:: IJEBD ::
(International Journal of Entrepreneurship and Business Development)
Volume 06 Number 06 November 2023
This work is licensed under a Creative Commons Attribution- ShareAlike 4.0 International License.
ISSN : 2597-4785 (ONLINE)
ISSN : 2597-4750 (PRINTED)

Implementation of Natural Language Processing for Spam Email Detection in Outcome based Education (OBE) Application

I Gede Susrama Mas Diyasa, Ikbar Athallah Taufik, Dimas Dzaky Daniswara, Ahmad Adiib Aminullah

Magister of Information Technology, University of Pembangunan Nasional "Veteran" Jawa Timur

Corresponding Author*: igsusrama.if@upnjatim.ac.id

ABSTRACT

Purpose: The Natural Language Processing (NLP) approach has been proven to be effective in spam detection in e-mail because of its ability to process text and identify patterns and distinctive characteristics of spam email.

Design/methodology/approach: Methods in this NLP approach include data pre-processing, such as removing punctuation, irrelevant common words, tokenization, stemming, and others, as well as classification techniques such as Support Vector Classifier (SVC), Naive Bayes, and others. In testing various models, there is one model that shows the highest precision with the number 0.98.

Findings: This study shows that the NLP approach provides better performance in spam detection compared to other methods. However, it is necessary to improve technology and develop more complex detection methods to improve the performance and accuracy of the email spam detection model

Paper type: Research paper

Keyword: *NLP, Spam, Email, Machine Learning, Detection*

Received : August 21th

Revised : October 18th

Published : November 30th

I. INTRODUCTION

The current technological advancements have significantly impacted communication through letters. It is rare to find people using postal services to send letters, as physical letters are no longer the primary means of communication between individuals. Letters have transformed into a digital format known as email. The existence of email facilitates electronic letter delivery based on specific needs or purposes (Dada, 2019).

Email, also known as electronic mail, is a popular communication method used in both internal and internet networks for information exchange. Its convenience has kept email in demand, even serving as an authentication tool in applications and social media synchronization, such as Instagram, Facebook, and Twitter. While email has significant benefits, its misuse can have negative impacts if not used wisely. Many email abuses, such as spam containing advertisements or fraudulent schemes, can harm other users (Ruskanda, 2019).

Spam, meaning Stupid Pointless Annoying Messages, comes in various types, including advertisements, phishing, malware viruses, scams, and others (Zainab, 2021). Spam can be distinguished from non-spam emails, mainly by observing the subject and content of the email (Madhavan, 2020). The subject refers to the title or topic in the email, and in spam, the subject often contains promotional words like "Discount for You." Meanwhile, the content or core of the email sent by spammers is also an important indicator in differentiating spam from other emails (Bhowmick, 2016).

The development of email is not without issues, including the possibility of spam emails entering someone's account. This causes users difficulty in distinguishing whether an email has the potential to be dangerous or just junk. In spam emails, various unwanted content, such as useless files or irrelevant documents, may be present. Moreover, spam in emails can also pose a dangerous threat if it contains viruses or malware that can harm users (Switalski, 2019). In this research, it was tested on the E-OBE (Outcome-Based Education) application (Masdiyasa, 2022).

To address these issues, this research developed a spam detection method in emails using Natural Language Processing (NLP) through the E-OBE application. NLP is one of the artificial intelligence technologies that enables computers to understand, analyze, and manipulate human language in a way similar to humans (Khensous, 2023). In email spam detection, NLP is used to examine the content of email messages and identify whether the email falls into the category of spam or not (Pria, 2021).

