ISSN:0975-9646

Anti-Spam Methodologies: A Comparative Study

Saima Hasib, Mahak Motwani, Amit Saxena
Truba Institute of Engineering and Information Technology
Bhopal (M.P),India

***Abstract*: E-mail is an essential communication tool that has been greatly abused by spam sender to disseminate unwanted information (messages) and spread malicious contents to Internet users. Current Internet technologies accelerated the distribution of spam. Effective controls need to be deployed to countermeasure the ever growing spam problem. Spam filters provide better protective mechanisms that are able to control spam. This paper summarizes most common techniques used for anti-spam filtering by analyzing the e-mail content and also looks into IP's adopted to detect and control spam. Each filter has its own strengths and limitations. Depending upon the scenarios different kind of filters is effective on their suitable scenarios.**

Key words: spam filters, Blacklist, Real-Time Blackhole List, Whitelist, Greylist, Word-Based Filters, Heuristic Filters, Bayesian Filters.

I. INTRODUCTION

Spam is anonymous, unsolicited bulk email from the recipients' point of view, it is unwanted detritus that chokes up their inboxes. Spam has become a part of our everyday lives. It is indicative of what is happening to the global economy. When looked at as a whole it is clear that the themes and development trends of spam closely correlate to the global financial situation. More than 70% of global e-mail traffic consists of spam. Dealing with spam incurs high costs for organizations, prompting efforts to try to reduce spam-related costs by installing spam filters. This is called as spam filter mechanism. The individual efficiency of a spam filter installation depends on the amount of spam that is received and on the level of knowledge about spam.[1,2,3]

Spam filters are mainly categorized as list based and content based spam filters. List-based filters attempt to stop spam by categorizing senders as spammers or trusted users, and blocking or allowing their messages accordingly. The various types of filters in this category are Blacklist filters, Real time Blackhole list and Whitelist filters. Content Based Filters Rather than enforcing across-the-board policies for all messages from a particular email or IP address, content-based filters evaluate words or phrases found in each individual message to determine whether an email is spam or legitimate.

A. Why spam is a problem?

There are many reasons unsolicited commercial e-mail is such a problem:

Cost shifting: Sending bulk e-mail is amazingly cheap with help of a modem, internet connection and computer. Spammers can send hundreds or thousands of messages per hour, and though that relatively minuscule cost of entry into the market is a potential advertiser's dream. It quickly becomes a nightmare for those who pay the costs of receiving it. The costs can range from the long-distance charges or per-minute access charges for dialling into an Internet service provider (ISP) to the cost of connectivity and disk storage space at the ISP and the inevitable administrative costs when the incoming flood outstrips capacity, resulting in system outages. These costs can be quite substantial. Here cost of opportunities is possible lost because of system outages, delayed services, and overflowing mailboxes.[4]

Fraud: In survey after survey, the overwhelming majority of Internet users dislike receiving spam. In response to such strong consumer opinion, many ISPs have taken a variety of costly steps to reduce the volume of spam transmitted through their systems, including the build-up of extra capacity to accommodate the demands of filtering and storing, Knowing that ISPs have taken those measures, senders of junk e-mail use tricks to disguise the origin of their messages. One of the most common is to relay their messages off the mail server of a third party. This tactic doubles the damages, because now both the receiving system and the innocent relay system are flooded with junk e-mail. For mail that gets through, many times the flood of complaints goes back to the innocent site because that site was made to look like the origin of the spam. Another common trick is to forge the headers of messages, making it appear as though the message originated elsewhere and again providing a convenient target upon which the anger of recipients and the flood of complaints will land.[4]

***Theft*:** The sending of spam results in one party's imposing costs on another, against the party's will and without permission. Some have called unsolicited e-mail a form of postage-due marketing. Others, quite correctly, call it a form of theft. Although some defend unsolicited commercial e-mail as just another form of free speech, those who bear the costs of someone else's speech are left to ask what part is "free."[4]

