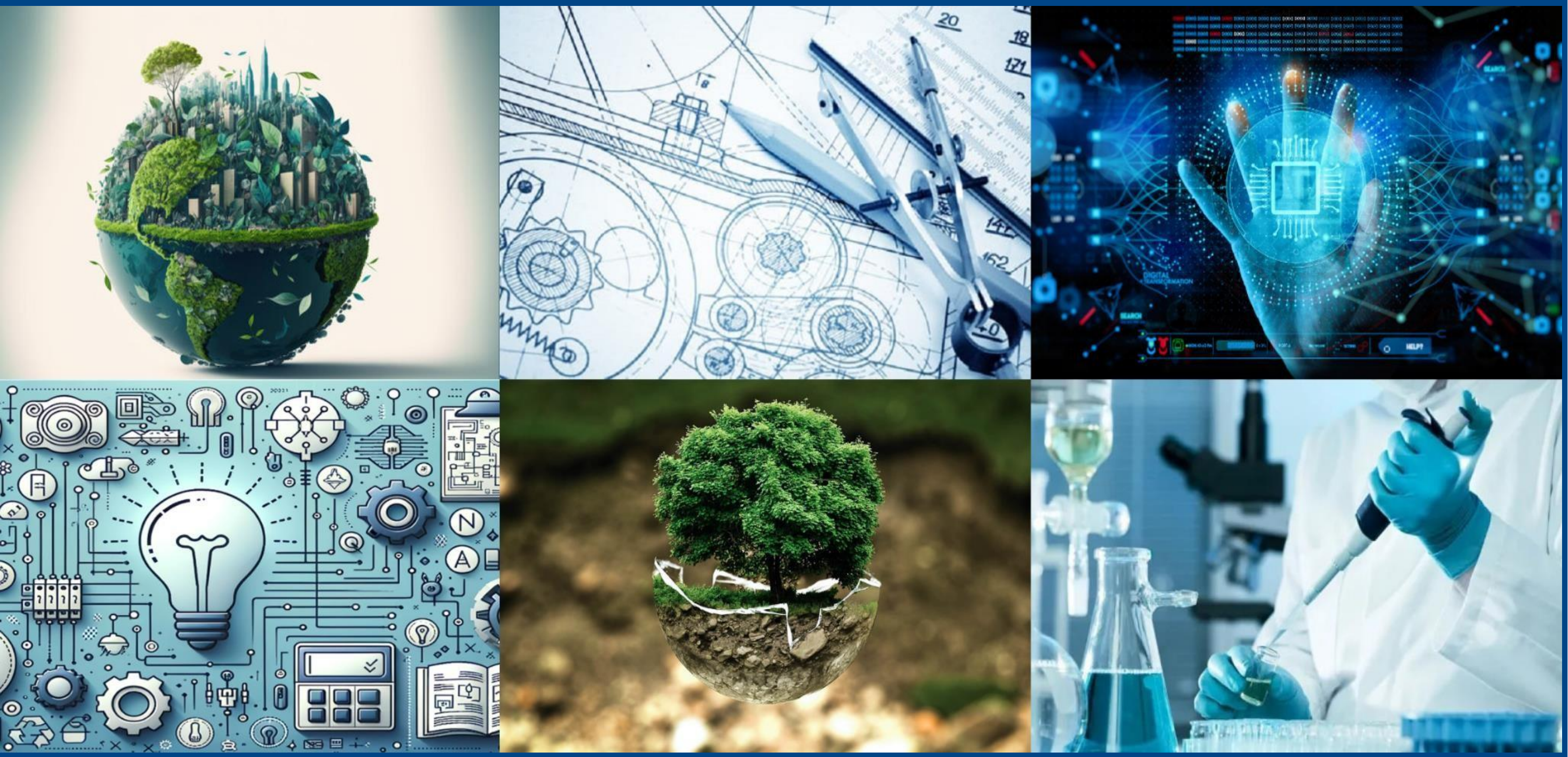
ISSN: 2582-7219

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 8, August 2025

www.ijmrset.com ✉ ijmrset@gmail.com ☎ +91 6381 907 438 ☎ +91 63819 07438

© 2025 IJMRSET | Volume 8, Issue 8, August 2025| DOI:10.15680/IJMRSET.2025.0808061

