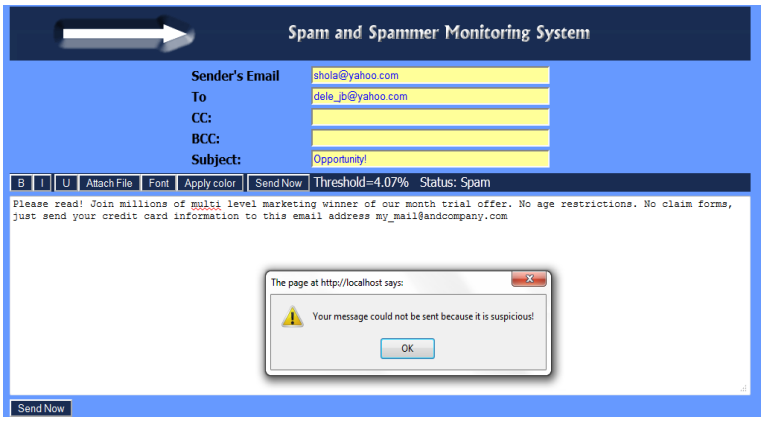

Figure 5: Spam message sent by user with spammy history

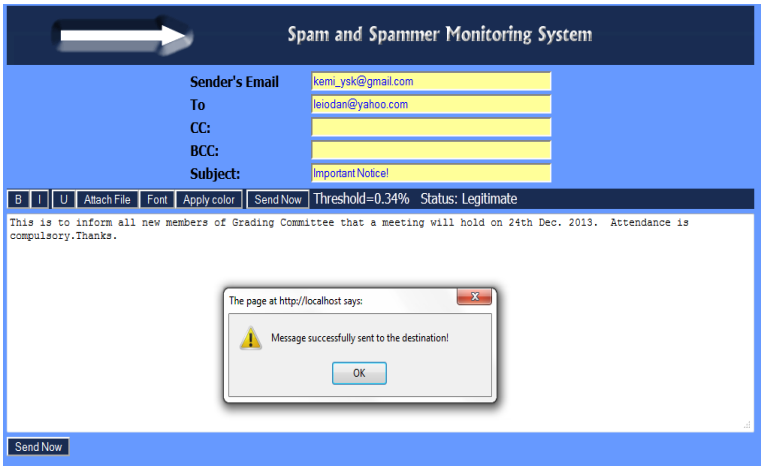

Figure 6: Legitimate message sent by a first time user

The message in figure 6 above was sent by a first time user and the system calculates the threshold as 0.34%. Since the user has no spammy history, a threshold of 5% was used by the system as the basis for classification. Based on the calculated threshold and the rules for classification, the user's message was classified as legitimate as shown in the figure. Thus, the message was sent successfully to the destination.

6. CONCLUSION AND RECOMMENDATIONS

In this paper, we presented a structural model for spam filtering which cannot be easily overcome by spammers. The technique employed heuristic approach for spam

filtering. The model was simulated and tested with different email messages for performance evaluation. A comprehensive review of recent machine learning approaches to spam filtering was also presented. The model is recommended to be incorporated in the architecture of the Internet Service Providers as well as email service providers for spam filtering. The dataset that will be generated by this system can also be used by researchers and law enforcement agencies for decision making.

REFERENCES

[1] Ahmed, S., and Mithun, F. (2004). Word Stemming to Enhance Spam Filtering. *Proceedings of the First Conference on Email and Anti-Spam (CEAS).* Retrieved July 15th, 2012 from http://www.ceas.cc/papers2004/167.pdf

[2] Almeida, T., Almeida, J., and Yamakami, A. (2011). Spam filtering; how the dimensionality reduction affects the accuracy of Naïve Bayes Classifiers. *Journal of Internet Services and applications*, Springer London.

[3] Awad , W. A. and Elseuofi S. M. (2011). Machine Learning Methods for Spam e-mail Classification. *International Journal of Computer Science and Information Technology*. Vol. 3. No. 1, pp 173-184.

[4] Bidgoli, H. et al. (2006). Handbook of Information Security. "Email threats and vulnerabilities". Wiley. ISBN 0-471-64833-7, vol. 3.

