

INTELLIGENCE IN ACTION: AI-DRIVEN NETWORKS

Checkpoint 3

Projeto em Informática 2024/2025

Hugo Ribeiro - 113402

Rodrigo Abreu - 113626

Eduardo Lopes - 103070

Jorge Domingues - 113278

Joao Neto - 113482

May 2025

TABLE OF CONTENTS

1. PREVIOUS PLAN
2. WORK DONE
3. PROBLEMS
4. PLAN
5. 5G CORE INTEGRATION



1. PREVIOUS PLAN

PREVIOUS CHECKPOINT PLAN

Complete the model(s) deployment and Integrate them in the pipeline.



Assess whether it's feasible to have enough data for a good attack classification model.



Assess whether to cold start the system or prepopulate the ML databases with sample data.



Integration of the pipeline into the 5G network (implementation of border APIs)



2. ML WORK DONE

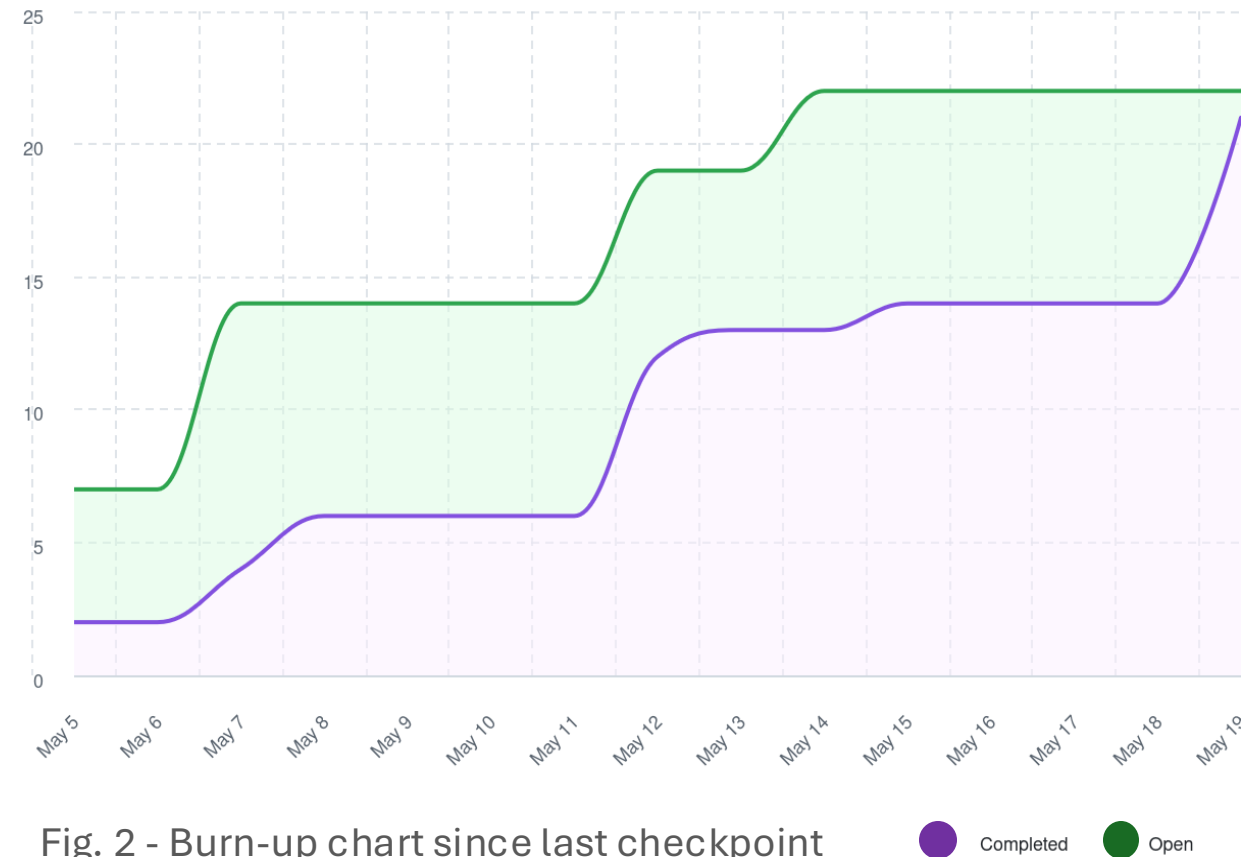
WORK DONE ML

- Increased the pipeline speed massively again so we could have more readily available data (Again).
- Integrated both the Binary Model (detect attack) and Classifier Model (attack type).
- Applied SMOTE and Undersampling techniques **automatically**, depending on data volume to increase accuracy.
- Displayed both model's inferences in the Chronograf dashboard.

Type and Number of Attacks		
time	Attack	network_processed_data.count
01/01/1970 01:00:00	Benign	5724.00
01/01/1970 01:00:00	DoS	1.00
01/01/1970 01:00:00	Exploits	42.00
01/01/1970 01:00:00	Shellcode	1.00

WORK DONE ML

- **Automatized** ML training, testing and deployment as new data arrives.
- Obtained good F1 Score results -> starts low but converge to 99% as overall data volume increases.
- Decided to **cold start** the system instead of pre-populating.
- Defined the **retraining strategy** to account for data drift and for new attack types.



3. ML PROBLEMS

ML Problems

- **Bias** was found and fixed on the binary ML Model.
- F1 Score **decreased**, but it is still converging to 99% over time.
- Define the best strategy for retraining and redeployment.



