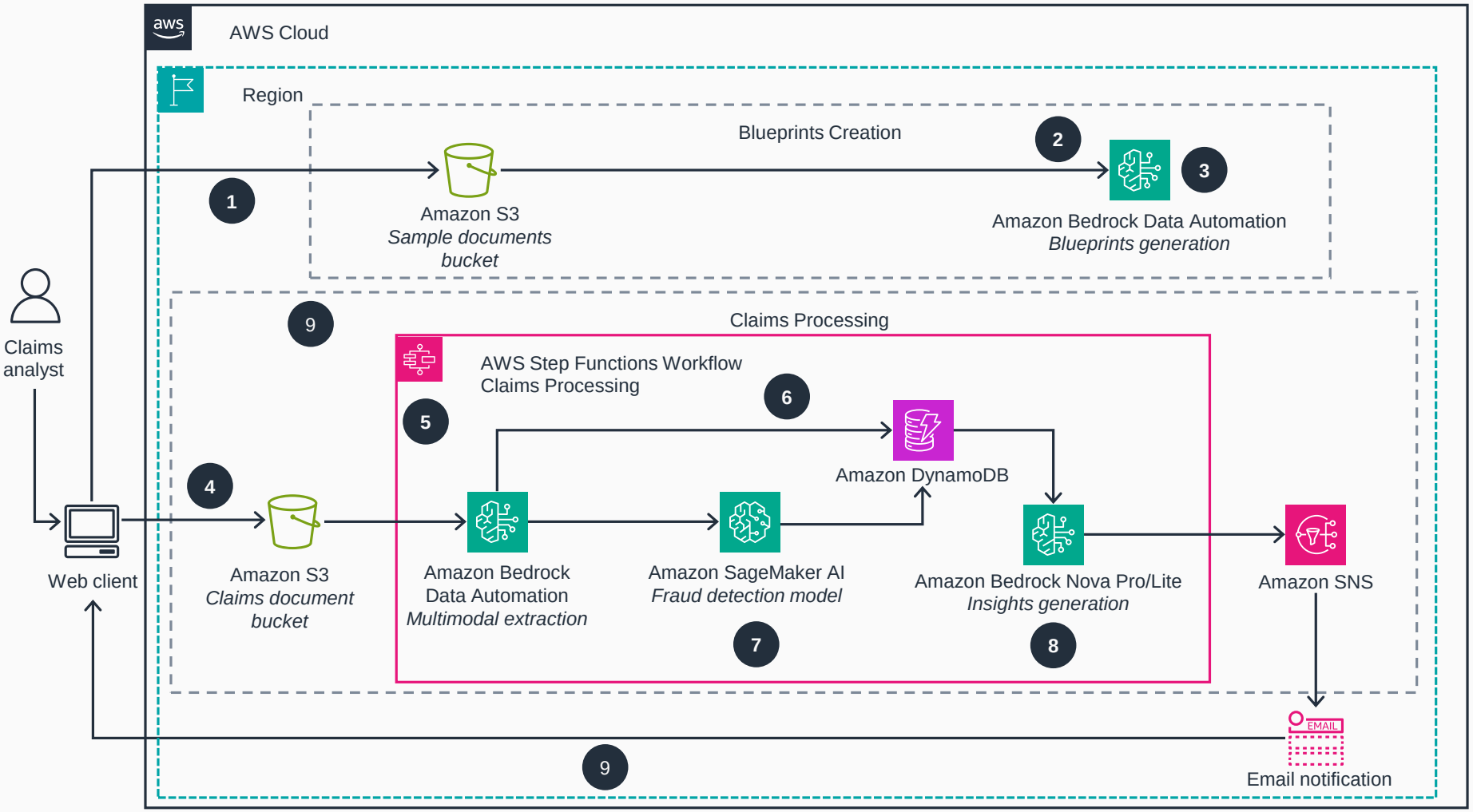
Guidance for Fraud Detection with Intelligent Document Processing on AWS

This architecture diagram illustrates how AWS services support fraud detection and Intelligent Document Processing (IDP) for insurance claims processing. The architecture combines computer vision models, Amazon Bedrock, and automated workflows to analyze claim documents, detect tampering, extract insights, and generate customized reports.



1. The claims analyst uploads sample documents through the web client to the **Amazon Simple Storage Service (Amazon S3)** bucket for blueprint creation.
2. **Amazon Bedrock Data Automation** uses JSON templates and Python scripts to create standardized blueprints for processing future claims file submissions.
3. **Amazon Bedrock Data Automation** refines and stores custom blueprints.
4. Claims analysts upload claim document packets that include supporting materials, such as claim forms, property damage pictures, identification documents, and audio files.
5. An **AWS Step Functions** (Claims Processing) workflow processes the submitted documents using the **Amazon Bedrock Data Automation** blueprints that were published in Step 2 to extract data.
6. The automated process stores extracted insights from text documents, audio files, and image metadata in **Amazon DynamoDB**.
7. A computer vision model hosted on **Amazon SageMaker AI** endpoints processes the submitted images to detect tampering and stores the results in **DynamoDB**. This model uses error level analysis (ELA), highlighting areas where compression levels don't match to reveal tampering.
8. **Amazon Nova Pro/Lite** foundation model analyzes the data stored in **DynamoDB** to generate summary reports, which users can view in the web client.
9. **Amazon Bedrock** processes the insights to generate customized reports for claims analysts or trigger automated notifications through **Amazon Simple Notification Service (Amazon SNS)** using email notifications.

Reviewed for technical accuracy May 15, 2025

AWS Reference Architecture