

## Project Design Phase-I

### Solution Architecture

|               |  |
|---------------|--|
| Date          | 13 November 2023                         |
| Team ID       | PNT2023TMID592150                        |
| Project Name  | Online Payments Fraud Detection using ML |
| Maximum Marks | 4 Marks                                  |

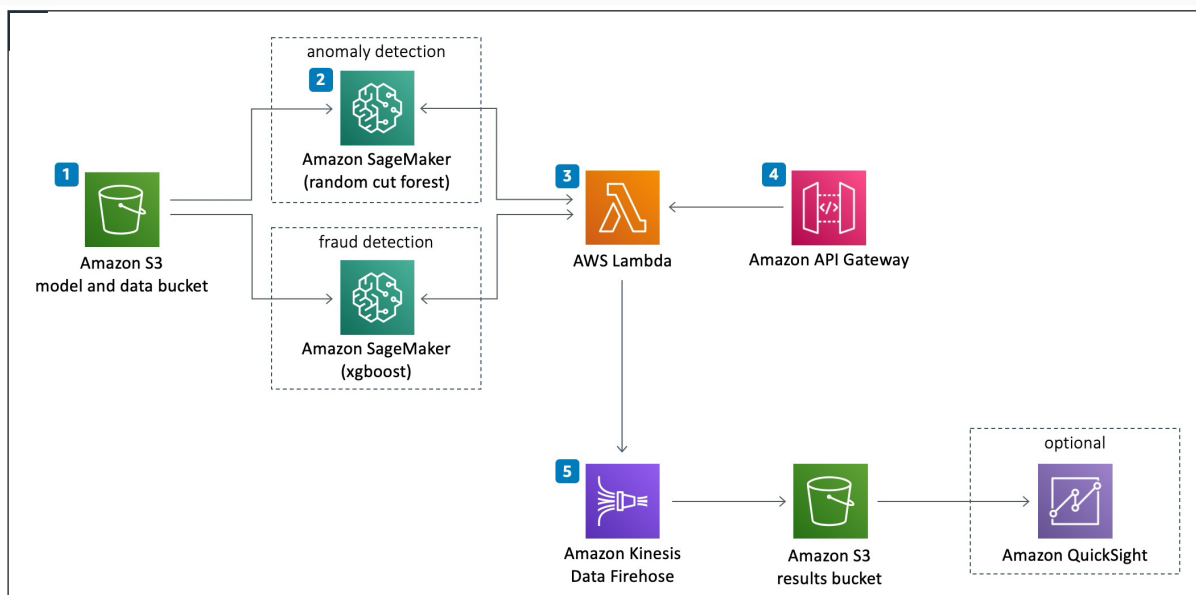
#### Solution Architecture:

Fraud Detection Using Machine Learning architecture  
The code deploys the following infrastructure:

1. An [Amazon Simple Storage Service](#) (Amazon S3) bucket containing an example dataset of credit card transactions.
2. An [Amazon SageMaker](#) notebook instance with different ML models that will be trained on the dataset.
3. An [AWS Lambda](#) function that processes transactions from the example dataset and invokes the two Amazon SageMaker endpoints that assign anomaly scores and classification scores to incoming data points.
4. An [Amazon API Gateway](#) REST API invokes predictions using signed HTTP requests.
5. An [Amazon Kinesis Data Firehose](#) delivery stream loads the processed transactions into another Amazon S3 bucket for storage.

The Guidance also provides an example of how to invoke the prediction REST API as part of the Amazon Sage maker notebook.

When the transactions have been loaded into Amazon S3, you can use analytics tools and services, including [Amazon QuickSight](#), for visualization, reporting, ad-hoc queries, and more detailed analysis.



#### Reference:

<https://aws.amazon.com/solutions/implementations/fraud-detection-using-machine-learning/>