Email Spam Classification Tool Using Artificial Neural Network (ANN) with Logistic Activation Function

Alvin Ericson Anthoni[1], Nurul Azma Abdullah[1*], P. Siva Shamala Palaniappan[2]

[1]Faculty of Computer Science and Information Techn0logy,
Universiti Tun Hussein Onn Malaysia (UTHM), 86400 Parit Raja, Batu Pahat, Johor, MALAYSIA

[2]Faculty of Computer and Mathematical Sciences,
Universiti Teknologi MARA, Segamat, Johor, MALAYSIA

Abstract: This project is all about developing a tool that has the ability to detect spam emails using Artificial Neural Network (ANN) with Logistic Activation Function. This project implements spam detection using an artificial neural network which helps to detect whether an email is spam or ham. Artificial Neural Network (ANN) is an information processing paradigm that is inspired by the way biological nervous systems, such as the brain, process information. In artificial neural network, it helps to detect the input whether it is a spam or ham in this case to give the output with a range from 0 to 1. This project will be able to overcome the weaknesses and flaws in the existing tool or application by giving output which can be trusted and maintains confidentiality, integrity, and availability.

Keywords: Email Spam, Artificial Neural Network, Logistic Activation Function

1. Introduction

These days, emails are being utilized for numerous purposes such as education and business. E-mail spam, known as spontaneous bulk Mail (UBE), garbage mail, or spontaneous commercial e-mail (UCE), is the example of sending undesirable email messages, habitually with commercial substance, in expansive amounts to an aimless set of beneficiaries. Agreeing to a report from Kaspersky labs for Q1 within the year 2015, out of the whole mail activity, 59.2% are spam accounts [1]. Concurring to the diary of financial matters points of view, within the year 2010, approximately 88% of the e-mail activity was spam [1].

In this venture, the approach utilized in machine learning is artificial neural network (ANN). This extension executes spam location utilizing manufactured neural organization which makes a difference to identify whether an e-mail is spam or ham. Artificial Neural Network (ANN) is a data handling worldview that's motivated by the way natural apprehensive frameworks, such as the brain, handle information [2]. The Artificial Neural Network (ANN) works in such a way that can be compared to the neurons in the human brain. Artificial Neural Network is actually a biologically inspired network of neurons which are configured to carry out specific tasks such as clustering, classification, and pattern recognition.

Besides, the existing tools, such as Spamihilator, Spampal, K9, and G-Lock SpamCombat that are available can be improved. This is because the existing tools sometimes cannot detect whether the email received is exactly spam or ham. There are some spam emails that are difficult to be identified by the existing system or tool whether it is spam or ham. Spam filters or detectors nowadays can be defeated as spammers are coming up with new techniques [3]. Hence, this spam detection tool using artificial neural networks detects spam effectively to confirm and give output which can be trusted.

Thus, this project will be able to overcome the weaknesses and flaws in the existing system or tool by giving output which can be trusted. So, the confidentiality, integrity, and availability is maintained.

2. Literature Review

This section discusses the literature review that had been carried out for the tool and the current existing tool. There are many sections in this chapter that will discuss briefly about certain topics that are related to the project.

2.1 Email

Email is used as one of the main communication tools for many organizations such as business organization, banks, schools, and universities. Nowadays, email is used as a premium tool that can be used for advertising and marketing because of certain reasons such as the wide usage of the internet and also communication without cost [4].

2.2 Types of Email Spam

There are many types of email spam. Some of the email spam that can be detected by this tool would be advertisements, chain letters, email spoofing, hoaxes, money scams, and malware warnings.

2.3 Methods of spammers

Spammers nowadays are becoming smarter and have developed many ways to send spam without being filtered by the tools available. Spammers use certain methods in order for them to get ready and prepared before launching any attack or sending spam. Some of the methods used by spammers would be gathering of addresses, obfuscating message content, defeating Bayesian filters and Spam-support services.

2.4 Issues with spam

There are many issues related to spam. This is because attackers or spammers use spam to attack the user with the intention to create an issue for the user. Some examples of issues with spam are viruses, server problems, hacking and phishing, productivity threats, and blank spam emails and forwarding spam emails.

2.5 Machine Learning algorithm applied in the field of email spam filtering

There are many machine learning algorithms that can be applied in the field of email spam filtering. In this project, the machine learning algorithm that will be used in the proposed tool would be Neural

Network. There are two conventional types of neural networks that are usually implied whenever ANN is used. They are the perceptron and the multilayer perceptron [5].

2.6 Email spam classification technique

There are many email spam classification techniques that can be applied in tools or tools. In this project, the machine learning algorithm that will be used in the proposed tool would be Artificial Neural Network (ANN). A typical ANN consists of a series of nodes arranged in three layers which are input, hidden, and output layers. The hidden nodes allow the ANN to model complex relationships between the input variables and the outcome [6].