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

Dr. M S Shashidhara, Dileep M R

Professor & HOD, Department of MCA, AMC Engineering College, Bengaluru, India

Student, Department of MCA, AMC Engineering College, Bengaluru, India

ABSTRACT: Email Spam has become a major problem nowadays, with Rapid growth of internet users, Email spams is also increasing. People are using them for illegal and unethical conducts, phishing and fraud. Sending malicious link through spam emails which can harm our system and can also seek in into your system. Creating a fake profile and email account is much easy for the spammers, they pretend like a genuine person in their spam emails, these spammers target those peoples who are not aware about these frauds. So, it is needed to Identify those spam mails which are fraud, this project will identify that spam by using techniques of machine learning, this paper will discuss the machine learning algorithms and apply all these algorithms on our data sets and best algorithm is selected for the email spam detection having best precision and accuracy.

KEYWORDS: Keywords: Email Spam, Machine Learning, Passive-Aggressive Classifier, TF-IDF, Flask, Real-Time Classification

I. INTRODUCTION

Email spam poses a major challenge in today's digital communication landscape, often leading to security threats such as phishing, malware, and identity theft. Traditional spam filters based on keywords or rule-based systems are increasingly ineffective as spammers evolve their tactics. Machine learning provides a more adaptive and intelligent approach to detect spam by learning patterns from historical email data. This paper presents a spam detection system using the Passive-Aggressive Classifier, a fast and efficient algorithm suitable for real-time classification. The proposed model is integrated into a web application, offering a reliable, scalable, and user-friendly solution for combating email spam.

II. LITERATURE SYRVEY

1) Email Spam Detection: An Empirical Comparative Study of Different ML and Ensemble Classifiers
AUTHORS: Suryawanshi, Shubhangi & Goswami, Anurag & Patil, Pramod.
Recent Development in Hardware and Software Technology for the communication email is preferred. But due to the unbidden emails, it affects communication. There is a need for detection and classification of spam email. In this present research email spam detection and classification, models are built. We have used different Machine learning classifiers like Naive Bayes, SVM, KNN, Bagging and Boosting (Adaboost), and Ensemble Classifiers with a voting mechanism. Evaluation and testing of classifiers is performed on email spam dataset from UCI Machine learning repository and Kaggle website. Different accuracy measures like Accuracy Score, F measure, Recall, Precision, Support and ROC are used. The preliminary result shows that Ensemble Classifier with a voting mechanism is the best to be used. It gives the minimum false positive rate and high accuracy.

2) A Comprehensive Survey for Intelligent Spam Email Detection.
AUTHORS: Karim, A., Azam, S., Shanmugam, B., Krishnan, K., & Alazab
The tremendously growing problem of phishing e-mail, also known as spam including spear phishing or spam borne malware, has demanded a need for reliable intelligent anti-spam e-mail filters. This survey paper describes a focused literature survey of Artificial Intelligence (AI) and Machine Learning (ML) methods for intelligent spam email detection, which we believe can help in developing appropriate countermeasures. In this paper, we considered 4 parts in the email's structure that can be used for intelligent analysis: (A) Headers Provide Routing Information, contain mail transfer agents (MTA) that provide information like email and IP address of each sender and recipient of where the

email originated and what stopovers, and final destination. (B) The SMTP Envelope, containing mail exchangers' identification, originating source and destination domains\users. (C) First part of SMTP Data, containing information like from, to, date, subject – appearing in most email clients (D) Second part of SMTP Data, containing email body including text content, and attachment. Based on the number the relevance of an emerging intelligent method, papers representing each method were identified, read, and summarized. Insightful findings, challenges and research problems are disclosed in this paper.

EXISTING SYSTEM

Traditional spam filters use Naïve Bayes, blacklist/whitelist methods, or content- based filtering. These systems are often bypassed by spammers using obfuscation, varied content, and new email patterns. There's a need for smarter, learning-based spam detection mechanisms.

