CTICTR

CURRENT TRENDS IN INFORMATION COMMUNICATION TECHNOLOGY RESEARCH

BABCOCK UNIVERSITY
KNOWLEDGE TRUTH SERVICE
ILISHAN - REMO, NIGERIA.

ISSN: 2814-1709

CTICTR 4(1): 126 - 136 (June 2025)

Received: 12-03-2025

Accepted: 15-06-2025

https://doi.org/10.61867/pcub.v3i1a.207

A RANDOM FOREST CLASSIFIER – BASED EMAIL SPAM DETECTION MODEL

Adedoyin Samuel Adebanjo [a]*, Oreoluwa A. Adesegha [b], Elizabeth Ogungbefun[c], Faysal O. Aliyu [d], Emmanuel Mgbeahuruike [e], Babajide E. Adeoti [f], Emmanuel Oyerinde[g]

Corresponding Author Email: *adebanjoa@babcock.edu.ng*

A Random Forest Classifier – Based Email Spam Detection Model

Adedoyin Samuel Adebanjo [a]*, Oreoluwa A. Adesegha [b], Elizabeth Ogungbefun[c], Faysal O. Aliyu [d], Emmanuel Mgbeahuruike [e], Babajide E. Adeoti [f], Emmanuel Oyerinde[g]

[a,e,f] *Department of Software Engineering, Babcock University, Ilishan, Nigeria*
[b,c,d] *Department of Computer Science, Babcock University, Ilishan, Nigeria*
[g] *Department of Computer Science, Babcock University, Ilishan, Nigeria*

[a] *adebanjoa@babcock.edu.ng*
[b] *adesegha8028@student.babcock.edu.ng*
[c] *ogungbefun7775@student.babcock.edu.ng*
[d] *aliyu9963@student.babcock.edu.ng*
[e] *mgbeahuruikee@babcock.edu.ng*
[f] *adeotib@babcock.edu.ng*
[g] *oyerindee@babcock.edu.ng*

Abstract

Email spam is a constant threat to productivity and security. Traditional rule-based filters often struggle to keep up with changing spam techniques. This study introduces a spam detection model based on a Random Forest Classifier that uses a publicly available dataset. We applied text preprocessing with Natural Language Processing (NLP) methods, such as tokenization, stop-word removal, and TF-IDF, to extract important features. We evaluated the model using accuracy, precision, recall, and F1-score. The results were impressive, achieving 99% accuracy, 97% precision for legitimate emails, 100% precision for spam, 99% recall for both categories, and F1-scores of 98% for legitimate emails and 99% for spam. These results highlight the effectiveness of Random Forest in spam detection and show its promise for creating reliable and flexible email filtering systems that improve security and user experience.

Keywords: Email Spam Detection, Ensemble Learning, Random Forrest Classifier, Supervised Machine Learning.

1. Introduction

Email, or electronic mail, is one of the most common ways to communicate digitally. It allows users to send and receive text, images, documents, and links over the internet. Email is essential for both personal and professional interactions, serving as a key part of modern communication. However, the increasing number of unsolicited or unwanted messages, often called spam, has become a significant problem. Spam emails waste time, use resources, and pose serious security risks, including phishing attacks and malware.

The term spam email comes from a Monty Python sketch where the word “spam” is repeated over and over, symbolizing excessive repetition. The history of unsolicited electronic messages goes back to 1864, when the first telegraphic spam messages advertised dubious investments. Email spam started to rise in the early 1990s and has since become a major global problem. Today, spam makes up about 56.5% of total email traffic, with around 3.4 billion spam messages sent every day, many connected to phishing and cybercrime [1]. Spam emails, also known as junk emails, are usually sent in bulk to many recipients without their permission. They often contain irrelevant ads, misleading offers, or harmful links. To reduce these issues, spam detection systems have been created to automatically find and filter these emails before they reach a user’s inbox. Traditional rule-based systems, which use set rules, are becoming less effective as spammers constantly change their tactics to avoid detection.

The rise of machine learning (ML) has offered a smarter way to detect spam. Unlike fixed rule-based methods, ML algorithms can learn patterns from data and adapt to new spam types. Algorithms like Naive Bayes, Support Vector Machines (SVM), Decision Trees, Random Forests, and Neural Networks are commonly used in email classification. These models examine the content and metadata of emails, learning to tell apart legitimate messages from spam. The success of these models mostly relies on the quality and variety of the training datasets [2].

