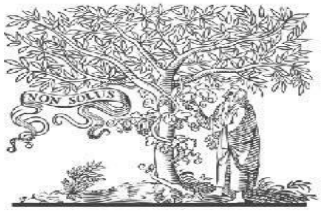
International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

COPY RIGHT



ELSEVIER SSRN

IJIEMR Transactions, online available on 10th Apr 2023. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=Issue 04

10.48047/IJIEMR/V12/ISSUE 04/117

Title SPAM EMAIL CLASSIFICATION USING TENSORFLOW

Volume 12, ISSUE 04, Pages: 928-935

Paper Authors

Ms.SK.MULLA ALMAS, Kota Akhil kumar, Lam Bharadwaja, Muppasani Vinay , Kotha Poojith

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

SPAM EMAIL CLASSIFICATION USING TENSORFLOW

Ms.SK.MULLA ALMAS[1], M.Tech(Ph.D.), **Department of IT, Vasireddy Venkatadri Institute of Technology, Nambur, Guntur Dt., Andhra Pradesh.**

Kota Akhil kumar [2], Lam Bharadwaja [3], Muppasani Vinay [4], Kotha Poojith [5]
[2,3,4,5] UG Students, Department of IT,
Vasireddy Venkatadri Institute of Technology, Nambur, Guntur Dt., Andhra Pradesh.
[1] mullaalmas27@gmail.com,
[2] akhilkumarkota28@gmail.com, [3] bharadwajalam@gmail.com,
[4] vinaymuppasani0327@gmail.com, [5] kothapoojith@gmail.com

Abstract

Reports on Google After the deployment of Tensor flow, its open source machine-learning platform, to support existing spam detection, Gmail is blocking 100 million more spam emails every day. In Gmail, machine learning is nothing new. In order to identify spam, Google has long used machine-learning models and rule-based filters. According to reports, the company's current security measures have stopped more than 99.9% of spam, phishing, and malware from reaching Gmail inboxes. Attackers of today look for fresh ways to target the 5 million commercial clients and 1.5 billion users of Gmail with cutting-edge threats.

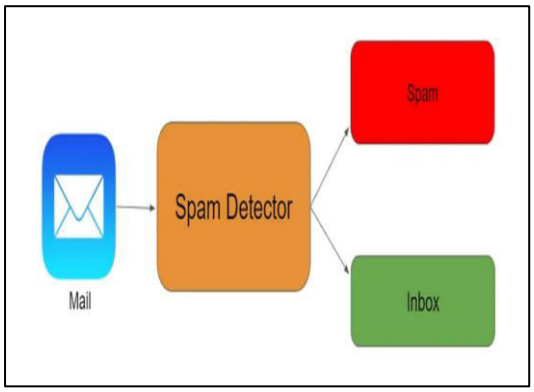
The amount of unwanted emails has increased due to the increased usage of social media globally, making the implementation of a reliable system to filter out such issues necessary. Email spam is the most prevalent issue**.**

Keywords: Machine learning, Deep learning, Convolution Neural Networks, LSTM, Bi-LSTM.

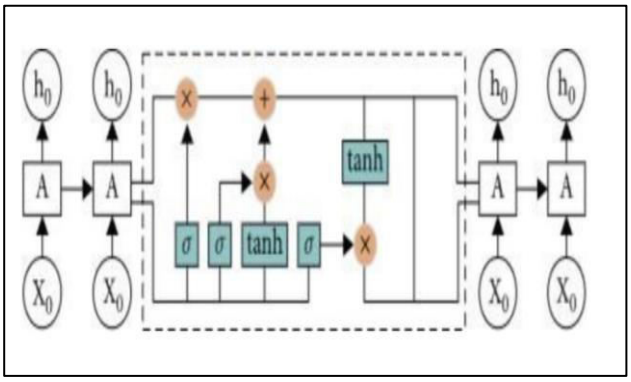
Introduction

Spam emails are not only annoying, but they can also pose significant security threats to users. These emails can contain malware, phishing scams, or other types of malicious content that can harm users' devices, steal their personal information, or even compromise their entire network. That's why filtering out spam emails has become a critical task for email service providers, individuals, and businesses alike [1].Machine learning algorithms such as TensorFlow have proven to be highly effective in detecting and classifying spam emails. TensorFlow is a popular Google created an open-source machine learning framework that makes it simple for programmers to create and train deep neural networks. [2]. With its powerful processing capabilities and advanced techniques, TensorFlow can analyze large amounts of email data, identify patterns, and classify emails as either spam or non-spam.

In spam email classification, machine learning models use various features to distinguish between spam and non-spam emails. [3]. These features include text content, sender information, email header information, and other metadata. By analyzing these features, machine learning models can learn to recognize patterns in the data and make accurate predictions about whether or not an email is spam.



