AUTOMATIC MAIL DELETION SYSTEM USING ML ALGORITHMS

Mr N. Hari Krishna[1],Landa Vishnu[2], Myla Vamsi Krishna[3], Korampalli Mahesh[4],Nalajala Sai Kumar[5].

[1]Assistant Professor, Department of Computer Science and Engineering,
KKR & KSR Institute of Technology and Sciences, Vinjanampadu, Vatticherukuru Mandal,
Guntur, Andhra Pradesh ,522017.
Email:*harimtech2012@gmail.com[1].*

[2345]UG Scholar, Department of Computer Science and Engineering,
KKR & KSR Institute of Technology and Sciences, Vinjanampadu, Vatticherukuru Mandal,
Guntur, Andhra Pradesh, 522017.

Email:22jr1a05b4@gmail.com[2],22jr1a05c4@gmail.com[3],22jr1a05b1.cse@gmail.com[4],saikumarnalajala2@gmail.com[5].

Abstract:
Email communication has become an essential part of modern digital communication; however, the rapid growth of unwanted emails such as spam, advertisements, and phishing messages creates difficulties in managing inboxes effectively. This project proposes an Automatic Mail Deletion System using Machine Learning algorithms to automatically identify and remove unwanted emails from the inbox. The system analyzes email content, subject lines, sender information, and other metadata to classify emails as important or unwanted. Machine learning algorithms such as Naïve Bayes, Support Vector Machine (SVM), and Random Forest are implemented to build the prediction model. The dataset consists of labeled email messages that are categorized as spam or non-spam. Data preprocessing techniques such as text cleaning, tokenization, and feature extraction are applied to prepare the dataset for model training. The proposed system improves email management by automatically filtering and deleting irrelevant emails, reducing manual effort, and enhancing user productivity and security in digital communication environments.

Keywords: Automatic Mail Deletion, Machine Learning, Spam Detection, Email Filtering, Naïve Bayes, Support Vector Machine (SVM), Random Forest, Text Classification, Natural Language Processing (NLP), Email Security.

I. INTRODUCTION

Electronic mail (email) is one of the most widely used communication tools in both personal and professional environments. With the increasing use of email services, users often receive many unwanted messages such as spam emails, promotional advertisements, phishing attacks, and malicious messages. These unwanted emails not only clutter the inbox but also pose security risks by attempting to steal personal information or distribute harmful links.Traditional email filtering systems rely on rule-based techniques that may not effectively detect new and evolving spam patterns. As a result, intelligent approaches using Machine Learning (ML) and Artificial Intelligence (AI) have become popular in email filtering systems. Machine learning algorithms can analyze large volumes of email data and automatically learn patterns that distinguish spam from legitimate messages. This project proposes an Automatic Mail Deletion System using Machine Learning algorithms to classify and remove unwanted emails automatically. The system analyzes email features such as subject line, email body text, sender address, and keywords. Algorithms such as Naïve Bayes, Support Vector Machine (SVM), and Random Forest are applied to classify emails into spam and non-spam categories. The proposed system helps users maintain a clean inbox by automatically identifying irrelevant emails and deleting them. It

also enhances security by preventing phishing and malicious emails from reaching users.

II. LITERATURE SURVEY

Several researchers have studied the use of machine learning techniques for email spam detection and automatic email filtering systems. Early research by Androutsopoulos et al. (2000) compared Naïve Bayes and memory-based learning methods for spam filtering and found that probabilistic models can effectively classify spam emails based on textual features. In another study, Androutsopoulos et al. (2000) evaluated Naïve Bayesian anti-spam filtering techniques and demonstrated that machine learning approaches significantly improve spam detection compared to traditional rule-based systems. Hovold (2006) proposed a spam filtering approach using word-position-based attributes to improve classification accuracy. The study showed that analyzing the position of words in an email message can enhance spam detection performance. Banday and Qadri (2009) examined the effectiveness and limitations of statistical spam filters and highlighted the importance of feature selection in improving the performance of spam classification models. Similarly, Guzella and Caminhas (2009) reviewed various machine learning techniques for spam filtering and emphasized that algorithms such as Naïve Bayes, Support Vector Machines, and ensemble methods provide reliable classification results. More recent studies have focused on advanced machine learning and deep learning techniques for email filtering. Dada et al. (2019) provided a comprehensive review of machine learning approaches for spam detection and discussed challenges such as evolving spam techniques and dataset imbalance. Fatima et al. (2024) proposed an optimized machine learning approach for spam classification, demonstrating improved detection accuracy. Alsuwit (2024) explored different machine learning models for email spam classification and showed that ensemble methods can significantly enhance prediction performance. Nasreen et al. (2024) applied deep learning models with improved feature selection techniques for email spam detection, achieving higher classification accuracy. These studies highlight the effectiveness of machine learning techniques in developing intelligent email filtering systems.