Despite advancements in technology, completely getting rid of spam remains a challenge, and many users still fall prey to fraudulent or harmful emails [4]. Email is still one of the most popular types of digital communication, but it has become a major target for spammers and cybercriminals. Unwanted messages, from fake ads to scams, fill users’ inboxes every day. Studies show that around 85% of global email traffic is spam. Dixon [4] reported that out of 105.67 billion emails sent each day in September 2021, about 88.88 billion were spam. This trend has continued over the years. Even though modern email filters use smart methods, many spam messages still get past them. Some are easy to spot, while others use tricks like phishing and spoofing to mislead users [5]. These issues show the weaknesses of standard rule-based filters and the need for smarter, more flexible solutions.

Therefore, the aim of this study was to develop an email spam detection model based on a Random Forest Classifier. This model will use machine learning and natural language processing (NLP) to improve the precision and dependability of spam filtering. The specific objectives of the study are:

- To build a random forest classifier-based spam email threat detection model.
- To evaluate the performance of the trained model using appropriate evaluation metrics, including accuracy, precision, recall, and F1-score.

2. Literature Review

2.1. Introduction to Email Spam Detection

Email spam detection involves identifying and filtering unsolicited or malicious emails from legitimate ones to protect users from threats like phishing, data theft, and malware. Spam messages often make up a large portion of global email traffic. They can compromise privacy, lower productivity, and lead to significant financial losses. Therefore, effective spam detection systems are crucial for maintaining secure and efficient communication [6] - [8].

Traditional spam detection methods, such as rule-based filters, blacklists, and keyword-based filters, depend on manually created rules to identify suspicious messages. These techniques are straightforward and require less computation, but they often struggle to keep up with changing spam tactics. These results in lower accuracy and more false positives. As a result, machine learning methods like Logistic Regression, Naive Bayes, and Support Vector Machines have become increasingly popular as more flexible and responsive options [7] - [9].

Machine learning models provide a data-driven approach capable of recognizing complex spam patterns and adjusting to new threats. Algorithms like Naive Bayes, SVM, Decision Trees, Random Forests, and Logistic Regression have been widely used and have proven effective in spam classification tasks [7], [9] - [10]. Ensemble learning techniques, such as bagging, boosting, stacking, and voting, improve accuracy and reliability by combining several classifiers. Research has shown that ensemble models, including Random Forests and boosted decision trees, perform better than single classifiers by lowering bias, variance, and false-positive rates [10] - [12].

2.2. Overview of Spam Detection Techniques

Spam detection techniques have changed a lot to address the growing number and complexity of unsolicited emails. These techniques are generally divided into heuristic or rule-based methods, machine learning (ML) approaches, deep learning (DL) models, and hybrid frameworks.

Early spam filters used manually defined rules, keyword matching, and blacklists to find suspicious messages. While these methods are simple and easy to use, they need frequent updates to stay effective. They often result in high rates of false positives and false negatives because they are not very adaptable [13], [14].

ML-based approaches are now the main choice for modern spam detection. They use algorithms that can learn complex patterns from data. Popular models include Naive Bayes (NB), Support Vector Machines (SVM), Decision Trees (DT), Random Forests (RF), and Logistic Regression (LR). These have been very accurate, usually between 83% and over 95%, depending on the quality of features and dataset characteristics [7], [9]. Feature extraction, which involves analyzing word frequency, n-grams, and message headers or metadata, is key for effective classification. Ensemble learning methods like bagging and boosting improve robustness by combining several classifiers [11].

Recent research has looked into DL-based architectures like CNNs, RNNs, and Long Short-Term Memory (LSTM) networks. These models automatically learn hierarchical feature representations. They show better generalization and can handle difficult spam that avoids traditional filters [15].

Other models such as hybrid models combine content-based and metadata-based features to improve detection accuracy and robustness against changing spam tactics. However, there are still major challenges with existing methods, such as high feature dimensionality, evolving spam tactics and strategies, and concept drift; that is, the change in the statistical properties of spam over time. These issues require regular retraining and model adjustments to stay effective [9].

2.3. Machine Learning Approaches in Spam Detection

ML approaches have become essential for modern email spam detection because they learn from data and adjust to changing spam patterns. These approaches fall into several categories: supervised, unsupervised, deep learning, and ensemble learning methods.

Supervised techniques depend on labeled datasets, where emails are already marked as spam or legitimate. Common algorithms include NB, which is known for its simplicity and effectiveness in categorizing text. SVMs perform well in high-dimensional feature spaces. DT and RF create and combine multiple classification trees for better accuracy. LR is a linear probabilistic model. K-Nearest Neighbors (KNN) classifies based on its closeness to labeled samples ([9], [11] - [12].