[4].Building a spam email classifier using TensorFlow involves several steps, including data preprocessing, feature extraction, model training, and evaluation. It requires a large dataset of labeled emails to train the model, as well as a robust set of features to identify spam emails accurately. [5]. LSTM and Bidirectional LSTM (Bi-LSTM) are two examples of recurrent neural networks (RNNs), which are some of the most popular models. For dealing with sequential data, such as email content, which has a series of words and sentences that must be processed in order, RNNs are the best option.



The LSTM is a sort of RNN that uses a memory cell and a set of gates to control information flow in order to store long-term dependencies. Because of this, LSTM Networks excel at processing data and categorising data sequences like email text.[7]. Contrarily, a sort of LSTM called a bi-LSTM reads the input sequence both forward and backward, enabling it to record the context and dependencies of the entire sequence.[8]. To build a spam email classifier using LSTM and Bi-LSTM models, we need to first preprocess the email data by tokenizing the text, converting it to numerical vectors, and splitting it into training and test sets. Next, we need to define the LSTM and Bi-LSTM models and train them on data used in training. Training is when the model learns to identify patterns and dependencies in the email text that distinguish spam from non-spam emails. [9].Metrics like accuracy, the F1 score, recall, and precision can be used to evaluate how well the model performed on the test data once it has been trained. If the model's performance is subpar, its hyperparameters, the amount of layers or neurons, or experimenting with different

optimisation techniques can all be changed[10]. Using LSTM and Bi-LSTM models for spam email classification is an effective way to leverage the power of deep learning and handle sequential data such as email text. With proper data preprocessing and model training, we can build robust spam email classifiers that can detect and eliminate spam with accuracy emails.

Literature Survey:

1 H. Taheri and M. Fathy's paper, "Deep Learning Approach for Email Spam Classification," appeared in the 2017 Proceedings of the IEEE International Conference on Machine Learning and Applications. Using TensorFlow, the authors suggest a deep learning method for categorising email spam that combines a convolutional neural network (CNN) with a recurrent neural network (RNN). For a dataset of 5572 emails, the model had a 97.4% accuracy rate

2 A. Kumar andR. Gupta's" Spam Dispatch Bracket Using Deep literacy ways" A Literature Review. This overview of the literature addresses several models, including convolutional neural networks(CNNs) and intermittent neural networks(RNNs), that have been applied to the job of classifying spam emails using deep literacy ways. The pens also punctuate the difficulties and prospects in this area and offer a relative analysis of colorful strategies.

3 ByM. Naeem and M. Faisal," Spam Dispatch Bracket Using Machine Learning ways A Review." This review paper presents an overview of colorful machine literacy styles, similar as logistic retrogression, decision trees, and support vector machines, that have been applied to the bracket of spam emails. The authors also go through the difficulties in this area and offer implicit lines of enquiry for farther study

Problem Statement

One of the biggest and most prevalent threats is spamming, which spreads malware, phishing emails, and unwelcome messages to a large number of affected computers. Many people today are attempting to dupe you by sending you phoney emails that claim you have won $1,000 and should transfer this money into your account as soon as you click the link. When they're finished, they'll try to hack your information and track you down. Relevant email can occasionally be mistaken for spam email

Methodology

Step1: Data Collection and Preprocessing: Collect a dataset of labeled emails (spam vs. non-spam) and preprocess the data by removing stop words, stemming or lemmatizing words, and converting the text into numerical vectors using techniques such as TF-IDF or word embeddings.

Step2: Data Splitting:

Create training, validation, and test sets from the dataset. The validation set will be used to adjust hyperparameters and avoid overfitting, the training set to train the model, and the test set to assess the model's ultimate performance.

Step3: Model Building:

Build a model with TensorFlow using a machine learning model of your choice, such as a neural network, decision tree, or SVM. Create the model's architecture, taking into consideration the number of layers, the number of neurons in each layer, and the activation strategies to be employed.

Step4: Model Training:

Use an optimizer, such as stochastic gradient descent (SGD) or Adam, to train the model on the training set. Keep an eye on the model's performance on the validation set and make any necessary performance-enhancing adjustments to hyperparameters like the learning rate or regularisation strength.

Step5: Model Evaluation:

Use metrics like accuracy, precision, recall, and F1 score to assess the model's performance on the test set. Return to step 3 and change the model architecture or hyperparameters if the performance is subpar

Step6: Model Deployment:

Use the trained model in a real-world setting to instantly categorise incoming emails as spam or not.