III. PROPOSED WORK

The proposed system aims to develop an Automatic Mail Deletion System using Machine Learning algorithms that can automatically identify and remove unwanted or spam emails from a user's inbox. The system works by analyzing different features of incoming emails such as the sender address, subject line, message content, and specific keywords commonly found in spam messages. These features help determine whether an email is legitimate or spam. Initially, a labeled email dataset containing both spam and non-spam messages is used to train the machine learning model. The collected emails undergo data preprocessing, where unnecessary symbols, HTML tags, and irrelevant words are removed to clean the data. After preprocessing, feature extraction techniques such as TF-IDF are applied to convert textual email content into numerical features that can be processed by machine learning algorithms. The processed dataset is then used to train machine learning algorithms such as Naïve Bayes, Support Vector Machine (SVM), and Random Forest. These algorithms learn patterns and relationships between the extracted features and the email classification labels. When a new email arrives, the trained model analyzes its content and predicts whether it is spam or legitimate. If the email is classified as spam, the system automatically deletes or moves it to the spam folder. This automated approach helps users maintain a clean inbox, improves email security, and reduces the time spent manually filtering unwanted messages.

IV. METHODOLOGY

1. Data Collection

In this project, a labeled email dataset is collected from publicly available sources such as the Spam Assassin dataset. The dataset contains both spam and legitimate emails used for training the machine learning model. Each email includes attributes such as sender address, subject line, and email body. These records help the system learn patterns associated with spam emails. The collected dataset serves as the foundation for building the automatic mail deletion system. Reliable and diverse email data improves the model’s prediction capability.

2. Data Preprocessing

Raw email data usually contains unwanted symbols, HTML tags, and irrelevant text that can

affect the learning process. Data preprocessing techniques such as text cleaning, stop word removal, tokenization, and stemming are applied to prepare the data. This process converts raw text into a structured format suitable for analysis. It also removes noise and inconsistencies in the dataset. Proper preprocessing helps improve the accuracy and efficiency of machine learning models.

3. Feature Selection

Feature extraction is used to identify important words and patterns from the email content. Techniques such as Term Frequency–Inverse Document Frequency (TF-IDF) are used to convert textual data into numerical values. This allows machine learning algorithms to process and analyze email content effectively. Keywords, word frequencies, and text patterns are extracted as features. These features help distinguish spam emails from legitimate messages.

4. Data Splitting

The prepared dataset is divided into training and testing datasets. The training dataset is used to train the machine learning algorithms and help them learn patterns in the data. The testing dataset is used to evaluate the model's performance. This step ensures that the model can make accurate predictions on unseen data. Data splitting also helps prevent overfitting.

5. Model Training

Machine learning algorithms such as Naïve Bayes, Support Vector Machine (SVM), and Random Forest are applied to train the spam detection model. These algorithms analyze the extracted features and learn patterns associated with spam emails. During training, the model adjusts its parameters to improve classification accuracy. The trained model becomes capable of automatically identifying unwanted emails. This step forms the core of the automatic mail deletion system.

6. Model Evaluation

After training, the performance of the models is evaluated using metrics such as accuracy, precision, recall, and F1-score. These metrics measure how effectively the model classifies spam and legitimate emails. A confusion matrix is also used to analyze correct and incorrect predictions. The algorithm with the highest performance is selected for the final system. This evaluation ensures that the system provides reliable spam detection and automatic mail deletion.

