SELF-ADAPTIVE FINANCIAL FRAUD DETECTION SYSTEM

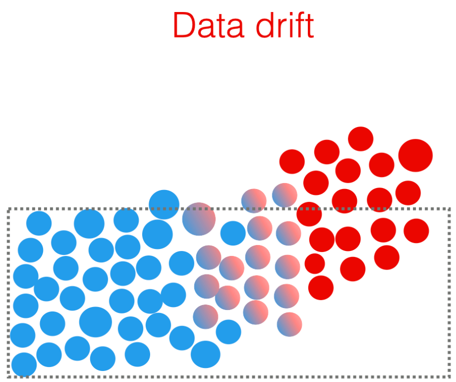
Team # 9

Aman Kumar & Manan Raheja
Electrical and Computer Engineering

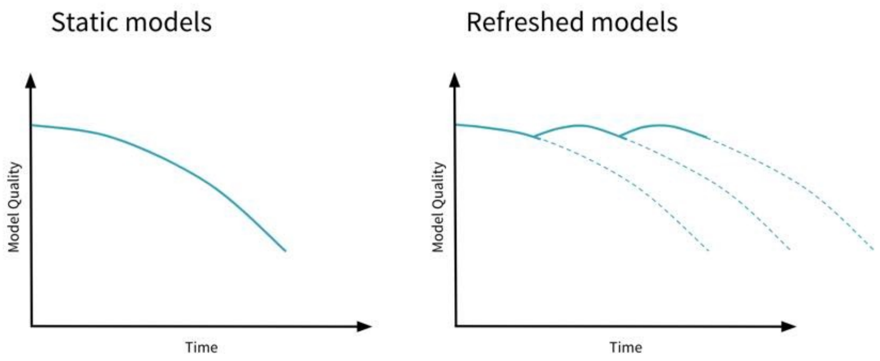
UNIVERSITY OF WATERLOO | FACULTY OF ENGINEERING

Motivation

- Detecting fraudulent transactions is one of the major challenges faced by financial institutes, causing heavy financial loss and negative user experience
- Machine learning to the rescue?
- Static ML models struggle with **data drift**, a "feature" of fraudulent transactions
- Reasons for the data drift:
  - fraudsters constantly changing their methods
  - evolving technology landscape
- **Objective of the project:**
  - A system that can adapt and self-optimize in response to data drift
  - Maintains optimal performance over time



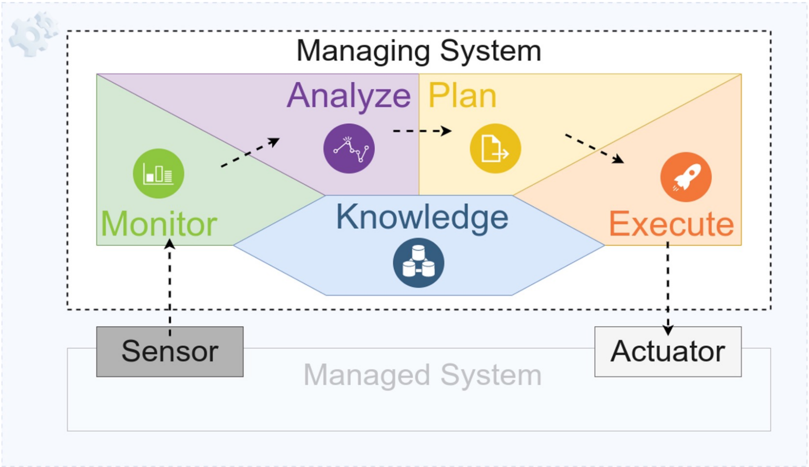
Source: [1]



Source: [2]

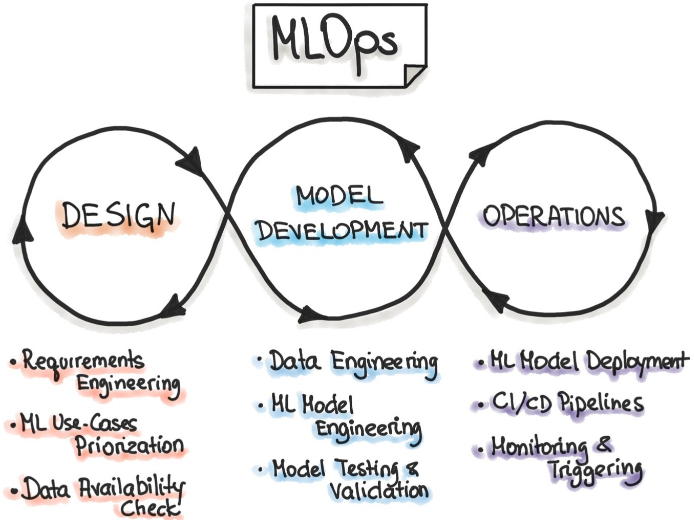
Our Approach

- Integrating principles of Self-Adaptative Systems (MAPE-K loop) into the MLOps lifecycle (Data Engineering -> Model Engineering -> Model Deployment).



