A Novel NLP based UNet classifier for detection of spam email

Nagashree N[1] . Bhulaxmi D[2] . Akshay[1]

[1]School of Computer Science and Engineering, REVA University, Bangalore, India
[2]SCOPE, Vellore Institute of Technology, Vellore, Tamil Nadu, India

Received: 23 August 2022 / Revised: 21 September 2022 / Accepted: 12 October 2022
©Milestone Research Publications, Part of CLOCKSS archiving

Abstract – In the era of internet, emails have become the part of parcel of every type of digital communication. Lots of email communication is happening in day-to-day basis be it a personal communication, business communication or any official communication. Spam mails are becoming more irritating factors which requires a lot of filtering before any mail must be read. There are many NLP based techniques to classify spam mails from unspam ones. Many Deep learning-based algorithms have also been worked by researchers. The proposed work is the UNet based novel method which classifies the spam mails. The accuracy of classification is around 97% and better than other classical approaches.

Index Terms – Spam detection, NLP, detection, identification, spam classification.

I. INTRODUCTION

A lot of spamming activity is noticed recently in digital communications. The major incidents of spams are through email communications. They try to manipulate the mischievous activities and a major threat to security. The major challenge in digital technology is the identification, detection, and classification of spam mails from the original ones. Many machines learning and deep learning-based approaches are in boom now and are getting better day by day in classifications. In the paper [1], authors have highlighted several features contained in the email header which will be used to identify and classify spam messages efficiently.

Those features are selected based on their performance in detecting spam messages. This paper also communalizes each feature contains in Yahoo mail, Gmail, and Hotmail so a generic spam message. In the paper [2], a new approach based on the strategy that how frequently words are repeated was used. The key sentences, those with the keywords, of the incoming emails must be tagged and thereafter the grammatical roles of the entire words in the sentence need to be determined, finally they will be put together in a vector in order to take the similarity between received emails. Random Forest algorithm is used to classify the received e-mail. Vector determination is the method used to determine to which category the e-mail belongs to.

In the paper [4], proposed system attempts to use machine learning techniques to detect a pattern of repetitive keywords which are classified as spam. The system also proposes the classification of emails based on other various parameters contained in their structure such as Cc/Bcc, domain, and header. Each parameter would be considered as a

feature when applying it to the machine learning algorithm.

The machine learning model will be a pre-trained model with a feedback mechanism to distinguish between a proper output and an ambiguous output. This proposed system will give good results in detection of spam mails by using random forest [5,6,7].

II. PROPOSED METHODOLOGY

Through NLP, one can make communication establish between humans and machines. There are several processes through NLP involving tokenization, lexical analysis, parsing and semantic analysis. The proposed technique of spam mail classification through UNet is as shown in the architecture below in fig 1.

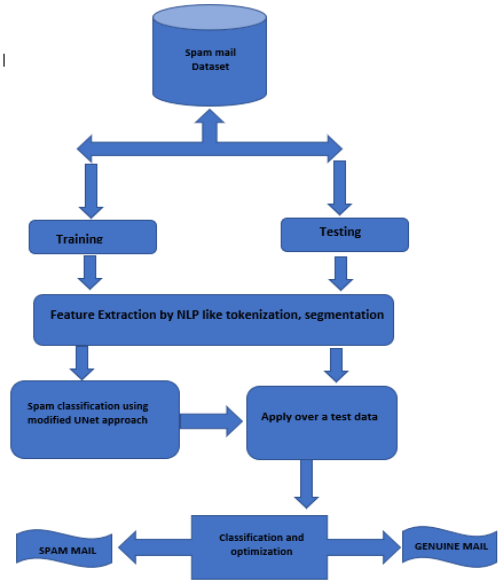

Fig 1: Proposed architecture for spam mail classification

In the proposed work to classify spam mails from the genuine ones, the following steps have been carried out.

Data set collection: First step being the data set collection where the data is been collected from different mails and sent through the series of processing steps. The proposed Deep Learning technique is divided into training and testing phases. Training: It involves feeding the set of spam mails to the CNN based Deep learning approach with initial pre-processing steps.