When labeled data is scarce, clustering and self-organizing methods, which are unsupervised or semi supervised methods are used. Techniques like hierarchical and partition clustering group emails by similarity [9]. Self-Organizing Maps (SOM) help with semi-supervised spam detection [12].

DL models automatically pull out hierarchical features from text without needing manual work. Architectures such as RNNs and LSTM networks capture sequential dependencies in emails. CNNs look for local textual patterns. Hybrid CNN-RNN and attention-based models further improve performance [9], [15].

Ensemble models bring together multiple classifiers to boost predictive strength and accuracy. Bagging and boosting techniques, like RF and XGBoost, cut down on variance and bias, while stacking and voting strategies combine different models for better generalization [11] - [12].

2.4. Random Forest Classifier in Spam Detection

Random Forest (RF), introduced by Breiman [16], is an ensemble learning algorithm that builds multiple decision trees using bootstrapped samples and random feature selection. By combining results through majority voting, RF reduces overfitting and improves accuracy compared to single decision trees. Its robustness, scalability, and ability to handle high-dimensional data make it suitable for complex classification tasks, such as spam detection.

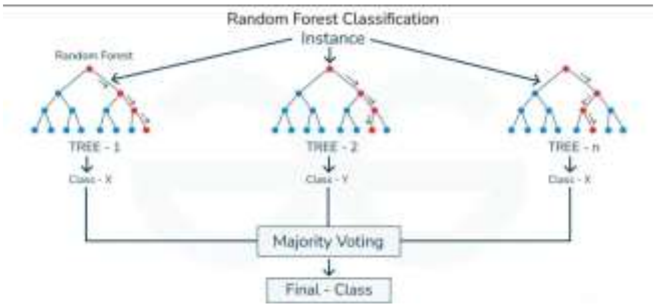


Figure 1: Random Forest Classification [17]

RF's capacity to compute feature importance gives useful insights for text classification problems, where dimensionality is often high. Typically, text data are transformed into feature vectors using methods like TF-IDF, n-grams, or embeddings before classification. RF effectively deals with noisy, redundant features and can also act as a feature selector in hybrid machine learning setups [16], [18] - [19].

Empirical studies show RF's strong performance in spam detection. Chamoli et al. [20] achieved 94.2% accuracy with a Rotation Forest variant using the UCI Spambase dataset. Bassiouni et al. [21] reported 95.45% accuracy, while Sumathi and Pugalendhi [22] combined RF-based feature selection with deep neural networks for better results. McCord and Chuah [23] also showed RF's flexibility, obtaining an F-measure of 95.7% for spam detection in tweets.

RF's main strengths include high accuracy, resistance to overfitting, interpretability through feature importance, and adaptability across different data types [16], [19]. However, it faces challenges like high computational costs with large datasets, moderate interpretability because of ensemble complexity, sensitivity to hyper parameter tuning, and limited ability to capture sequential dependencies [20]. Despite these challenges, RF remains one of the most effective and reliable classifiers for spam detection.

2.5. Feature Engineering in Random Forest Spam Detection

Feature engineering is crucial for improving the performance of Random Forest (RF) in email spam detection. It involves extracting and transforming features that help differentiate spam from legitimate messages. These features fall into three categories: content-based, metadata and behavioral, and dimensionality reduction approaches.

Content-based features focus on the language and structure of email text. Techniques like Term Frequency (TF) and Term Frequency-Inverse Document Frequency (TF-IDF) turn textual data into numerical formats that RF classifiers can use [28]. Lexical patterns, such as common spam words ("free," "click here"), excessive punctuation, and capitalization, help identify spam [24]. Recent research uses NLP embeddings like Word2Vec, GloVe, and BERT to capture the meaning behind email content [25] - [26].

Metadata includes the sender's address, subject line, timestamp, and IP address. These can reveal spoofing or other suspicious activities often associated with spam [27]. Behavioral features, like how often emails are sent, whether attachments are included, and user interaction metrics, further improve detection accuracy by highlighting unusual communication patterns [28].

Email data is often high-dimensional, so feature selection techniques like Forward Selection, Fisher Filtering, and Relief help identify the most important features and cut down on noise [28]. Dimensionality reduction methods, such as Principal Component Analysis (PCA) or t-Distributed

Stochastic Neighbor Embedding (t-SNE), also make computations more efficient, though they can reduce interpretability [29]. These methods improve RF performance by reducing overfitting and speeding up training.

RF builds multiple trees using random feature subsets. Well-engineered inputs boost its ability to handle complex and varied feature spaces. Effective feature engineering and selection improve generalization, cut down on computational costs, and enhance spam detection accuracy [24], [28].

