MLOps

Lec 1

Course Evaluation

Assignment with Viva (1) - 50%

Major Assignment with Viva: 50%

Objective of the Course

To cover topics of ML systems, including applications and products with machine learning algorithms.

What are we going to cover

Machine Learning Systems: Concepts and Stages (data collection to model development), Challenges, and Solutions

ML Data Structure and Data Processing

Machine Learning Accelerators (ML Compilers), Virtual Environments, Git, Docker, Containers

Experiment Tracking, Reproducibility, and Reusability

Quantized and Low-precision Machine Learning

Deployment: Platforms and Infrastructure

Machine Learning System Versioning, Tracking, Testing, and Debugging

Traditional ML Workflow

Example Task: Predicting House Prices

Goal: Predict median house value (MEDV) using features like number of rooms, crime rate, etc.

1. Data Collection

    Download data.csv manually from a website or load it from sklearn.datasets.

    No logging of where or when data was collected.

2. Data Preprocessing

    Data is cleaned in a Jupyter notebook.

    Missing values are imputed manually.

    Feature scaling (e.g., normalization) is done ad hoc.

    Code is scattered across multiple notebook cells.

Traditional ML Workflow

3. Model Training

    A Random Forest Regressor is trained using scikit-learn.

    Hyperparameters are manually tuned by trial and error.

    Metrics like RMSE are printed to the console.

4. Model Saving

    Model is saved to a .pkl file locally.

    No standard location or documentation.

5. Deployment

    A simple Flask app is written for inference.

    There’s no monitoring or version control.

Traditional ML Workflow

Stage	Problem	Consequence
Data Collection	No versioning or source tracking	Can't reproduce results if dataset changes
Preprocessing	Manual and undocumented	Inconsistent between training and inference
Model Training	Manual hyperparameter tuning	Time-consuming, low reproducibility
Model Saving	No versioning or metadata	Risk of overwriting models or losing context
Deployment	No CI/CD or monitoring	If the model fails or drifts, no one notices
Collaboration	Everything is local and informal	Other team members can’t reliably reuse or extend the work

Challenges in Traditional ML Workflows

Fragile Pipelines

Manual, ad hoc data preprocessing and model deployment

Poor Reproducibility

Difficult to recreate experiments due to changing data, code, or environments

Slow Iteration

Lack of automation in training, testing, and deployment cycles

Scaling Issues

Models fail to scale with growing data or infrastructure demands

Why MLOps Matters

Automation of end-to-end ML lifecycle (data → training → deployment)

Versioning & Tracking of datasets, code, and models

Continuous Integration / Continuous Deployment (CI/CD) for ML

Monitoring & Reproducibility of experiments and outputs

Infrastructure Abstraction (Docker, Cloud-native tools)