UNIVERSITÀ DEGLI STUDI DI TRIESTE

Project: Fraud Detection as a Service

Master Course:

Data-driven Systems Engineering (ML Operations)

440MI and 305SM

Agenda

- Problem
- Solution Overview
- Model as a Service
- Flask

Problem

Business Objective: Detect fraudulent credit card transactions using a supervised classification model.

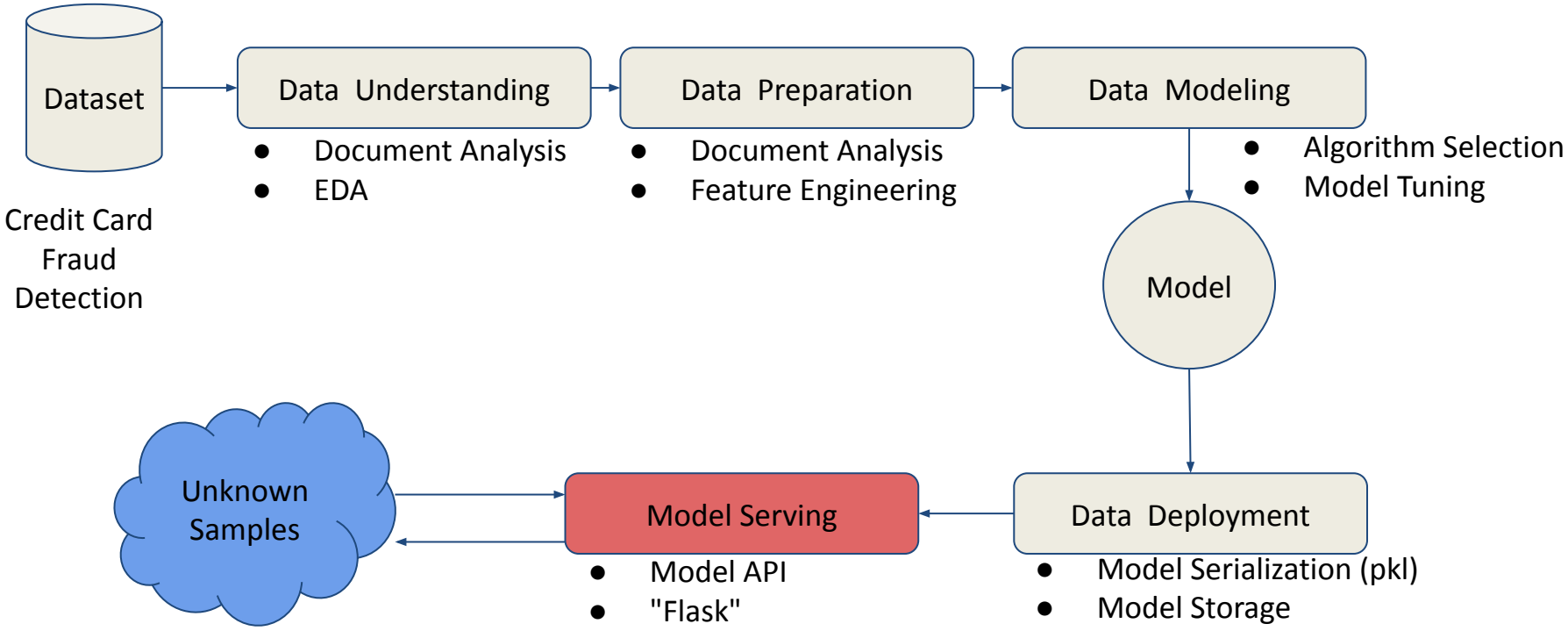
Data Overview:

- Source: Kaggle (European cardholder transactions)
- 284,807 transactions
- 30 features (V1–V28, Time, Amount)
- Target variable: is_fraud (1 = Fraud, 0 = Legitimate)

Model Pipeline:

- Data Preprocessing – Renaming columns, scaling, and splitting data.
- Model Training – Classifier with parameter tuning.
- Evaluation – Confusion matrix and classification report.
- Serialization – Model exported as model.pkl.
- Deployment – Flask-based REST API exposing the /predict endpoint.

Solution Overview



Model as a Service

- Model as a Service (MaaS) is a **deployment paradigm** that enables trained machine learning models to be hosted and accessed as cloud-based services.
- Users can send data to the model through an Application Programming Interface (API) and receive predictions in real time, without direct interaction with the underlying infrastructure.
- Key Characteristics:
    - Decouples model development from model consumption.
    - Ensures scalability, availability, and version control of deployed models.
    - Enables integration with business systems, dashboards, and automation pipelines.

What is flask?

- Flask is a lightweight and flexible web framework for Python designed to build web applications and APIs quickly.
- It is particularly suitable for deploying machine learning models as web services.
- Key Features:
  - Simple and minimalistic core.
  - Built-in development server and debugger.
  - Support for RESTful request handling.
  - Extensible with numerous plugins and libraries.
- Common Use Cases:
  - RESTful API creation.
  - Model deployment and prediction services.
  - Prototyping web applications.
  - Integration with data processing and machine learning pipelines.

What is flask?

Flask Architecture:

Core Components:

- **WSGI Server**: Middleware interface between the Flask app and web server.

Basic Application Structure:

```
project_folder/
    ├── app.py
    ├── templates/
    ├── static/
    └── model.pkl
```

Execution:

- Run with flask run or python app.py
- Access the application via http://localhost:5000

What is flask?

Example:

```python
from flask import Flask
app = Flask(__name__)

@app.route('/')
def home():
    return 'Flask API is running!'

if __name__ == '__main__':
    app.run(debug=True)
```

What is flask?

Class6_model_api.py > ...

```python
from flask import Flask, request, jsonify
import pickle
import numpy as np

app = Flask(__name__)
model = pickle.load(open("notebooks/best_random_forest_model.pkl", "rb"))

@app.route("/")
def index():
    return jsonify({"message": "Model API running"}), 200

@app.route("/predict", methods=["POST"])
def predict():
    data = request.get_json(force=True)
    features = np.array(data["features"]).reshape(1, -1)
    pred = model.predict(features)[0]
    return jsonify({"prediction": int(pred)})

if __name__ == "__main__":
    app.run(host="0.0.0.0", port=5001, debug=True)
```

What is flask?

Python Request

```
response = requests.post("http://127.0.0.1:5002/predict", json={"features": sample})
print("API Response:", response.json())
```

Terminal Request

```
curl -X POST http://127.0.0.1:5002/predict \
    -H "Content-Type: application/json" \
    -d '{"features": [5.1, 3.5, 1.4, 0.2]}'
```

Let's start!!!

Full documentation:

FraudDetectionAsaService.pdf