AI-Powered Phishing Email Detection Using NLP

Abstract:
Phishing attacks continue to be a major threat to individuals and organizations, and detecting phishing emails can be challenging due to the sophistication of modern attacks. This project aims to develop an **AI-powered phishing email detection system** using **NLP** to identify phishing attempts in email communications.

Methodology:
The system will analyze email content by applying **NLP techniques** such as **tokenization**, **entity recognition**, and **semantic analysis** to detect suspicious patterns. It will focus on **text features** like urgency, request for personal information, and the presence of malicious links. **Machine learning algorithms** such as **Naive Bayes**, **Random Forest**, and **XGBoost** will be used to classify emails as phishing or legitimate. Additionally, deep learning models like **LSTM** and **BERT** will be employed for more nuanced context understanding and improving detection accuracy.

Outcome:
The outcome will be a real-time, automated phishing email detection system capable of accurately classifying phishing attempts, thereby reducing the risk of attacks. This system will be beneficial for both individuals and organizations, helping protect sensitive information and enhancing cybersecurity.