RESEARCH ARTICLE WWW.PEGEGOG.NET

A MULTILINGUAL SPAM REVIEWS DETECTION BASED ON WORD EMBEDDING AND WEIGHTED SWARM SUPPORT VECTOR MACHINES

[1]Mrs. E. KRISHNAVENI REDDY, [2]CH. ANJALI, [3]C. CHARITHA, [4]D. RISHIKA

[1]Associate Professor, Department of Computer Science and Engineering, Sridevi Women's Engineering College, Hyderabad, India

Email:ekrishnavenireddy@gmail.com

[2,3,4,]B.Tech Student, Department of Computer Science and Engineering, Sridevi Women's Engineering College, Hyderabad, India

ABSTRACT

Customers look for online reviews as a valuable source of information before making a purchase. In addition, businesses get valuable insight about their goods and services from these evaluations. Particularly during the COVID-19 epidemic, when people were cooped up at home and reading evaluations online at an unprecedented rate, the credibility of such sources became paramount. Aside from an increase in reviews, the epidemic also changed the environment and tastes. Reviewers of spam take note of these shifts and work to refine their deceitful methods. Reviews that are considered spam sometimes include false, misleading, or deceptive information with the intent to trick consumers or hurt rivals. Therefore, a WSVM and an HHO are introduced in this study for the purpose of spam review identification. When it comes to hyper parameter optimization and feature weighting, the HHO is like an algorithm. The multilingual challenge in spam reviews has been addressed by using three distinct language corpora as datasets: English, Spanish, and Arabic. Along with three-word representation approaches (NGram-3, TFIDF, and One-hot encoding), pre-trained word embedding (BERT) has also been used. There have been four such experiments, each of which has shown and solved a distinct aspect. The suggested method outperformed other state-of-the-art algorithms in every experiment. Put simply, the WSVM-HHO attained an accuracy of 84.270% for the Multilingual dataset, 89.565% for the English dataset, 71.913% for the Spanish dataset, and 88.565% for the Arabic dataset.Additionally, the review context both before and after the COVID-19 incident has been thoroughly investigated. Also, it has been created to combine its prior textual characteristics into a new dataset with statistical features, which will improve detection performance.

Keywords: spam reviews detection, multilinguality, support vector machine, spam detection.

INTRODUCTION:

Online purchasing and selling have both grown in recent years due to the widespread use of the online. Internet business sites have become a primary means by which many people acquire goods. Many online

Corresponding Author e-mail: ekrishnavenireddy@gmail.com

How to cite this article: 1Mrs. E. KRISHNAVENI REDDY, 2CH. ANJALI, 3C. CHARITHA, 4D. RISHIKA. A MULTILINGUAL SPAM REVIEWS DETECTION BASED ON WORD EMBEDDING AND WEIGHTED SWARM SUPPORT VECTOR MACHINES.Pegem Journal of Education and Instruction, Vol. 13, No. 3, 2023, 468-477

Source of support: Nil **Conflicts of Interest:** None.

DOI: 10.47750/pegegog.13.03.47

Received: 12.09.2023

Accepted: 22.10.2023 **Published:** 24.11.2023

marketplaces let shoppers compare products based on product knowledge. Therefore, it might be helpful for various customers to make decisions on products to buy. Online surveys are essential for businesses, and they're also great for customers and trade groups. Customer surveys may aid with product selection, and business surveys can help with quality control by allowing companies to see how customers rate certain products. Choosing the right business decisions may be really beneficial. Customers clearly consider the opinions of others before making a final decision on a purchase.This motivates some customers or organisations to publish spam reviews that promote or criticise brands or certain products, services, persons, or ideas without disclosing their true intentions. The term "Sentiment Spam" or "Audit Spam" describes this kind of spammed emotional data. Many people's fundamental purchasing decisions have been impacted by online customer evaluations of both products and shipping companies. With evaluations being so easily accessible and having such a significant impact on merchants, there is a growing push to regulate the surveys, which are mostly motivated by profit. Conclusion spam is increasingly targeting websites that host customer surveys. - Unjustified favorable or negative evaluations; reviews written for the sake of writing rather than actual product usage. Consequently, the importance of survey spam detection is growing in the present day. They have been the target of criticism from a number of experts today. Review spam finding often employs one of two approaches: supervised methods or unsupervised strategy. Constructing a classifier allows for the execution of monitored systems. Cases that can be physically stamped are used to put up this classifier. The social affair get ready dataset is the starting point for machine learning. Installing a classifier on the preparedness data is the next stage. A few examples of often used controlled approaches include support vector machine (SVM), Naïve Bayes classifier, computedelapse, K-NN classifier, and others. Review spam in the area of sentiment mining is the focus of this research, which also provides an analysis of its methods in this context. This ocument is addressed in the following ways: Section II provides a visual representation of the most popular unsupervised algorithms used for review spam detection, while Section III lays out the most popular controlled methodologies for survey spam localization.

