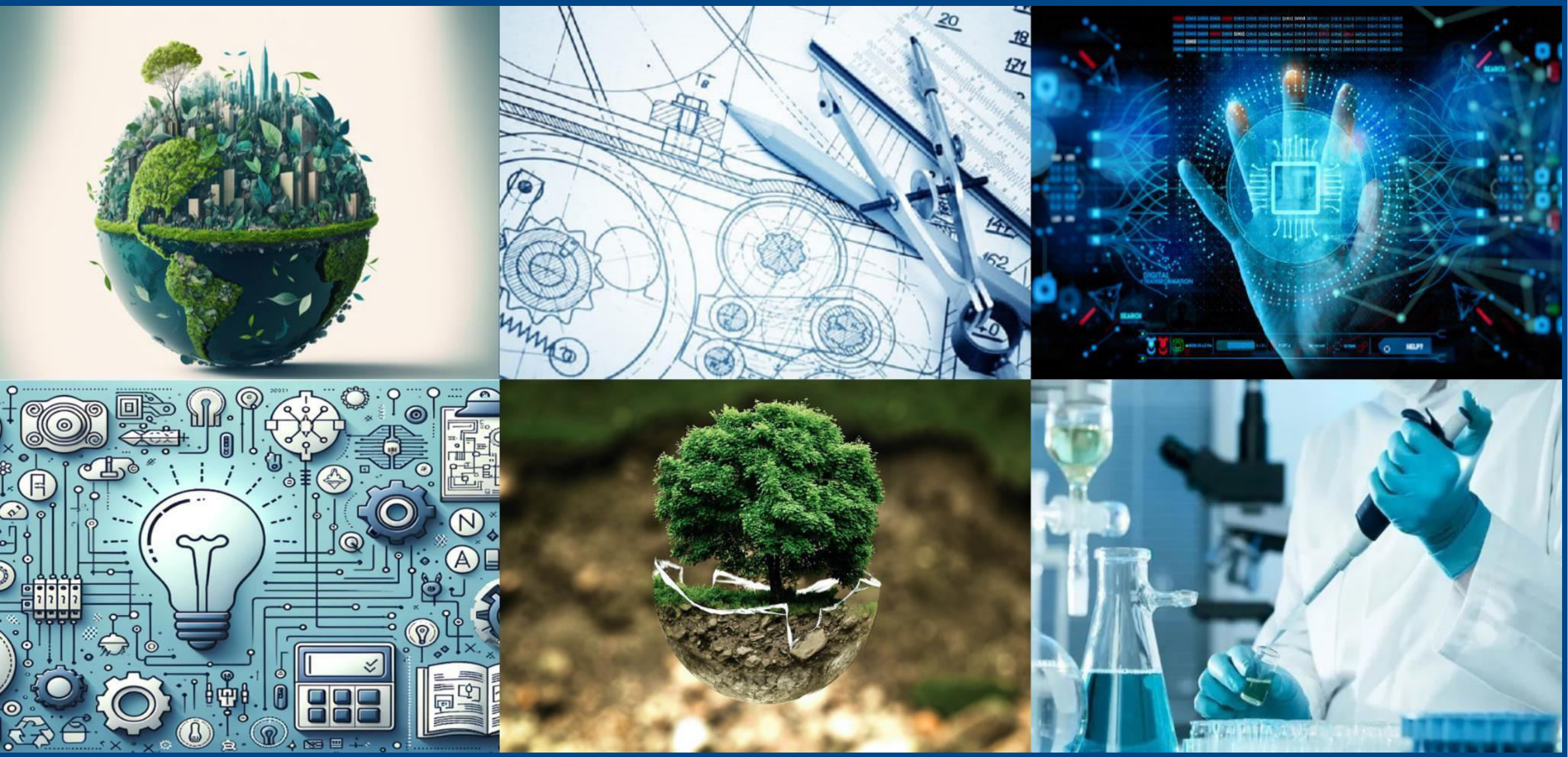
ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206

Volume 8, Issue 12, December 2025

© 2025 IJMRSET | Volume 8, Issue 12, December 2025| DOI:10.15680/IJMRSET.2025.0812029

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Email Spam Detection using Machine Learning Algorithm

Sahana G[1], Maheshwari M Desai[2]

PG Student, Dept. of MCA, City Engineering College, Bengaluru, India[1]

Assistant Professor, Dept. of MCA, City Engineering College, Bengaluru, India[2]

ABSTRACT: Electronic mail is a fundamental communication medium in modern personal, educational, and professional environments, yet it has become increasingly exposed to spam-related threats such as deceptive phishing attempts, malicious software delivery, financial exploitation, and intrusive promotional content. Conventional spam filtering systems depend on rigid rules and fixed keyword sets, which fail to respond effectively to the constantly evolving behaviour of spammers. In an effort tackle all of this work proposes an intelligent email spam identification model designed by machine learning technology. Natural Language Processing (NLP) is implemented in the framework.

