

Name: Harsh Rameshkumar Mangukiya

Student ID: 2433852

Assignment title: Research methods & professional development

Research topic: Performance Evaluation of Machine Learning Models for Email Spam Filtering

Contents

1. Introduction.....	3
1.1 Context and Background.....	3
1.2 Research Problem	4
1.3 Research Aim and Objectives	4
1.4 Significance of the Research.....	5
2. Literature Review	6
3. Research Design and Methodology	9
3.1 Research Design.....	9
3.2 Research Methods and Materials	10
3.3 Ethical Considerations	12
4. Expected Outcome.....	13
4.1 Anticipated Results	13
4.2 Implications.....	13
4.3 Limitations	13
5. Timeline	13
6. References.....	15

1. Introduction

1.1 Context and Background

Spamming emails refer to an elementary element of online security, whose purpose is to differentiate between spam and spam, as well as legitimate and spam communications. As the number of emails sent or received every day is growing, it has become a very important activity that every individual and organizations should protect themselves with fraud and phishing attacks, among other unhealthy activities. The classification process is based on different methods such as statistical techniques, pattern recognition, and machine learning to give precision in labelling emails as either spam or ham (legitimate) [1], [2].

Spam detection is vital since spam emails in most cases hold unsolicited messages e.g. advertisements, phishing attempt, or malicious attachments that can affect personal privacy as well as company security. There is a continuous challenge on the email users and service providers to ensure high rates of accuracy of spam-detecting, since the email allowed to the inbox should not be a spam email, and additionally reducing the amount of spam emails received by the inboxes [3]. It is an especially tough task since the scammers keep on refining their methods and methods of concealing themselves which often sounds like genuine ways of communication or employs advanced methods of obfuscation.

Machine learning and text mining are important in email spam classification. Text mining is associated with the extraction of meaningful pieces of information through unstructured text data e.g. email data. It uses the idea of natural language processing (NLP) to process and analyze text and thus obtain the identification of the relevant patterns and features that can be employed to classify the text. Machine learning, by contrast, employs algorithms that are capable of learning labelled examples of spam and ham emails [4], [5]. With training on these labeled datasets, machine learning models are able to label new unexplored emails on the basis of the patterns and features that the machine learners have learned. Popular machine learning models that are used to detect spam include Naive Bayes, Support Vector Machines (SVM), and Random Forests.

It is hard to overestimate the role of machine learning in spam classification. It allows scalable automated procedures to manage huge volumes of email data, affording the users and the organization real time capabilities to filter deploy spam. In addition, retraining machine learning models with new data can enhance its capacity to respond to alterations in the trajectory of spamming, as new forms of spam are introduced [3]. The crossroad of spam detection, text mining as well as machine learning is

therefore the focus of coming up with sound dynamic email filtering systems that are not only fundamental in the contemporary realm of digital security.

1.2 Research Problem

Classification of spam is very essential in ensuring that there is integrity and security of digital communication system. With the volume of emails steadily increasing in the world, the necessity of having efficient spam filters has gained more relevance in the provision of individuals and business. Through spam emails, there are usually malicious links, phishing attacks, or other malicious content that not only endanger the privacy of users but also causes financial damage and sensitive information leakages. The difficulty here is coming up with an efficient and accurate approach to classifying emails that ensure the spam is always detected and the chances of false positives, where an email that is legally right is treated as spam, are kept to the bare minimum.

False positive is considered to be one of the major issues in spam classification. False positives are validated emails that are wrongly defined as spam, and it may result in loss of communication, lowered productivity and unpleasant use. Conventional spam filters like the use of simple keyword-based or heuristics-based rules can find it difficult to strike the balance between accuracy and efficiency and can either overfilter or fail to protect against new spamming strategies.

In addition, most traditional spam filters are inefficient in terms of computation. These filters may consume resources e.g. when processing huge number of emails in real-time which affects the performance of the system. The fact that these rules are determined or that they consist of simple algorithms implies that traditional filters can hardly adapt to new varieties of spam or sophisticated email signatures.