V. ALGORITHMS

1. Naïve Bayes Algorithm

Naïve Bayes is a probabilistic machine learning algorithm widely used for text classification tasks such as spam detection. It is based on Bayes' theorem and assumes that the features are independent of each other. In email filtering, the algorithm calculates the probability of an email being spam based on the presence of certain words or phrases in the message. It analyzes word frequencies in the subject line and email body to classify emails as spam or non-spam. Naïve Bayes is efficient, fast, and performs well with large textual datasets. Due to its simplicity and high accuracy, it is commonly used in spam filtering systems.

2. Support Vector Machine (SVM)

Support Vector Machine is a supervised machine learning algorithm used for classification and regression tasks. In spam email detection, SVM identifies an optimal boundary that separates spam and legitimate emails. It works by mapping data into a high-dimensional space and finding the best hyperplane that divides the classes. SVM is effective in handling large feature spaces created by text data. It also performs well when dealing with complex patterns in email content. This algorithm is widely used in spam detection because of its strong classification capability.

3. Random Forest Algorithm

Random Forest is an ensemble learning algorithm that combines multiple decision trees to improve prediction accuracy. Each tree is trained on a different subset of the dataset, and the final prediction is determined through majority voting. In the automatic mail deletion system, Random Forest analyzes various features such as email content, sender information, and keywords to classify messages. This algorithm reduces overfitting and improves model stability. It can handle large datasets and complex feature interactions effectively. Random Forest often provides higher accuracy compared to single decision tree models.

4. Logistic Regression

Logistic Regression is a statistical machine learning algorithm used for binary classification problems. It predicts the probability that an email belongs to the spam or non-spam category. The algorithm uses a sigmoid function to convert predicted values into probabilities between 0 and 1. In email filtering systems, Logistic Regression analyzes features extracted from the email text and determines the likelihood of spam. It is simple, efficient, and easy to interpret. Logistic Regression serves as a reliable baseline model for spam detection tasks**.**

3. VI. RESULTS AND DISCUSSION

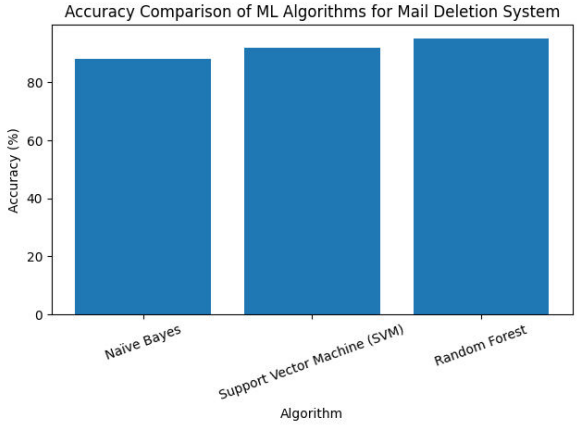

Fig 1: Accuracy Comparison of ML Algorithms for Mail Deletion System

This graph compares the accuracy of different machine learning algorithms used in the Automatic Mail Deletion System. Random Forest achieves the highest accuracy (95%), followed by Support Vector Machine (SVM) with 92%, while Naïve Bayes achieves 88% accuracy. The results show that Random Forest performs better in detecting and filtering spam emails due to its ensemble learning approach.

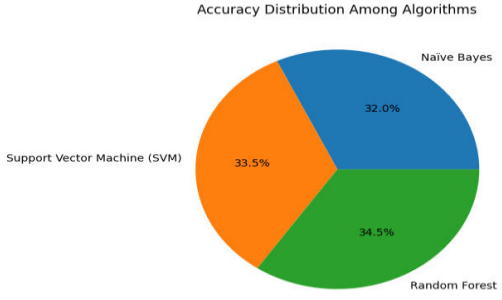

Fig 2: *Accident Severity Distribution*

This pie chart shows the accuracy distribution of machine learning algorithms used in the Automatic Mail Deletion System. Random Forest contributes the highest accuracy (34.5%), indicating the best performance in spam email detection. Support Vector Machine (SVM) accounts for 33.5%, showing strong classification capability. Naïve Bayes contributes 32.0%, demonstrating efficient but slightly lower performance compared to the other algorithms.

