DDoS Attack Detection in SDN – Machine Learning-Based DDoS Detection in Software-Defined Networking

The **DDoS Attack Detection in SDN** project focuses on using **machine learning** to identify and mitigate **Distributed Denial-of-Service (DDoS) attacks** in **Software-Defined Networking (SDN)** environments. SDN offers centralized network management but is vulnerable to large-scale DDoS attacks due to its centralized control plane.

This system utilizes **supervised learning algorithms such as Random Forest, XGBoost, and SVM** to analyze network traffic patterns and detect anomalies. The SDN controller collects flow statistics, extracts relevant features, and classifies traffic as either legitimate or attack traffic. The system integrates with **OpenFlow-enabled switches** to dynamically block malicious traffic and protect the network.

The backend is developed using **Python, Scikit-learn, and TensorFlow**, while the SDN controller (e.g., **Ryu, ONOS, or Floodlight**) manages the network flow. The model is trained using datasets such as **CICDDoS2019** and tested in an **SDN simulation environment (Mininet)**.

By leveraging **real-time traffic analysis and AI-driven detection**, this system enhances **network security, scalability, and performance** in SDN-based architectures.