Many sources provide explanations regarding spam detection, where efforts have been made to detect spam through various methods with the aim of finding an accurate detection model or obtaining a precise classification model, as described in the reference "Performance Evaluation of Machine Learning Algorithms for Email Spam Detection" [6], which successfully found a high accuracy level in the machine learning model they used. Other research includes that conducted by Pragna (2019), which discusses Natural Language Processing (NLP) and Text Classification in the research context. This study aims to address the problem of classifying messages as spam or ham by applying NLP methods such as Tokenizing, part-of-speech tagging, stemming, and chunking. Model training is conducted using various machine learning algorithms, including K-Nearest Neighbors (KNN), Decision Tree Classifier, Random Forest Classifier, Logistic Regression, SGD Classifier, Multinomial Naive Bayes (NB), and Support Vector Machine (SVM). The experimental results show that the SVM algorithm achieves an average accuracy of 98.49% on the 'SMS Spam Collection' dataset. Another researcher, Rayan (2021), discusses feature extraction and classification to detect email spam and temporary email addresses. The proposed Natural Language Processing-based Random Forest (NLP-RF) approach aims to achieve the research goals. With the help of this approach, spam emails can be reduced, enhancing the accuracy of spam filtering as NLP enables the system to detect the natural language used by users, and the Random Forest approach uses multiple decision trees and random nodes to filter spam [8]. In contrast, the study conducted by Salloum (2021) focuses on using Natural Language Processing (NLP) and Machine Learning (ML) to detect phishing emails. This research analyzes various NLP strategies currently used to identify phishing emails, with an emphasis on ML strategies. These approaches are evaluated and compared, providing an overview of the problem, immediate solutions, and future research directions.

Based on the aforementioned studies, this research discusses email spam detection using NLP implemented in the E-OBE application. E-OBE is an application used for an outcome-based education approach, focusing on concrete, measurable, and observable learning achievements (Masdiyasa, 2023). In OBE, learning objectives are clearly defined, and the learning process is designed to achieve these objectives. This approach emphasizes the importance of evaluating the outcomes achieved by students as indicators of success, rather than merely assessing the learning process or acquired knowledge, which is done based on the Information System. The E-OBE system provides a user-friendly dashboard. Additionally, the study explores NLP techniques used in email spam detection, along with their strengths and weaknesses. The aim of this research is to contribute to email users in addressing the issue of email spam and enhancing productivity in email usage, with its implementation applied to the E-OBE application.

II. METHODS

It should be mention time and place of research in first part. All materials and methods that used such chemical for analysis, treatment and experimental design must be stated clearly and briefly. State the objectives of the work and provide an adequate background, avoiding a detailed literature survey or a summary of the results. A Theory section should extend, not repeat, the background to the article already dealt with in the Introduction and lays the foundation for further work. a Calculation section represents a practical development from a theoretical basis. Materials and methods must be written using 400 until 600 words. Figure 1 depicts the research method that can be conducted in the detection of email spam using Natural Language Processing (NLP).

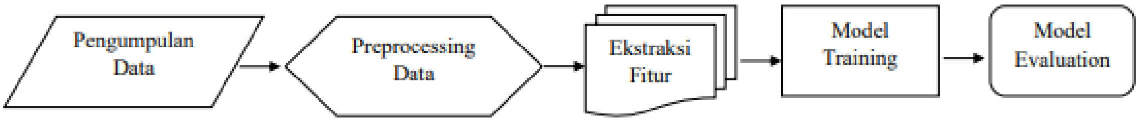


Figure 1. Flow of Research Method

The following are the steps in this research:

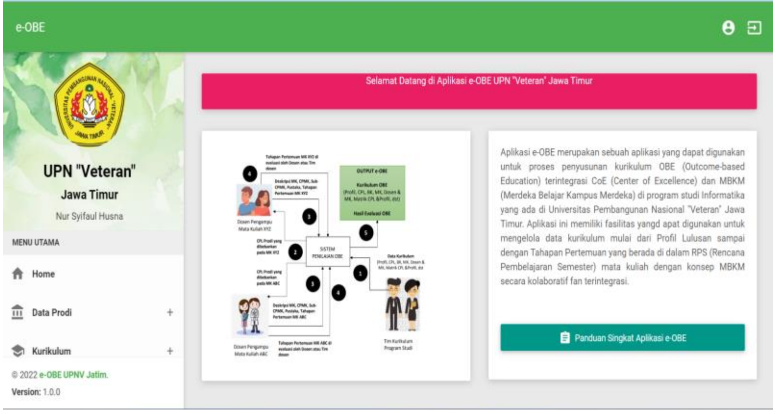
1. Data Collection.
   The first step is to collect email data that will be used to train and test the spam email detection algorithm. The data should include various types of emails, both spam and non-spam. Data collection can be done by

extracting data from various sources or using publicly available datasets. In this article, the data was obtained from a public site that provides access to the dataset (Bharathi, 2020). The total amount of data in this dataset is 6046, with 1896 of them being spam and 4150 being non-spam. These data are numbered from 0 to 6046 for processing purposes.