Related Work:

Identifying, Analyzing, and Preventing the Expenses of Spam Traffic

Messages sent via spam may offer illicit goods, spread malware, and even lead to phishing attacks. Users and network operators both pay for these messages, but it's hard to put a price on spam and find out who pays for it. The authors provide a technique to measure the transit costs of spam traffic by tracking the paths taken by spam messages gathered from five honey pots. They demonstrate that stub networks consistently incur large expenses due to spam traffic by combining spam volume with trace route measures and an internetwork business connection database. Also, they prove that certain networks make money off of spam and aren't concerned about blocking it. Lastly, a simple technique is introduced to determine whether networks might save expenses on transit by working together to filter spam traffic at its source.

A Classification-Based Approach to E- Mail Filtering

Because of its convenience, speed, and cheap sending cost, e-mail has quickly become one of the most used forms of electronic communication. There does seem to be a major issue with this Internet programmer in the form of spam emails, however. One significant way to separate such spam emails is by using filtering. In this study, we provide a classification- based strategy for spam email filtering. This method examines the text of emails and gives certain phrases (features) more weight in order to distinguish between spam and legitimate communications. Using a dictionary to identify which phrases are relevant and which ones aren't is an attempt to lower the dimensionality of the retrieved characteristics. The suggested filtering method has been shown effective by a comprehensive comparison examination of several categorization algorithms. The Enron dataset was used to assess the method.

A Classifier for Spam Email Using a Neural Network

Despite the ever-increasing volume of spam, most email users devote a non-trivial amount of effort on a daily basis to removing unwanted communications. Making artificial classifiers that can differentiate between valid and spam e-mail is a continuous problem. Many commercial applications also use Naïve Bayesian methods, and a small number of research have looked into spam detectors that employ these approaches together with big collections of binary data to identify frequent spam keywords. The spammers are aware of these filters and have figured out ways to get around them, but human readers can usually see these patterns in their own letters quite fast. So, we've taken a different approach than previous methods by using descriptive features of words and sentences that a human reader would use to detect spam.

Using a single user's email corpus and a neural network (NN) classifier, this exploratory research evaluates this alternate strategy. This study's findings are contrasted with those of earlier spam detectors that relied on Naïve Bayesian classifiers. Furthermore, it seems that commercial spam detectors are starting to
include the usage of descriptive characteristics as suggested above.

Spam filtering using machine learning: a survey

Focusing on both textual and image-based techniques, this study provides a thorough overview of recent advancements in the application of machine learning algorithms to spam filtering. We stress the need of taking Spam filtering's unique features, including idea drift, into account while developing new filters, rather than seeing it as a generic classification issue. The challenges of updating a classifier using the bag-of-words representation and a key distinction between two early naive Bayes models are addressed, two features that are notably absent from the existing literature. Overall, we find that a lot more needs to be investigated, particularly in more practical assessment contexts, even if significant progress has been achieved in the last several years.

Applications Mediated by Email and Spam Filtering

Two major areas of study in intelligent email processing—email filtering and email-mediated applications—are covered in this chapter. We lay up a plan to demonstrate the whole email filtering procedure. We present a new ensemble learning-based filtering model and provide a new way of merging several filters inside the framework. Here, we present the idea of operable email (OE) for use in email-mediated applications. In order to fulfil the requirements of the World Wide Wisdom Web (W4), it is contended that future email systems would rely heavily on operable email. Here, we show how the World Social Email Network (WSEN) can be enhanced with an email assistant and other smart applications by using OE.

Detector of image spam

The spammers are always coming up with new and improved methods to evade anti-spam measures; the most recent example of this is image-based spam. The latest wave of picture-based spam use basic image processing techniques to manipulate the content of individual messages, altering things like background colours, font kinds, foreground colours, and even rotating and artifacting the images. That is why traditional spam filters find them so difficult to handle. Global picture characteristics, such as colour and gradient orientation histograms, are used to establish if an incoming picture is spam or not in this research. A probabilistic boosting tree is used in this system. The system is able to detect spam withoutoptical character recognition (OCR) and remains resilient when confronted with the types of variations seen in modern spam photos. According to the test findings, the algorithm accurately identifies 90% of spam photos and incorrectly identifies just 0.86% of non-spam images as spam.

