**AI-Powered Email Spam Detection Using Machine Learning**

**Problem Statement:**

1. Email communication has become an essential medium for both personal and professional interactions. However, the rapid increase in unsolicited and malicious messages, commonly referred to as spam, poses significant challenges to data security, user productivity, and system efficiency. Traditional rule-based spam filters are often rigid, require constant manual updates, and fail to adapt to evolving spam patterns. This project aims to design and develop an AI-driven email spam classifier using machine learning techniques. The process begins with the collection of a large dataset containing emails labeled as “spam” or “ham” (non-spam). The dataset undergoes preprocessing, including removal of unnecessary elements (headers, HTML tags, and punctuation), tokenization of text, elimination of stop words, and application of stemming or lemmatization to normalize words. The preprocessed data is transformed into numerical representations using TF-IDF (Term Frequency–Inverse Document Frequency), ensuring that significant terms are highlighted while redundant ones are minimized. These features are then used to train machine learning models such as Logistic Regression, Naïve Bayes, Support Vector Machines, and Random Forests. The models are evaluated through metrics like accuracy, precision, recall, F1-score, and confusion matrix to determine their effectiveness. The final spam classifier is integrated into an email system to automatically filter out spam messages. Moreover, the model is designed to be updated periodically with new data, making it adaptive to emerging spam strategies and ensuring long-term reliability..