EasyChair Preprint

№ 7627

Email Behaviour Detection Using Text Recognisation

Utkarsh Agarwal, Shubham Rastogi and Srashti Singhal

March 28, 2022

EMAIL BEHAVIOUR DETECTION USING TEXT RECOGNISATION

By:
Utkarsh Agarwal , Subham Rastogi, Srashti (B.TEch. Final year Students)

Under the Guidance
Mr. Joney Kumar
Information Technology Department
Meerut Institute of Engineering & Technology, Meerut, U.P. (India)

Abstract:

Emailing have replaced modern messing whether it is personal or professional messaging all the industries depend on emailing even email is official messaging platform for Government organizations. with more and more usages of emailing made it prone to security issues like Malicious Email or email which have is an attack by attacker which creates a duplicate of an existing web page to make fool users in to submitting personal, financial, or password details data to what they think is their service provider's website. There are many solutions available to stop security issues like firewall extra.

To categories. email for a range of activities, machine learning and AI based detection algorithms are implemented to model the user's email behavior. The method have been used to find content based behavior of email clustering and classification, spam detection, and forensic analysis to provide information about user behavior.

This paper advocate categorization of email on the bases of it content whether is useful or dangerous for society

Keywords: SVM,KNN, FER, DNN, VGG16

INTRODUCTION

In the previous 25 years, file structure for storing email message storage has not altered much. Emails are often stored in data files or folders with no organised relationship (flat files), making anything more than a keyword search extremely time-consuming. Messages

can be moved into time-ordered sub-folders of similar messages by users. According to studies, average users may create anywhere from tens to hundreds of folders in a very short period of time. Finding a specific prior message among many sub-folders might quickly become a difficult chore. Not only is the email being searched for, but so is the folder in which it may have been saved! Attachments within these flat file folders are encoded in MIME format, making analysis possible. The common characteristics of the hyperlinks in malicious e-mails. Our analysis identifies that the malicious hyperlinks share one or more characteristics as listed below:

In addition to these organization issues, the Achilles heel of the current email system is its relative ease of abuse. The protocols were based on the assumption that email users would not abuse the privilege of sending messages to each other. The misuse and abuse of the email system has taken on many forms over the years. Typical misuse include forged emails, unwanted emails (spam), fraudulent schemes, and identity theft and fraud through "Phishing" emails. Abuse includes virus and worm attachments, and email DOS attacks.

Problem

When analyzing large sets of emails or attachments generated by a single user or group of users, the common approach is to treat the problem as if the data was one large email box. The most sophisticated analysis is to count of the number of messages in a user created sub-folder. Basic flat searches and name, date, and topic sorting are the most commonly available functions. In addition, current email clients have no analysis tools for quickly analyzing past messages or attachments within a user's email box. Profile views of the data for different tasks should be made available to the user, to enable them to understand a message in its historical context. For example an automatic list of emails which have not received responses can be generated for the user to show them any 'open issues' they might have in their email box.

Related Work

Jindal.L et al. Spam reviews are classified into three types: brand reviews, non-reviews, and spam reviews. Brand Reviews are tied to product sellers, and these reviews disregard user comments concerning the product. Non-reviews are added to a product review to confuse buyers by including reviews of other non-relevant items. Untrue reviews are ones that give related information yet the information presented is incorrect.

Hernández F. et al. presented PU Learning that builds a binary classifier. In PU Learning two sets were trained: set of positive instances (P) and set of both negative and positive instances but without a label (U). PU Learning technique depicts improvement in results compared to other techniques. Heydari, A. et al. introduces a system for detecting spam reviews using time series. They investigate fake reviews posted at doubtful time intervals. Moreover, they employ rating behaviors, context similarity, and people activeness in each time interval to differentiate between spam reviews and legitimate reviews.

Luyang, B, W, T., et al. uses Sentence Convolutional Neural Network (SCNN) and Sentence Weighted Convolutional Neural Network (SWNN) to detect spam reviews. SCNN and SWNN were designed by modifying document-representation learning model. The time complexity of the SCNN and SWNN model is O(n*d2). The SWNN model gives an accuracy of 86.1% as compared to the basic convolution neural network.

Shreyas Aiyar, N. S.et al. proposed the spam review detection using N-gram. Their model improves the accuracy of classification, whereas we have also identified the research gaps in implementing techniques used for spam review detection.

Nidhi A. Patel at el. presents the techniques and datasets used for spam review detection. Moreover, they discuss the limitations of datasets such as limited number of features and unlabeled datasets whereas along with all these we have proposed taxonomy, which classifies the existing techniques and

approaches so that the most appropriate approach can be figured out.

SP. Rajamohana at el. discusses the accuracy of adapted techniques using evaluation metrics whereas we have also discussed the open issues and challenges in the domain of detecting spam review.

Methodology

To properly model the information in an email collection, we must express it in a manner that can be analysed.

Classification Models

The pattern we are attempting to understand is Target Function - or class label. In the spam detection job, for example, given an unknown email, we would like to predict with some degree of certainty whether it is spam or not. The goal function in this example is "is it spam?"