PROPOSED SYSTEM

The proposed system is a web-based application designed to detect and classify emails as spam or non-spam using a machine learning approach. The system architecture consists of three main components: the backend, the frontend, and the machine learning model. The backend is developed in Python, utilizing the Flask framework to handle server-side operations, process requests, and manage the machine learning pipeline.

The Passive Aggressive classification algorithm is implemented as the core model due to its effectiveness in online learning and handling large textual data streams. The model is trained on a dataset containing 2,910 email records, each comprising an identifier, the email text, and a corresponding label indicating spam or non-spam status.

III. SYSTEM ARCHITECTURE

The architecture of the proposed email spam detection system is designed for efficiency, scalability, and real-time performance

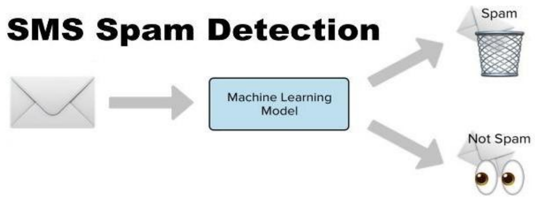


Fig 3.1 System Architecture

IV. METHODOLOGY

The methodology of this project follows a systematic pipeline, beginning with the collection of a labeled dataset comprising 2,910 emails from Kaggle, each annotated as spam or not spam. The raw email texts undergo preprocessing, including the removal of punctuation, special characters, and stop words, followed by tokenization and stemming to normalize the content. Next, the cleaned text is transformed into numerical features using the Term Frequency–Inverse Document Frequency (TF-IDF) vectorization technique, which helps emphasize important terms while reducing the influence of commonly used words. The Passive-Aggressive Classifier, selected for its efficiency in handling large-scale, real-time classification tasks, is then trained on 70% of the dataset, with the remaining 30% used for testing and validation. The model's performance is evaluated using metrics such as accuracy, precision, recall, F1-score, and a confusion matrix, achieving an accuracy of 99.02%. Finally, the trained model and vectorizer are saved using Pickle and integrated into a Flask-based web application, enabling users to input or upload email content and receive instant classification results in a lightweight and user-Friendly environment.

V. DESIGN AND IMPLEMENTATION

The design of the email spam detection system is centered around a modular architecture that ensures scalability, accuracy, and ease of use. The system is implemented using Python and is divided into three main layers: the user interface, the backend server, and the machine learning model. The user interface, developed with HTML, CSS, and JavaScript, allows users to input or upload email content for analysis. The backend, powered by the Flask framework, handles routing, manages the ML pipeline, and processes requests asynchronously to ensure responsive interactions. The machine learning component is built using the Passive-Aggressive Classifier from the Scikit-learn library. The classifier is trained on TF-IDF-transformed email text data, enabling it to efficiently distinguish between spam and non-spam messages. Once trained, the model and the vectorizer are serialized using the Pickle library for reuse during runtime without re-training. The system is optimized for fast performance, with classification results delivered in real time. Additionally, visual output such as accuracy reports and confusion matrices are generated to aid in understanding the model's performance. This design ensures a seamless integration between machine learning and web technologies, making the application both technically robust and user-friendly.

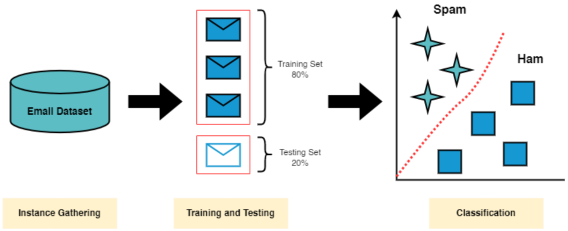


Fig 5.1 Flowchart of Working System

VI. OUTCOME OF RESEARCH

The developed email spam detection system demonstrated high efficiency, accuracy, and real-time performance. By utilizing the Passive-Aggressive Classifier and TF-IDF vectorization, the system achieved a test accuracy of 99.02%, effectively distinguishing between spam and non-spam emails.

