Spam Mail Detector

Farhana Sultana Smrity
Your ID: 2013–2–60–046

Maria Yasmin Nila
Your ID: 2013–2–60–047

Jannatul Ferdous
Your ID: 2013–3–60–001

Course Name: Artificial Intelligence
Course Code: CSE365, Section: 1
Course Instructor: Amit Kumar Das
Lecturer, Department of CSE, East West University

Department of Computer Science and Engineering
East West University
Dhaka-1212, Bangladesh

Spring, 2017

Abstract

"Email is one of the crucial aspects of web data communication. The increasing use of email has led to a lucrative business opportunity called spamming. A spam is an unwanted data that a web user receives in the form of email or messages. This spamming is actually done by sending unsolicited bulk messages to indiscriminate set of recipients for advertising purpose. These spams messages not only increase the network communication and memory space but can also be used for some attack. This attack can be used to destroy user's information or reveal his identity or data. In this paper, we discuss some approaches for spam detection."

Table of Contents

Chapter 1

Introduction

In recent years, internet has become an integral part of our life. With increased use of internet, numbers of email users are increasing day by day. It is estimated that 294 billion emails are sent every day. This increasing use of email has created problems caused by unsolicited bulk email messages commonly referred to as Spam [1]. It is assumed that around 90 percentage of emails sent everyday are spam or viruses.

1.1 spam filter

A spam filter is a program that is used to detect unsolicited and unwanted email and prevent those messages from getting to a user's inbox. Like other types of filtering programs, 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) can be 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.

1.1.1 Email spam

Email spam, also known as junk email, is a type of electronic spam where unsolicited messages are sent by email. Many email spam messages are commercial in nature but

may also contain disguised links that appear to be for familiar websites but in fact lead to phishing web sites or sites that are hosting malware. Spam email may also include malware as scripts or other executable file attachments. Spam is named after Spam luncheon meat by way of a Monty Python sketch in which Spam in the sketch is ubiquitous, unavoidable and repetitive. Email spam has steadily grown since the early 1990s. Botnets, networks of virus-infected computers, are used to send about 80 percentage of spam Since the expense of the spam is borne mostly by the recipient, it is effectively due advertising. The legal status of spam varies from one jurisdiction to another. In the United States, spam was declared to be legal by the CAN provided the message adheres to rules set by the Act and by the FTC. ISPs have attempted to recover the cost of spam through lawsuits against spammers, although they have been mostly unsuccessful in collecting damages despite winning in court. Spammers collect email addresses from chatrooms, websites, customer lists, newsgroups, and viruses that harvest users' address books. These collected email addresses are sometimes also sold to other spammers. The proportion of spam email was around 80 percentage of email messages sent, in the first half of 2010.

Chapter 2

Related Work

Related work discussed in connection with the present study is divided into categories. This study deals with the detection of the fraudulent emails, which are known as a kind of illicit emails, therefore, the related work is presented for various illicit emails detection including spam emails detection, suspicious emails detection and phishing emails detection. Also another dimension of research regarding illicit emails is considered to be the authorship identification of anonymous emails. We also present some overview of the literature for email authorship identification.

Chapter 3

Proposed Project

Spam emails are the illicit emails that a receiver is not interested in. The spam emails are unsolicited emails which are often sent in bulk. Spam emails are usually sent with different intentions, but advertisement and fraud are considered to be the major reasons. Spam email detection is often considered to be the classification task. It is believed that there is no such technique which can provide complete solution against spam. Youn and McLeod presented a comparative study of various classification methods for spam emails detection. In the comparative study, the authors used Naive Bayes, SVM, J48, and neural networks classification techniques. The authors concluded that J48 classification is a suitable technique for the spam email detection task, because of the reasons the technique produced promising results. In another study, Youn and McLeod presented an ontology based spam filtering method. The authors used J48 algorithm in order to formulate rules to generate concepts of the ontology. The study by Renuka and Hamsapriya adapted the use of word stemming instead of simply content based words for spam email detection. The authors showed that stemming based method is more efficient as compared to content based methods. It should be noted that Youn and McLeod accentuated on the use of stemming based method, because the authors argued that the spammers use misspellings in order to deceive keyword based spam detection filters. The most famous spam email detection filter "Spambayes" used by Microsoft outlook as a plug-in uses Baye's theorem and uses keyword based approach for spam email detection.