Operations including token segmentation, removal of non-informative words, word normalization, and TF–IDF-based feature representation—to convert raw email messages into structured numerical vectors. A few examples of supervised learning algorithms, consist of Support Vector Machine (SVM), Logistic Regression, Naive Bayes, and Random Forest, are trained and evaluated for spam classification. Experimental findings confirm that machine learning-based approaches significantly enhance classification precision, adaptability, and durability as opposed with standard filtering mechanisms.

KEYWORDS: NLP, machine learning, with spam detection, Text Mining, TF-IDF, Supervised Classification

I. INTRODUCTION

Email continues to be among the most efficient and economical communication tools due to its rapid delivery and ease of access. However, the dramatic rise in spam emails has introduced critical challenges, including cyber fraud, identity misuse, phishing schemes, and the spread of malicious software. These unsolicited messages not only disrupt communication but also offer significant dangers to data privacy and system security. Conventional spam detection systems rely heavily on predefined rules and keyword-based filtering, which are increasingly ineffective as spammers frequently alter message structure and vocabulary to avoid detection. To address these limitations, machine learning-driven spam detection solutions have emerged as a highly valuable alternative. These systems have the ability to create intricate patterns from previous email data and dynamically adapting to new spam trends without requiring continuous manual intervention. This project aims to develop a supervised machine learning-based email spam detection framework that improves detection accuracy, scalability, and system robustness. By integrating NLP techniques with statistical learning models, the proposed system efficiently classifies emails into spam and legitimate categories.

II. LITERATURE SURVEY

1. Title: A Comparison connected to the Classification of Models for Machine Learning Email Spam
Writers: A.Chatterjee, R.Kumar, and S. Sharma
Abstract: This study evaluates Support Vector, Decision Trees, and Naive Bayes Machines, among other examples of typical machine learning methods Logistic Regression to identify spam. Experimental results on public datasets show that SVM gives higher accuracy, even though naive Bayes is still useful for real-time filtering due to its low processing cost.

2. Title: Intelligent The Use of Deep Learning for the Detection of Spam Emails Framework
Writers: M.Verma and A.Gupta

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Abstract: For automated spam email classification, the authors look at CNN and LSTM networks. By capturing semantic text representations, models for deep learning perform greater efficiency than conventional methods.

3. Title: Improved Email Spam Filtering Using a Hybrid Ensemble Method
Writers: R.Banerjee and K.Singh
Abstract: This work proposes a hybrid ensemble that includes Random Forest, Gradient Boosting, and AdaBoost. When compared to individual classifiers, the ensemble improves robustness and reduces false positives.

4.Title: Enhanced Feature Engineering Methods for Spam Email Identification
Writers: R.Nair and P.Das
Abstract: This work proposes a hybrid ensemble that combines Random Forest, Gradient Boosting, and AdaBoost. When compared to a single classifier, the ensemble improves robustness and reduces false positives.

5.Title: Machine Learning-Based Real-Time Spam Classification on Cloud Platforms
Writers: S.Rodrigues and L.Menon
Abstract: The main emphasis of this study is the application of ML-based spam filters in cloud systems. The system effectively handles massive email volumes by utilising scalable designs. Cloud-deployed Random Forest models provide high throughput and low latency.

6.Title: Comparative Assessment of Probabilistic Spam Detection Algorithms
Writers: J.D'Souza and R.Thomas
Abstract: This study examines probabilistic classifiers such as multinomial models, Bayesian nets, and Naïve Bayes. Multinomial Naive Bayes shows its suitability for email classification applications by providing the highest precision for text-rich datasets.

III. METHODOLOGY

3.1 Existing Problem:

Traditional email spam filtering approaches primarily depend on static rule sets and keyword-based matching techniques. These methods require manually curated rules and predefined spam vocabularies, making them rigid and unable to respond effectively to newly emerging spam strategies. Consequently, such systems often experience increased Negative results and fake positives rates. Moreover, The requirement for regular manual updating significantly impacts scalability and long-term maintenance.