***Harm to the marketplace*:** When a spammer sends an e-mail message to a million people, it is carried by numerous other systems en route to its destinations, once again shifting cost away from the originator. The carriers in between suddenly are bearing the burden of carrying advertisements for the spammer. The number of unsolicited messages sent out each day is truly remarkable.[4]

***Consumer perception*:** E-mail is increasingly becoming a critical business tool. Yet despite the best efforts of service providers, for many people the accessing of e-mail still represents a bit of a struggle. Many of the major online services remain difficult to access at peak traffic times, and network congestion can make it an arduous task to simply download your e-mail.[4]

***Global implications*:** Like the fax machine before it, electronic mail is a marvellous tool of business and personal communication. It's simple, it's accessible, and it's becoming more and more an indispensable part of our professional lives, But there are even more far-reaching

potentials of e-mail that may be lost if the medium's functionality and utility get destroyed by the proliferation of junk e-mail. The Internet is an incredible tool for spreading information critical to the development of freedom and democracy around the world. [4]

Ultimately, the problems caused by spam on the Internet--and the solutions applied--will fundamentally shape the ways individuals and businesses use the medium. A myriad of technological, legislative, regulatory, and societal measures have been suggested for curbing the damage caused. However, no matter what solution or combination of solutions is proved to be most effective, a solution must be found because no less than the future of the Internet may be at stake.

II. List-Based Filters

A. Blacklist: This popular spam-filtering method attempts to stop unwanted email by blocking messages from a preset list of senders that you or your organization's system administrator creates. Blacklists are records of email addresses or Internet Protocol (IP) addresses that have been previously used to send spam. When an incoming message arrives, the spam filter checks to see if its IP or email address is on the blacklist; if so, the message is considered spam and rejected. Though blacklists ensure that known spammers cannot reach users' inboxes, they can also misidentify legitimate senders as spammers. These so-called false positives can result if a spammer happens to be sending junk mail from an IP address that is also used by legitimate email users. Also, since many clever spammers routinely switch IP addresses and email addresses to cover their tracks, a blacklist may not immediately catch the newest outbreaks.[5]

B. Real-Time Blackhole List: This spam-filtering method works almost identically to a traditional blacklist but requires less hands-on maintenance. That's because most real-time blackhole lists are maintained by third parties, who take the time to build comprehensive blacklists on the behalf of their subscribers. Your filter simply has to connect to the third-party system each time an email comes in, to compare the sender's IP address against the list. Since blackhole lists are large and frequently maintained, your organization's IT staff won't have to spend time manually adding new IP addresses to the list, increasing the chances that the filter will catch the newest junk-mail outbreaks. But like blacklists, real-time blackhole lists can also generate false positives if spammers happen to use a legitimate IP address as a conduit for junk mail. Also, since the list is likely to be maintained by a third party, you have less control over what addresses are on — or not on — the list.[6]

