MLOps Fundamentals

Core Principles of MLOps

Overview

MLOps (Machine Learning Operations) is the set of best practices for **scaling, monitoring, and managing ML models** in production. This lesson covers the fundamental principles that ensure **robust, scalable, and maintainable ML workflows**.

Learning Objectives

By the end of this microlesson, you will:

- **Understand** why MLOps is essential for ML lifecycle management.
- **Identify** key challenges in deploying ML models.
- **Apply** core MLOps principles to streamline ML workflows.

Why MLOps Matters

The Problem: ML Models in Production

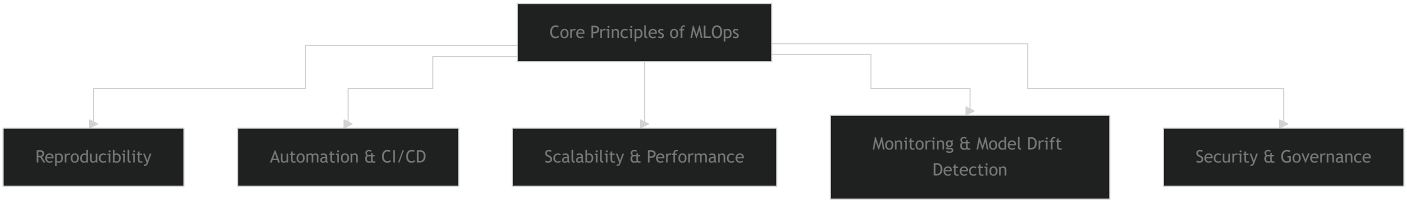
Many organizations build machine learning models but struggle with:

- **Reproducibility issues** – Hard to track model versions and training parameters.
- **Scalability challenges** – Models work in development but fail in production.
- **Lack of automation** – Manual deployment processes are error-prone and inefficient.

The Solution: MLOps

MLOps introduces practices from DevOps to machine learning, ensuring: ✅ **Version control** for datasets, models, and code.
✅ **Automated deployment pipelines** for continuous integration (CI) and delivery (CD).
✅ **Monitoring & logging** to detect model drift and performance issues.
✅ **Collaboration between teams** (data scientists, ML engineers, IT).

Core Principles of MLOps



1. Reproducibility

- Track every ML experiment (datasets, hyperparameters, results).
- Use **MLflow, DVC, or Git** for logging and versioning.

2. Automation & CI/CD

- Automate training, testing, and deployment.
- Use **Docker, Kubernetes, Jenkins, or GitHub Actions**.

3. Scalability & Performance

- Optimize models for large-scale deployment.
- Use **batch processing, parallelization, and cloud services**.

4. Monitoring & Model Drift Detection

- Implement **real-time monitoring** of model predictions.
- Track **data distribution shifts** to retrain models as needed.

5. Security & Governance

- Ensure compliance with **data privacy laws**.
- Use **role-based access control (RBAC)** and encrypted storage.

Quick Discussion: Analyzing MLOps Challenges

Task: Identify Issues in an ML Workflow

Look at the following ML workflow and answer: **What MLOps principles are missing?**

Copy

```
1. Data scientist trains a model locally with no version control.
2. Model is manually deployed by copying files to a server.
3. No automated testing or monitoring is in place.
```

Discussion Questions:

- What are the risks of this workflow?
- How would you improve it using MLOps principles?

4. Key Takeaways

✅ MLOps **bridges the gap** between ML development and deployment.
✅ Reproducibility, automation, scalability, monitoring, and security are key.
✅ Implementing MLOps practices **ensures reliability and efficiency** in ML systems.