AI-Powered Intrusion Detection System (IDS)

# 📌 Project Overview

This project implements an AI-powered Intrusion Detection System (IDS) using a Random Forest Classifier. It leverages features from the UNSW-NB15 dataset such as protocol, packet length, source and destination ports, and TCP flags to detect malicious network activity. The system preprocesses data, encodes categorical features, normalizes numerical data, and trains the model to classify network traffic as either normal or malicious.

# 📁 Dataset Used

The UNSW-NB15 training dataset is used in this project. It includes a wide range of real and synthetic network traffic data, including both normal and various forms of attack traffic. The dataset was processed to extract features relevant for real-time intrusion detection, such as protocol, source/destination ports, flags, and packet length (sbytes + dbytes).

# 🧮 Features Used

- proto (Protocol)  
- pkt\_len (Total packet length = sbytes + dbytes)  
- src\_port (Source port - Dummy value)  
- dst\_port (Destination port - Dummy value)  
- flags (TCP flag - Dummy value)

# 🧠 Model Training

The system uses a Random Forest Classifier with 100 estimators. Categorical features are label-encoded, and numerical features are scaled using StandardScaler. The model is trained on 80% of the data and evaluated on the remaining 20%.

# 💾 Model Export

The trained model is saved using `joblib` in a file named `ids\_model.pkl`, allowing for deployment in a real-time intrusion detection environment.

# 📜 License

This project is licensed under the MIT License - see the LICENSE file for details.