Artificial Intelligence and Machine Learning (AIML)-Project

# Names: N V V S S Jayakanth Kamisetti - 2320090050 (Sec: 5)

# Problem Statement: Building AI-Based Cybersecurity Pipelines

As cyber threats become increasingly sophisticated, traditional security measures are often inadequate in detecting and mitigating these threats in real-time. This project aims to develop an AI-based cybersecurity pipeline that leverages advanced machine learning algorithms and automation to enhance threat detection, prevention, and response in dynamic cyber environments. The integration of AI into cybersecurity operations seeks to bridge the gap between reactive and proactive defence mechanisms.

# Dataset:

1. Title: Various cybersecurity datasets containing network traffic data, malware samples, and system logs.  
 Source: Open-source repositories and simulated environments.

# Algorithm:

1. Data Collection:  
 - Collection of cybersecurity-related data from online sources and real-world environments.  
  
2. Data Preprocessing:  
 - Cleaning and normalisation of data to ensure accuracy and consistency.  
  
3. Threat Detection Models:  
 - Development of machine learning models for detecting anomalies and potential threats.  
  
4. Pipeline Automation:  
 - Integration of models into a continuous pipeline that automates threat detection and response.  
  
5. Evaluation and Refinement:  
 - Continuous testing and refinement of models using feedback loops to improve accuracy and efficiency.

# Expected Outcome:

This project aims to deliver a robust AI-powered cybersecurity pipeline capable of identifying and responding to cyber threats in real-time. The use of machine learning models is expected to significantly improve the detection rates of complex threats, reduce false positives, and automate the response process, thereby enhancing overall security posture. The outcomes of this project have the potential to be utilised in various industries, contributing to a more secure digital infrastructure.