2. Data Pre-processing
   After collecting email data, the next step is to perform data pre-processing (Babanejad, 2020). This stage involves cleaning the data, removing special characters, converting all letters to lowercase, removing common words, and so on. By doing this data pre-processing, email data will become cleaner and more structured, helping to build an accurate spam email detection model (Bacanin).
   a. Cleaning: Cleaning the data by removing punctuation, hashtags, special characters, and other symbols, as well as converting text to lowercase, is a step taken (Jakhotiya, 2022). Words like "Book" and "book" have the same meaning, but if not converted to lowercase, they will be represented as different words in the vector space model, resulting in more dimensions (Khader, 2019).
   b. Tokenize: Tokenizing means separating sentences into words, so documents can be broken down into smaller parts. This makes it easier to analyze the words in the document (Lourdusamy, 2018).
   c. Removing stop words: Removing words that do not have meaning if there are no other words like: and, I, or.
   d. Stemming: Changing words that originally had affixes to no longer have affixes or revert to their original base word.
3. Feature Extraction After email data has undergone pre-processing, the next step is to perform feature extraction. Features that can be used in spam email detection include specific keywords, word frequency, and email length. These features will be inputs to the spam email detection model (Tabassum, 2020).
4. Model Building After extracting features, the next step is to build the spam email detection model. Models can be created using various Machine Learning algorithms such as Gaussian Naive Bayes, Multinomial Naive Bayes, Bernoulli Naive Bayes, Decision Tree, K-Nearest Neighbors (KNN), Support Vector Classifier (SVC), Logistic Regression, and Stochastic Gradient Descent (SGD) Classifier. This model will be trained using pre-processed and feature-extracted email data.
5. Model Evaluation After the model is built, the next step is to evaluate the model. This evaluation is done to measure the performance of the model in detecting spam and non-spam emails. Some metrics that can be used in model evaluation include accuracy and precision (Collobert, 2021).
6. Testing After the model has been successfully tested and proven accurate in detecting spam emails, the next step is to test it on a dataset of emails that has never been seen before. This testing aims to evaluate the model's performance in detecting spam emails in general.

By implementing the research methods above, it is expected to produce an accurate spam email detection model. This model is expected to help email users overcome the common problem of spam emails.

Some of the displays used in the E-OBE application for testing are shown in Figure 1 and Figure 2. Figure 1 is the initial view of the website, featuring the home page with various menus such as LOGIN, Home, Quick Guide to the E-OBE Application, and Account Registration. On this home page, there is also a brief description of the E-OBE Application itself and the system flow of the E-OBE Application. Before logging in as a user, users can click on the LOGIN menu to enter as an Admin, Curriculum, Lecturer, or Student. Thus, when this application is used for the email verification process to check whether it enters the email contacts or spam, and this is tested on several users, using NLP methods will enable detection. Figure 2 shows the results of the email verification.



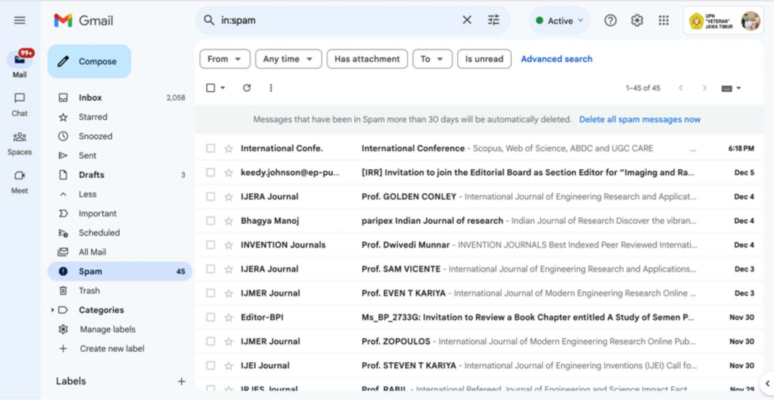
Selamat Datang di Aplikasi e-OBE UPN "Veteran" Jawa Timur