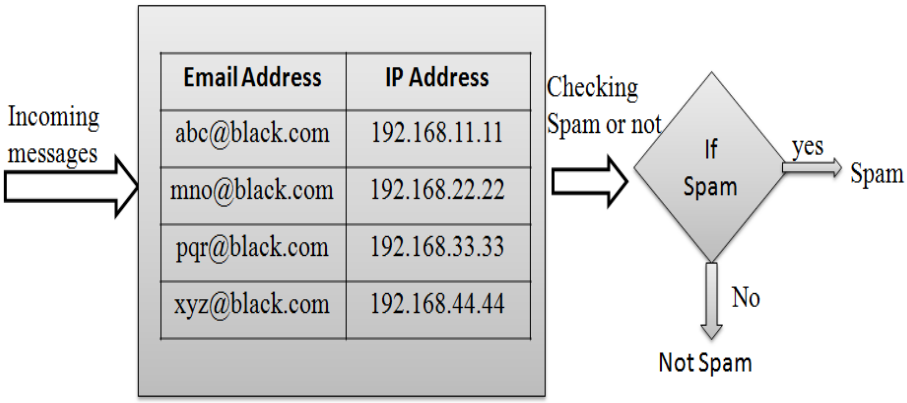

Figure 1: Blacklist Spam Filter

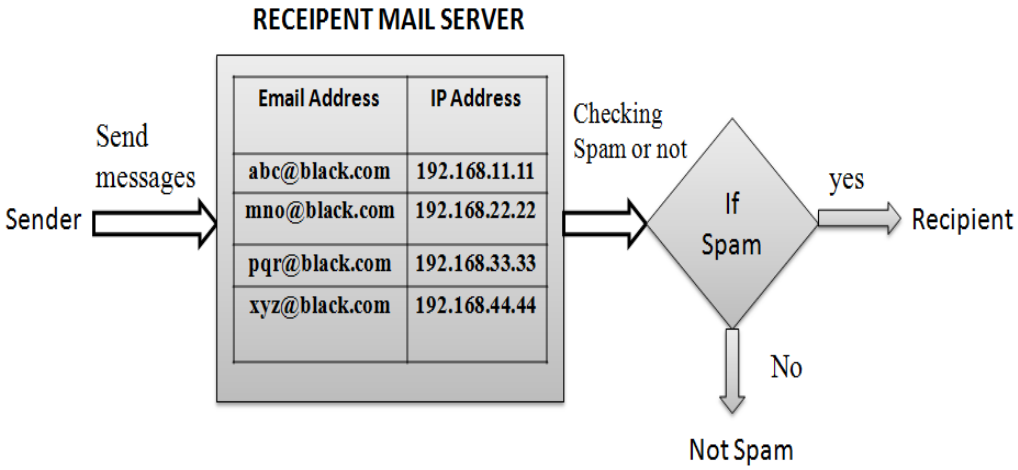

Figure 2: Real Time Blackhole Based Spam Filter

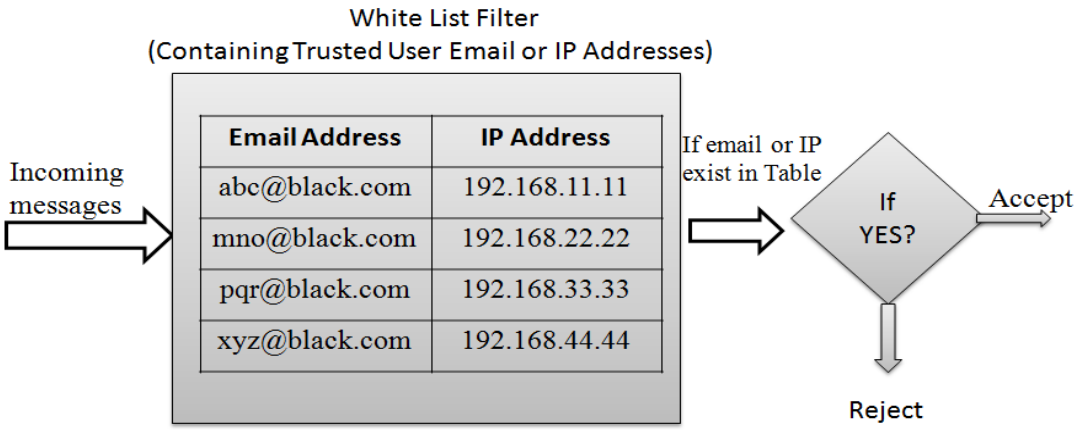

Figure 3: White List Filter

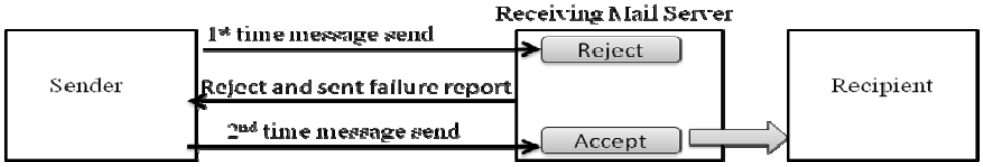

Figure 4: Grey List Filter

C. Whitelist: A whitelist blocks spam using a system almost exactly opposite to that of a blacklist. Rather than letting you specify which senders to block mail from, a whitelist lets you specify which senders to allow mail from; these addresses are placed on a trusted-users list. Most spam filters let you use a whitelist in addition to another spam-fighting feature as a way to cut down on the number of legitimate messages that accidentally get flagged as spam. However, using a very strict filter that only uses a whitelist would mean that anyone who was not approved would automatically be blocked. Some anti-spam applications use a variation of this system known as an automatic whitelist. In this system, an unknown sender's email address is checked against a database; if they have no history of spamming, their message is sent to the recipient's inbox and they are added to the whitelist.[5]

D. Greylist: A relatively new spam-filtering technique, greylists take advantage of the fact that many spammers only attempt to send a batch of junk mail once. Under the greylist system, the receiving mail server initially rejects messages from unknown users and sends a failure message to the originating server. If the mail server attempts to send the message a second time — a step most legitimate servers will take — the greylist assumes the message is not spam and lets it proceed to the recipient's inbox. At this point, the greylist filter will add the recipient's email or IP address to a list of allowed senders. Though greylist filters require fewer system resources than some other types of spam filters, they also may delay mail delivery, which could be inconvenient when you are expecting time-sensitive messages.[5]

III. Content-Based Filters

A. Word-Based Filters: A word-based spam filter is the simplest type of content-based filter. Generally speaking, word-based filters simply block any email that contains certain terms. Since many spam messages contain terms not often found in personal or business communications, word filters can be a simple yet capable technique for fighting junk email. However, if configured to block messages containing more common words, these types of filters may generate false positives.