Existing spam detection solutions have major gaps. Although machine learning methods have been promising, most of the models are not strong enough to deal with the ever-changing tactics used by spammers. Also, a pervasive problem with large-scale implementation in practice is the conflict between high detection quality and computational resources.

1.3 Research Aim and Objectives

Aim

This study seeks to explore how different machine learning algorithms can be used to rank emails based on labeling spam or legitimate (ham) email, put differently, the research objective is to find ways of optimizing the performance of the machine learning algorithms to maximize classification

accuracy, less false positives, and to optimize their computational effectiveness of a given spam detection system.

Objectives:

- a) To preprocess the email data, such as clean up of the text, feature extraction, transformation to made the data to be in a format that can be used by the machine learning algorithms.
- b) To conduct and test several machine learning machines (Naive Bayes, Support Vector Machine, and Random Forest) to classify spam and genuine mails.
- c) To compare the results of every model on the major indicators, such as accuracy, precision, recall, F1-score and confusion matrix to assess their performance in spam detection.
- d) To calibrate the model to minimize the false positives and maximize model performance by tuning thresholds and hyper parameters used.
- e) To determine the computation efficiency of each model in terms of training time, prediction speed as well as memory consumption with the aim of establishing the most scalable and efficient model to be used in spam filtering in real-time.

1.4 Significance of the Research

Enhancement of spam detection and minimization of false positive is essential in determining the effectiveness and reliability of email systems. Spam mails do not only clog in-boxes but mostly have noxious contents like phishing, viruses, and churns. The solution to such threat against users is to have effective spam detecting programs which ensure that user digital safety is not compromised. Also, there is a strong impact of false positives i.e. when the illegitimate email is correctly classified as spam. Among them is a loss of vital messages, low efficiency and possible ruin of career bonds. Hence, the reduction of false positives and high detection rate takes priority in the life of any spam detecting engine.

Applications of this research practically can be spread over various areas of concern. Cybersecurity and spamming are two aspects, where it is possible to determine by detecting and filtering spam emails to prevent phishing attacks and malware spread, minimizing the chances of the data breach, identity theft, and financial fraud. Best email marketing also issues is facilitated through proper spam filtering which can effectively deliver established marketing messages to target audience at enhancing service delivery and consumer satisfaction. In the aspect of privacy of data, strong spam filtering software is quite important in ensuring that important information does not leak to the hands of dangerous parties. Through their effective detection and filtering of unsolicited emails, organizations are able to preserve

the privateness of the individual and business information, and make sure that they adhere to the data protection laws, like the GDPR.

This study fits in these research areas by coming up with machine learning-based methods that ensure that it is able to not only find the spamming classification more precise but also correct the computational inefficiencies offering a more extensible and flexible solution. The developments will contribute towards improvement of email security, promotion of the ethical behavior of email marketing and the overall objective of safeguarding privacy of the users in the digital era.

2. Literature Review

2.1 Introduction to the Literature Review

The literature review is systematic and provides a review of the current research in email spam classification, which uses machine learning in order to establish the major trends and gaps, which guide the current study. This review discusses the most common methods of algorithms, such as Naive Bayes, Support Vector Machines, and ensemble methods, and the methods of feature extraction, such as TF-IDF and n-grams. It determines some of the emerging trends and models on accuracy and performance optimization as well as some of the research gaps that remain outstanding on how to reduce false positives, to increase the computational capability of real-time filtering as well as changing spam strategies as they keep evolving. This review offers the theoretical basis of comparative model evaluation and the prospects of improving machine learning solutions to current constraints in existing spam detection systems because it extends the results of the various research to provide a suitable theoretical background.

2.2 Organize Literature Thematically or Chronologically

The email spam detection literature may further be divided into themes of machine learning model, benchmark datasets, and feature engineering methods. Experiments shifted towards rule-based filters, but supervised learning was investigated as a solution to the problem that the same set of keywords rules is unable to keep up with changing spam trends [6], [7], [8].