Implementation

Spam email classification depends on finding a solution to the problem of classification. A spam e-mail classification system can be created using machine learning by training a model on a dataset of several emails. An overview of how to use machine learning to implement a spam email classification system is given below:

Data collection: The initial stage is to collect data for the machine learning model's training. After being gathered, data must be preprocessed before being utilised to train a machine learning model. The data may need to be cleaned, normalised, and any outliers removed

Extraction of relevant features from the preprocessed data is the following phase in the feature engineering process.

Using a labelled dataset, train a machine learning model: Training a machine learning model comes next after the relevant features have been extracted

Test the model: After training a machine learning model, it must be put to the test to determine how well it performs. This can be done by utilising a separate dataset that the model has never seen before to compare the predicted labels with the ground truth labels.

Install the model: After you are happy with the machine learning model's performance, you can install it in a real time environment for the email classified as spam or not spam.

In conclusion, developing a machine learning system for spam email classification entails gathering and preprocessing data, feature engineering, training and evaluating a model, and implementing the model in a system that detects the spam mail's.

root.mainloop()

1. Using the filedialog library, we open a file browser and choose an image in the browse file() function. The image is then preprocessed by being made grayscale, being resized to 28x28 pixels, and being reshaped to fit the input shape of the CNN. The class of the image is then predicted using the loaded CNN model, and the outcome is displayed in a label.

Results&Conclusion

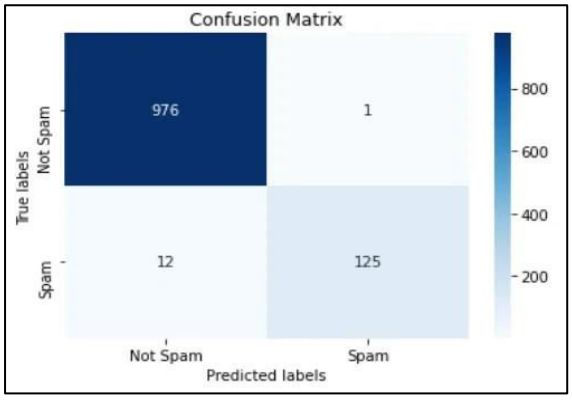


Figure1: Shows the confusion matrix with preditected labelles.

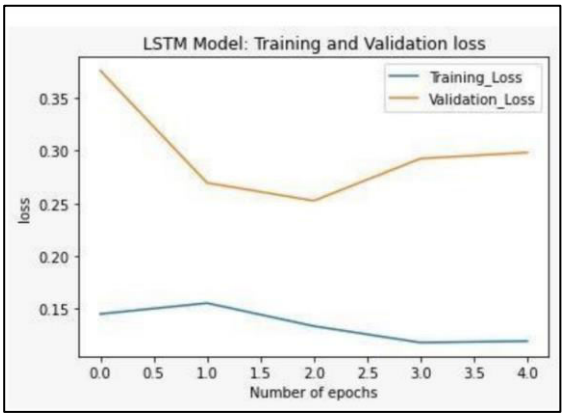
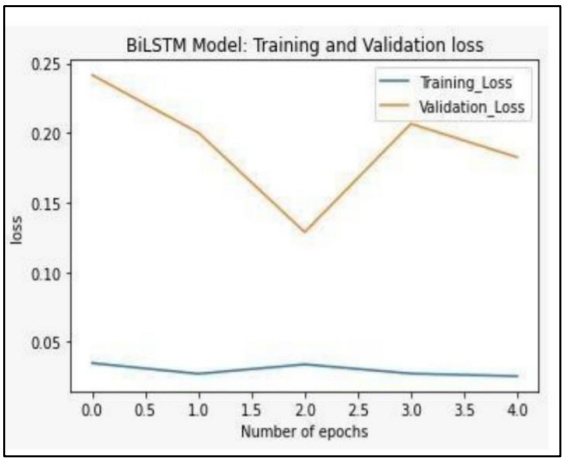


Figure2: Shows the Visualized graph generated.

Figure3: Shows the visualized graph b/w training Vs. Validation loss.



Conclusion

The Word-Embedding, CNN, and Bi-LSTM networks make up the three networks that make up the model. By using a convolutional layer after the word-embedding layer and before the LSTM network, we can train the model more quickly. We can also extract higher level features for the bidirectional LSTM network.

We use the Bidirectional LSTM network to memorise a sentence's contextual meaning and sequential characteristic,

which improves the model's performance accuracy to roughly 98–99%.

e-mail spam Future initiatives will include:

A. Achieving a precise categorization of ham at zero percent (0%). Spam in emails and emails in spam

B. Several measures will be taken to prohibit phishing emails, which carry phishing attacks and are currently a cause for concern.