3.1 Suspicious email detection

Suspicious emails are another category of illicit emails. Suspicious emails are those which contain some material which is doubtful. For instance, an email may contain some text regarding some illicit activity; a threatening email; or it may contain certain material which is worth analysis. Suspicious emails are deemed to be those which contain some clue regarding some illicit activities, which need to be further investigated by law enforcement agencies. There are some evidences regarding the exchange of suspicious emails before the events of 9/11 took place. In the literature, the researchers also have contributed to this sensitive problem of suspicious email detection. The study by Nizamani et al. presented the suspicious email detection model based on enhanced feature selection. The authors employed the use of "indicators" features in addition to the keywords for suspicious email detection. Further, the authors emphasized on the use of the feature selection, in order to detect suspicious emails. A study by Appavu et al. applied the association rule mining for suspicious email detection task. In the article, the authors added a specialized class of suspicious emails as an alert or the information using verb. An email is considered suspicious if in addition to keywords it contains future tenses to consider it as an alarm for future suspicious activity. It should be noted that in the articles , the suspicious emails considered are the terrorism related emails which give some clue regarding future terrorist acts[2].

3.1.1 Phishing email detection

Phishing emails are specialized class of illegitimate emails, which are intended to obtain useful information from the receiver of email. Phishing problem is believed to be a security and privacy concern. Phishing problem is considered to be the hard problem, due to the fact that an attacker can easily make the replicated website which may resemble to the legal bank of a user. Phishing emails are the emails which are planned to acquire crucial

information from the receiver. The crucial information includes username, password, credit card details, bank account information, etc. These emails resemble to the emails from trustworthy websites. The emails contain such a text that the receivers immediately turn to respond the email by clicking on the links provided in the email or send the crucial information in reply. Chandrasekaran et al., in their study consider phishing email detection as a classification problem and used style maker and structural features and applied SVM classification methods in order to detect phishing emails.

3.1.2 Email authorship identification

Email authorship identification is considered to be the task of identifying the most probable author of an email by analyzing the past emails of the suspected authors Li et al. emphasized on the importance of writeprints in order to prevent cybercrimes. Authors argued that writeprints are as important as fingerprints are for identifying the criminals in real life. The authors presented a write-print based model for mining frequent patterns in the emails in order uniquely identify the authors of emails. Nizamani and Memon presented the model CEAI, which is CCM-based email authorship identification model. In the study, the authors employed traditional stylometric features along with their extended feature set and achieved promising results.

3.1.3 Detection of the fraudulent emails

The aim of the research is to separate fraudulent emails from the normal ones, with the intention that the receiver may not get affected from the fraudulent email in due course. The fraudulent emails often contain certain words, that, the receiver performs specific actions instantly which are harmful and result in frauds.

It should be noted that in this paper, we consider detection of the fraudulent email as a classification problem. For any classification problem one needs a feature set and a classification algorithm. We have raw emails as input and in training each email is

assigned a label/class fraud or normal.

Chapter 4

Conclusion

Spam emails are the biggest problem for the web data. This paper explored different approaches to deal with this problem. From all of these approaches no one can provide 100high false positive rates and false negative rates. There is very much scope for identifying mail as spam emails or legitimate mails for text as well as multimedia messages[3].

Bibliography

[1] C. J. Hawthorn, K. P. Weber, and R. E. Scholten, "Littrow configuration tunable external cavity diode laser with fixed direction output beam," *Review of Scientific Instruments*, vol. 72, no. 12, pp. 4477–4479, December 2001. [Online]. Available: http://link.aip.org/link/?RSI/72/4477/1

[2] C. E. Wieman and L. Hollberg, "Using diode lasers for atomic physics," *Review of Scientific Instruments*, vol. 62, no. 1, pp. 1–20, January 1991. [Online]. Available: http://link.aip.org/link/?RSI/62/1/1

[3] A. S. Arnold, J. S. Wilson, and M. G. Boshier, "A simple extended-cavity diode laser," *Review of Scientific Instruments*, vol. 69, no. 3, pp. 1236–1239, March 1998. [Online]. Available: http://link.aip.org/link/?RSI/69/1236/1