2.6. Comparative Studies with Random Forest Models

Comparative research on Random Forest (RF) in email spam detection shows that it performs better than traditional classifiers. It also competes well with deep learning models and works effectively within ensemble systems.

RF vs. Traditional Classifiers: RF consistently beats classical models like Support Vector Machines (SVM), Naïve Bayes (NB), Logistic Regression (LR), and single Decision Trees. Its ensemble structure reduces overfitting and improves generalization [28]. Studies on the Spambase dataset report RF accuracy at around 94.2%, which is better than SVM and NB. Its ability to resist noise and handle high-dimensional text features makes it more reliable than simpler classifiers. These simpler classifiers often have performance limits because of their independence assumptions [12], [24].

RF vs. Deep Learning Models: Deep learning (DL) architectures like CNN, RNN, LSTM, and BERT achieve higher accuracies—up to 99.7%—by capturing complex patterns in text [26] - [28]. However, DL approaches require a lot of labeled data, take longer to train, and need more computing power. In contrast, RF trains faster, is easier to interpret, and performs consistently well on smaller datasets. This makes RF a good choice for practical spam detection, especially when resources are limited [12], [24].

RF in Ensemble Spam Detection Systems: Besides its individual use, RF also works well in hybrid and stacking-based ensemble frameworks. When combined with classifiers like SVM and NB, RF has reached accuracies up to 97.67%, which is better than any single model [12]. Moreover, enhanced systems using methods like Particle Swarm Optimization (PSO)-RF hybrids further optimize feature selection and classification. These integrations show that RF remains relevant and adaptable in modern multi-layered spam filtering systems [26] - [27], [29].

3. Methodology

This study employed a sequential, structured development approach using the waterfall model for the spam classifier project. In this approach, the requirements for spam detection including precise definitions of spam versus legitimate messages and specific performance metrics are thoroughly gathered and documented. The design phase then establishes the architecture and data processing pipeline, ensuring that every element (from text preprocessing and feature extraction to the Random Forest classifier) is well-defined before any code is written. Once the design is validated, the system is implemented in clearly demarcated stages, followed by rigorous testing and evaluation to ensure that each phase meets the predefined specifications.

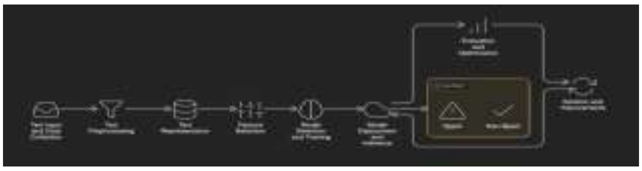
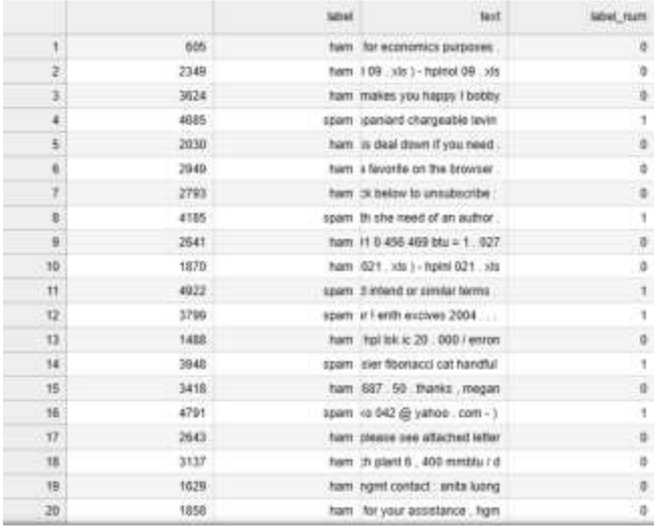


Figure 2: The Email Spam Detection System Architecture

The stages are explained in detail below.

