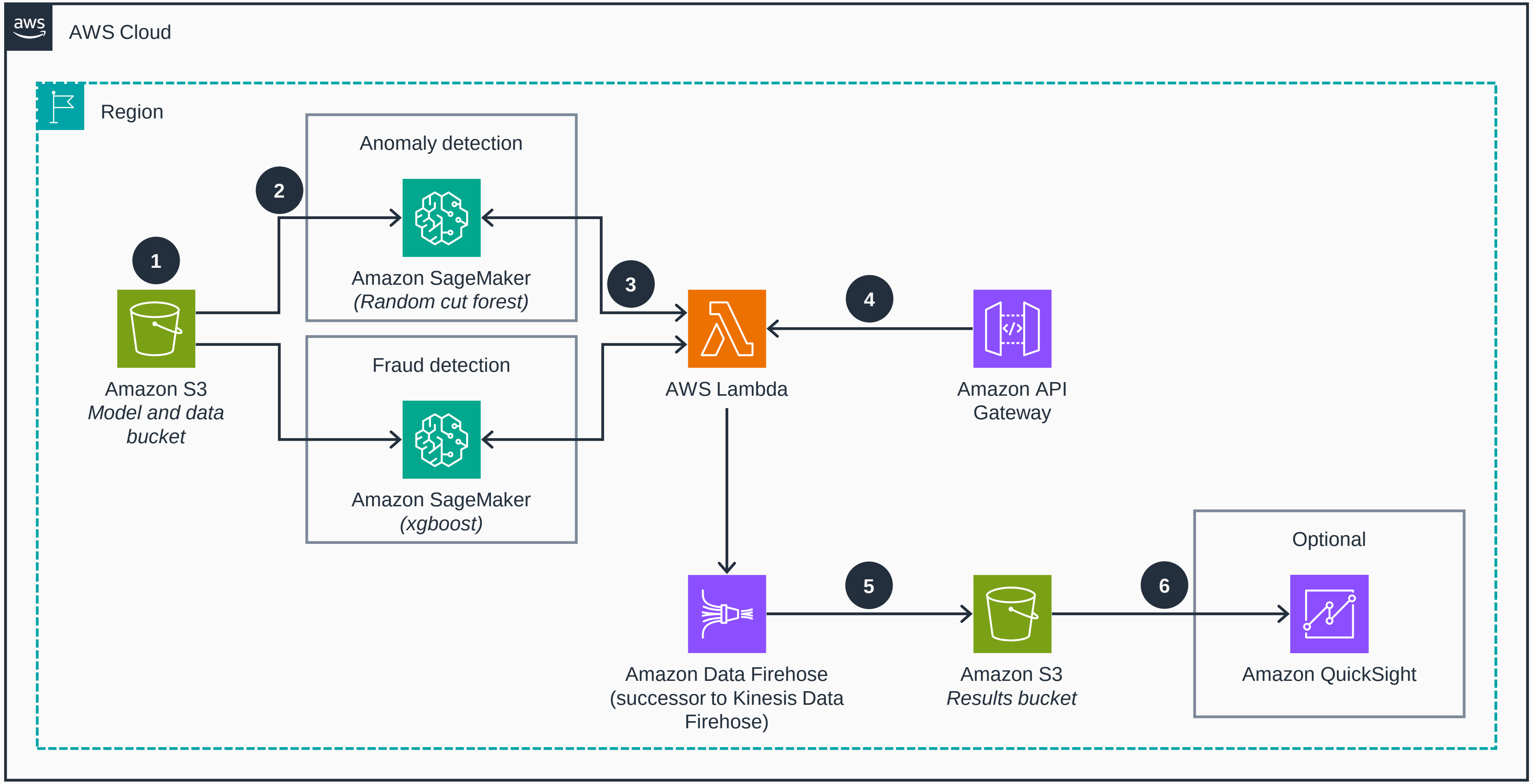
Guidance for Fraud Detection Using Machine Learning on AWS

This architecture diagram shows how to use a sample credit card transaction dataset to train a self-learning ML model that can recognize fraud patterns so that you can automate fraud detection and alerts.



1 An **Amazon Simple Storage Service (Amazon S3)** bucket contains an example dataset of credit card transactions.

2 An **Amazon SageMaker** notebook instance contains different ML models that will be trained on the dataset.

3 An **AWS Lambda** function processes transactions from the example dataset and invokes two **SageMaker** endpoints, which assign anomaly and classification scores to incoming data points.

4 An **Amazon API Gateway** REST API invokes predictions using signed HTTP requests.

5 An **Amazon Data Firehose (successor to Kinesis Data Firehose)** delivery stream loads the processed transactions into another **Amazon S3** results bucket for storage.

6 When the transactions have been loaded into **Amazon S3**, you can use analytics tools and services, including **Amazon QuickSight**, for visualization, reporting, individual queries, and more-detailed analysis.

Reviewed for technical accuracy October 7, 2024

AWS Reference Architecture