4. PLAN

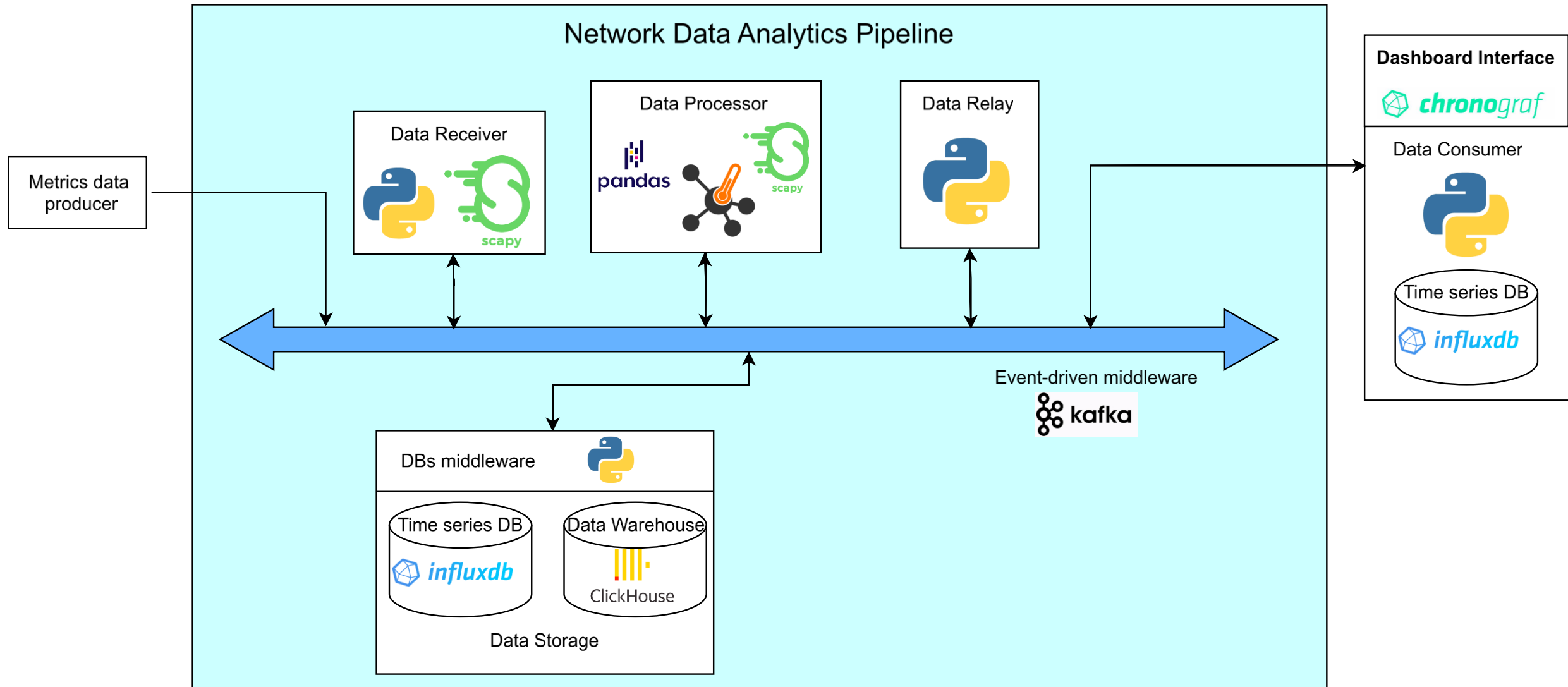
PLAN

- Develop the additional **retraining triggers** (ex: retrain, when new type of attack is detected).
- Apply **hyperparameter tuning**, to optimize results.
- Save each model F1 Score over time and **plot the data** to analyze results evolution.
- Support NWDAF **model training requests** via API.
- Deploy the project using **kubernetes**.