Aplikasi e-OBE merupakan sebuah aplikasi yang dapat digunakan untuk proses penyusunan kurikulum OBE (Outcome-based Education) terintegrasi CoE (Center of Excellence) dan MBKM (Merdeka Belajar Kampus Merdeka) di program studi Informatika yang ada di Universitas Pembangunan Nasional "Veteran" Jawa Timur. Aplikasi ini memiliki fasilitas yangd apat digunakan untuk mengelola data kurikulum mulai dari Profil Lulusan sampai dengan Tahapan Pertemuan yang berada di dalam RPS (Rencana Pembelajaran Semester) mata kuliah dengan konsep MBKM secara kolaboratif fan terintegrasi.

© 2022 e-OBE UPNV Jatim.
Version: 1.0.0

This work is licensed under a Creative Commons Attribution- ShareAlike 4.0 International License.

Figure 1 - The initial view of the website in the E-OBE Application



Messages that have been in Spam more than 30 days will be automatically deleted. Delete all spam messages now

International Confe.	**International Conference** - Scopus, Web of Science, ABDC and UGC CARE ...	6:18 PM
keedy.johnson@ep-pu...	**[IRR] Invitation to join the Editorial Board as Section Editor for "Imaging and Ra...**	Dec 5
IJERA Journal	**Prof. GOLDEN CONLEY** - International Journal of Engineering Research and Applicat...	Dec 4
Bhagya Manoj	**paripex Indian Journal of research** - Indian Journal of Research Discover the vibran...	Dec 4
INVENTION Journals	**Prof. Dwivedi Munnar** - INVENTION JOURNALS Best Indexed Peer Reviewed Internati...	Dec 4
IJERA Journal	**Prof. SAM VICENTE** - International Journal of Engineering Research and Applications...	Dec 3
IJMER Journal	**Prof. EVEN T KARIYA** - International Journal of Modern Engineering Research Online ...	Dec 3
Editor-BPI	**Ms_BP_2733G: Invitation to Review a Book Chapter entitled A Study of Semen P...**	Nov 30
IJMER Journal	**Prof. ZOPOULOS** - International Journal of Modern Engineering Research Online Pub...	Nov 30
IJEI Journal	**Prof. STEVEN T KARIYA** - International Journal of Engineering Inventions (IJEI) Call fo...	Nov 30
IRJES Journal	**Prof. RABII** - International Refereed Journal of Engineering and Science Impact Fact	Nov 29

Figure 2 - Display of Spam Verification in Email

III. RESULTS AND DISCUSSION

The use of Natural Language Processing (NLP) in detecting email spam is one of the methods used to filter incoming emails into a user's inbox. In this research, the implementation of several NLP techniques, such as text classification and natural language processing, is carried out for email spam detection.

Firstly, email data is collected from a web source and then provided in the form of a dataset. This dataset is imported into a programming language along with the necessary libraries for NLP processing. The imported data undergoes simple analysis by examining variables, data size, and data types. Subsequently, the data is cleaned to avoid errors in the NLP process. Exploratory data analysis is also performed to visualize diagrams and heat maps of the data.

The next processing step involves data pre-processing, such as converting text to lowercase, tokenization, removing special characters, eliminating common words (stop word removal), and stemming. The goal of this step is to obtain cleaner and more structured data. Next, feature extraction is performed using the TF-IDF method to transform each email into a feature vector that can be used by the model [3]. After the feature extraction process is completed, the data is divided into training and testing sets.

After successfully completing the previous steps, the next step is to implement the model. In this implementation, several classification algorithms such as Gaussian Naive Bayes, Multinomial Naïve Bayes, Bernoulli Naïve Bayes, Decision Tree, K-Nearest Neighbors (KNeighbors), Support Vector Classifier (SVC), Logistic Regression, and SGD Classifier are used to classify emails into two categories: spam and non-spam, ss seen in Table 1.