One of these themes is benchmark datasets which allow similar evaluation in the studies, as noted by Ahmed et al. (2022). Numerous studies are based on a collection of public corpora like the UCI Spambase to investigate ham versus spam classification in a realistic setting, and variations of Enron style email collections as argued by Janez-Martino et al. (2024). New curated datasets are also presented in recent studies such as topic based corpora such as SPEMC 15K to represent various spam

types and help to model more finely. They serve to compare the systematic results of algorithms based on these resources and, in addition, enable researchers to investigate the balance of classes and distributional changes to spam content [7], [9], [10], [11].

The second theme is feature extraction, mostly using text based representations that are increasingly using more contextual and metadata indicators. In classical methods, machine learning classifiers are trained to understand email bodies and email subject lines that have been coded as bag of words, using TF IDF weighting, and using n grams, as discussed by Al-Dmour et al. (2024). A number of works build on this adding header details, identity of sender and other metadata to detect patterns like suspicious domains or abnormal routing that enhance the detection of advanced or obfuscated spam [6], [8], [10], [12], [13], [14].

The third theme is on the comparative analysis of supervised models. Various works demonstrate that Naive Bayes is still a competitive spam filtering tool due to simplicity and very fast training and prediction, but can be outperformed not only by the more expressive models. Support Vector Machines are generally found to be highly accurate on high dimensional text features particularly when optimised by careful kernel and hyperparameter tuning. Ensemble models such as the Random Forest, and other ensemble approaches to machine learning, can often portend solid overall performance and sensitivity and hybrid bagging or voting systems based on Random Forest have been shown to further reduce errors as compared to the performance of individual base learners. The following trends underpin the selection of Naive Bayes, SVM and Random Forest as the main baselines of the modern spam detection studies [7], [7], [11], [13], [15], [16], [17].

2.3 Key Contributions and Gaps

Some of the most significant contributions in the literature of spam classifications are the transition of the rule based filters to models of supervised machine learning that was far more accurate and flexible to the changing trends of spam. Research has shown that the Naive Bayes, Support Vector Machines, Random Forest, and hybrid method of bagging or ensemble algorithms are able to reach a high detection rate when paired with a good feature engineering strategy and well-tuned decision threshold. The recent literature further generalises these models to complex patterns in email content and metadata by adding advanced feature selection, incremental learning and deep or hybrid architectures to these models [7], [18], [19], [20], [21].

Despite these developments major gaps still exist in existing methodologies. False positive rates are still very high in many systems, making them to classify legal emails as spam and spoiling user confidence in automated filters. Computational inefficiencies are also still an issue especially when

dealing with models that are resource intensive, deployed in real time, large scale email infrastructures where latency and memory constraints are important. Moreover, some of the studies note difficult complications in class imbalance, lack of data variety and lack of robustness to concept drift, and more scalable, adaptive and efficiency aware spam detection frameworks, capable of sustaining any good performance.

2.4 Theoretical and Technical Frameworks

Inspired by supervised learning, the theoretical basis of spam classification studies is that models can be trained on a set of email features to binary labels spam or ham as per a set of labeled examples. Supervised classification tools like Naive Bayes, Support Vector machines, logistic regression, decision trees, and ensemble methods assume that every email takes the form of a point in a high dimensional space of features and maximize a decision surface that distinguishes between classes at minimal classification error.

Technical models describing the processing of emails content usually begin with text processing, such as text tokenization and stop-word elimination, and the conversion of text into numerical vectors. The standard techniques are bag of words, festival frequency-inverse document frequency (TF IDF) weighting, and n gram representations that can yield the significance of the word and the locality of the subject line and body. In the previous research on textual spam filtering, these representations are always combined with the supervised model in order to give high accuracy as well as strong generalization to the representation.