METHODOLOGY:

1. Upload Spam Base Dataset 2.Preprocess

Dataset

3. Run KNN, Naive Bayes & Multilayer Perceptron Algorithms

4. Run SVM, Decision Tree & AdaBoost Algorithms'

5. Run Random Forest & CNN Algorithm
6. Accuracy Comparison Graph
7. Recall Comparison Graph' 8.Precision

Comparison Graph

1. Upload SpamBase Dataset:

The selecting and uploading 'spambase.data' dataset and then click on 'Open' button to load dataset. Then the dataset may loaded.

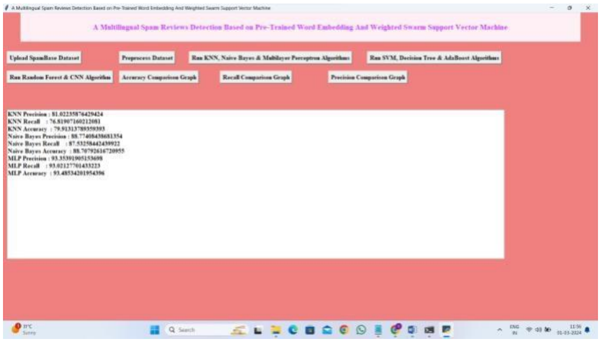
2. Preprocess Dataset:

Preprocessing is the second module in our project. To read all values from dataset and then split data into train and test part where application used 80% dataset for training and 20% dataset for testing.

3. Run KNN, Naive Bayes & Multilayer Perceptron Algorithms:

We have to run all 3 algorithms and get there prediction metrics, we got evaluation metrics such as accuracy, recall and precision for all 3 algorithms.

4. Run SVM, Decision Tree & AdaBoost Algorithms


A Multilingual Spam Reviews Detection Based on Pre-Trained Word Embedding And Weighted Swarm Support Vector Machine
A Multilingual Spam Reviews Detection Based on Pre-Trained Word Embedding And Weighted Swarm Support Vector Machine
Upload SpamBase Dataset
Preprocess Dataset
Run KNN, Naive Bayes & Multilayer Perceptron Algorithms
Run SVM, Decision Tree & AdaBoost Algorithms
Run Random Forest & CNN Algorithm
Accuracy Comparison Graph
Recall Comparison Graph
Precision Comparison Graph

```
KNN Precision : 81.02235876429424
KNN Recall    : 76.81907160212081
KNN Accuracy  : 79.91313789359393
Naive Bayes Precision : 88.77408438681354
Naive Bayes Recall    : 87.53258442439922
Naive Bayes Accuracy  : 88.70792616720955
MLP Precision : 93.35391905153698
MLP Recall    : 93.02127701433223
MLP Accuracy  : 93.48534201954396
```

First we have to run Run SVM, Decision Tree & AdaBoost Algorithms. Then we got metrics for SVM, decision tree and AdaBoost algorithms.

5. Run Random Forest & CNN Algorithm:

We should run Random Forest & CNN Algorithm, then we got accuracy for CNN and random forest algorithms.

6. Accuracy Comparison Graph:

In graph x-axis represents algorithm name and y-axis represents accuracy of all those algorithms and from above graph we can conclude that MLP neural network give better prediction accuracy compare to all other algorithms.

7. Recall Comparison Graph:

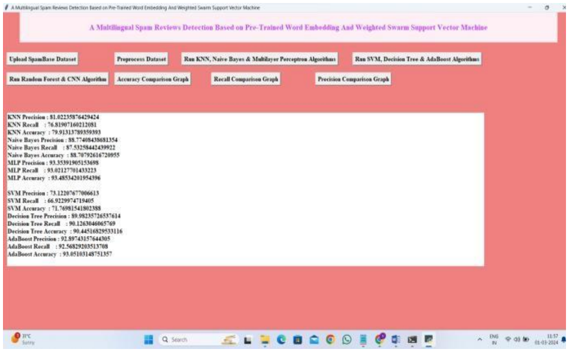
In graph x-axis represents algorithm name and y-axis represents Recall values of all those algorithms.