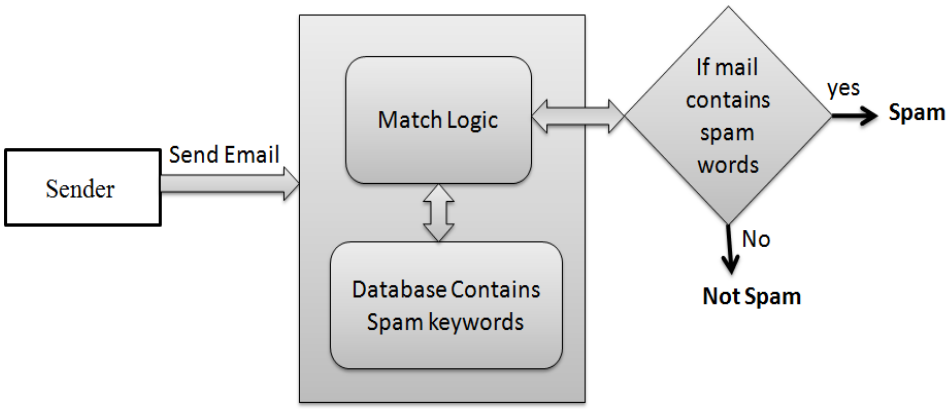

Figure 5: Word Based Spam Filter

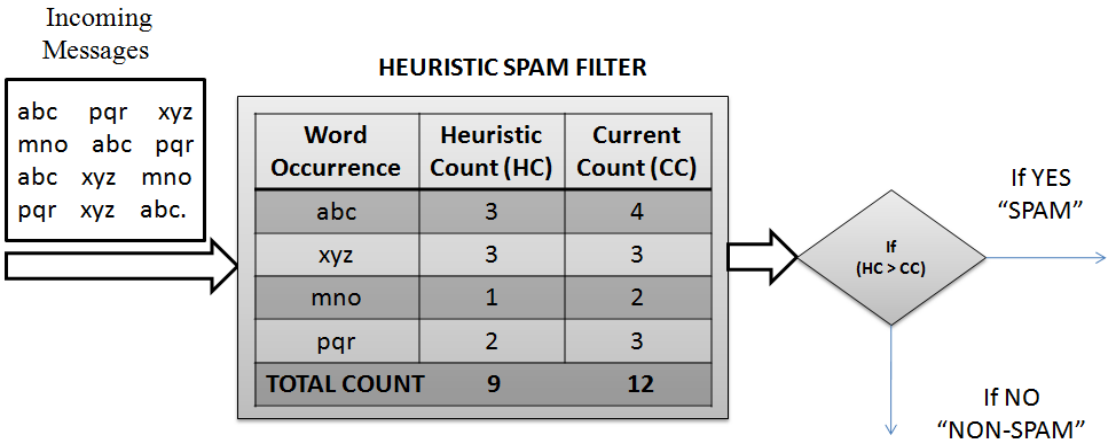

Figure 6: Heuristic Filter

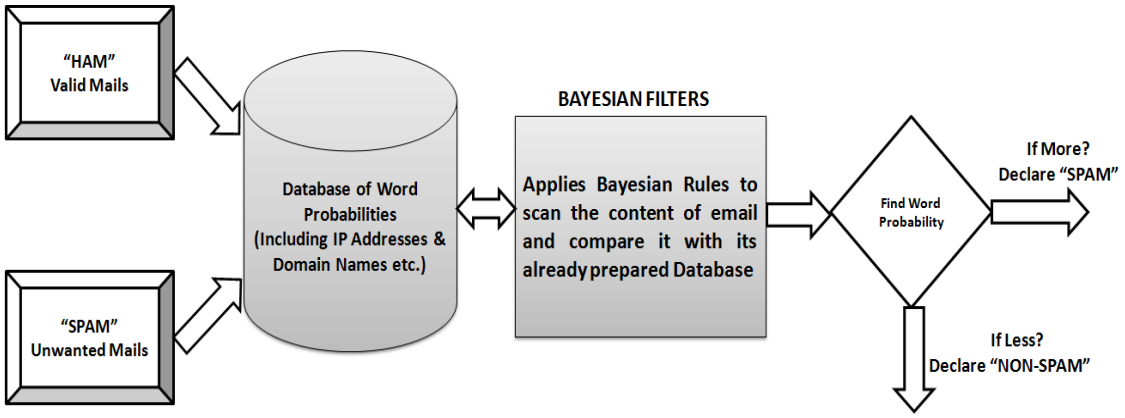

Figure 7: Bayesian Filter

For instance, if the filter has been set to stop all messages containing the word "discount," emails from legitimate senders offering your non-profit hardware or software at a reduced price may not reach their destination. Also note that since spammers often purposefully misspell keywords in order to evade word-based filters, your IT staff will need to make time to routinely update the filter's list of blocked words.[5]

B. Heuristic Filters: Heuristic (or rule-based) filters take things a step beyond simple word-based filters. Rather than blocking messages that contain a suspicious word, heuristic filters take multiple terms found in an email into consideration.[5,6]Heuristic filters scan the contents of incoming emails and assigning points to words or phrases. Suspicious words that are commonly found in spam messages, such as "Rolex" or "Viagra," receive higher points, while terms frequently found in normal emails receive lower scores. The filter then adds up all the points and calculates a total score. If the message receives a certain score or higher (determined by the anti-spam application's administrator), the filter identifies it as spam and blocks it. Messages that score lower than the target number are delivered to the user. Heuristic filters work fast — minimizing email delay — and are quite effective as soon as they have been installed and configured. However, heuristic filters configured to be aggressive may generate false positives if a legitimate contact happens to send an email containing a certain combination of words. Similarly, some savvy spammers might learn which words to avoid including, thereby fooling the heuristic filter into believing they are benign senders.[7]

C. Bayesian Filters: Bayesian filters, considered the most advanced form of content-based filtering, employ the laws of mathematical probability to determine which messages are legitimate and which are spam. In order for a Bayesian filter to effectively block spam, the end user must initially "train" it by manually flagging each message as either junk or legitimate. Over time, the filter takes words and phrases found in legitimate emails and adds them to a list; it does the same with terms found in spam.

