**📌 Phase 1: Project Initialization and Research**

**Objective: Set up the foundation for the IDPS project with clear goals and requirements.**

**Tasks:**

* **Define system goals (Detection + Prevention).**
* **Research existing IDS/IPS systems and ML approaches.**
* **Choose suitable datasets (e.g., NSL-KDD, CIC-IDS).**
* **Set up the project repository and environment (Python, libraries).**

**Deliverables:**

* **Project plan and system architecture.**
* **Dataset sources and project setup.**

**📌 Phase 2: Data Collection and Preprocessing**

**Objective: Prepare quality data for model training.**

**Tasks:**

* **Download and explore datasets (NSL-KDD, CIC-IDS).**
* **Data cleaning: handle missing values, duplicates, and noise.**
* **Feature extraction and selection.**
* **Encode categorical variables and normalize data.**

**Deliverables:**

* **Clean and processed datasets ready for modeling.**
* **Data exploration and feature selection report.**

**📌 Phase 3: Model Development (Detection Engine)**

**Objective: Develop and train machine learning models to detect intrusions.**

**Tasks:**

* **Split data into training and testing sets.**
* **Implement various models (Random Forest, SVM, Neural Networks).**
* **Evaluate model performance (accuracy, precision, recall, F1-score).**
* **Optimize models through hyperparameter tuning.**

**Deliverables:**

* **Trained and validated intrusion detection model.**
* **Model performance comparison report.**

**📌 Phase 4: Real-Time Threat Detection**

**Objective: Implement real-time detection by integrating live network monitoring.**

**Tasks:**

* **Capture live network traffic using Scapy or PyShark.**
* **Convert live packet data into model-compatible format.**
* **Integrate the detection model for real-time predictions.**
* **Log detected threats.**

**Deliverables:**

* **Functional real-time detection engine.**
* **Live detection testing results.**

**📌 Phase 5: Threat Prevention Module**

**Objective: Automate blocking of malicious traffic.**

**Tasks:**

* **Develop an automated blocking mechanism (e.g., modify firewall rules, IP blocking).**
* **Integrate with detection engine for prevention actions**