8. Precision Comparison Graph:

In graph x-axis represents algorithm name and y-axis represents Precision values of all those algorithms.

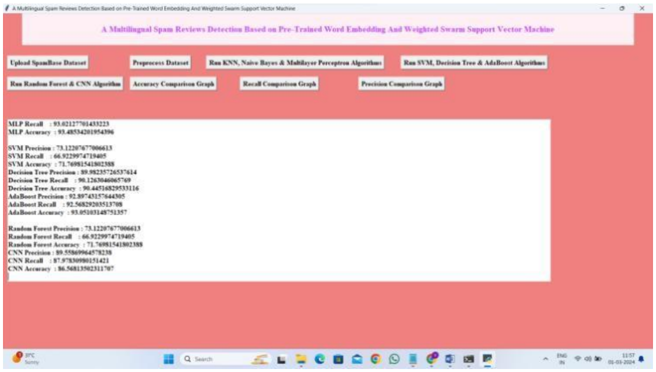
RESULTS:

Click the "Run SVM, Decision Tree & AdaBoost Algorithms" button to run all three algorithms simultaneously. On the previous page, we can see evaluation metrics like recall, precision, and accuracy for each method.


A Multilingual Spam Reviews Detection Based on Pre-Trained Word Embedding And Weighted Swarm Support Vector Machine
A Multilingual Spam Reviews Detection Based on Pre-Trained Word Embedding And Weighted Swarm Support Vector Machine
Upload SpamBase Dataset
Preprocess Dataset
Run KNN, Naive Bayes & Multilayer Perceptron Algorithms
Run SVM, Decision Tree & AdaBoost Algorithms
Run Random Forest & CNN Algorithm
Accuracy Comparison Graph
Recall Comparison Graph
Precision Comparison Graph
31°C
Sunny
Search
ENG
IN
11:57
01-03-2024

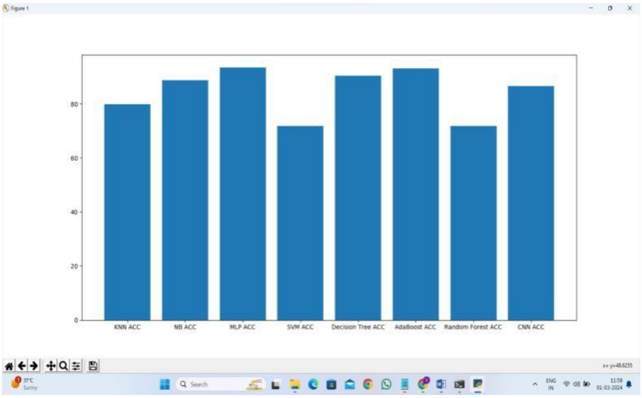
```
KNN Precision : 81.02235876429424
KNN Recall    : 76.81907160212081
KNN Accuracy  : 79.91313789359393
Naive Bayes Precision : 88.77408438681354
Naive Bayes Recall    : 87.53258442439922
Naive Bayes Accuracy  : 88.70792616720955
MLP Precision : 93.35391905153698
MLP Recall    : 93.02127701433223
MLP Accuracy  : 93.48534201954396

SVM Precision : 73.12207677006613
SVM Recall    : 66.9229974719405
SVM Accuracy  : 71.76981541802388
Decision Tree Precision : 89.98235726537614
Decision Tree Recall    : 90.1263046065769
Decision Tree Accuracy  : 90.44516829533116
AdaBoost Precision : 92.89743157644305
AdaBoost Recall    : 92.56829203513708
AdaBoost Accuracy  : 93.05103148751357
```

After seeing the metrics for the SVM, decision tree, and AdaBoost algorithms on the previous page, we may run both algorithms by clicking the "Run RandomForest & CNN Algorithm" button. The results will be shown below.

