Chapter 11
Detection and Prediction of Spam Emails Using Machine Learning Models

Salma P. Z
NSS College of Engineering, Kerala, India

Maya Mohan
NSS College of Engineering, Kerala, India

ABSTRACT

One of today's important means of communication is email. The extensive use of email for communication has led to many problems. Spam emails being the most crucial among them. It is one the major issues in today's internet world. Spam emails contain mostly advertisements and offensive content, which are often sent without the recipient's request and are generally annoying, time consuming, and wasting space on the communication media's resources. It creates inconveniences and financial loss to the recipients. Hence, there is always the need to filter the spam emails and separate them from the legitimate emails. There are a lot of content-based machine learning techniques that have proven to be effective in detecting and filtering spam emails. Due to a large increase in email spamming, the emails are studied and classified as spam or not spam. In this chapter, three machine learning models, Recurrent Neural Network (RNN), Long Short-Term Memory (LSTM), and Bidirectional LSTM (BLSTM), are used classify the emails as spam and benign.

INTRODUCTION

Electronic mail or email is one of today's most prominent and fastest methods of exchanging messages between people using digital devices over the internet. Email is one of the easiest and most common means of communication in our time. One of the major communication platforms in today's age is the internet and hence emails are considered to be the fastest and essential way of communication means. Email communication contributes to the major part of conversations in almost all domains. It is one

DOI: 10.4018/978-1-7998-5728-0.ch011

of the most effective and commonly used sources of communication. The cost-effective and speed in communication made email communication popular among the users.

Spam emails, often known as junk email, is the unrequested messages which are sent in bulk through email communication. These unwanted emails are generally annoying and time-consuming and wasting space on the communication media's resources. Spam emails result in many issues such as reduced performance of the email engines, occupation of unnecessary space in the mailbox, and destroying the stability of mail servers. In certain cases, it also contains viruses, trojans, and other materials that may be potentially harmful to certain categories of users (Shrivastava and Anju, 2017). There have been several studies on spam emails and it shows a steady growth of spam emails by 90% from the early 1990s till 2014. Issues related to spam mail has also been growing exponentially over time. Users receive hundreds of spam emails with new content and new sources and these spams are generated by spammers using automatic robot software. The organizations face an influence financially due to the proliferation of spam emails. Spam emails not only invade the user's email but also produces a huge volume of unwanted data thus limiting the network's usage and capacity. Email spamming is also the first step in targeted attacks in organizations, which is currently an important issue. Email spam is not merely an innocuous waste of time (Alurkar et al., 2017). It is a tool for malicious activities such as spear phishing, whaling, clone phishing, website forgery, and much more. Classifying emails as spam or ham is thus of utmost importance from a security perspective for the user. The issues related to spam mails are escalating with the increased usage of the web. The fact that out of 80 billion emails received every day, 48 billion of them being spam highlights the importance and urgency of implementing effective classification procedures for emails (Harisinghaney et al., 2014).

With the increasing network bandwidth and improving technology, spam emails have become more sophisticated and it is necessary to use advanced algorithms to create efficient spam filters. Despite the huge amount of research work that has taken place in this sphere, there is no spam filter that is 100% efficient. Hence, there is a need to develop a more sophisticated and accurate classifier model to eliminate the problem of spam emails. All emails share a common structure i.e. subject of the email and the body of the email. Spam emails are identified through the contents of the email, based on the assumption that the content of the spam mail is different than the legitimate or ham mail. The frequently used words in spam emails are words that are related to any product, the recommendation of services, dating related content, etc.

The process of spam email detection can be broadly categorized into two approaches (Ma et al., 2009): knowledge engineering and machine learning approach. Knowledge engineering is a network-based approach in which IP (internet protocol) address, network address along with some set of defined rules are considered for the email classification. This is a fruitful method but bares the limitation of time consumption. The updating of rules and maintenance are also tedious for users. As an alternative, machine learning techniques can be used which does not involve any set of rules. Comparatively, it is much efficient than the former method (Guzella and Caminhas, 2009). Several classification algorithms are used which classifies the emails based on its content and attributes.

BACKGROUND

H. Karamollaoglu et al. (2018) explained the detection of spam emails with machine learning methods. In this study, the content information of emails written in Turkish were analyzed with the help of