Source: [3]

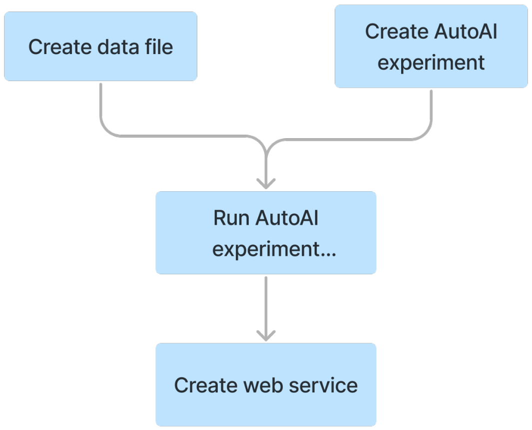
+

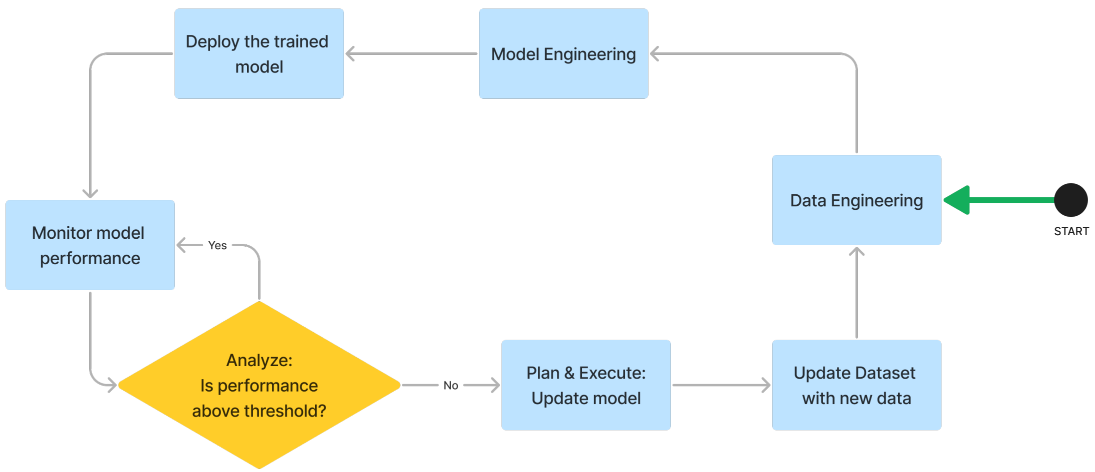


Source: [4]

Architecture of the System

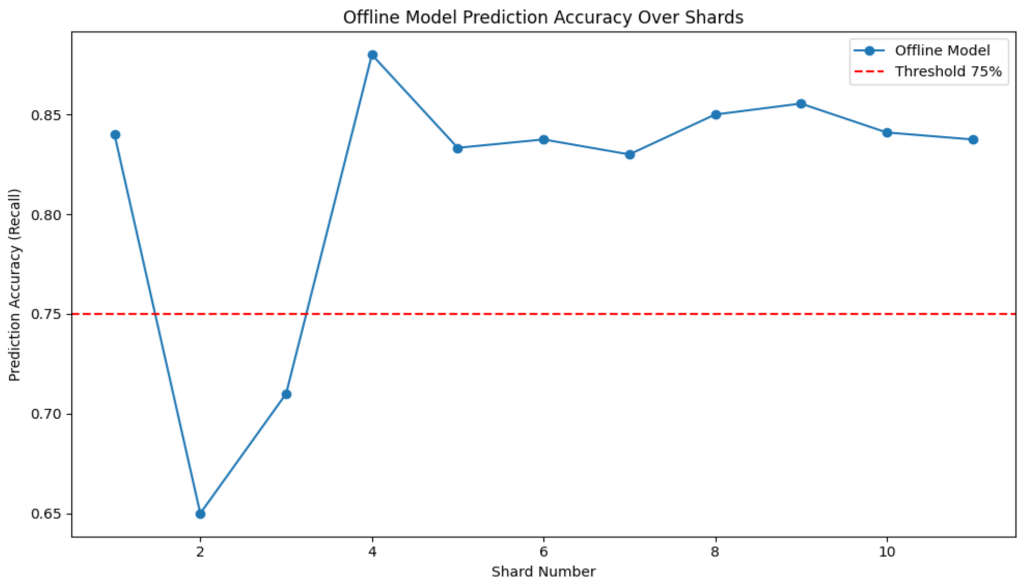
- **3** main components -
  1. **Data Streamer:** Simulates a data stream from a static dataset
  2. **MLOps pipeline:** Data Preprocessing -> Model Training -> Deploy
  3. **Driver program:** Orchestrates the complete self-adaptative process