The model is evaluated using accuracy and precision metrics to measure its performance. The evaluation results show that the Bernoulli Naive Bayes algorithm has an accuracy of 0.94 and a precision of 0.98, indicating better performance compared to other algorithms. On the other hand, the K-Nearest Neighbors (KNeighbors) model has an accuracy of 0.39 and a precision of 0.33, indicating lower performance. Therefore, this model is not suitable for use as a spam detection model in emails.

In this study, the weaknesses of the email spam detection technique with NLP are also considered. One of the main weaknesses is the limitation in understanding the context of emails and dynamic content. This can lead to errors in email classification, where emails that should be considered as spam may be detected as regular emails, and vice versa

Table 1-Modelling Results

Model	*Accuracy*	*Precision*
GaussianNB	*0,90*	*0,83*
MultinomialNB	*0,93*	*0,89*

BernoulliNB	*0,94*	*0,98*
SVC	*0,95*	*0,90*
KNeighbors	*0,39*	*0,33*
Decision Tree	*0,88*	*0,79*
Logistic Regression	*0,93*	*0,88*
SGDClassifier	*0,96*	*0,90*

IV. CONCLUSION

In conclusion, the NLP approach has proven to be one of the effective methods in detecting email spam. In the future technological developments, the NLP approach has the potential for further development to address new challenges and enhance information security in emails. The NLP approach excels in providing more accurate results in email spam detection compared to conventional approaches. However, continuous technological advancements and the development of more complex detection methods are still needed to improve the performance and accuracy of email spam detection models.

Overall, the use of email spam detection techniques with NLP provides an effective solution to the problem of email spam. In future technological developments, the NLP approach has the potential for further development to address new challenges and enhance information security in emails. Additionally, in its evolution, NLP techniques can be expanded by applying deep learning methods such as Convolutional Neural Network (CNN) and Recurrent Neural Network (RNN) to improve accuracy and effectiveness in detecting email spam. For future research development, it is suggested to explore the use of deep learning techniques like Convolutional Neural Network (CNN) or Recurrent Neural Network (RNN) to enhance the performance of spam detection in emails. These methods can learn more complex text representations and capture deeper contexts.

ACKNOWLEDGMENTS

The author expresses gratitude to all parties who have contributed to the completion of this article. Firstly, thanks to the Research and Community Service Institute (LPPM) of UPN "Veteran" East Java, for the grant provided, colleagues, and friends for the valuable support and input. Also, thanks to the family for their continuous support in pursuing the author's dreams. The author extends thanks to the University and the Faculty of Computer Science for providing the necessary facilities and opportunities to complete this research. Additionally, the author would like to express appreciation to the readers of this article who have taken the time to read the author's writing. Hopefully, this article can provide meaningful benefits and contributions to the development of knowledge in the researched field.

REFERENCES

Babanejad N., Ameeta A., Aijun A., Manos P., ‘A Comprehensive Analysis of Preprocessing for Word Representation Learning in Affective Tasks’, *Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics*, pp. 5799–5810, 2020.

Bacanin, N, M. Zivkovic, C. Stoean, Milos A. , Stefana J, Marko S., and Ivana S. , ‘Application of Natural Language Processing and Machine Learning Boosted with Swarm Intelligence for Spam Email Filtering’, *Mathematics*, Vol. *10*, 4173, pp. 1-32, 2022, https://doi.org/10.3390/math10224173

Bhowmick A., Shyamanta M. H., ‘Machine Learning for E-mail Spam Filtering: Review, Techniques and Trends,’ https://www.researchgate.net/publication/320703241, pp. 1-28, 2016

Collobert R., Princeton NJ, Jason W., L´eon B., Michael K., Koray K., Pavel K., ‘Natural Language Processing (almost) from Scratch’, *Journal of Machine Learning Research* 1, Vol. 1-48, pp. 1-32, 2000

Dada E. G., Bassi J. S., Chiroma H., Abdulhamid S. M., Adetunmbi A. O., and Ajibuwa O. E., ‘Machine learning for email spam filtering: review, approaches and open research problems,’ *Heliyon*, vol. 5, no. 6, 2019, doi: 10.1016/j.heliyon.2019.e01802.