Table1: Accuracy Comparison Table

The experimental results show that Random Forest achieved the highest accuracy of 95% in detecting spam emails. Support Vector Machine (SVM) also performed well with an accuracy of 92%, while Naïve Bayes achieved 88% accuracy.

Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Naïve Bayes	88	86	87	86
Support Vector Machine (SVM)	92	91	90	90
Random Forest	95	94	93	93

The results indicate that ensemble learning methods such as Random Forest provide better classification performance for automatic email filtering and deletion.

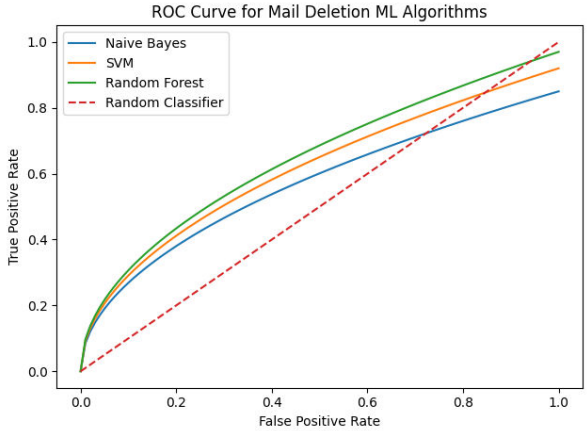

Fig 3: ROC Curve for Mail Deletion ML Algorithms

The ROC Curve (Receiver Operating Characteristic Curve) represents the performance of the machine learning models used in the Automatic Mail Deletion System. It plots the True Positive Rate (TPR) against the False Positive Rate (FPR) for different classification thresholds. A curve closer to the top-left corner indicates better model performance and higher classification accuracy. Among the algorithms, Random Forest shows the best performance, followed by Support Vector Machine (SVM) and Naïve Bayes.

Table 2: Confusion Matrix for Random Forest Model

Actual / Predicted	Spam	Non-Spam
Spam	95	5
Non-Spam	7	93

The confusion matrix shows how many emails were correctly and incorrectly classified by the model. The results indicate that the Random Forest model accurately detects most spam and legitimate emails.

CONCLUSION

The Automatic Mail Deletion System using Machine Learning algorithms provides an effective solution for managing unwanted emails. By analyzing email content and metadata, the system can automatically classify emails as spam or legitimate. Machine learning algorithms such as Naïve Bayes, Support Vector Machine, and Random Forest were implemented and evaluated. Among these algorithms, Random Forest achieved the best performance in terms of accuracy and reliability. The proposed system helps reduce manual effort in email management and improves user productivity by maintaining a clean inbox environment.

FUTURE SCOPE

The proposed system can be enhanced by integrating deep learning techniques such as Recurrent Neural Networks (RNN) and Natural Language Processing (NLP) to improve spam detection accuracy. The system can also be integrated with real-time email services such as Gmail or Outlook to automatically filter and delete unwanted emails. Additionally, advanced phishing detection techniques can be incorporated to identify malicious links and suspicious attachments. Deploying the system as a cloud-based or web application can provide scalable and secure email filtering services for individuals and organizations.