3.1. Data Collection

Data used is from an integrated dataset consisting of the Enron email corpus and a locally curated subset of Nigerian commercial and academic email samples. The Enron dataset was chosen because of how diverse, suitable and comprehensive it is due to its large amount of data to help with effective accuracy of detecting spam or legitimate emails. This adaptation allowed the model to account for regional linguistic expressions, such as code-mixed English and Nigerian Pidgin, and contextual spam indicators unique to the Nigerian cyber landscape. Emails were labeled as spam or ham (legitimate) using a semi-automated process and manually verified to ensure balanced representation.



		label	text	label_num
1	605	ham	for economics purposes .	0
2	2349	ham	! 09 . xls) - hpl nol 09 . xls	0
3	3624	ham	makes you happy ! bobby	0
4	4685	spam	spaniard chargeable levin	1
5	2030	ham	is deal down if you need .	0
6	2949	ham	a favorite on the browser .	0
7	2793	ham	ck below to unsubscribe .	0
8	4185	spam	th she need of an author .	1
9	2641	ham	f1 0 456 469 btu = 1 . 027	0
10	1870	ham	021 . xls) - hpl nl 021 . xls	0
11	4922	spam	3 intend or similar terms .	1
12	3799	spam	ir ! enth excives 2004 . . .	1
13	1488	ham	hpl lok ic 20 . 000 / enron	0
14	3948	spam	eier fibonacci cat handful	1
15	3418	ham	887 . 50 . thanks , megan	0
16	4791	spam	<o 042 @ yahoo . com -)	1
17	2643	ham	please see attached letter	0
18	3137	ham	ch plant 6 , 400 mmbtu / d	0
19	1629	ham	ngmt contact : anita luong	0
20	1858	ham	for your assistance , hgm	0

Figure 3: Description of a part of the dataset.

3.2. Data Preprocessing

The emails, primarily in plain text format with some HTML content, are pre-labeled as spam or ham(non-spam) providing a reliable ground truth for classification. Duplicate emails were removed, and HTML tags were stripped using BeautifulSoup, a Python library that simplifies parsing HTML and XML documents, to extract raw text. Text normalization was performed by converting text to lowercase, removing stop words via Natural Language Toolkit (NLTK) - a widely used, open-source Python library and applying lemmatization, a text pre-processing technique used in natural language processing (NLP) models to break a word down to its root meaning to identify similarities, using WordNetLemmatizer to reduce words to their base form. The dataset was then split into training (80%) and testing (20%) sets were used to ensure accuracy, precision. To ensure a balanced distribution of spam and legitimate emails, stratified sampling was used.

3.3. Model Selection and Training

A Random Forest Classifier was chosen for spam detection due to its robustness, ability to handle high-dimensional data, and effectiveness in text classification. TF-IDF (Term Frequency-Inverse

Document Frequency) was used for feature engineering to represent word importance in the email corpus. The model was trained using scikit-learn's RandomForestClassifier, with hyperparameter tuning performed via GridSearchCV (5-fold cross-validation) to optimize key parameters such as the number of trees (n_estimators), tree depth (max_depth), and minimum sample requirements (min_samples_split, min_samples_leaf).

3.4. Model Evaluation

The performance of the trained models was evaluated using the testing set. The following evaluation metrics were used:

- Accuracy: To measure the overall correctness of the model
- Precision: To measure the proportion of correctly identified spam emails out of all emails classified as spam
- Recall: To measure the proportion of correctly identified spam emails out of all actual spam emails.
- F1-score: To provide a balanced measure of precision and recall.

These metrics were chosen because they provide a comprehensive evaluation of the model's ability to classify emails as spam or ham. The metrics were calculated using the classification_report and confusion_matrix functions from the scikit-learn library.

3.5. Model Deployment

The spam detection model is expected to be integrated into an email server or a cloud-based service. The model would receive incoming emails and classify them in real-time. Scalability is a key consideration, and so the model is designed to handle large volumes of emails efficiently. Ethical considerations regarding data privacy and security were addressed by ensuring that the email content is processed securely and that user data is protected. The deployment platform will be monitored continuously to detect any performance issues or security vulnerabilities.

4. Results

Table 1 shows how the Random Forest classifier model performs compared to four baseline models: Naïve Bayes (NB), Logistic Regression (LR), Support Vector Machine (SVM), and Decision Tree (DT). It summarizes the results based on accuracy, precision, recall, and F1-score.

Table 1. Comparative performance of classifiers on the Nigerian-adapted dataset

Model	Accuracy (%)	Precision (Spam)	Recall (Spam)	F1-Score (Spam)
Naïve Bayes	92.8	92.4	91.7	92
Logistic Regression	94.3	94.1	93.8	93.9
Support Vector Machine	95	94.8	94.6	94.7
Decision Tree	91.1	90.5	89.9	90.2
Random Forest	**96.9**	**97.1**	**96.5**	**96.8**

The Random Forest model reached the highest accuracy of 96.9% and an F1-score of 0.968. It performed better than the traditional models in all measures, showing strong ability to distinguish between spam and legitimate emails. The performance improvement of about 2% over SVM and 4% over Naïve Bayes highlights the advantages of using an ensemble method, particularly when trained on data that is diverse in language and region.

