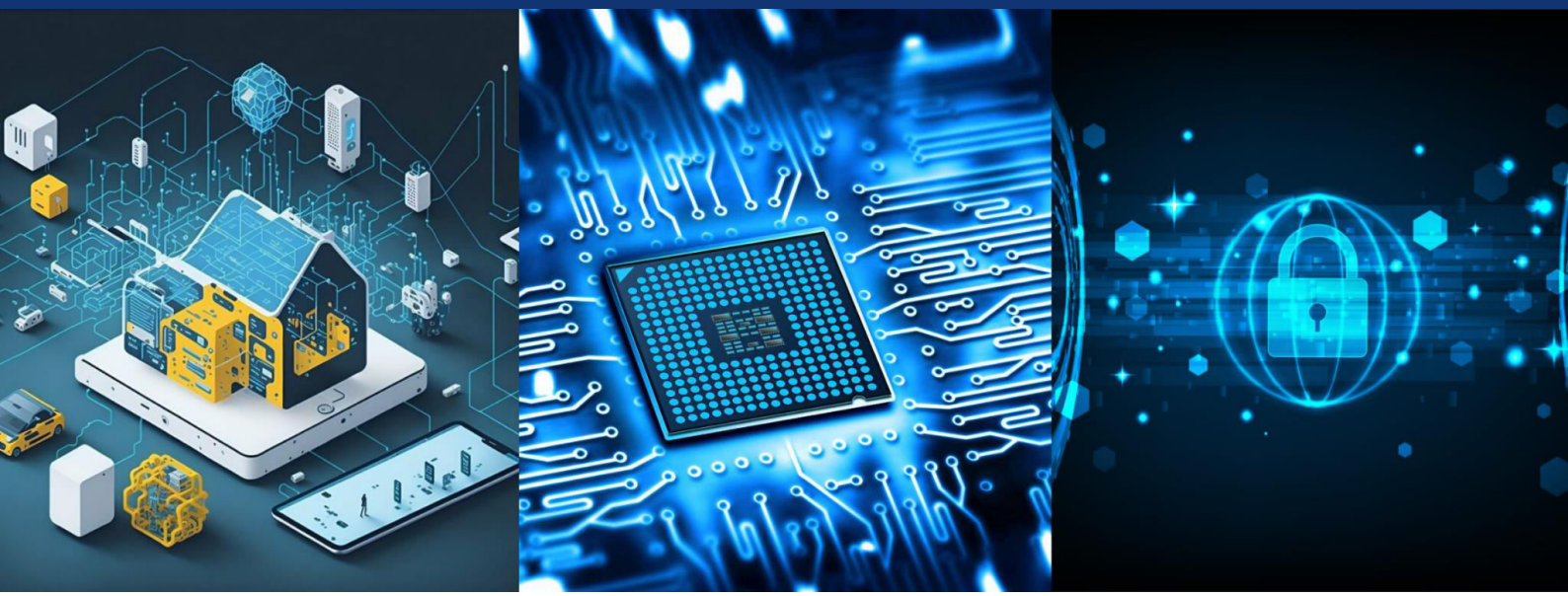
IJIRCCE

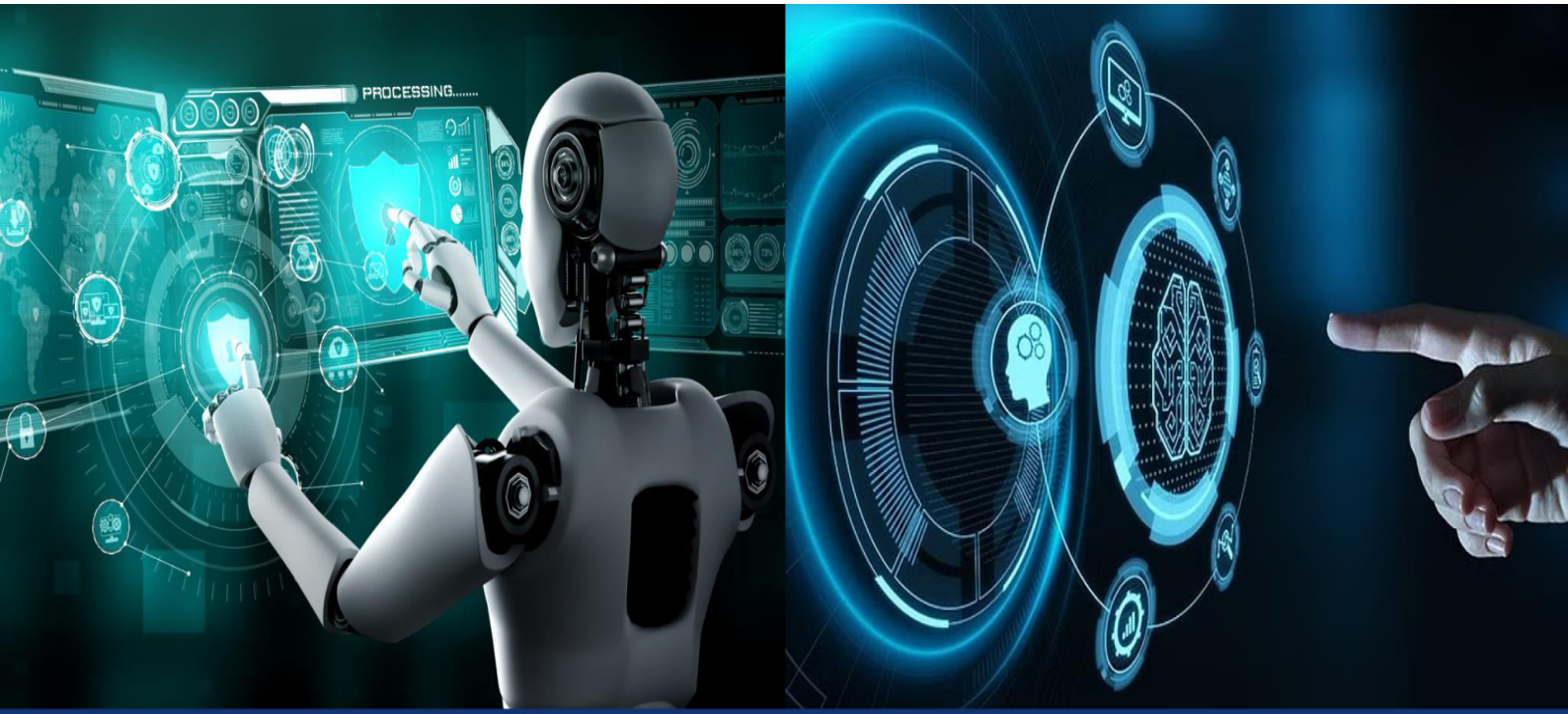
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

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



Impact Factor: 8.771

Volume 13, Issue 3, March 2025

© 2025 IJIRCCE | Volume 13, Issue 3, March 2025| DOI: 10.15680/IJIRCCE.2025.1303016

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

Email Spam Detection using Machine Learning

Jyoti Patil[1], Radhika Patil[2], Vedanti Kole[3], Sanjana Relekar[4], Prof. M. A. Pardesi[5]

UG Students, Dept. of CSE., D. Y. Patil College of Engineering and Technology, Kolhapur, Maharashtra, India [1,2,3,4]

Associate Professor, Dept. of CSE., D. Y. Patil College of Engineering and Technology, Kolhapur, Maharashtra, India[5]

ABSTRACT: Email spam detection is a crucial component of cybersecurity, designed to protect users from unwanted and potentially harmful content. This project focuses on developing a machine learning-based solution to accurately classify emails as spam or non-spam. Leveraging a combination of natural language processing (NLP) techniques and machine learning algorithms, the proposed system preprocesses and analyzes email text to identify patterns indicative of spam. The project employs Python as the primary programming language, utilizing libraries such as Scikit-Learn for model training, Pandas for data manipulation, and NLTK for text preprocessing. Additionally, the model's performance is enhanced through various feature extraction methods, including tokenization, stemming, and lemmatization, coupled with techniques to handle imbalanced datasets. The end goal is to build a robust and scalable spam detection model that can be filter out spam emails, thereby improving user experience and security. Experimental results demonstrate the model's effectiveness, showcasing high accuracy and efficiency in identifying spam across diverse datasets.

