# Machine Learning Operations (MLOps) Syllabus

# Course Objectives

- Understand the core principles and practices of MLOps.
- Understand the Infrastructure requirements for ML Operations.
- Gain familiarity with the tools and technologies that enable efficient ML workflows.
- Learn how to design and implement robust ML pipelines.
- Acquire the skills to monitor, manage, and maintain ML systems in production.
- Develop a comprehensive understanding of security, privacy, and compliance considerations in MLOps.
- Apply your knowledge through hands-on projects that simulate real-world scenarios.

# Course Structure

The syllabus is structured into several modules, each focusing on a different aspect of MLOps. We expect the course to be heavy on practical assignment. Topic coverage will be based on the ability of the class to keep pace with the assignments in the syllabus.

# Prerequisites

Before beginning this course, it is recommended that you have:

- A basic understanding of machine learning concepts and models.
- Experience with python programming.
- Familiarity with data handling and processing.

# Course Contents

## Introduction to MLOps

- Overview of MLOps and its importance
- Difference between MLOps, DevOps, and DataOps
- Key concepts and terminologies in MLOps

## Module 1: Machine Learning Lifecycle

- Understanding the ML lifecycle stages
- Problem definition
- Data pre-processing and feature engineering
- Model development, training, and evaluation
- Model deployment strategies

- Model monitoring, maintenance, and continuous improvement

## Module 2: MLOps Tools and Technologies

- Overview of MLOps tools and platforms
- Introduction to version control systems (e.g., Git)
- Data versioning tools (e.g., DVC)
- Model packaging – FastAPI, Pickle files
- Experiment tracking and management (e.g., Kubeflow)
- Model serving frameworks (e.g., Kserve)
- Containerization with Docker
- Orchestration with Kubernetes

## Module 3: MLOps Infrastructure

- Setting up scalable ML infrastructure
- Cloud computing services (AWS)
- Infrastructure as Code (IaC) using tools like Terraform
- Continuous Integration and Continuous Deployment (CI/CD) for ML
- End-to-end automation pipelines

## Module 4: Data and Model Management

- Data storage and pipelines
- Feature stores and their role in MLOps
- Model registry and model store concepts – AWS Sagemaker
- Model governance – Model Explainability

## Module 5: Deployment Strategies

- Batch inference vs. real-time inference
- Canary releases and A/B testing for models
- Multiarmed Bandits

## Module 6: Monitoring and Operations

- Logging, monitoring, and alerting for ML systems
- Monitoring and Tracing
- Model performance metrics and evaluation
- Incident management and troubleshooting

## Module 7: Security, Privacy, and Compliance

- Security best practices for MLOps
- Data privacy and handling sensitive information
- Ethical considerations in ML operations

## Module 8: Best Practices and Case Studies

- Best practices for implementing MLOps in organizations
- Case studies of MLOps in the Agriculture sector

## Module 9: Hands-On Projects

- Setting up a complete MLOps pipeline
- Deploying a machine learning model to production
- Monitoring and maintaining a deployed model
- Implementing CI/CD for a machine learning project

# Conclusion

- Recap of key MLOps concepts
- Final assessment through Mini Projects / Assignments

# Additional Resources

- Recommended reading materials and online resources
- Communities and forums for MLOps professionals
- Ongoing learning and development in the field of MLOps

# Notables:

- There will be an element of dynamicity with the course and it’s contents considering it’s industry driven.
- Access to Syngenta systems (including AWS) will not be provisioned as part of the course.