Table 1 shows the classification results for the Multinomial Logistic Regression approach and the Artificial Neural Network model as used in this research work. The Mean Correct Classification Rate for the Artificial Neural Network was shown that it is higher when compared to the Multinomial Logistic Regression. The best efficiency was 95.83% and 80.83% respectively.

Table 1: Table of model comparison

Model Comparison	Mean Correct Classification Rate CCR (%)
Multinomial Logistic Regression (MLR)	$CCR_{MLR} = 80.83\%$
Artificial Neural Network (ANN)	$CCR_{ANN} = 95.83\%$

2.7 Activation Function

This section discusses the activation function used in the tool. The activation function is usually used in artificial neural networks. An activation function is used to increase the expression ability of a neural network model, which can make the neural network truly have the significance of artificial intelligence [7].

The logistic activation function that is being used in this tool is a common non-linear activation function. The output of this function is bounded, and it was widely used as the activation function in deep neural networks during the early age of deep learning [7]. The network parameters will be trained to produce a desired output.

2.8 Critical attributes of email detected by the tool

This section discusses the critical attributes that will be detected by the proposed tool which are email address, header of the email, and message of the email. These features are important to be detected by the tool to enhance the detection and also to improve the accuracy. In fact, experimental results confirm that the email header provides powerful cues for machine learning algorithms to efficiently filter out spam emails [8], [9].

2.9 Datasets

There are two datasets used in this project which are training dataset and testing dataset. Dataset provides the specification of the data that is stored in the files such as the file containing the dataset which will be used for training the model and also the file containing the dataset which will be used for testing the model. The dataset contains emails features which are being interpreted into numbers.

2.10 Programming language - Python

This project which involves spam classification using Artificial Neural Network (ANN) will be carried out using Python programming language. Python programming language is a powerful programming language used in the field of machine learning.

2.11 Comparison with existing tool

The great number and variety of spam filtering methods results in the need for evaluation and comparison of them [10]. The comparison of existing tools with the proposed tool were done to show and clarify the similarities and differences between the existing tool and the proposed tool. Some of the existing tools that were compared are Spamihilator, SpamPal, K9, and G-Lock SpamCombat.

3. System Methodology

This section would explain briefly in detail about all the activities that had been carried out in each phase to complete this project. In addition, this chapter will also provide a clear view about how the prototype model is used in this project.

3.1 Object-Oriented Tool Development Methodology

This project uses object-oriented tool development methodology. The proposed tool adopts the Object-Oriented Tool Development Model as the methodology of development. The main phases of this methodology will be Requirement Analysis phase, Planning and Design phase, Development and Implementation phase, Testing phase, Deployment phase, and Maintenance phase.

3.1.1 Requirement Analysis Phase

Requirement analysis phase is the first phase in the tool development model. First of all, for the functionality requirement, the tool development technology or machine learning algorithm and existing tool which will be useful for the deployment the proposed tool is studied and analysed. In addition, in this requirement analysis, the software and hardware requirements play an important role.

3.1.2 Planning and Design Phase

After the requirement analysis phase, the planning phase will be carried out where all the information gathered will be processed to come up with ideas for many aspects such as the user interface design, the applicable technology and machine learning algorithm, and also the programming language that will be used for the project.

The designing phase is actually the consideration of the design of the tool which is separated into two different aspects. The two different aspects would be the user interface design and also the implementation design. The user interface design needs to be user-friendly. The implementation design includes all the processes that will be carried out to develop the proposed tool.

3.1.3 Development and Implementation Phase

Besides development of the interface of the tool which is listed in the objectives of the project, the dataset is also prepared and the machine learning algorithm is implemented to the tool in this development phase. The implementation of this project will be coded in Python IDLE and the Python Shell will help in showing the tool interface preview.

In this development phase, all the sub-modules will be combined into the main module. Hence, the prototype of the spam detection tool will be ready and prepared to be tested for further updates or changes to be done.

3.1.4 Testing Phase

Testing needs to be done to ensure the availability of the proposed tool to provide its service. The testing process mainly focuses on finding flaws in the development phase.

3.1.5 Deployment Phase

The deployment phase is the phase where the tool will be analyzed about the availability of the tool for the user to use.

3.1.6 Maintenance Phase

The maintenance phase is the phase where the tool is updated or any changes are made to the tool. This phase is to ensure that tool is up-to-date with the latest type of spam detection. This phase will also repair any fault or flaws in the tool to ensure that the user is always satisfied with the tool.

4. Analysis and Design

4.1 Tool Requirement Analysis

Requirements are actually the brief explanation about the needs of both the user and the tool. In addition, to make sure that the user will be provided a good user experience, the functional requirements and non-functional requirements are determined and analysed.

4.2 Unified Modeling Language (UML) Specification

This section which is UML Specification shows that it is used and applied in the analysis phase of the proposed tool. The main motive of the UML Specification is to show in detail about the functionality and the workflow of the proposed tool.

4.2.1 Use Case Diagram

There are five use cases and the environment of the proposed tool. The use case diagram will be applied in the analysis process. In the analysis process, it will be used to capture the specific requirements of the proposed tool.