2.5 Relation to Your Study

The research expands the current spam classification literature due to its specific comparison of the Naive Bayes, Support Vector Machine, as well as the Random Forest against each other with the help of the uniform preprocessing pipeline and equivalent evaluation framework. It also fills in constraints of the existing literature that have focused on accuracy, but less on the aspect of a false positive and resource consumption in their analysis, by directly discussing precision, recall, and F1 score, as well as training time and prediction speed. By so doing, the study offers deployment orientated information and viable advice on the choice on scalable, high performing models in actual world spam filtering.

2.6 Literature Summary

Available literature indicates that machine learning models on spam that are supervised using TF IDF and n gram features have high accuracy in spam detection under standard email datasets. Nonetheless,

research is regularly citing shortcomings, such as continuing false positive rates, algebraic inefficiency, bias in classes and subpar resistance to changing spam trends.

3. Research Design and Methodology

3.1 Research Design

The general study design of the research will be quantitative and will concern the usage of the machine learning classification models with an aim of testing and enhancing the spam detection systems. The study shall entail a comparative analysis of the various learning algorithms based on their level of supervision to categorize emails as spam or legitimate (ham) based on a dataset of labeled emails of both categories. This solution can be applied to the research issue since it enables objective and measurable outcomes which are quantified in terms of performance metrics, including accuracy, precision, recall, F1-score and computational efficiency.

This paper focuses on the application of supervised learning algorithms, which are models that are built to acquire patterns based on the training information that is labeled. With spam classification, the labeled data will be the emails that have already been classified as either spam or ham, so that the algorithm can develop a model based on these classifications. This task is best served by supervised learning due to the fact that the problem of spam detection is a classification task by its nature since the input features (email text, metadata) are to be entered into predetermined output categories (spam or ham). The algorithms can discover the distinguishing features and thus learn how to classify new unseen emails rather well by using this labelled data.

The decision to use machine learning rather than conventional systems based on rules is due to the fact that there is a complexity and dynamism surrounding spam emails. The spam methods are constantly changing and in the same manner the rule based filters cannot keep pace. Conversely, machine learning models, specifically supervised based ones are able to evolve to such changes through learning of new data and with time, their accuracy will increase. Also, machine learning algorithms have been demonstrated to be effective in order to work with large volume of data and therefore they are best suited to scalable spam detection in real-life applications.

This study will therefore consider a variety of machine learning models whereby a comprehensive evaluation as to the strengths and weaknesses of the models will be established in regards to the classification of spam.

3.2 Research Methods and Materials

Methods

The study will adopt a quantitative method in order to test the spam detection systems using machine learning models. The main procedures in the methodology are the processes of data collection, feature extraction, model selection, and evaluation.

1. Data Collection:

The data that will be utilized to conduct this study is the Enron Spam Dataset which includes labeled malmails that were also identified as spam or ham (legitimate). The emails that are part of the dataset are pre-labeled, which means that they can be directly used when performing supervised machine learning. The emails will be divided into training and test sets in which 80% will be used to train and the remaining 20% will be used to test. This enables the models to train on a large percentage of the data and is tested on unseen examples.

2. Feature Extraction:

The text of the raw email would be subjected to the text preprocessing so that it could be converted into the machine learning format. This will involve:

- Tokenization: The process of dividing the text of the email into single words or tokens.
- Stopword Removal: Removing frequent words (e.g., "the", "and" "is" etc.) not contributing to the classification task.
- Stemming/Lemmatization: Removing words into their root forms (i.e. running becomes run).

TF-IDF (Term Frequency-Inverse Document Frequency) will then be used as an extraction feature after the preprocessing has been done. It is implemented by the frequency of words as well as frequency of words divided by the frequency of words in the entire dataset which measures how significant the words are in the emails. Also, the combination of n-grams (n words together) as part of the email will be done to describe a context in the email, further increasing the degree of prediction of the model.

