Email Spam Detection

Group No: BT3435
SEMESTER-5 BTECH CSE

GROUP MEMBERS-

Noman Ali 21SCSE1010302 SEC-2
Abuzar 21SCSE1010356 SEC-2
Amit Verma 21SCSE1010873 SEC-2

GUIDE NAME-

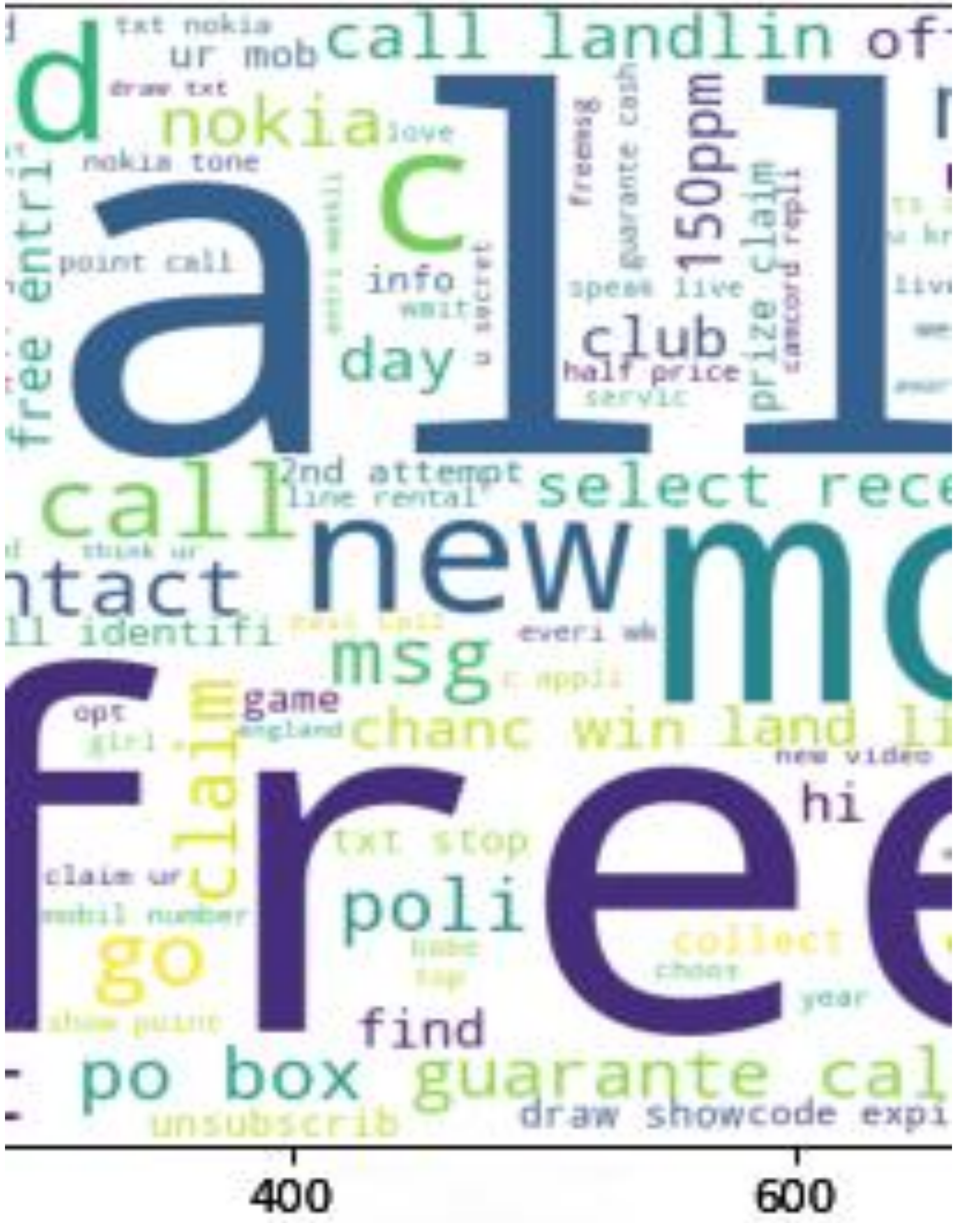
DR.AKHILESH KUMAR SINGH

REVIEVER NAME-

Mr. Akhilesh Kumar

EmailSpamDetection usingMachineLearning

Discover how machine learning algorithms can accurately identify and filter out email spam, ensuring a clean inbox and improved productivity.



Definition of Email Spam

Email spam refers to unsolicited and unwanted messages that are sent in bulk to a large number of recipients. It often contains irrelevant or malicious content.