To determine which incoming messages are classified as spam, the Bayesian filter scans the contents of the email and then compares the text against its two-word lists to calculate the probability that the message is spam. For instance, if the word "valium" has appeared 62 times in spam messages list but only three times in legitimate emails, there is a 95 percent chance that an incoming email containing the word "valium" is junk.

Because a Bayesian filter is constantly building its word list based on the messages that an individual user receives, it theoretically becomes more effective the longer it's used. However, since this method does require a training period before it starts working well, you will need to exercise patience and will probably have to manually delete a few junk messages, at least at first.[7,8]

IV. COMPARATIVE STUDY

Table-I: Filter Suitable Condition and Disadvantage

S.No	Spam Filter	Suitable Condition	Disadvantage
1	Blacklist Filter	If spam suspected IP addresses are fixed or known.	Suspected IP detection is difficult and contains errors.
2	Real-Time Blackhole List Filter	If spam suspected IP addresses are fixed or known and third party is reliable.	Suspected IP detection is difficult and contains errors.
3	Whitelist Filter	If trusted IP addresses are fixed.	Unknown genuine mail may declare as spam
4	Greylist Filter	If trusted sender always sends message two times.	If trusted sender not send message two times mail will lost.
5	Word-Based Filter	Suspected keywords are known.	Genuine mail may contain suspected keywords.
6	Heuristic Filter	Suspected keywords are known and best heuristic function is available.	Genuine mail may contain suspected keywords.
7	Bayesian Filter	Suspected keywords are known with their spam probability.	Genuine mail may contain suspected keywords.

V. CONCLUSION

Spam is one of the most annoying and malicious additions to global computer world. Normally spam filter software is not able to cope with vast volumes of spam. As spam problems escalate, effective and efficient spam filters are required to control them. There are various different spam filters are available which are effectively work on their suitable scenarios. Some of list base filters and some of content based filters. Content based filters are more effective than list based filters. Based on this research, Bayesian filter is the most effective content based filter. The effectiveness of a Bayesian spam filter can be increased with pre-processing steps that are applied to the spam keywords training.

REFERENCES

[1]. Wu, C. T., Cheng, K. T., Zhu, Q., Wu, Y. L., "Using Visual Features For Anti-Spam Filtering, " 2005 IEEE International Conference on Image Processing (ICIP2005), pp. 509–512, 2005.

[2]. postini : Email Monitoring + Email Filtering Blog. http://www.dicontas.co.uk/blog/quick-facts/emailspam-traffic-rockets/65/.

[3].Toshihiro Tabata, "SPAM mail filtering : commentary of Bayesian filter, " The journal of Information Science and Technology Association, Vol.56, No.10, pp.464-468, 2006.

[4]. Surf-Control's Anti-Spam Prevalence Study 2002, URL:http://www.surfcontrol.com/resources/Anti-Spam_Study_v2.pdf.

[5].http://www.cs.nmt.edu/~janbob/SPAM,Spam corpus, SMS corpus,

[6].http://www.comp.nus.edu.sg/~rpnlpir/downloads/corpora/smsCorpus/

[7].Amayri O, Bouguil N (2009). Online Spam Filtering Using Support Vector Machines. IEEE., pp. 337- 340.

[8].C. Pu, S. Webb, O. Kolesnikov, W. Lee, and R. Lipton. Towards the Integration of Diverse Spam Filtering Techniques. In Proc. of IEEE International Conference on Granular Computing, pages 7 – 10, 2006.