The percentage of instances that our model mistook as the target idea is referred to as the false positive rate. In general, we want to reduce this measurement while without increasing the error rate. In general, the cost of false positives is larger than the cost of false negatives. The false positive rate is calculated as follows:

The False Negative Rate (FNR) is the percentage of target instances that were incorrectly reported as non-target. We must strike a balance between false negatives and false positives while fine-tuning the detection algorithm. Over all cases, a threshold is applied; the higher the threshold, the more false negatives and the less false positives. The false negative rate is calculated as follows:

Sample Error Rate - is the percentage of training instances misclassified by the model divided by the total number of examples viewed. This is one metric for determining how successfully the classifier learns the target function.

True Error Rate - this is the likelihood that the model will misclassify an example given a specified training sample and sample error rate. This is a difficult measurement to make, but it may be estimated if the training set roughly

approaches the real distribution of future cases. In other words, if we train on half spam and half non-spam instances, yet 90% of the data are spam, the sample error will not be an appropriate representation of the model's error rate.

Bias is the mismatch between how we anticipate the model to behave and how it actually performs. Classification bias refers to a machine-learned model's propensity to bias its output towards any one output value as measured during concept training.

Training is the process of instructing a model on a certain notion. During training, the model is presented particular instances that are used to tweak the model's parameters.

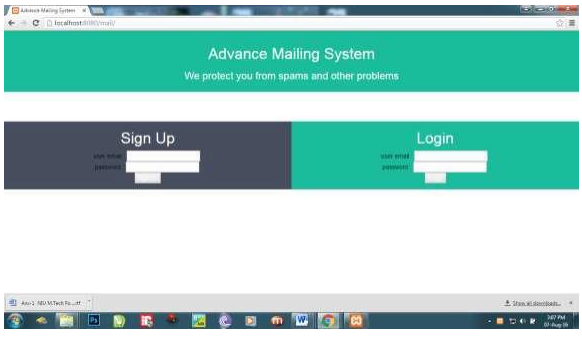
Testing is the process of determining the efficacy of a model's categorization. We may quantify a classifier's accuracy to generalise the training examples if we have a labelled set of instances that are not presented to the classifier during training and make the assumption that the testing set represents an accurate statistical sample of cases.

Noise is faulty labelled data, or data that has been mislabeled for one cause or another. Certain algorithms are resilient, that is, they are unaffected by noise in the training data, whereas others require clean data to measure ground truth. Real-world data is frequently noisy, and obtaining clean data is generally difficult and expensive.

Implementation :

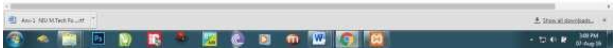
To categorise email on the bases of its content we have implemented the project in WAMP server here we have designed complete emailing system with server and client based here user send message on opening a URL and send it to other user, when other user open URL with his credentials he find email in categorised form in deferent folders

LOGIN PAGE:



REGISTRATION FORM:

USER ID:



Conclusion

Link Guard for Windows XP has been implemented. Our tests shown that Link Guard is lightweight and capable of detecting up to 96 percent of undiscovered harmful assaults in real-time. We think that Link Guard can protect users against harmful or unwanted links in Web sites and Instant messaging in addition to identifying malicious activities. Our next work will involve expanding the Link Guard algorithm to address CSS (cross-site scripting) attacks.

REFERENCES:

[1] R. Barbado, O. Araque, and C. A. Iglesias, "A framework for fake review detection in online consumer electronics retailers," Information Processing & Management, vol. 56, no. 4, pp. 1234-1244, 2019.

[2] Y. Liu and B. Pang, "A unified framework for detecting author spamicity by modeling review deviation," Expert Systems with Applications, vol. 112, pp. 148-155, 2018.

[3] M. Luca, "Reviews, reputation, and revenue: The case of Yelp. com," Harvard Business School NOM Unit Working Paper, pp. 12-16, 15 March 2016

2016

[4] M. R. Martinez-Torres and S. L. Toral, "A machine learning approach for the identification of the deceptive reviews in the hospitality sector using unique attributes and

sentiment orientation," Tourism Management, vol. 75, pp. 393-403, 2019.

[5] D. T. Tanya Gera , Jaiteg Singh "Identifying Deceptive Reviews Using Networking.pdf," International Conference on Computing and Communications Technologies 2015

[6] K.-I. L. Kuldeep Sharma, "Review Spam Detector with Rating Consistency Check," ACM, 2013.

[7] A. O. D. Cennet Merve Yılmaz " SPR2EP A Semi- Supervised Spam Review Detection.pdf," IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining August 2018 2018.

[8] D. K. U. SP.Rajamohana, M.Dharani, R.Vedackshya "A SURVEY ON ONLINE REVIEW SPAM DETECTION TECHNIQUES "

IEEE International Conference on Innovations in Green Energy and Healthcare Technologies(ICIGEHT'17) 2017.

[9] E. F. Cardoso, R. M. Silva, and T. A. Almeida, "Towards automatic filtering of fake reviews," Neurocomputing, vol. 309, pp. 106-116, 2018.

[10] R. M. K. Saeed, S. Rady, and T. F. Gharib, "An ensemble approach for spam detection in Arabic opinion texts," Journal of King Saud University - Computer and Information Sciences, 2019.

[11] Anna V. Sandifer , Casey Wilson, and A. Olmsted, "Detection of fake online hotel reviews," The 12th International Conference for Internet Technology and Secured Transactions (ICITST-2017), 2017.

.