Jakhotiya A., Harshada J., Bhavik J., Charmi C., ‘Text Pre-Processing Techniques in Natural Language Processing: A Review,’ *International Research Journal of Engineering and Technology (IRJET),* Vol. 09 (02), pp. 878-880, 2022

Khensous G., Kaouter L., Zohra L., ‘Exploring the evolution and applications of natural language processing in education,’ *Romanian Journal of Information Technology and Automatic Control*, Vol. 33, No. 2, pp. 61-74, 2023

Khader M., Arafat A., and Ghazi A., ‘The Impact of Natural Language Pre-processing on Big Data Sentiment Analysis,’ *The International Arab Journal of Information Technology*, Vol. 16, No. 3A, Special Issue, pp. 506-512, 2019

Lourdusamy R., Stanislaus A., ‘A Survey on Text Pre-processing Techniques and Tools’, *International Journal of Computer Sciences and Engineering,* Volume-6, Special Issue-3, pp. 138-157, 2018

Masdiyasa I.G.S, Dita P. P., Ika M.M, Rafka M. A., Rangga L.A., ‘Integrated Evaluation and Learning System with OBE Ecosystem and “MBKM”, *Jurnal Nusantara Science and Technology Proceedings* (International Seminar of Research Month 2022), hal. 494-500, 2023, 2023 http://dx.doi.org/10.11594/nstp.2023.3381

Masdiyasa I.G.S, Dita P. P., Ika M.M, ‘Implementation of innovation in integrated evaluation and learning system using outcome-based education ecosystem’, *IJEBD (International Journal of Entrepreneurship and Business Development),* Vo. 6 (1), pp. 78-83, 2022

Mirhoseini S. R., Fatemeh V., Jalal A N., ‘E-Mail phishing detection using natural language processing and machine learning techniques,’ *Conference: 7th National Congress of New Findings of in Electrical Engineering* Iran, pp. 1-9, 2020

Pragna B., RamaBai M., ‘Spam Detection using NLP Techniques’, *International Journal of Recent Technology and Engineering (IJRTE),* Volume-8, Issue-2S11, pp. 2423-2426, 2019

Priya B., Nandhini J.M and Gnanasekaran T., ‘An Analysis of the Applications of Natural Language Processing in Various Sectors *Smart Intelligent Computing and Communication*, pp. 598-602, 2021, doi:10.3233/APC210109

Rayan A., ‘Ahmed I. T., ‘Detection of Email Spam using Natural Language Processing Based Random Forest Approach’, *Research Square*, pp. 1-12, 2021, DOI: https://doi.org/10.21203/rs.3.rs-921426/v1

Ruskanda. F. Z., ‘Study on the Effect of Preprocessing Methods for Spam Email Detection,’ *Indones. J. Comput.*, vol. 4, no. 1, p. 109, 2019, doi: 10.21108/indojc.2019.4.1.284.

Salloum S., Tarek G.**,** Sunil V., and Khaled S., ‘Phishing Email Detection Using Natural Language Processing Techniques: A Literature Survey,’ *Procedia Computer Science* Vol. 189, pp. 19–28, 2021

Świtalski P., Mateusz K., ‘Machine Learning Methods in E-mail Spam Classification’, *Studia Informatica Systems and information technology Nr*, Vol. 1-2 (23), pp. 57-76, 2019, DOI: 10.34739/si.2019.23.04

Tabassum A., Rajendra R. P., ‘A Survey on Text Pre-Processing & Feature Extraction Techniques in Natural Language Processing,’ *International Research Journal of Engineering and Technology (IRJET)* Volume: 07 Issue: 06, pp. 4864-4867, 2020

Zainab A., Hewage C, Nawaf L and Khan I, ‘Phishing Attacks: A Recent Comprehensive Study and a New Anatomy,’ *journal Frontiers in Computer Science Front. Comput. Sci.* 3:563060, pp. 1-24, 2021, doi: 10.3389/fcomp.2021.563060