4.2.2 Class Diagram

The proposed tool contains seven classes. The seven classes consist of BrowseTrainingFile, UploadTrainingDataset, TrainModel, BrowseTestingFile, UploadTestingDataset, TestModel, and GenerateReport.

4.2.3 Activity Diagram

The purpose of the activity diagram is to show briefly all the activities flow of the proposed tool. The activities are such as browsing and uploading files into the tool and also generating reports.

4.3 Tool Architecture

The architecture of the tool is very important because it ensures that when the deployment of the proposed tool is being carried out, the proposed tool would adopt the right technologies that have been planned and discussed in the previous phases.

4.4 Interface Design

Interface design is very crucial because it plays an important role in showing the appearance of the proposed tool that is going to be deployed.

4.4.1 Tool Interface

The tool interface consists of instructions for the user to follow and also buttons for the user to upload files that contain the dataset for training and testing the model. The browse and upload training file button is used to search and upload the file which contains the dataset for training the model. The train the model button is used to train the model with the uploaded dataset.

The browse and upload testing file button is used to search and upload the file which contains the dataset for testing the model. The test the model button is used to compare and test the model with the uploaded dataset. The generate report button is used to generate a report of the classified emails.

5. Implementation and Testing

5.1 Implementation

In this section of the implementation phase, Pycharm software development platform is used to implement all the functional requirements of the proposed tool and is written in Python programming language.

5.2 Testing

The proposed tool's testing includes functional testing on the proposed tool's functionalities. The functional testing includes Browse and Upload Training Dataset File Module, Browse and Upload Testing Dataset File Module, and Generate Report Module.

6. Conclusion

The Email Spam Classification Tool using Artificial Neural Network with Logistic Activation Function is a tool to classify spam emails. The proposed tool uses a dataset to train the model and dataset to test the model. Then, the tool will be able to generate a report of the classified emails.

The advantages of the proposed tool that can be identified are listed below:

i. The tool will classify the spam emails with higher accuracy.
ii. The tool is user friendly and can be used by users from any age group.
iii. The interface of the tool is designed with buttons according to the current user's expectation that has been studied.
iv. The tool does not require internet connection and can be used offline.

The disadvantages of the proposed tool that can be identified are listed below:

v. The proposed tool can only work when there are classified datasets for training dataset and testing dataset.
vi. The proposed tool takes up to several minutes to start when clicked on the application file which is an executable file.
vii. The proposed tool has only dark mode for background.

The recommendations of the proposed tool that can be identified are listed below:

i. The proposed tool is suggested to make some changes in the coding to enable it to work even without the classified email datasets.
ii. The proposed tool is suggested to make it start faster within several seconds to prevent users from waiting too long when clicked on the application file which is an executable file.
iii. The proposed tool is suggested to have bright mode or custom mode for background according to each user's expectation.

The proposed tool has contributions in improving the shortcomings of the existing tools. The objectives of the project are successfully achieved by the proposed tool.

References

[1]   J. M. Rao & D. H. Reiley. The economics of spam. Journal of Economic Perspectives, 26(3), 87–110. https://doi.org/10.1257/jep.26.3.87. (2012).

[2]   M. Zakaria , M. Al-Shebany & S. Sarhan. Artificial Neural Network : A Brief Overview. Journal of Engineering Research and Applications Www.Ijera.Com, 4(2), 7–12. (2014).

[3]   V. Desai. A STRUCTURE BASED TECHNIQUE FOR SPAM DETECTION AND EMAIL CLASSIFICATION. The British Journal of Psychiatry, 111(479), 1009–1010. https://doi.org/10.1192/bjp.111.479.1009-a. (1965).

[4]   C. Sciences, C. Christi & A. Cheruvu. EMAIL SPAM DETECTOR : A TOOL TO MONITOR AND DETECT SPAM ATTACKS. (2012)

[5]   E. Gbenga, J. Stephen, H. Chiroma, A. Olusola & O. Emmanuel. Heliyon Machine learning for email spam filtering : review, approaches and open research problems. 5(May). https://doi.org/10.1016/j.heliyon.2019.e01802. (2019).

[6]   S, M. P. H. E. Informatics in Radiology Comparison of Logistic Regression and Artificial Neural Network Models. (2010).

[7]   Y. Wang, Y. Li, Y. Song & X. Rong. The influence of the activation function in a convolution neural network model of facial expression recognition. Applied Sciences (Switzerland), 10(5). https://doi.org/10.3390/app10051897. (2020).

[8]   C. C. Lai & M. C. Tsai. An empirical performance comparison of machine learning methods for spam e-mail categorization. Proceedings - HIS'04: 4th International Conference on Hybrid Intelligent Systems, 44–48. (2005).

[9]   J. J. Sheu. An efficient two-phase spam filtering method based on e-mails categorization. International Journal of Network Security, 9(1), 34–43. (2009).

[10]   B. Enrico A Survey of Learning-Based Techniques of Email Spam Filtering. 49, 1–12. (2008).