Pre-Processing: This phase involves extracting features from the mail. Features here are the distinct descriptors to define the specific instances of the data. The pre-processing phase involves basic NLP steps like i) Tokenization ii) segmentation iii) Tagging. This goes through the following NLP pipeline as shown in fig 2.

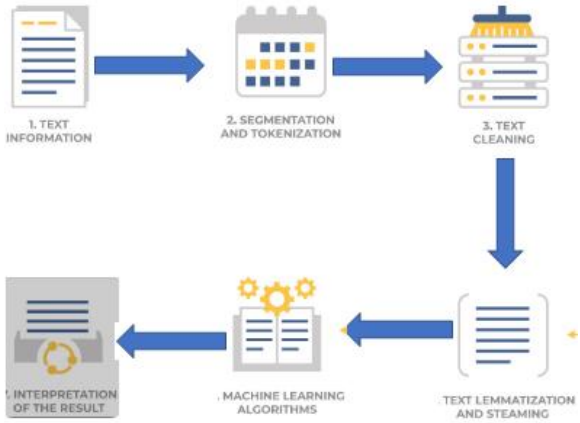

Fig 2: NLP pipeline for pre-processing

Classification using modified UNet: Further the features which are extracted out the NLP pipeline is fed into convolution layers using UNet classifier. The steps of the modified UNet algorithm are as follows:

Step 1: The features in the form of segments are fed as convolution layers
Step 2: On each set consider a function variable
Step 3: Apply convolution filter 3 times
Step 4: Repeat the process until contraction
Step 5: Display classified results in a graph

III. RESULTS AND DISCUSSION

The experiment was conducted over 100 mails taken from different inboxes and fed through pre-processing NLP phases such as segmentation and tokenization. The work was carried our using BERT tool in NLP under python platform and the result of segmentation of emails are represented in fig 3 as below.

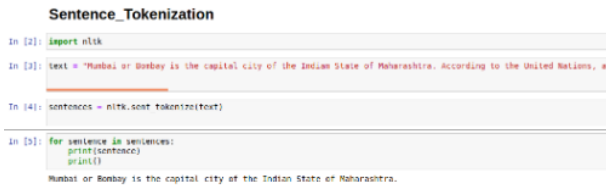

Fig 3: Email statement tokenization

The initial segmentation process involves lot of outliers in the result. The process of document cleaning must be carried out to extract only the relevant data from the segmented data. The python result of implementing text cleaning is shown in fig 4.

Fig 4: Result of Text cleaning applied in python using NLTK

Later tagging is stemming is performed so that the better features are obtained for UNet classifier. The result of tagging is shown in the below result in fig 5.

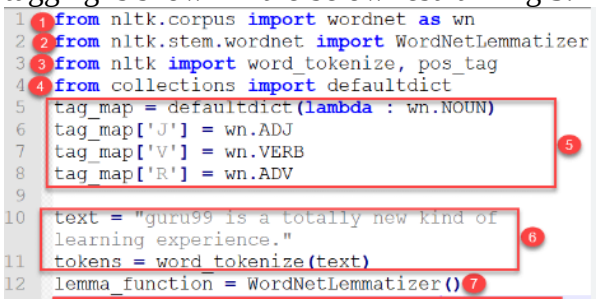

Fig 5: Result of Stemming and stems are taken as features for UNet

The result of classification using modified UNet is shown in the graph displayed by python tool. The result of classification is shown in fig 6.