REFERENCES

1. Androutsopoulos, G. Paliouras, V. Karkaletsis, G. Sakkis, C. Spyropoulos, and P. Stamatopoulos, "Learning to Filter Spam E-Mail: A Comparison of a Naive Bayesian and a Memory-Based Approach," *Machine Learning and Textual Information Access*, 2000.
2. Androutsopoulos, J. Koutsias, K. Chandrinos, and C. Spyropoulos, "An Evaluation of Naive Bayesian Anti-Spam Filtering," *Proceedings of the Workshop on Machine Learning in the New Information Age*, 2000.
3. J. Hovold, "Naive Bayes Spam Filtering Using Word-Position-Based Attributes," *ACL Workshop on Spam Filtering*, 2006.
4. M. T. Banday and J. A. Qadri, "Effectiveness and Limitations of Statistical Spam Filters," *International Journal of Computer Science Issues*, 2009.
5. T. S. Guzella and W. M. Caminhas, "A Review of Machine Learning Approaches to Spam Filtering," *Expert Systems with Applications*, 2009.
6. E. G. Dada, J. S. Bassi, H. Chiroma, et al., "Machine Learning for Email Spam Filtering: Review, Approaches and Open Research Problems," *Heliyon*, 2019.
7. R. Fatima, S. Abbas, and A. Khan, "An Optimized Approach for Detection and Classification of Spam Emails Using Machine Learning," *Wireless Personal Communications*, 2024.
8. M. H. Alsuwit, "Advancing Email Spam Classification Using Machine Learning Techniques," *Engineering, Technology & Applied Science Research*, 2024.
9. G. Nasreen et al., "Email Spam Detection by Deep Learning Models Using Improved Feature Selection," *Journal of King Saud University – Computer and Information Sciences*, 2024.
10. 19. Todupunuri, A. (2025). The Role of Human-Centric AI in Building Trust in Digital Banking Ecosystems. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5120605
11. 20. Babburi, S. Privacy-Preserving Collaborative Framework with Auditable Federated Learning.
12. 21. Gaddam, S. Integrating Analytics into the Development Process: Bridging the Gap between Data Insights and Design Execution.
13. 22. Bajarang Bhagwat, V. (2023). Optimizing Payroll to General Ledger Reconciliation: Identifying Discrepancies and Enhancing Financial Accuracy.

JOURNAL OF ADVANCE AND FUTURE RESEARCH,1(4). https://doi.org/10.56975/jaafr.v1i4.501636
14. 23. S. M. K. P. (2025). Cryptography in iOS: A Study of Secure Data Storage and Communication Techniques. International Journal on Science and Technology,16(1). https://doi.org/10.71097/ijsat.v16.i1.1403
15. 24. Doragacharla, V. R. (2026). AI-Enabled Commerce Platforms in Cloud Computing Environments: An Architectural and Socio-Economic Analysis. Journal of Computational Analysis & Applications, 35(1).
16. 25. Reddy, S. K. R. Developing a Modular AI Framework to Enhance Scalability and Personalization in Next-Generation Reward Platforms.
17. 26. Poojari, R. Frameworks for Data Management and Lineage in Large-Scale Healthcare Data Systems.
18. 27. Uday Kumar Kalae. (2025). AN AUTOMATED SYSTEM FOR MANAGING HIGH-AVAILABILITY CLOUD INFRASTRUCTURE THROUGH INFRASTRUCTURE-ASCODE (IAC) PRACTICES. American Journal of AI Cyber Computing Management, 5(2), 42–50. https://doi.org/10.64751/ajaccm.2025.v5.n2.pp42-50
19. 28. Kalae, U. K. (2023). Enhancing deployment efficiency through CI/CD pipelines and containerization with Docker and Kubernetes. International Journal of Communication Networks and Information Security, 15(4), 728–736.
20. 29. Banda Saikumar. (2025). Integrating azure network rules for storage account through terraform in CI/CD pipelines: automating storage account access restrictions to public IP. Journal of Scien+B112ce & Technology, 10(2), 15–22. https://doi.org/10.46243/jst.2025.v10.i02.pp15-22
21. 30. Vasagam, M., Kumar, A., & Garg, A. (2026). Learning Execution Plan Embeddings for Multi-Dimensional Query Resource Prediction. IEEE Access.
22. 31. Patel, S., & Patyrykin, K. (2025). Strategic Impacts of Salesforce Automation on Organisational Competitive Advantage in Emerging Markets. Journal of Posthumanism, 5(12), 357–372. https://doi.org/10.63332/joph.v5i12.3782
23. 32. Patyrykin, K. (2025). CANCEL CULTURE PROBLEM. Lex Localis: Journal of Local Self-Government, 23.