3.2 Proposed Solution:

The proposed solution applies supervised machine learning algorithms in combination with NLP-based text processing to automatically differentiate spam emails from legitimate ones. Unlike conventional filtering methods, the system learns from labelled email datasets and continuously improves classification accuracy as new data becomes available. Email messages are pre-processed and transformed into feature vectors using numbers using TF-IDF representation, which serve as inputs for training classification models.

3.3 Proposed Methodology:

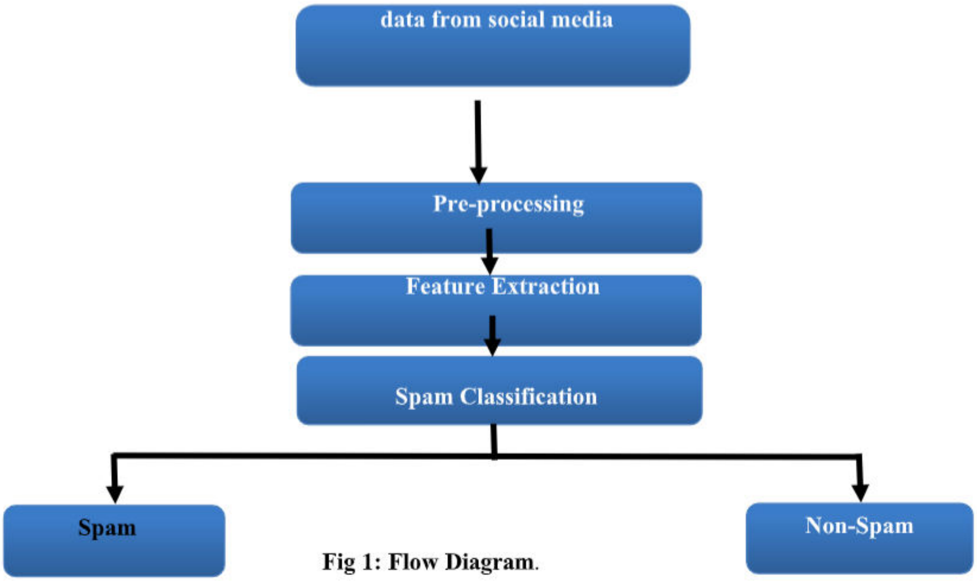


Fig 1: Flow Diagram.

IV. SYSTEM DESIGN

The system design illustrates the coordinated functioning of multiple modules involved in spam detection. Incoming emails from datasets or user inboxes are first passed through a preprocessing unit, where relevant features are extracted. Following that, these traits are examined. by trained machine learning classifiers to ascertain the nature of the email. The final classification decision is communicated to the user. The learning-based design enables continuous improvement, scalability, and enhanced detection accuracy over time.

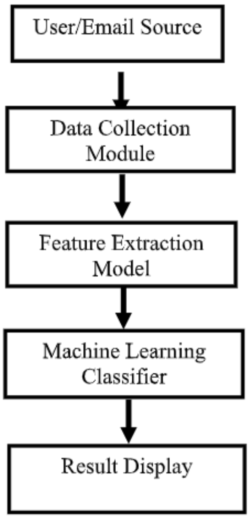


Fig 2: System Design

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

V. SYSTEM ARCHITECTURE & DESIGN

The architecture is structured around two principal entities: users and administrators. Users are responsible for sending emails, accessing inbox and spam folders, and labelling emails when required. Administrators oversee dataset management, model training, and performance monitoring. This architecture supports iterative learning and systematic evaluation to effectively address newly emerging spam patterns.