KEYWORDS: Spam Detection, Machine Learning, Natural Language Processing, Email Classification, Feature Extraction

I. INTRODUCTION

Email spam has become a significant problem in today's digital age, posing challenges for individuals, businesses, and organizations alike. Spam emails are unsolicited messages that flood inboxes, wasting valuable time and resources while potentially exposing users to malicious content or scams.

Machine learning algorithms can learn from labelled email datasets to build models capable of recognizing patterns indicative of spam. These models can then be used to automatically classify new, unseen emails. By analysing various email attributes such as sender information, subject line, content, and embedded URLs, machine learning algorithms can identify spam characteristics and make accurate predictions. There are several machine learning techniques commonly employed for email spam detection. These include Naive Bayes, Support Vector Machines (SVM), Decision Trees, Random Forests, and Neural Networks. These algorithms can be trained on labelled datasets, allowing them to learn the underlying patterns and relationships between spam and non-spam emails. The success of email spam detection using machine learning heavily relies on the quality and diversity of the training data.

II. RELATED WORK

Email spam detection has been widely researched using various machine learning and natural language processing (NLP) techniques. Traditional rule-based methods relied on keyword filtering and blacklists but proved ineffective against evolving spam tactics. Machine learning models, such as Naïve Bayes, Support Vector Machines (SVM), Random Forest, and Deep Learning approaches, have significantly improved accuracy in spam classification. Researchers have explored feature extraction techniques like TF-IDF, Bag of Words (BoW), and word embeddings to enhance text representation. Additionally, preprocessing techniques such as tokenization, stemming, and lemmatization improve model performance. Addressing imbalanced datasets using oversampling and under sampling has also been a key focus. Recent studies incorporate neural networks and transformer-based models like BERT for improved detection. The integration of real-time spam filtering and adaptive learning mechanisms remains an ongoing area of research to enhance efficiency and accuracy.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

III. PROPOSED SYSTEM

A. Technology Stack and Core Features:

- Developed using Python with libraries like Scikit-Learn, NLTK, Pandas, and TensorFlow.
- Uses Natural Language Processing (NLP) for email text analysis.
- Implements machine learning models (Naïve Bayes, SVM, Random Forest, BERT) for classification.
- Handles email metadata, links, and attachments for improved spam detection.
- Includes a user-friendly interface for email classification and visualization.

B. Learning Methodology and Detection Approach:

The system follows a structured approach for spam classification, involving preprocessing, feature extraction, model training, and evaluation.

Step 1: Email Preprocessing and Feature Extraction

- Remove stop words, special characters, and HTML tags from email text.
- Extract TF-IDF, n-grams, word embeddings, and email metadata features.
- Apply tokenization, stemming, and lemmatization for text normalization.

Step 2: Machine Learning Model Selection and Training

- Train models using labeled datasets (spam vs. non-spam).
- Use Naïve Bayes for probabilistic classification and deep learning (BERT) for contextual analysis.
- Optimize models through hyperparameter tuning and cross-validation.

Step 3: Spam Detection and Evaluation

- Classify incoming emails based on probability scores.
- Evaluate model performance using Accuracy, Precision, Recall, F1-score, and AUC-ROC.
- Continuously improve detection using adaptive learning and real-time feedback.

IV. WORKING

A. Gmail Clone Interface & Email List

- Users see an interface similar to Gmail with a list of emails.
- Each email can be selected for spam detection analysis.