Results

- Simulating data drift with 2 datasets (original, augmented)
- Conducted an extensive series of experiments with **15 models** to find the best-performing ML model
- Built a **custom voting classifier** combining XGBoost, Random Forest and Gaussian Naïve Bayes
- The observations demonstrate system's ability to sustain optimal performance and adaptability even under significant data drift



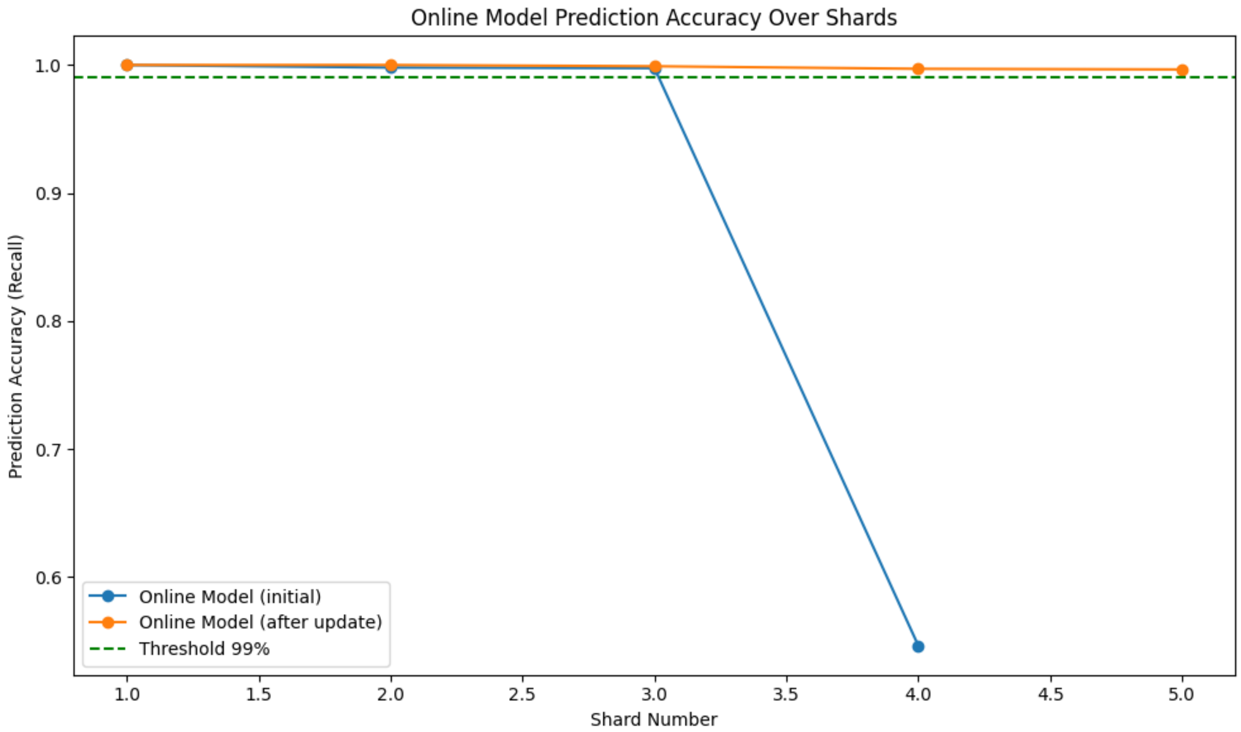
Classifier	Recall
AdaBoost	74.48%
Bagging Classifier	80.61%
BernoulliNB	63.26%
Calibrated Classifier CV	63.26%
DecisionTreeClassifier	75.51%
ExtraTreeClassifier	76.53%
ExtraTreesClassifier	82.64%
GaussianNB	84.69%
KNeighborsClassifier	80.61%
XGBoost	82%
LinearSVC	78%
SVC	67%
Random Forest	81%
Logistic Regression	65%
Gradient Boosting (max_depth=15)	78%
Custom Voting Classifier	83%

TABLE I: Performance of different classifiers on the Credit Fraud Dataset

UNIVERSITY OF WATERLOO | FACULTY OF ENGINEERING

Results (Cloud Runtime)

- Pipeline 1 trains and deploys initial model.
- Model achieves 99.99% Recall due to data augmentation and model selection.
- Pipeline 2 retrains and redeploys the model when accuracy drops.



UNIVERSITY OF WATERLOO | FACULTY OF ENGINEERING

THANK YOU! :)

Any questions?

Image Credits

[1] - https://www.evidentlyai.com/ml-in-production/data-drift

[2] - https://www.databricks.com/blog/2019/09/18/productionizing-machine-learning-from-deployment-to-drift-detection.html

[3] - https://learn.uwaterloo.ca/d2l/le/content/949359/viewContent/5154165/View

[4] - https://ml-ops.org/content/mlops-principles