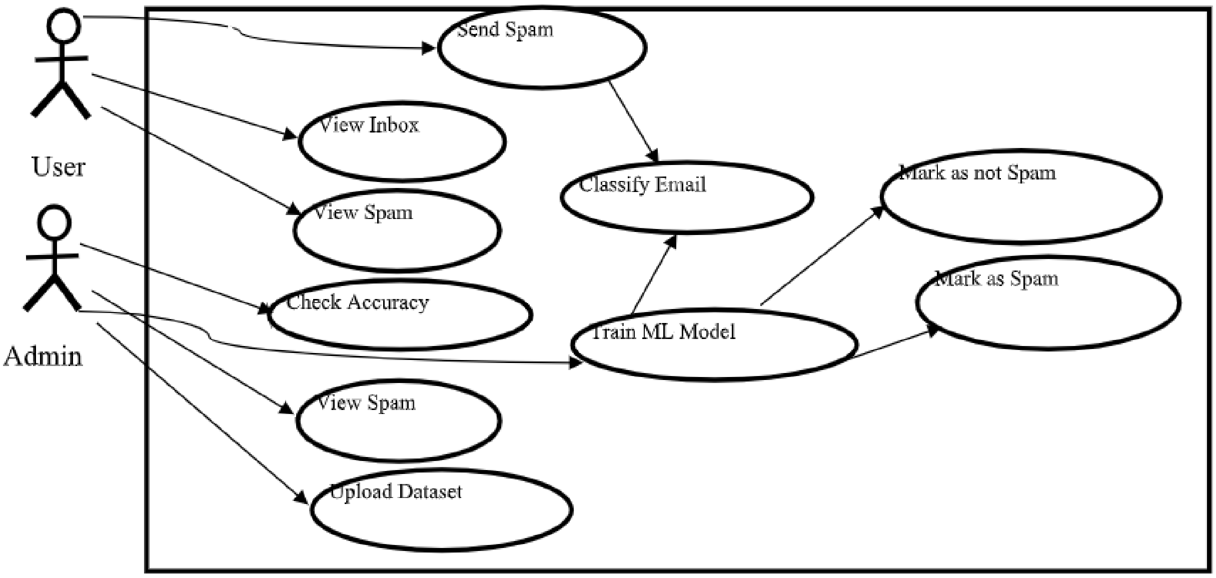


Fig 3: UML Diagram

VI. IMPLEMENTATION

The email spam detection model is implemented as a supervised binary classification system, categorizing emails into spam and non-spam classes. A labelled dataset containing email content and corresponding class annotations is used for both training and evaluation. The implementation begins with extensive text preprocessing, including the removal of punctuation, numerical characters, and irrelevant tokens, followed by stemming or lemmatization to normalize word forms.

TF-IDF is utilized for feature extraction to emphasize words that are extremely pertinent within individual emails but less common across the dataset. These feature vectors are then supplied to artificial intelligence classifiers like Random, Naive Bayes, SVM, and Logistic Regression Forest.Among these models, Naive Bayes demonstrates strong efficiency due to Its ease of use and efficiency in handling text-based data.

VII. RESULT & DISCUSSION

The results of the experiment show that the proposed machine learning-based spam detection system performs reliably in distinguishing spam from legitimate emails. The Naïve Bayes classifier shows particularly strong results by accurately identifying messages containing promotional language, suspicious hyperlinks, and repetitive textual patterns. Performance indicators such as F1-score, recall, accuracy, and precision reflect a balanced classification capability. High recall values confirm effective spam capture, while low frequencies of false positives Make sure minimal misclassification of genuine emails. Certain inaccuracies are observed in emails containing ambiguous content, highlighting potential locations for improvement in the future.

VIII. CONCLUSION

This study presents a highly effective email spam detection framework utilizing machine learning techniques. By applying NLP-based preprocessing and TF-IDF feature representation, unstructured email content is successfully converted into meaningful numerical features suitable for classification. Supervised learning algorithms, particularly Naive Bayes, achieve accurate spam detection with minimal computational complexity. The experimental findings show that the suggested strategy works noticeably better than conventional rule-based filtering systems and adapts effectively to evolving spam behaviours. Although minor challenges persist in handling ambiguous emails, the system proves to be a reliable and practical solution for strengthening email security.

REFERENCES

[1] Mst. U. Ayman et al., “A comprehensive approach to identify scam emails using Machine Learning algorithms,” IEEE CS BDC Symposium, 2024.
[2] A. Alam et al., “SHRED: An Ensemble-Based Machine Learning Model to Sift Email Messages for Real-Time Spam Detection,” Access to IEEE, vol. 13, 2025.
[3] R. S. and V. Rathinasamy, “Machine Learning-Based Email Spam Detection” and Vectorization,” ICCCNT, 2024.
[4] A. Tazwar et al., “Enhancing Spam Email Detection with a Soft Voting Ensemble,” IEEE COMPAS, 2024.
[5] M. Bansal and R. Saha, “Machine Learning-Based Spam Detection: A CRISP-DM Approach,” IEEE INDICON, 2024.
[6] O. Tonkal and R. Kocaoglu, “Multimodal Spam Email Classification Using DistilBERT,” Electronics, vol. 14, no. 19, 2025.

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com