3. Model Selection:

There will be three machine learning models who will be used in classification:

- Naive Bayes: It is a probabilistic classifier which is effective with text classification when conditionally independent feature.
- Support Vector Machine (SVM): This is an effective classification algorithm that determines an optimal hyperplane that classifies data in high-dimensional feature spaces.
- Random Forest: This is an ensemble technique, resulting in the formation of multiple decision trees and Integrating the results to enhance accuracy and alleviate overfitting.

4. Evaluation:

Evaluation of the performance of every model will be achieved with the help of several assessment measures:

- Accuracy: The percentage of the correctness of classifications (spam and ham) of all predictions.
- Precision: The ratio of the correctly predicted spam emails with regard to all the emails that were correctly predicted as spam.
- Recall: Fraction of the number of correctly predicted spam mail of total actual spam mail.
- F1-score: The harmonic average of both precision and recall, which provides a compromise between the two.

These measures will enable the effective evaluation of the potential of each model to effectively categorize the emails and reducing the errors, false positives, and false negatives to as minimum as possible.

Materials

Research Data:

This research will use the Enron Spam Dataset based at Kaggle as its primary dataset. This data set will consist of a set of emails which correspond to spam or ham (legitimate). Because of its richness and diversity, it is generally applied in spam classification. The data is in plain text shape of emails which commercializes prior processing to eliminate unwanted characters, stopwords, and noise.

The data will be subjected to a number of preprocessing procedures before it is presented to the machine learning. These steps include:

- **Cleaning:** Eliminating non alpha numeric and HTML elements and any irrelevant material (e.g., email made ups or email signatures).
- **Tokenization:** Individualize the text in terms of words or tokens.
- **Stopword Removal:** Removing the common words (e.g., the, and, of) which do not add any meaning to the classification.
- **Stemming or Lemmatization:** The act of shortening words down to their root word (e.g. running turns into running).

The data will be washed and pre-processed, and then divided into training (80) and test (20) sets to make sure that the models will be trained using one part of the data and the results will be taken on previously unknown data. Such division enables adequate check of model performance and generalization.

Software:

The study will be done through the python programming language which is a popular machine learning language. In the use of the libraries, the following libraries will be used:

- **Scikit-learn:** To construct and estimate machine learning models.
- **NLTK (Natural Language Toolkit):** To process texts i.e. tokenization, stemming and removal of stopwords.
- **Pandas:** Complete way to manipulate data, process it and extract features.
- **NumPy:** To perform mathematical matters and effective administration of arrays and matrices.

Hardware:

In the case of training a model, a typical CPU existing system will be utilized. A GPU can be used however, when it is necessary to accelerate the training process, e.g., when the model under consideration can use parallel processing in the training process (such as SVM or Random Forest).

3.3 Ethical Considerations

The ethical implication that is brought with the use of email data in this study is that sensitive issues such as privacy and informed consent. Because the dataset will include actual email messages, one will need to make sure that any personal or sensitive data will be anonymized or eliminated to safeguard the privacy of the people involved. Also, despite the availability of the Enron dataset publicly, the researcher needs to make sure that valid consent is taken to utilize such data, that these

data are not violating ethical principles of research and other data protection regulations such as GDPR.

4. Expected Outcome

4.1 Anticipated Results

The Support Vector Machine (SVM) is expected to have a high level of classification since it can efficiently manage data that has a high dimensionality. Generalization properties of SVM are supposed to work effectively in discriminating between spam and ham email. However, the false positive rates will be lower in Naive Bayes, since it is famous to be less biased when classifying true emails to be spam. All in all, the two models are prone to perform competitively, although they possess different advantages of precision and false positive minimization.

4.2 Implications

The results of this study have great implications to the real-life practice in enhancing the email spam filters to be more effective and accurate. Improved spam classification models also have a potential to improve cybersecurity, phishing and malware is less likely to happen and email marketing systems can be improved since legitimate messages get to the target audience.