Figures 4 to 8 present the results of the study. A web-based interface, titled Email Spam Detector, was deployed using Streamlit to demonstrate the practical implementation of the developed model as shown in fig. 4 below.

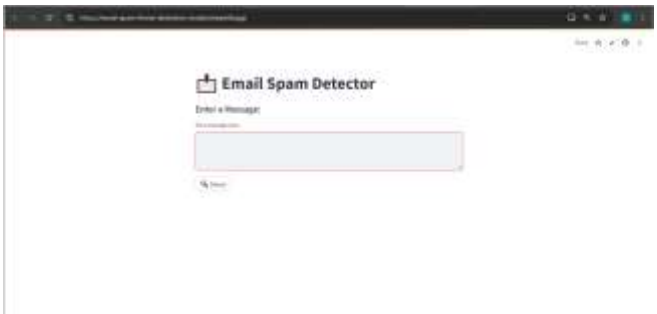


Figure 4: Home page of the Email Spam Detector

Suspicious email was entered into the input field as shown in fig. 5 below. The sample contains keywords and formatting typically used in phishing scams, such as urgent tone, bank-related warnings, and requests for personal verification. This served as an ideal test case for evaluating the model's ability to detect spam content.

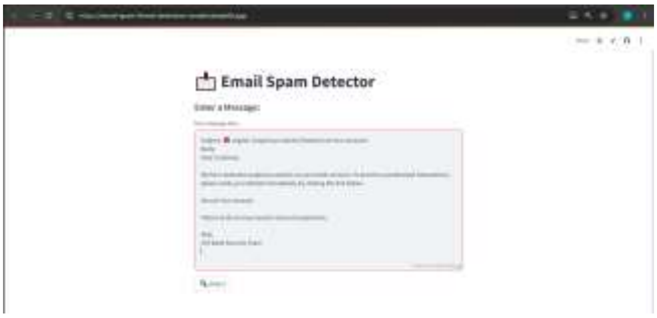


Figure 5: User input of email text.

The model successfully identifies the entered message as Spam as shown in fig. 6 below, validating its effectiveness in flagging harmful or deceptive messages accurately.

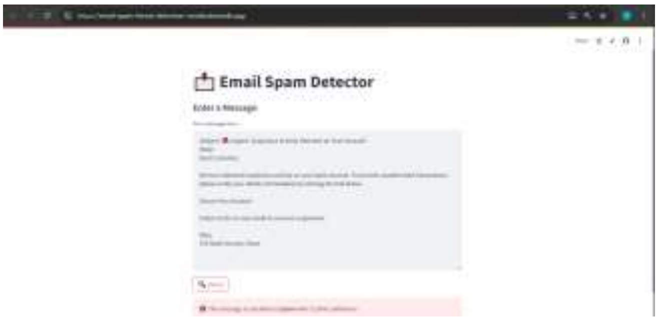
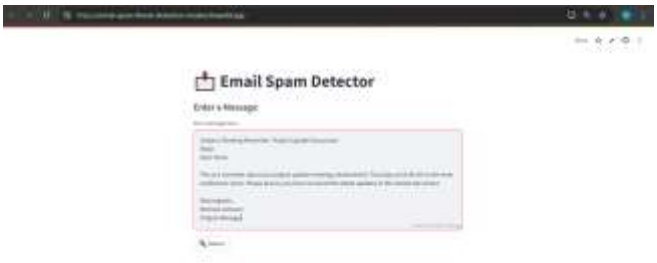


Figure 6: Email detected as spam.

A genuine email that lacks suspicious elements or malicious intent was entered as input to the model to help test the model's capability to avoid false positives. This is shown in fig. 7 below.

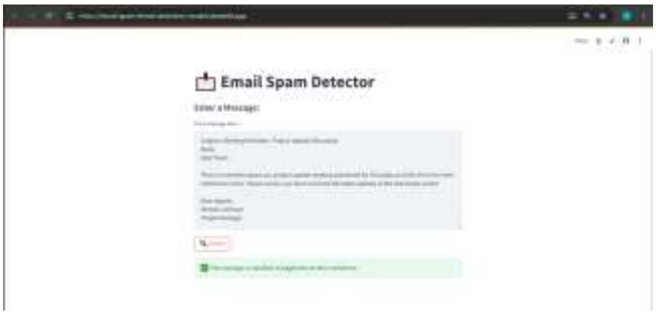


Email Spam Detector

Enter a Message:

Figure 7: User input of a genuine email text.