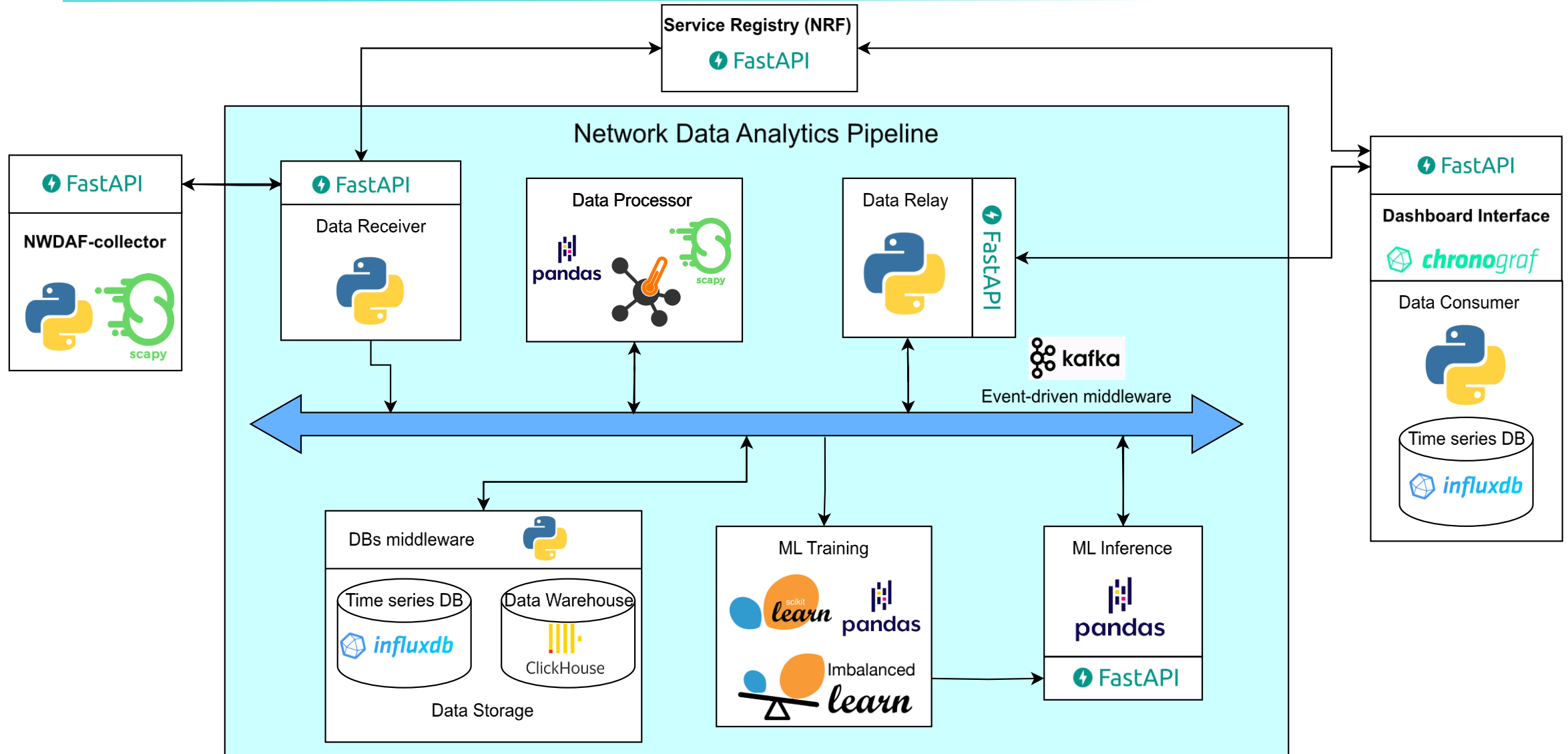


5. 5G Core Integration