4.3 Limitations

Some of the limitations that may be encountered in this study include data quality problems like noisy or incomplete email messages. Also the imbalance of the classes (more ham mail compared to spam mail) may interfere with model performance and there is a possibility of model overfitting where the model will act correctly on the training data and fail to generalize to the new data.

5. Timeline

The project shall take a period of 12 weeks to be achieved and the phases are well spelt out and arranged to facilitate on time occurrence. The key tasks and milestones are listed below:

Week	Task	Details
Week 1	Data Collection and Preprocessing	Collect and clean the Enron Spam dataset.

Week 2-3	Feature Extraction and Preprocessing	Apply tokenization, stopword removal, and feature extraction (TF-IDF).
Week 4-5	Model Selection and Training	Train Naive Bayes, SVM, and Random Forest models.
Week 6-7	Model Evaluation and Hyperparameter Tuning	Evaluate models on accuracy, precision, recall, and F1-score. Tune hyperparameters.
Week 8-9	Computational Efficiency Analysis	Analyze training time, inference speed, and resource usage.
Week 10	Final Testing and Evaluation	Test models on unseen data and finalize results.
Week 11	Report Writing	Write up the methodology, results, and discussions.
Week 12	Final Review and Submission	Review and finalize the research proposal.

The following timeline should provide sufficient time to each one of the tasks and engage in consistent improvement in reaching the goal of the proposal.

6. References

- [1] M. H. Alsuwit, M. A. Haq, and M. A. Aleisa, "Advancing Email Spam Classification using Machine Learning and Deep Learning Techniques," *Eng. Technol. Appl. Sci. Res.*, vol. 14, no. 4, pp. 14994–15001, Aug. 2024, doi: 10.48084/etasr.7631.
- [2] P. Prasad, "Exploring Machine Learning Algorithms for Email Spam Filtering," *SPAST Rep.*, vol. 1, no. 6, Aug. 2024, doi: 10.69848/sreports.v1i6.5079.
- [3] P. Joglekar, J. Rajurkar, M. Shinde, P. Tayde, and V. Gadmade, "Machine Learning Based Email Spam Detection: Achieving High Accuracy and Efficiency," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 12, no. 5, pp. 3575–3580, May 2024, doi: 10.22214/ijraset.2024.62390.
- [4] F. Agusman, "Comparative study of DistilBERT and ELECTRA-Small Models in Spam Email Classification," *J. Inform.*, vol. 12, no. 2, pp. 113–121, Aug. 2025, doi: 10.31294/inf.v12i2.25528.
- [5] P. P. Ghogare and M. P. Patil, "Enhancing Spam Email Classification Using Effective Preprocessing Strategies and Optimal Machine Learning Algorithms," *Indian J. Sci. Technol.*, vol. 17, no. 15, pp. 1545–1556, Apr. 2024, doi: 10.17485/IJST/v17i15.2979.
- [6] M. S. Islam, A. A. Mahmud, and M. R. Islam, "Machine Learning Approaches for Modeling Spammer Behavior," Aug. 25, 2010, *arXiv*: arXiv:1008.4249. doi: 10.48550/arXiv.1008.4249.
- [7] A. Rayan, "Analysis of e-Mail Spam Detection Using a Novel Machine Learning-Based Hybrid Bagging Technique," *Comput. Intell. Neurosci.*, pp. 1–12, Aug. 2022, doi: 10.1155/2022/2500772.
- [8] O. Stephen Agboola, "Spam Detection Using Machine Learning," *Comput. Eng. Intell. Syst.*, May 2020, doi: 10.7176/CEIS/11-3-04.
- [9] N. Ahmed, R. Amin, H. Aldabbas, D. Koundal, B. Alouffi, and T. Shah, "Machine Learning Techniques for Spam Detection in Email and IoT Platforms: Analysis and Research Challenges," *Secur. Commun. Netw.*, vol. 2022, pp. 1–19, Feb. 2022, doi: 10.1155/2022/1862888.
- [10] F. Janez-Martino, R. Alaiz-Rodriguez, V. Gonzalez-Castro, E. Fidalgo, and E. Alegre, "Classifying spam emails using agglomerative hierarchical clustering and a topic-based approach," Feb. 07, 2024, *arXiv*: arXiv:2402.05296. doi: 10.48550/arXiv.2402.05296.
- [11] D. Kaushik, "A Comparative Study of Machine Learning Algorithms for Email Spam Detection," *Int. J. Multidiscip. Res.*, vol. 7, no. 3, p. 49517, June 2025, doi: 10.36948/ijfmr.2025.v07i03.49517.
- [12] N. A. Al-Dmour, S. Kousar, A. Khan, A. Ihsan, T. Abbas, and A. Q. Saeed, "Enhancing Email Spam Detection Using Advanced AI Techniques," in *2024 International Conference on Decision Aid Sciences and Applications (DASA)*, Manama, Bahrain: IEEE, Dec. 2024, pp. 1–6. doi: 10.1109/DASA63652.2024.10836525.
- [13] C. Dewi, F. A. Indriawan, and H. J. Christanto, "Spam classification problems using support vector machine and grid search," *Int. J. Appl. Sci. Eng.*, vol. 20, no. 4, pp. 1–10, 2023, doi: 10.6703/IJASE.202312_20(4).006.
- [14] D. K. Yadav, A. Raj, Rajlakshmi, N. Kumar, and R. Kumari, "Enhancing Email Security: A Real-Time Machine Learning-Based Spam Detection System," *Internet Technol. Lett.*, vol. 8, no. 5, p. e618, Sept. 2025, doi: 10.1002/itl2.618.
- [15] N. Bhavana and A. Sowmya, "Machine Learning Algorithm Based Email Spam Detection," *Int. J. Innov. Sci. Res. Technol.*, pp. 3014–3016, June 2025, doi: 10.38124/ijisrt/25may1564.
- [16] S. P. Gond, S. S. Yadav, M. A. Alam, and S. Sahoo, "Email Spam Detection Ensemble Methods," in *2025 3rd International Conference on Disruptive Technologies (ICDT)*, Greater Noida, India: IEEE, Mar. 2025, pp. 1561–1567. doi: 10.1109/ICDT63985.2025.10986443.
- [17] S. Verma, S. Agrawal, S. Gulati, and Gouthaman. P, "A Comparative Study on Spam Identification using Naive Bayes and SVM," in *2024 5th International Conference on Data*