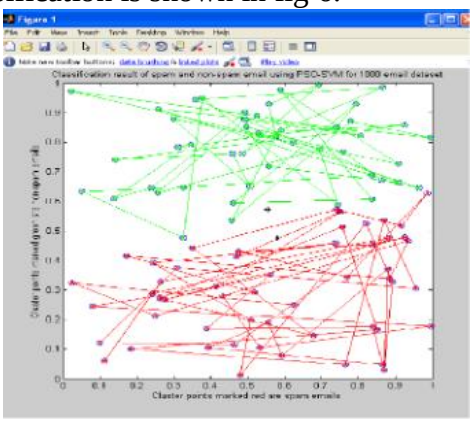

Fig 6: Result showing email spam classification

IV. CONCLUSION

The proposed modified UNet classifier has been given a promising result as compared to other classical classifiers. The main purpose behind efficiency is the initial pre-processing techniques carried out. As a part of pre-processing to extract the relevant features from the dataset, lemmatization and stemming have been given greater number of optimal features. There is many deep learning like UNet frameworks have been proposed earlier in the literature but the combination of NLP technique-based CNN has given a promising result.

REFERENCES

1. Debnath, K., & Kar, N. (2022, May). Email Spam Detection using Deep Learning Approach. In *2022 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COM-IT-CON)* (Vol. 1, pp. 37-41). IEEE.
2. Junnarkar, A., Adhikari, S., Fagania, J., Chimurkar, P., & Karia, D. (2021, February). E-mail spam classification via machine learning and natural language processing. In *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)* (pp. 693-699). IEEE.
3. Nagashree, N., Patil, P., Patil, S., & Kokatanur, M. (2021, June). Alpha beta pruned UNet-a modified unet framework to segment MRI brain image to analyse the effects of CNTNAP2 gene towards autism detection. In *2021 3rd International Conference on Computer Communication and the Internet (ICCCI)* (pp. 23-26). IEEE.

MILESTONE RESEARCH PUBLICATIONS

4. Cheng, Q., Xu, A., Li, X., & Ding, L. (2022, March). Adversarial Email Generation against Spam Detection Models through Feature Perturbation. In *2022 IEEE International Conference on Assured Autonomy (ICAA)* (pp. 83-92). IEEE.
5. Nagesh, N., Patil, P., Patil, S., & Kokatanur, M. (2022). An architectural framework for automatic detection of autism using deep convolution networks and genetic algorithm. *International Journal of Electrical & Computer Engineering (2088-8708)*, *12*(2).
6. Basha, S. M., Ahmed, S. T., Iyengar, N. C. S. N., & Caytiles, R. D. (2021, December). Inter-Locking Dependency Evaluation Schema based on Block-chain Enabled Federated Transfer Learning for Autonomous Vehicular Systems. In *2021 Second International Conference on Innovative Technology Convergence (CITC)* (pp. 46-51). IEEE.
7. Gibson, S., Issac, B., Zhang, L., & Jacob, S. M. (2020). Detecting spam email with machine learning optimized with bio-inspired metaheuristic algorithms. *IEEE Access*, *8*, 187914-187932.
8. Ahmed, S. T., Koti, M. S., Muthukumaran, V., & Joseph, R. B. (2022). Interdependent Attribute Interference Fuzzy Neural Network-Based Alzheimer Disease Evaluation. *International Journal of Fuzzy System Applications (IJFSA)*, *11*(3), 1-13.
9. Sreedhar Kumar, S., Ahmed, S. T., & NishaBhai, V. B. Type of Supervised Text Classification System for Unstructured Text Comments using Probability Theory Technique. *International Journal of Recent Technology and Engineering (IJRTE)*, *8*(10).
10. Liu, X., Lu, H., & Nayak, A. (2021). A spam transformer model for SMS spam detection. *IEEE Access*, *9*, 80253-80263.
11. Yaseen, Q. (2021). Spam email detection using deep learning techniques. *Procedia Computer Science*, *184*, 853-858.
12. Nagashree, N., Patil, P., Patil, S., & Kokatanur, M. (2022). InvCos curvature patch image registration technique for accurate segmentation of autistic brain images. In *Soft Computing and Signal Processing* (pp. 659-666). Springer, Singapore.
13. Nagashree, N., Patil, P., Patil, S., & Kokatanur, M. (2019). Performance metrics for segmentation algorithms in brain MRI for early detection of autism. *Int. J. Innovative Technol. Exploring Eng.(IJITEE)*, *9*.