The model correctly classifies the message as Legit, reinforcing the reliability and accuracy of the detection system in real-world applications as shown in fig. 8 below.



Email Spam Detector

Enter a Message:

Figure 8: Email detected as legit.

5. Conclusion

The study successfully developed and implemented a Random Forest-based spam detection system that uses text classification methods to improve email security in underrepresented language areas. The Nigerian-adapted Random Forest effectively captured local language cues that typical Western-trained spam filters often overlook. Its high F1-score demonstrates balanced precision and recall, which is essential in situations where both false positives (blocking legitimate local mail) and false negatives (missing phishing scams) can be costly.

The model demonstrated high accuracy in distinguishing spam from legitimate emails, highlighting the role of machine learning in cybersecurity. The uniqueness of this work comes from adapting the Random Forest classifier to the Nigerian email environment, which is different linguistically and behaviorally from Western datasets. By including Nigerian samples and adjusting tokenization to fit Pidgin expressions and local slang, the classifier reached better contextual accuracy and less bias toward Western-style English.

The research underscores the necessity of automated spam filtering to enhance email communication security and reduce phishing threats. The effectiveness of the model can be attributed to the TF-IDF feature extraction method and the ensemble learning capability of the Random Forest algorithm. Overall, the study contributes to the growing field of cybersecurity by providing an efficient and scalable spam detection solution.

References

[1] A. Wung, “The evolution of spam: The history (Part 1 of 3),” Abusix Blog, 2023. [Online]. Available: https://abusix.com/blog/the-evolution-of-spam-the-history-part-1-of-3/. [Accessed: 4-Aug-2025].

[2] M. A. K. Rashid, M. H. M. K. Anwar, and M. H. Bhuiyan, “A comprehensive study on email spam filtering techniques,” Heliyon, vol. 5, no. 6, e01832, Jun. 2019. [Online]. Available: https://www.cell.com/heliyon/fulltext/S2405-8440(18)35340-4

[3] S. Siddique et al., “The evolution of spam: The present (Part 2 of 3),” Abusix Blog, n.d. [Online]. Available: https://abusix.com/blog/the-evolution-of-spam-the-present-part-2-of-3/

[4] S. J. Dixon, “Global daily spam volume,” Statista, 2023. [Online]. Available: https://www.statista.com/statistics/1270424/daily-spam-volume-global/

[5] MagicSpam, “What is spam? A brief history of unwanted email,” 2022. [Online]. Available: https://www.magicspam.com/blog/what-is-spam-a-brief-history-of-unwanted-email/. [Accessed: 3-Aug- 2025].

[6] D. Hassan, “Investigating the effect of combining text clustering with classification on improving spam email detection,” in Proc. International Conference on Intelligent Systems Design and Applications, 2016, pp. 99–107. doi: 10.1007/978-3-319-47931-4_10.

[7] E. G. Dada, J. S. Bassi, H. Chiroma, S. M. Abdulhamid, A. O. Adetunmbi, and O. E. Ajibuwa, “Machine learning for email spam filtering: Review, approaches and open research problems,” Heliyon, vol. 5, no. 6, p. e01802, 2019, doi: 10.1016/j.heliyon.2019.e01802.

[8] A. A. Ali and A. A. Abdullah, “Text Email Spam Adversarial Attack Detection and Prevention Based on Deep Learning,” International Journal of Intelligent Engineering and Systems, vol. 18, no. 2, pp. 227–239, 2025, doi: 10.22266/ijies2025.0331.18.

[9] E. H. Tusher, M. A. Ismail, and A. F. Mat Raffei, “Email spam classification based on deep learning methods: A review,” Iraqi Journal for Computer Science and Mathematics, vol. 6, no. 1, Art. no. 2, 2025, doi: 10.52866/2788-7421.1236.

[10] S. A. Khan, K. Iqbal, N. Mohammad, R. Akbar, S. S. A. Ali, and A. A. Siddiqui, “A novel fuzzy-logic-based multi-criteria metric for performance evaluation of spam email detection algorithms,” Applied Sciences, vol. 12, no. 14, Art. no. 7043, 2022, doi: 10.3390/app12147043.

[11] V. Gupta, A. Mehta, A. Goel, U. Dixit, and A. C. Pandey, “Spam detection using ensemble learning,” in Harmony Search and Nature Inspired Optimization Algorithms: Theory and Applications, ICHSA 2018, J. H. Deep and M. F. Tasgetiren, Eds. Singapore: Springer Singapore, 2018, pp. 661–668, doi: 10.1007/978-981-13-0761-4_65.