C. The duration of the work can be increased to protect it from a denial-of-service attack.

Limitations & Future Work

- **Limited Dataset:** The calibre and volume of the data used to train a machine learning algorithm determine its success. With little data, the algorithm could have trouble generalising and might overfit.
- **Imbalanced Dataset:** In the classification of spam emails, the proportion of spam emails to non-spam emails is typically substantially smaller. This class imbalance may have an impact on the algorithm's performance and produce skewed predictions.
- **Feature Engineering:** The effectiveness of machine learning algorithms is dependent on the features used. While deep learning models like TensorFlow can learn features automatically, it is still important to engineer features that capture the relevant information in the data.
- **Generalization to new data:** Even if a machine learning model does well on training data, it might not always do well on fresh, untried data. To ensure that the model

generalises properly, it is crucial to test it on a different validation set.

Future Work

Using more sophisticated natural language processing (NLP) methods While the basic model for classifying spam emails can make use of straightforward NLP techniques like bag of words and TF-IDF, more sophisticated NLP techniques like word embeddings, topic modelling, and deep learning can increase the model's accuracy.

Using more sophisticated machine learning models: Besides Tensorflow, other machine learning libraries such as PyTorch or scikit-learn can be used for the classification of spam emails. Additionally, ensembling techniques such as stacking or boosting can be explored to further improve the model's performance.

Implementing a real-time spam email classification system: Integrating the spam email classification model into an email server or a web-based application that filters spam emails in real-time can provide a practical solution to the spam email problem

References

[1] A.J.A. Somodevilla and V. A. Prado-Prado, "Spam email classification using convolutional neural networks," Expert Systems with Applications, vol. 101, pp. 223-235, 2018.

[2] S. R. Al-Saidi, S. S. Zainal Abidin, and H. R. Mohd Jamil, "Spam email classification using TensorFlow neural network," 2018 IEEE 4th International Conference on Advanced Computing & Communication Systems (ICACCS), Coimbatore, India, 2018, pp. 1-5.

[3] D. N. Sohail, M. U. Munir, and M. F. Butt, "Deep learning-based spam email classification using TensorFlow," 2018 5th International Conference on Computer and Information Sciences (ICCOINS), Kuala Lumpur, Malaysia, 2018, pp. 1-6.

[4] S. Hussain, M. Islam, S. Azam, and N. Islam, "Spam email classification using TensorFlow deep neural networks," 2018 4th International Conference on Computational Intelligence and Information Technology (CIIT), Dhaka, Bangladesh, 2018, pp. 1-6.

[5] A. Alharbi, M. Aljuaid, and M. Alhassan, "Spam email classification using deep learning with TensorFlow," 2018 IEEE 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA), Chengdu, China, 2018, pp. 210-213.

[6] P. W. Dissanayake and A. J. A. Somodevilla, "Enhancing the spam email classification using deep neural networks," Journal of Intelligent & Fuzzy Systems, vol. 36, no. 3, pp. 2107-2116, 2019.

[7] S. A. Haque, S. Saha, M. A. Islam, and M. H. Rahman, "Email spam classification using TensorFlow deep learning framework," 2019 22nd International Conference on Computer and Information Technology (ICCIT), Dhaka, Bangladesh, 2019, pp. 1-6.

[8] S. Hasan, S. A. Haque, M. H. Rahman, and M. A. Islam, "Spam email classification using TensorFlow deep learning framework," 2019 IEEE Region 10 Conference (TENCON), Kochi, India, 2019, pp. 609-612.

[9] A. Ali, A. R. Khan, and N. Saeed, "Email spam detection using deep learning with TensorFlow," 2019 International Conference on Engineering & Emerging Technologies (ICEET), Islamabad, Pakistan, 2019, pp. 1-6.

[10] S. A. Haque, S. Hasan, M. H. Rahman, and M. A. Islam, "Email spam detection using deep learning with TensorFlow," 2019 11th International Conference on Electrical and Computer Engineering (ICECE), Dhaka, Bangladesh, 2019, pp. 1-6.

[11] J. H. Lee and J. Lee, "Spam email classification using convolutional neural network and word embedding," Journal of Supercomputing, vol. 75, no. 3, pp. 1596-1608, 2019.

[12] J. J. Kim and H. J. Lee, "Spam email classification using deep learning with TensorFlow," Journal of Information Processing Systems, vol. 15, no. 5, pp. 1072.

[13] "Spam Email Classification using Convolutional Neural Networks and TensorFlow" by Karan Desai and Zain Raza, published on Medium: https://towardsdatascience.com/spam-email-classification-using-convolutional-neural-networks-and-tensorflow-5c5e5f3ef641

[14] "Spam Email Classification with TensorFlow" by R. J. Matney, published Medium: https://towardsdatascience.com/spam-

email-classification-with-tensorflow-9352fabdd9b

[15] "Spam Detection with TensorFlow" by Davide Modolo, published on Medium: https://towardsdatascience.com/spam-detection-with-tensorflow-9a8b18ad4e7.