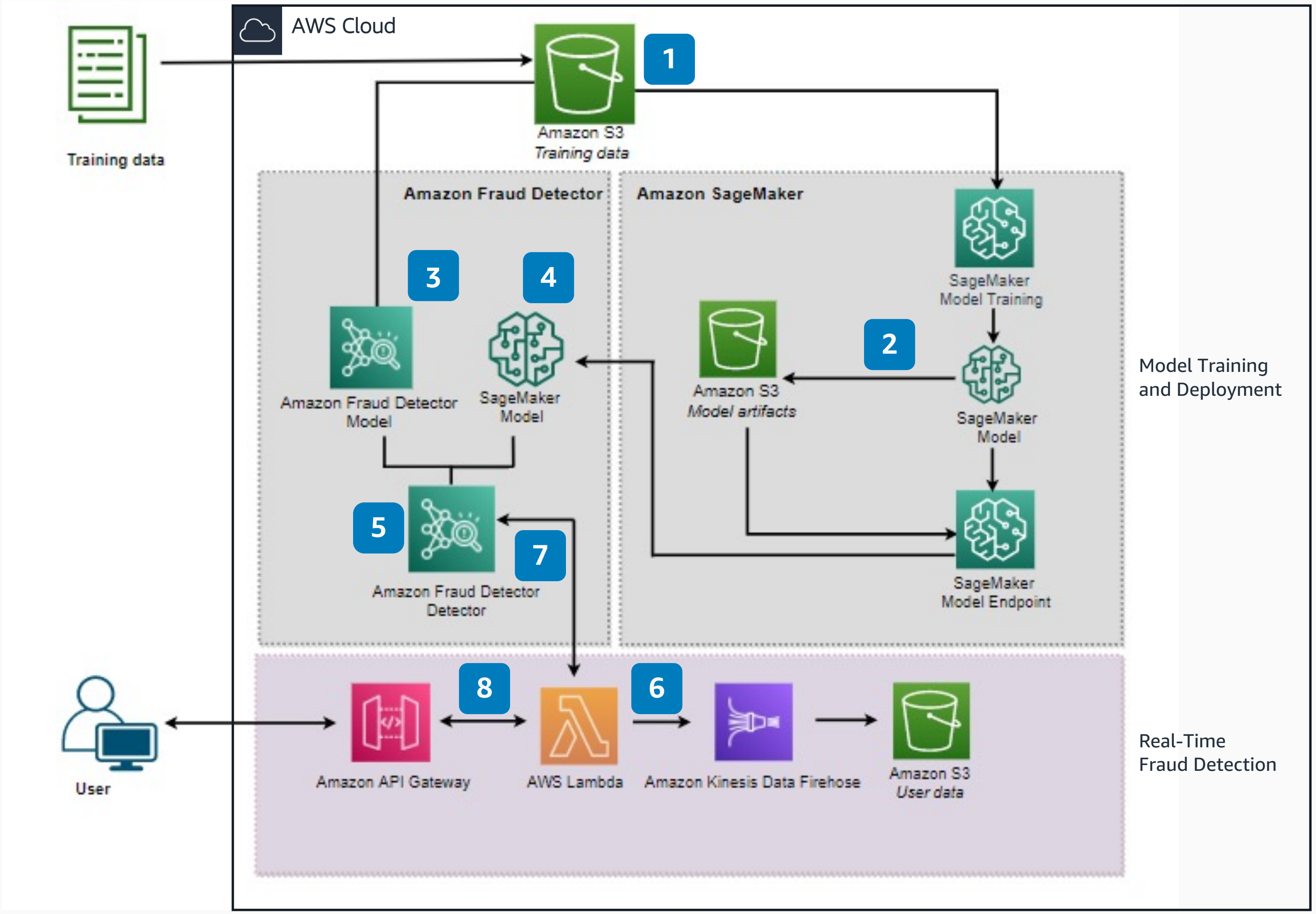
Hybrid Fraud Detector Engine

Create a real-time ensemble fraud detection engine using Amazon SageMaker and Amazon Fraud Detector.



1 The user uploads the data into an **Amazon Simple Storage Service (Amazon S3)** bucket to be used for training both a custom model in **Amazon SageMaker** and a model in **Amazon Fraud Detector**.

2 The custom fraud detection model is trained in **SageMaker**, model artifacts are saved in an **S3** bucket with server-side encryption enabled, and the model is deployed using a **SageMaker** model endpoint.

3 A fraud detection model is created in **Amazon Fraud Detector**.

4 The custom **SageMaker** model is exported to **Amazon Fraud Detector** using the deployed **SageMaker** endpoint created in step 2.

5 A detector that combines scores from both the **SageMaker** model and the **Amazon Fraud Detector** model is created, which has multiple decision rules.

6 At the time of inference, the incoming request coming from the user is received and sent to **AWS Lambda** for processing and invoking the fraud models. A copy of the data can be also saved on an **S3** bucket through **Amazon Kinesis** streaming services.

7 When **AWS Lambda** receives the data to use for inference, it invokes the **Amazon Fraud Detector** endpoint and receives the prediction.

8 The prediction output is communicated back downstream by **AWS Lambda** to the user or other downstream applications, as required.

Reviewed for technical accuracy September 25, 2021

AWS Reference Architecture