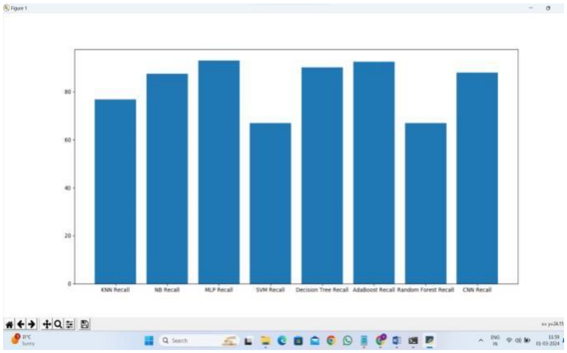

A Multilingual Spam Reviews Detection Based on Pre-Trained Word Embedding And Weighted Swarm Support Vector Machine
A Multilingual Spam Reviews Detection Based on Pre-Trained Word Embedding And Weighted Swarm Support Vector Machine
Upload SpamBase Dataset
Preprocess Dataset
Run KNN, Naive Bayes & Multilayer Perceptron Algorithms
Run SVM, Decision Tree & AdaBoost Algorithms
Run Random Forest & CNN Algorithm
Accuracy Comparison Graph
Recall Comparison Graph
Precision Comparison Graph

```
MLP Recall    : 93.02127701433223
MLP Accuracy  : 93.48534201954396

SVM Precision : 73.12207677006613
SVM Recall    : 66.9229974719405
SVM Accuracy  : 71.76981541802388
Decision Tree Precision : 89.98235726537614
Decision Tree Recall    : 90.1263046065769
Decision Tree Accuracy  : 90.44516829533116
AdaBoost Precision : 92.89743157644305
AdaBoost Recall    : 92.56829203513708
AdaBoost Accuracy  : 93.05103148751357

Random Forest Precision : 73.12207677006613
Random Forest Recall    : 66.9229974719405
Random Forest Accuracy  : 71.76981541802388
CNN Precision : 89.55869964578238
CNN Recall    : 87.9783098015142l
CNN Accuracy  : 86.56813502311707
```

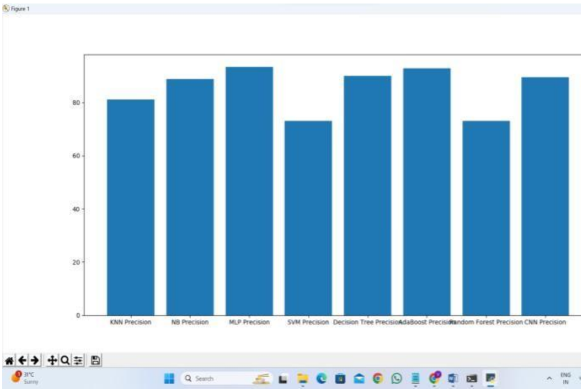
You can see how the various algorithms compare in terms of accuracy by clicking the "Accuracy Comparison Graph" button below; the previous screen also displayed results for the CNN and random forest techniques.



From the graph above, where the x-axis shows the names of the algorithms and the y-axis shows their respective accuracy levels, we may deduce that the MLP neural network provides the most accurate predictions. A recall graph is available below; to access it, click the "Recall Comparison Graph" button.



To access the precision graph below, click on the "Precision Comparison Graph" button.



Accuracy, precision, and recall are all improved in all three graphs by using MLP.

CONCLUSION

Machine learning techniques and their use in spam filtering were the focus of this research. In order to categorize communications as spam or legitimate, we take a look at the most recent algorithms in this field. There was a discussion of the many researchers' efforts to address spam using machine learning classifiers. In order to circumvent filters, spam has changed over the years. An examination of the fundamental design of an email spam filter as well as the procedures involved in this process was conducted. Any spam filter's efficacy may be evaluated using the publicly accessible datasets and performance measures assessed in the article. We compared the various machine learning techniques available in the literature and highlighted the difficulties of using these algorithms to effectively deal with the spam threat. Along with that, we uncovered a few unanswered questions about spam filters. We may conclude from the quantity and quality of the literature that this area has seen and will continue to see substantial advancements. Now that we've covered the unanswered questions about spam filtering, we need to conduct further studies to find ways to make them better. Because of this, academics and professionals in the business will keep studying how to improve spam filters using machine learning methods. Our purpose in writing this study is to provide the groundwork for future qualitative research on spam filtering using ML, DL, and DALM algorithms.

REFERENCES

[1] M. Awad, M. Foqaha, Email spam classification using hybrid approach of RBF neural network and particle swarm optimization, Int. J. Netw. Secur. Appl. 8 (4) (2016).

[2] D.M. Fonseca, O.H. Fazzion, E. Cunha, I. Las-Casas, P.D. Guedes, W.

Meira, M. Chaves, Measuring characterizing, and avoiding spam traffic costs, IEEE Int. Comp. 99 (2016).

[3] Visited on May 15, 2017, Kaspersky Lab Spam Report, 2017, 2012, https://www. securelist.com/en/analysis/204792230/Spam_Report_April_2012.