The lightweight web application provided an intuitive and responsive interface for users to input or upload email content and instantly receive classification results.

VII. RESULT AND DISCUSSION

The performance of the email spam detection system was evaluated using standard classification metrics such as accuracy, precision, recall, and F1-score. The model, trained on a dataset of 2,910 emails, achieved a high test accuracy of **99.02%**, indicating its strong capability to differentiate between spam and legitimate emails. The confusion matrix revealed very low false positives and false negatives, confirming the reliability of the model in practical scenarios. Precision and recall scores were both close to 1.0, demonstrating the classifier's balance in identifying spam without misclassifying non-spam messages. The real-time prediction capability of the system, powered by the Flask backend, ensured that email classification results were delivered instantly with minimal latency. Furthermore, the user-friendly interface allowed smooth interaction, making the system suitable for both technical and non- technical users. The discussion highlights that the chosen Passive-Aggressive algorithm, when paired with proper preprocessing and TF-IDF feature extraction, offers a powerful and scalable solution for modern email spam detection.

VIII. CONCLUSION

The implementation of the email spam detection system using the Passive- Aggressive Classifier has proven to be an effective and efficient solution for identifying unwanted emails. By leveraging TF-IDF feature extraction and robust preprocessing techniques, the model achieved a high accuracy of 99.02% on the test dataset, demonstrating its reliability in distinguishing spam from legitimate messages. The integration of the trained model into a Flask-based web application enables real-time classification and provides an accessible, user-friendly interface. This system not only enhances email security but also offers a scalable architecture that can be integrated into existing email platforms. Overall, the project validates the practical application of machine learning in combating spam and improving digital communication integrity.

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)

REFERENCES

1. Suryawanshi, Shubhangi & Goswami, Anurag & Patil, Pramod. (2019). Email Spam Detection: An Empirical Comparative Study of Different ML and Ensemble Classifiers. 69- 74.10.1109/IACC48062.2019.8971582.

2. Karim, A., Azam, S., Shanmugam, B., Krishnan, K., & Alazab, M. (2019). A Comprehensive Survey for Intelligent Spam Email Detect ion. IEEE Access, 7, 168261-168295. [08907831]. https://doi.org/10.1109/ACCESS.2019.2954 791

3. K. Agarwal and T. Kumar, "Email Spam Detect ion Using Integrated Approach of Naïve Bayes and Particle Swarm Optimization," 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2018, pp. 685- 690.

4. Harisinghaney, Anirudh, Aman Dixit , Saurabh Gupta, and Anuja Arora. "Text and imagebased spam email classificat ion using KNN, Naïve Bayes and Reverse DBSCAN algorithm." In Optimization, Reliabilty, and Information Technology (ICROIT), 2014 Internat ional Conference on, pp.153-155. IEEE, 2014

5. Mohamad, Masurah, and Ali Selamat . "An evaluat ion on the efficiency of hybrid feature selection in spam email classification." In Computer, Communications, and Control Technology (I4CT), 2015 Internat ional Conference on, pp. 227-231. IEEE, 2015

6. Shradhanjali, Prof. Toran Verma "E-Mail Spam Detect ion and Classification Using SVM and Feat ure Extraction" in International Jouranl Of Advance Reasearch, Ideas and Innovation In Technology,2017 ISSN: 2454-132X Impact factor: 4.295

7. W.A, Awad & S.M, ELseuofi. (2011). Machine Learning Methods for Spam E-Mail Classification. International Journal of Computer Science & Information Technology.
3. 10.5121/ijcsit .2011.3112.

8. Tasnim Kabir, Abida Sanjana Shemont i, At if Hasan Rahman. "Notice of Violation of IEEE Publication Principles: Species Identification Using Partial DNA Sequence: A Machine Learning Approach", 2018 IEEE 18th International Conference on Bioinformat ics and Bioengineering (BIBE), 2018

INTERNATIONAL JOURNAL OF

MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

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

www.ijmrset.com