MINI PROJECT

Email spam detection

Abstract:

Email spam has become a significant concern in the digital era due to the exponential growth of internet users. Spam emails are frequently used for malicious activities such as phishing, fraud, and the distribution of harmful links that can compromise system security. Spammers exploit the ease of creating fake profiles and email accounts, often impersonating legitimate individuals to deceive unsuspecting users. To combat this issue, an efficient and automated system is required to identify and filter out spam emails.

This paper proposes a robust email spam detection system leveraging Python and machine learning techniques. Various machine learning algorithms, including supervised and unsupervised models, are explored and implemented to analyze email datasets. Feature extraction techniques such as Natural Language Processing (NLP) and Term Frequency-Inverse Document Frequency (TF-IDF) are employed to process and analyze email content. The algorithms are evaluated on key performance metrics, including precision, recall, and accuracy, to determine the most effective model for spam detection. The proposed system demonstrates the potential to significantly reduce spam-related threats and enhance email security by providing a reliable and scalable solution.