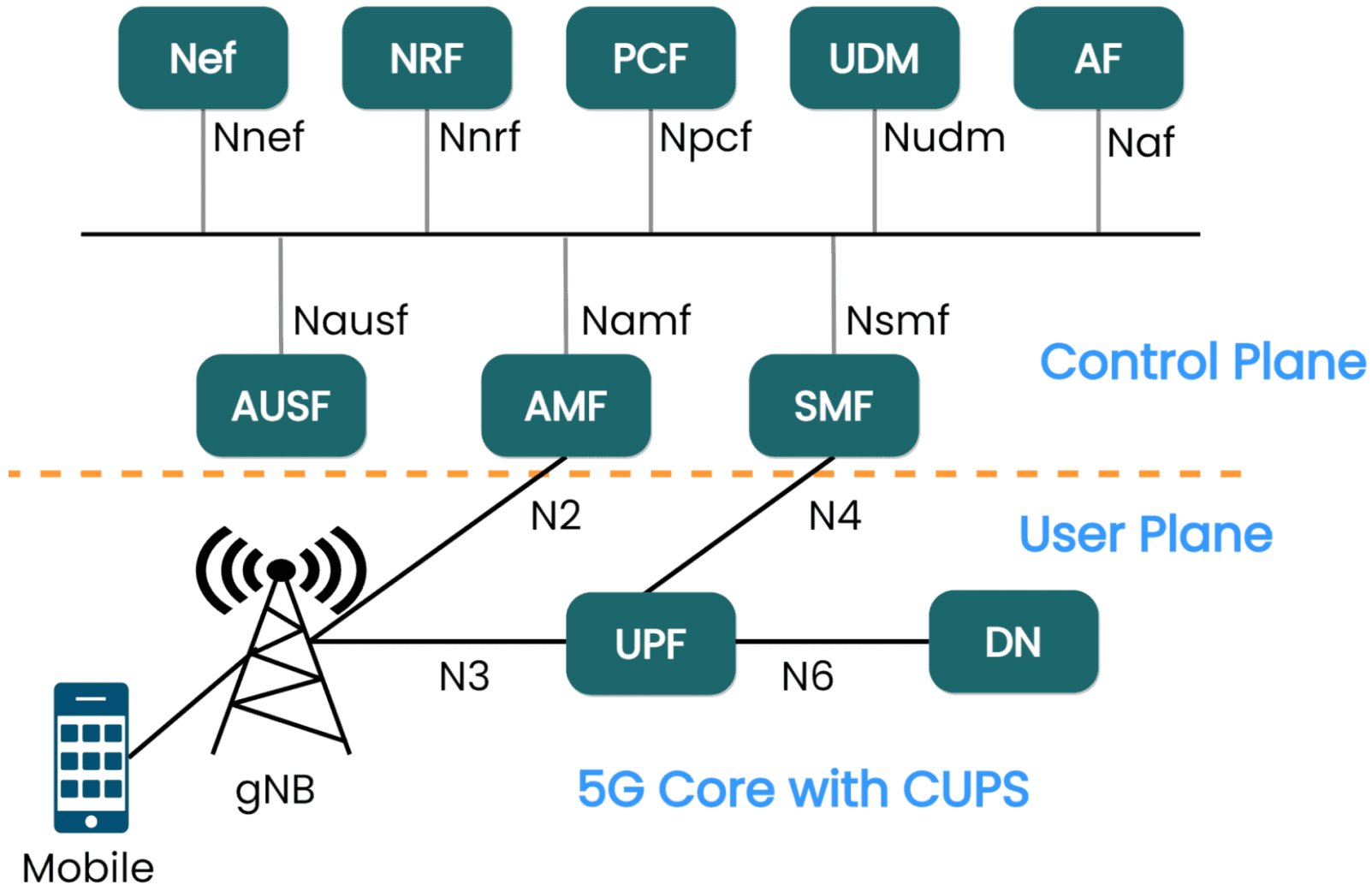
Architecture (OLD)