Importance of Email Spam Detection

Effective email spam detection is crucial to protect users from phishing attacks, malware, and scams. It ensures the security and privacy of personal information.

Types of Email Spam Detection Techniques

Rule-based Filtering

Simple and predefined rules are used to identify and block spam based on characteristics such as keywords or sender reputation.

Content-based Filtering

The content of the email is analyzed using various techniques like text classification and natural language processing to determine its spam probability.

Machine Learning-based Techniques

Advanced algorithms are trained to learn patterns and features from pre-labeled spam and non-spam emails for accurate detection.

Machine Learning Algorithms for Email Spam Detection

Naive Bayes

A probabilistic classifier that calculates the probability of an email being spam based on the occurrence of words or features.

Support Vector Machines

A powerful algorithm that uses a hyperplane to separate spam and non-spam emails based on their feature vectors.

Random Forests

An ensemble learning method that combines multiple decision trees to classify emails as spam or non-spam based on various features.

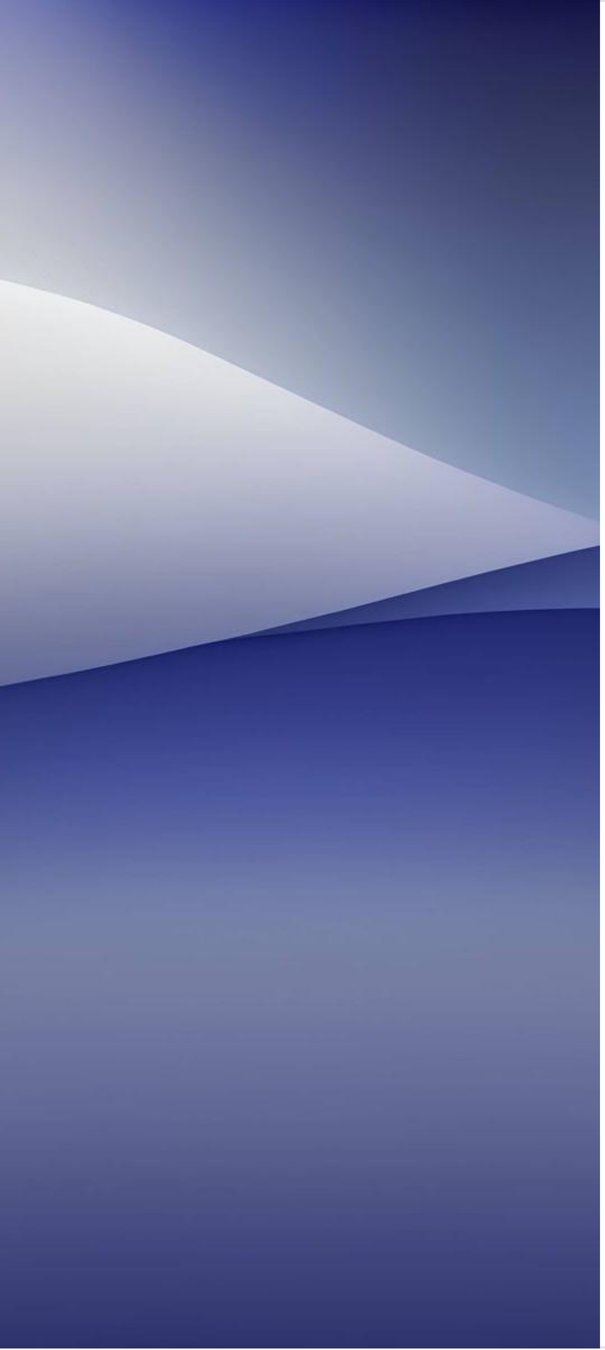
Feature Extraction for Email Spam Detection

Bag-of-Words Model

A common approach that represents an email as a collection of words and ignores their order, enabling the algorithm to identify important terms.

TF-IDF

A technique that assigns a weight to each word in an email based on its frequency in the email and importance in the overall corpus.



Evaluation and Performance Metrics

1 **Precision, Recall, and F1 Score**

Metrics used to evaluate the performance of spam detection models by analyzing the true positives, false positives, and false negatives.

2 **Confusion Matrix**

A table that visualizes the performance of a classification algorithm by comparing the predicted and actual labels of spam and non-spam emails.

3 **Receiver Operating Characteristic (ROC) Curve**

A graphical representation of the trade-off between the true positive rate and the false positive rate of a classification algorithm.

Conclusion and Future Directions

Email spam detection using machine learning continues to evolve with advancements in algorithms, feature extraction techniques, and evaluation metrics.