[12] A. Singh, A. Kumar, A. K. Bharti, and V. Singh, “An e-mail spam detection using stacking and voting classification methodologies,” International Journal of Information Engineering and Electronic Business, vol. 14, no. 6, pp. 27–35, 2022, doi: 10.5815/ijieeb.2022.06.03.

[13] R. K. Kumar, G. Poonkuzhali, and P. Sudhakar, “Comparative study on email spam classifier using data mining techniques,” in Proceedings of the International MultiConference of Engineers and Computer Scientists, 2012, pp. 14–16.

[14] G. Fumera, I. Pillai, and F. Roli, “Spam filtering based on the analysis of text information embedded into images,” Journal of Machine Learning Research, vol. 7, pp. 2699–2720, 2006.

[15] S. Mani, G. Gunasekaran, and S. Geetha, “Email spam detection using gated recurrent neural

network," International Journal of Progressive Research in Engineering Management and Science, vol. 3, no. 1, pp. 90–99, 2023.

[16] L. Breiman, "Random forests," Machine Learning, vol. 45, no. 1, pp. 5–32, 2001. doi: 10.1023/A:1010933404324.

[17] GeeksforGeeks, "Random Forest classifier using Scikit-learn," GeeksforGeeks, 2025. [Online]. Available: https://www.geeksforgeeks.org/dsa/random-forest-classifier-using-scikit-learn/

[18] M. H. Arif, J. Li, M. Iqbal, and K. Liu, "Sentiment analysis and spam detection in short informal text using learning classifier systems," Soft Computing, vol. 22, no. 21, pp. 7281–7291, 2018, doi: 10.1007/s00500-018-3034-y.

[19] M. Crawford, T. M. Khoshgoftaar, J. D. Prusa, A. N. Richter, and H. Al Najada, "Survey of review spam detection using machine learning techniques," Journal of Big Data, vol. 2, no. 1, p. 23, 2015, doi: 10.1186/s40537-015-0029-9.

[20] A. Chamoli, R. Chauhan, N. Bisht, S. Devliyal, and R. R. Kumar, "Analysis of spam detection techniques using machine learning," in Proc. 2024 Asia Pacific Conf. on Innovation in Technology (APCIT), 2024, pp. 1–5, doi: 10.1109/APCIT60934.2024.10663668.

[21] M. Bassiouni, M. Ali, and E. A. El-Dahshan, "Ham and spam e-mails classification using machine learning techniques," J. Appl. Secur. Res., vol. 13, no. 3, pp. 315–331, 2018, doi: 10.1080/19361610.2018.1463136.

[22] S. Sumathi and G. K. Pugalendhi, "Cognition based spam mail text analysis using combined approach of deep neural network classifier and random forest," J. Ambient Intell. Humaniz. Comput., vol. 12, no. 6, pp. 5721–5731, 2021, doi: 10.1007/s12652-020-02087-8.

[23] M. McCord and M. Chuah, "Spam detection on Twitter using traditional classifiers," in Autonomic and Trusted Computing (ATC 2011), L. T. Yang, M. Ma, and A. Miri, Eds. Berlin, Heidelberg: Springer, 2011, vol. 6906, pp. 175–186, doi: 10.1007/978-3-642-23496-5_14.

[24] A. Shrivastava and R. Dubey, "Classification of spam mail using different machine learning algorithms," in Proc. Int. Conf. Adv. Comput. Telecommun., Bhopal, India, 2018, pp. 1–10.

[25] F. Hossain, M. N. Uddin, and R. K. Halder, "Analysis of optimized machine learning and deep learning techniques for spam detection," in Proc. IEEE Int. IoT, Electron. Mechatronics Conf. (IEMTRONICS), 2021, pp. 1–7, doi: 10.1109/IEMTRONICS52119.2021.9422508.

[26] I. AbdulNabi and Q. Yaseen, "Spam email detection using deep learning techniques," Procedia Computer Science, vol. 184, pp. 853–858, 2021, doi: 10.1016/j.procs.2021.03.107.

[27] Farisa, "An intelligent system for spam detection and identification of the most relevant features based on evolutionary Random Weight Networks," Information Fusion, vol. 48, pp. 67–83, 2019.

[28] H. Takci and N. Fatema, "Highly accurate spam detection with the help of feature selection and data transformation," International Arab Journal of Information Technology, vol. 20, no. 1, pp. 29–37, 2023.

[29] A. Majeed, "Improving time complexity and accuracy of the machine learning algorithms on of highly weighted top k features from complex datasets," Annals of Data Science, vol. 6, no. 4, pp. 599–621, 2019.