Model Monitoring and Audit Logging for Financial ML Models

Motivation

In regulated financial environments, machine learning (ML) models are used for credit scoring, fraud detection, risk assessment, and trading. These models must comply with strict regulatory standards (e.g., SR 11-7 guidance by the Federal Reserve, GDPR, and local financial compliance rules). Continuous monitoring of model performance and data drift is essential to ensure:

- The model remains valid under changing market conditions.
- Compliance with fairness, accuracy, and transparency requirements.
- Quick detection of anomalous behavior or input distribution shifts.
- Comprehensive audit trails for accountability and explainability.

Need for Drift Detection

Data Drift: Occurs when the statistical properties of input data change over time, leading to model underperformance.

Concept Drift: Occurs when the relationship between inputs and outputs changes (e.g., macroeconomic shifts affecting default rates).

Failure to detect and correct drift can result in financial losses, compliance violations, and reputational damage.

Algorithm Outline

1. **Collect Incoming Data:** Continuously or in batches.
2. **Compute Performance Metrics:** Accuracy, AUC, precision, recall, etc., on labeled data.
3. **Detect Data Drift:** Using statistical tests (e.g., Population Stability Index (PSI), Kolmogorov-Smirnov (KS) test).
4. **Set Thresholds:** Define acceptable ranges for metrics and drift scores.

5. **Generate Alerts:** If drift or performance degradation exceeds thresholds.

6. **Log Predictions and Metrics:** Store model inputs, predictions, and corresponding performance metrics in an audit log (file or database) for traceability.

7. **Retrain or Recalibrate:** Optionally trigger retraining workflows when drift persists.

Conclusion

A robust monitoring and audit logging system is critical to maintaining trust, regulatory compliance, and the long-term success of ML applications in finance. This document lays out the foundation for implementing such a system in a production-ready manner.