Intelligence and Cognitive Informatics (ICDICI), Tirunelveli, India: IEEE, Nov. 2024, pp. 914–919. doi: 10.1109/ICDICI62993.2024.10810925.

- [18] Y. Bilgen and M. Kaya, “EGMA: Ensemble Learning-Based Hybrid Model Approach for Spam Detection,” *Appl. Sci.*, vol. 14, no. 21, p. 9669, Oct. 2024, doi: 10.3390/app14219669.
- [19] S. Munga Ngigi, R. Mathenge, J. Karani, and N. Muriithi, “Spam Detection in Emails Using Machine Learning Techniques: A Review,” *Int. J. Comput. Inf. Technol.-0764*, vol. 13, no. 3, Oct. 2024, doi: 10.24203/gsdamd68.
- [20] G. Sanghani and K. Kotecha, “Incremental personalized E-mail spam filter using novel TFDCCR feature selection with dynamic feature update,” Apr. 27, 2019, *arXiv*: arXiv:1904.12118. doi: 10.48550/arXiv.1904.12118.
- [21] Walter Oluchukwu Ugwueze, Sylvester Okwudili Anigbogu, Emmanuel Chibuogu Asogwa, Doris Chinedu Asogwa, and Kenechukwu Sylvanus Anigbogu, “Enhancing Email Security: A Hybrid Machine Learning Approach for Spam and Malware Detection,” *World J. Adv. Eng. Technol. Sci.*, vol. 12, no. 1, pp. 187–200, May 2024, doi: 10.30574/wjaets.2024.12.1.0160.