[4] E.M. Bahgat, S. Rady, W. Gad, An e-mail filtering approach using classification techniques, in: The 1st International Conference on Advanced Intelligent System and Informatics (AISI2015), November 28-30, 2015, Springer International Publishing, BeniSuef, Egypt, 2016, pp. 321–331.

[5] N. Bouguila, O. Amayri, A discrete mixture-based kernel for SVMs: application to spam and image categorization, Inf. Process. Manag. 45 (6) (2009) 631–642.

[6] Y. Cao, X. Liao, Y. Li, An e-mail filtering approach using neural network, in: International Symposium on Neural Networks, Springer Berlin Heidelberg, 2004, pp. 688–694.

[7] F. Fdez-Riverola, E.L. Iglesias, F. Diaz, J.R. Mendez, J.M. Corchado, SpamHunting: an instance-based reasoning system for spam labelling and filtering, Decis. Support Syst. 43 (3) (2007) 722–736.

[8] S. Mason, New Law Designed to Limit Amount of Spam in E-Mail, 2003. http://www.wral.com/technolog.

[9] I. Stuart, S.H. Cha, C. Tappert, A neural network classifier for junk e-mail, in: Document Analysis Systems VI, Springer Berlin Heidelberg, 2004, pp. 442–450.

[10] J. Han, M. Kamber, J. Pei, Data Mining: Concepts and Techniques, Elsevier, 2011.

[11] S.N. Qasem, S.M. Shamsuddin, A.M. Zain, Multi-objective hybrid algorithms for radial basis function neural network design, Knowl. Based Syst. 27 (2012) 475–497.

[12] J.D. Schaffer, D. Whitley, L. Eshelman, Combinations of genetic algorithms and neural networks: a survey of the state of the art, Combinations of Genetic Algorithms and Neural Networks, 1992, pp. 1–37.

[13] E. Elbeltagi, T. Hegazy, D. Grierson, Comparison among five evolutionary-based optimization algorithms, Adv. Eng. Inf. 19 (2005) 43–53.

[14] L.H. Gomes, C. Cazita, J.M. Almeida,

V. Almeida, W.J. Meira, Workload models

of spam and legitimate e-mails, Perform. Eval 64 (7–8) (2007) 690–714.

[15] C.C. Wang, S.Y. Chen, Using header session messages to anti-spamming, Comput. Secur. 26 (5) (2007) 381–390.

[16] T.S. Guzella, W.M. Caminhas, A review of machine learning approaches to spam filtering, Expert Syst. Appl. 36 (7) (2009) 10206–10222.

[17] C.P. Lueg, From spam filtering to information retrieval and back: seeking conceptual foundations for spam filtering, Proc. Assoc. Inf. Sci. Technol. 42 (1) (2005).

[18] X.L. Wang, Learning to classify email: a survey, in: 2005 International Conference on Machine Learning and Cybernetics (Vol. 9, pp. 5716-5719), IEEE, Aug 2005.

[19] W. Li, N. Zhong, Y. Yao, J. Liu, C. Liu, Spam filtering and email-mediated applications, in: Paper presented at the International Workshop on Web Intelligence Meets Brain Informatics, 2006.

[20] G.V. Cormack, Email spam filtering: a systematic review, Found. Trends Inf. Retr. 1 (4) (2008) 335–455.

[21] E.P. Sanz, J.M.G. Hidalgo, J.C.C. Perez, Email spam filtering, Adv. Comput. 74 (2008) 45–114.

[22] S. Dhanaraj, V. Karthikeyani, A study on e-mail image spam filtering techniques, in: Paper presented at the International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME), 2013.

[23] A. Bhowmick, S.M. Hazarika, Machine Learning for E-Mail Spam Filtering: Review, Techniques and Trends, arXiv:1606.01042v1 [cs.LG] 3 Jun 2016, 2016, pp. 1–27.

[24] C. Laorden, X. Ugarte-Pedrero, I. Santos, B. Sanz, J. Nieves, P.G. Bringas, Study on the effectiveness of anomaly detection for spam filtering, Inf. Sci. 277 (2014) 421–444.

[25] I. Katakis, G. Tsoumakas, I. Vlahavas, Email mining : emerging techniques for email management, in: A. Vakali, G. Pallis (Eds.), Web Data Management Practices: Emerging Techniques and Technologies, Idea Group Publishing, USA, 2007 chap 10.