Architecture

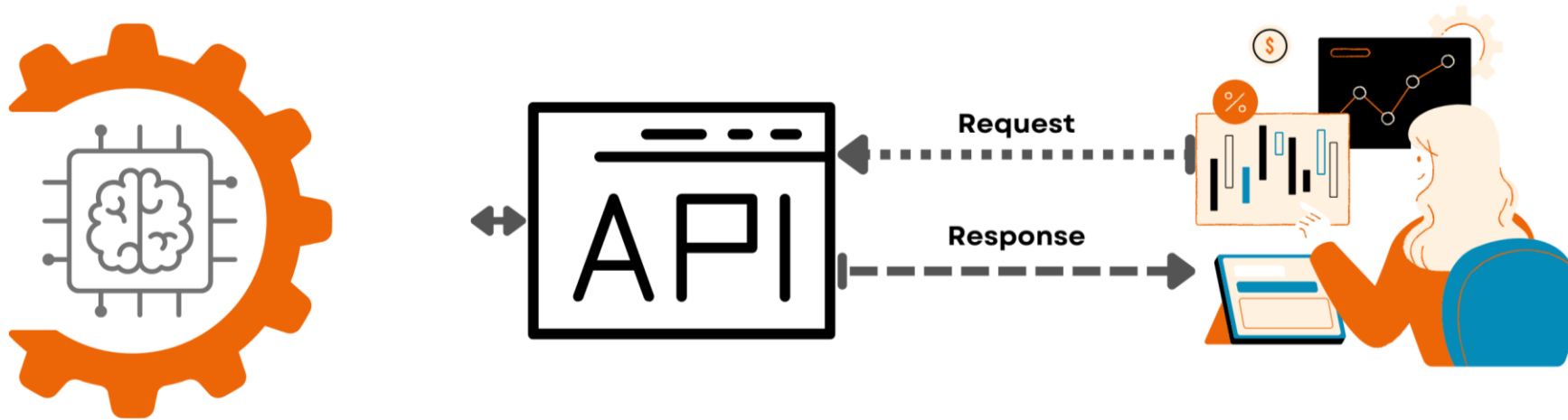


5G Integration



5G Integration Future Work

- In the NWDAF architecture, model training can be carried out at the request of the network operator via **API**.
- Implement an API for model training, to choose the model to train when it's possible.
- This API will expose the model training **evaluation metrics**.



Scan the QR code to check our documentation website.



Or click [here](#).

THANK
YOU