MLOps Assignment 4: Model Monitoring
Luke Schwenke
November 27, 2023

<u>Platform for Model Monitoring: AWS SageMaker Model Monitor</u>

Summary: Amazon SageMaker Model Monitor allows you to create a set of baseline statistics and constraints using the data with which your model was trained, then set up a schedule to monitor the predictions made on your endpoint.

Question #1: What algorithm(s) does AWS SageMaker use to detect model drift?

Amazon SageMaker Model Monitor offers built-in analysis in the form of statistical rules, to detect drifts in data and model quality. You can also write custom rules and specify thresholds for each rule. The rules can then be used to analyze model performance. SageMaker Model Monitor runs rules on the data collected, detects anomalies, and records rule violations.

Some of these statistical rules used to detect various drift are the following:
- Significant changes in Mean, Standard Deviation, Skewness of the prediction distribution
- Significant changes in the prediction residuals
- Two-Sample Tests like Kolmorgorov-Smirnov distribution of feature values between data

Question #2: What are 3 things that can improve the model platform for monitoring?

1. **Automate the Model Monitoring Process More:** Currently on the platform you need work have AWS SageMaker setup in addition to Model Monitor. If you want a visualization tool you need to integrate with AWS Clarify. If you want alarms you need to have SageMaker send logs to be consumed by CloudWatch and then create alarms from there. Then SNS can be configured to send email alerts. In other words a lot of these critical and helpful steps in AWS are somewhat siloed until they are connected. This connection process takes time and requires IAM roles and permissions to be in-order which can increase complexity. It would be great if some of these were integrated more automatically into SageMaker from the start.

2. **Feedback Loop Integration:** AWS could develop built-in mechanisms for easily incorporating human feedback (Human-in-the-loop) or external domain expertise into the monitoring process, allowing for more nuanced evaluations of model behavior. This would add an additional dimension to detecting drift that their current statistical tests may not necessarily capture.

3. **Interpretability Enhancement:** AWS could enhance interpretability in model monitoring by offering detailed insights into feature contributions during drift detection. Currently, users can determine drift, but there is a lack of information on the specific features driving the changes. A new solution could involve providing explicit breakdowns of how individual features impact model output, supported by visualizations with Clarify. Additionally, implementing correlation analyses would enable users to quickly identify features strongly linked to observed drift. Overall, this enhancement could help identify the specific element(s) impacting drift aside from just informing that a drift has occurred.