[5] Brinker, K. (2003). Incorporating Diversity in Active learning with support vector machine. In the Twentieth ICML (2003) Washington DC.USA pp. 59-66.

[6] Clark, J., Koprinska, I. and Poon, J. (2003). A Neural Network Based Approach to Automated Email Classification. *IEEE International Conference on Web Intelligence*, pp. 702-705.

[7] Dickinson, D. (2004). An Architecture for Spam regulation. *Federal Communications Law Journal*, vol. 57.No. 1.

[8] Druker, H. Wu, D., and Vapnik, V. N. (1999). Support Vector Machines for Spam Categorization. *IEEE Transactions on Neural networks.* 10(5), pp. 1048-1054.

[9] Ferris Research (2009). Spam, Spammers and Spam control A white paper. Retrieved July 15th, 2012 from http://apac.trendmicro.com/imperia/md/content/us/pdf/products/enterprise/interscanmessagingsecuritysuite/wp01_antispamferris_090311us.pdf

[10] Freschi , V., Seraghiti , A. and Bogliolo, A. (2005). Filtering Obfuscated Email Spam by means of Phonetic String Matching. Retrieved July 17th, 2012 from http://www.sti.uniurb.it/seraghiti/publications/ECIR06.pdf

[11] Graham, P. (2002). Better Bayesian Filtering. Retrieved June 15th, 2012 from http://www.paulgraham.com.

[12] Harley, D., Slade, R. and Gattiker, U. (2001). Viruses Revealed. Retrieved June 20th, 2012 from http://go.eset.com/us/resources/white-papers

[13] Lobato, D.H. and Lobato, J.M. (2008). Bayes Machines for Binary Classification Pattern Recognition Letters. Elsevier 29; pp. 1466-1473.

[14] Muhammad, N., Marsono, M., Watheq, E. and Fayez, G. (2009). Targeting spam control on middle boxes; Spam detection based on layer-3 email content classification. *Elsevier computer networks*.

[15] Owen, K. and Richard, G. (2012). Spam Detection using Artificial Neural Networks (perceptron Learning Rule), *Online Journal of Physical and Environmental Science Research*, ISSN 2315-5027, 1(2), pp. 22-29.

[16] Rafiqul, I. and Morshed, U. C. (2005). Spam Filtering Using Machine Learning Algorithms. *IADIS International Conference on www/internet*. ISBN: 972-8924-02, pp 419-426.

[17] Sahami, M., Dumais, S., Heckerman, D., and Horvitz, E. (1998). A Bayesian Approach to Filtering Junk E-mail. In Learning for Text Categorization Papers from the AAAI Workshop, pp. 55-62. Retrieved July, 2nd, 2012 from http://ftp.research.microsoft.com/pub/ejh/junkfilter.pdf

[18] Sebastiani F. (2002). Machine learning in automated text categorization. *ACM computing Surveys*, vol. 34. No 1, pp. 1-47.

[19] Thamarai, S., Hamid, A. J. and Alaa, Y. T. (2010). Overview of textual anti-spam filtering techniques. *International Journal of the Physical Science*, vol. 5(12), pp. 1869-1882.

[20] Wang, Q., Guan, Y. and Wang, X. (2006): SVM-based spam filter with active and online learning. The Fifteenth Text Retrieval Conference (TREC 2006)

Proceedings. Retrieved July 17th, 2012 from http://www.trec.nist.gov/pubs/trec15/paper/hit.spam.final.final.pdf.

[21] Weiss, A. (2003). Ending Spam's free ride network. Retrieved July 12th, 2012 from http://www.my.safaribooksonline.com/books/

[22] Wosotowsky, A. and Winkler, E. (2009). Spam Report McAfee. Discovers and Discusses Key spam Trends. Retrieved July 17th, 2012 from http://www.mcafee.com/us/local_content/reports/7736rpt_spam_1209.pdf

[23] Wu, C. (2009). Behaviour-based spam detection using a hybrid method of rule-base technique and neural networks. Retrieved July 15th, 2012 from http://dl.acm.org/citation.cfm?id=149753.1498392.

[24] Zhang J. et al. (2003). Modified Logistic Regression. An approximation to SVM and its applications in large-scale text categorization. *Proceedings of the 20th international conference on machine learning*. AAAI press, pp. 888-895.