B. Spam Prediction with "Predict" Button

- When the user clicks the "Predict" button, the selected email is analyzed.
- The system classifies the email as Spam or Non-Spam instantly.

C. Machine Learning-Based Classification

- Email text is preprocessed using NLTK for tokenization, stemming, and stopword removal.
- A trained ML model (e.g., Naïve Bayes, SVM,) predicts whether an email is spam.

D. Real-Time Classification & User Feedback

- After prediction, a message is displayed indicating if the email is spam.
- Users can manually verify and take action on classified emails.

© 2025 IJIRCCE | Volume 13, Issue 3, March 2025| DOI: 10.15680/IJIRCCE.2025.1303016

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

V. UML DIAGRAMS

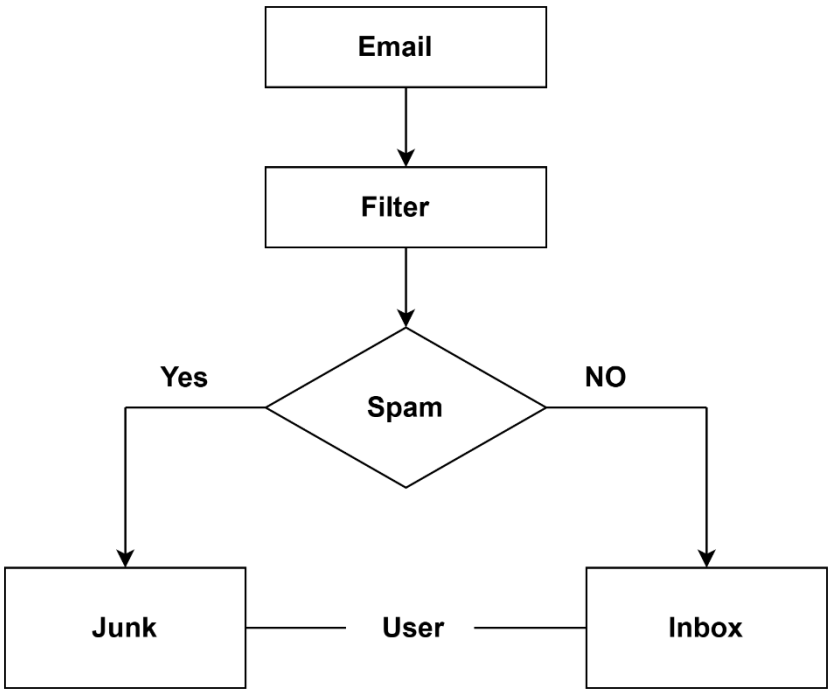


Fig 1. Flow Chart

VI. RESULTS

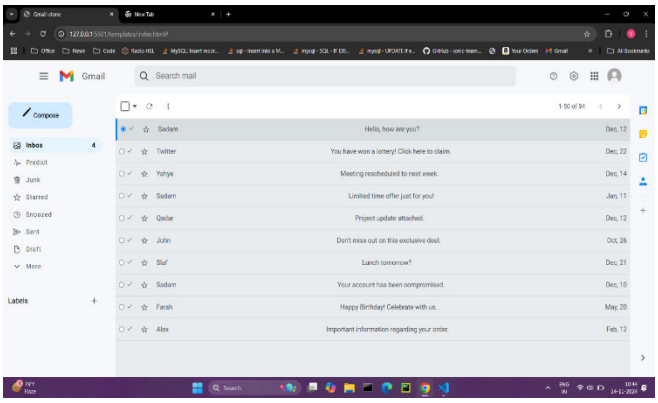


Fig 2. Main Interface

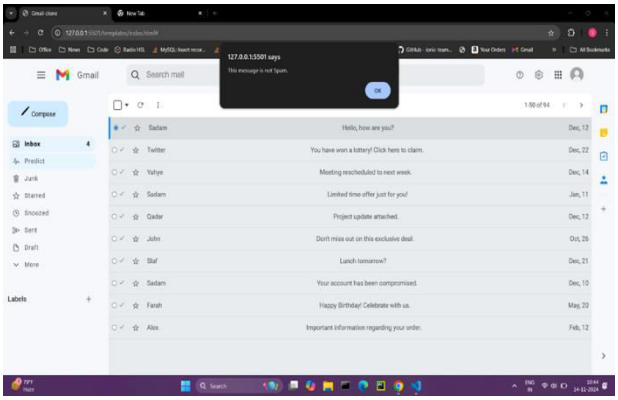


Fig 3. Select Message and Predict Button

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

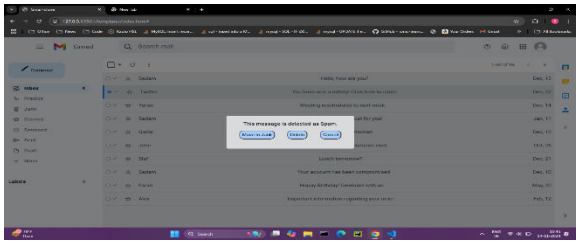


Fig 4. Spam Prompt

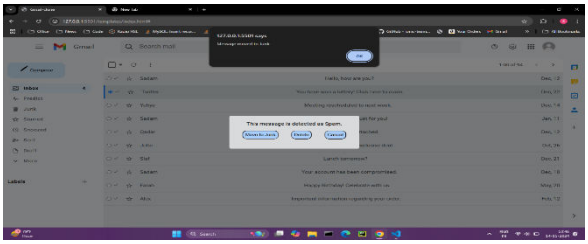


Fig 5. Message Moved to Junk

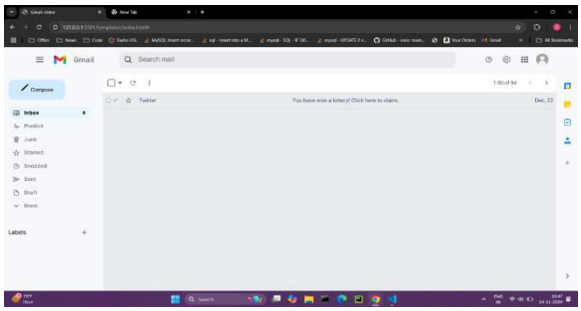


Fig 6. Junk View

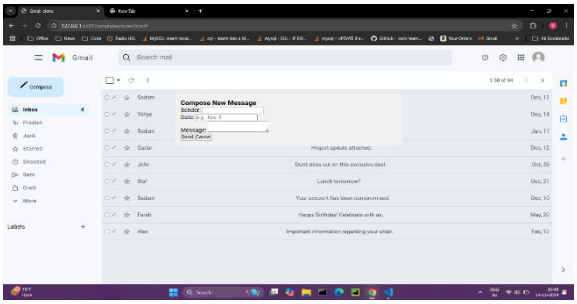


Fig 7. Compose Form

VII. CONCLUSION AND FUTURE WORK

This project successfully implements an email spam detection system in a Gmail clone, allowing users to predict whether an email is spam or not by clicking a button. The system enhances user experience by automating spam detection and efficiently moving spam emails to the Junk folder or deleting them. The implementation improves email security and minimizes unnecessary clutter in the inbox.

For future work, the system can be enhanced by integrating machine learning models that adapt over time based on user interactions. Additional features like advanced filtering, user feedback mechanisms, and phishing detection can be included. Implementing real-time notifications and expanding support for multiple email platforms will further improve usability and efficiency.

REFERENCES

1. Advanced Email Spam Detection: A Machine Learning Solution : https://www.researchgate.net/publication/377610231_Advanced_Email_Spam_Detection_A_Machine_Learning_Solution
2. "A Comprehensive Survey for Intelligent Spam Email Detection" - Reviews AI techniques and their adaptability
3. "Next-Generation Spam Filtering" - Focuses on leveraging GPT-4 and BERT for robust spam and phishing

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details