Level 2. CI/CD ML pipeline automation

- Rapid & reliable update of ML pipeline.
- Automating build / test / deployment of ML pipelines
- New Ideas can be brought into production easily

Level 2 stages (CI/CD)

(1) Dev / Experiment: i/p – data

perform → perform various frequent experiment for new ML idea
each step is orchestrated.

o/p → source code of ML pipeline steps.

(2) Pipeline CI:

i/p → prev o/p.

perform → build / Run tests

o/p → Packages, containers (Docker), executables & artifacts.

(3) Pipeline CD: i/p → prev o/p

perform → Deployment of (prev o/p) into larger environment

o/p → Deployed pipeline with new ML ideas.

④ Automated triggering (or CT) :

i/p : Deployed pipeline

perform : trigger training in production based on schedule ⑦ etc... {.covered prev}.

o/p : Trained models → pushed → model registry.

⑤ Model CD :

i/p : "

perform : pick model from model registry & serve as prediction service API/APP.

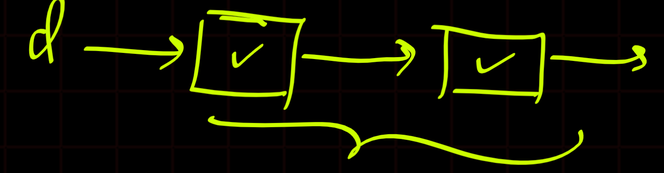
o/p : Deployed model as prediction service API/APP.

⑥ Monitoring :

perform : collect live stats of live model performance on new data

o/p → trigger execution of pipeline
" new experiment cycle.

More about CI in ML systems



1. unit testing of feature engineering logic
2. 11 —— 11 of various methods / function implemented in source code.
3. Test for model training convergence
4. Testing of each pipeline component whether we are getting expected outputs
5. Testing for barking of NaN, divide by zero, Caye no. o/p from model. { Proper handling of exception }
6. Test the pipeline integration

More about - CD ?

How to handle CD in a smooth way?

(1) Verify compatibility of the model with the target environment or infrastructure

eg: check for packages required, memory requirements

(2) Testing prediction service API by calling this API

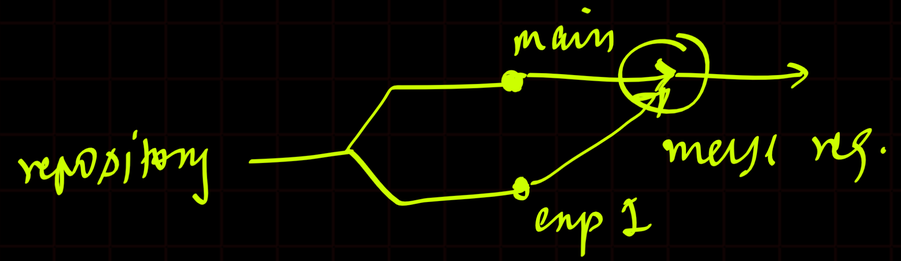
↳ to ensure that you are getting expected o/p ~~expected~~ desired format - JSON

(3) Testing the prediction service performance eg
→ load testing → query per second
model latency.

④ ~~Key~~ Verify model performance w.r.t. set benchmark

⑤ Deployment strategy :-

- Automated deployment
  - deploy in production once you push changes into deployment/main branch.
- Semi automatic
  - ~~You have~~



- Manual deployment ☆
  - after several successful iteration in pre production deploy manually to production.

Summarize :-

① Adapting to change in data or business environment

eg: before & after pandemic

②

When we need AI/MLOps.

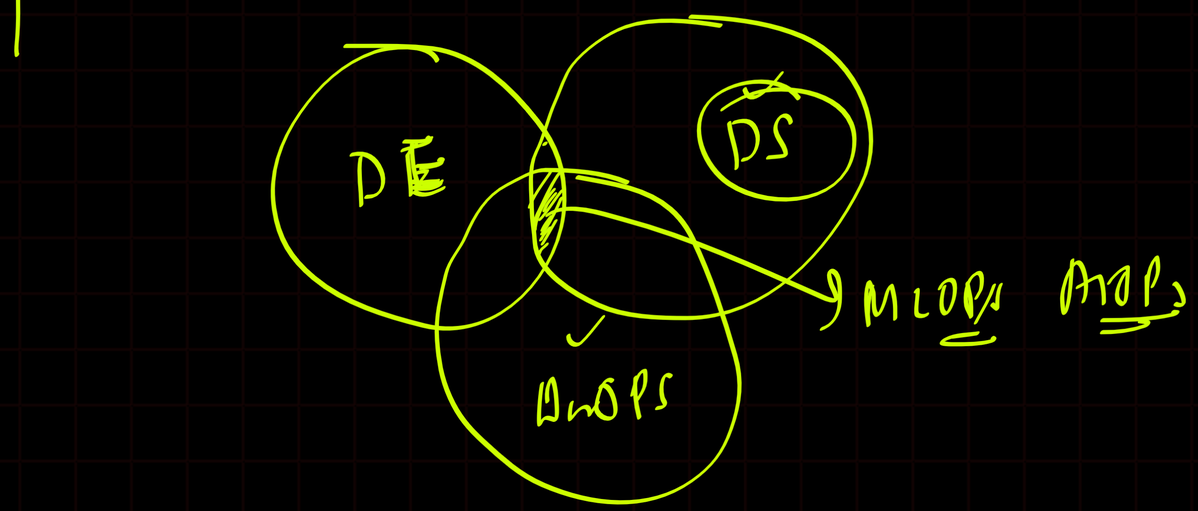
(1) When you are in experiment phase ? ✗

(2) you have a user base for your deployed model !? ✓

↳ scalability -

↳ frequent updates ✓

دا


DE
DS
MLOps
AIOps
DevOps


ETL