Security & Privacy Concerns



Mark Nunnikhoven AWS COMMUNITY HERO @marknca markn.ca

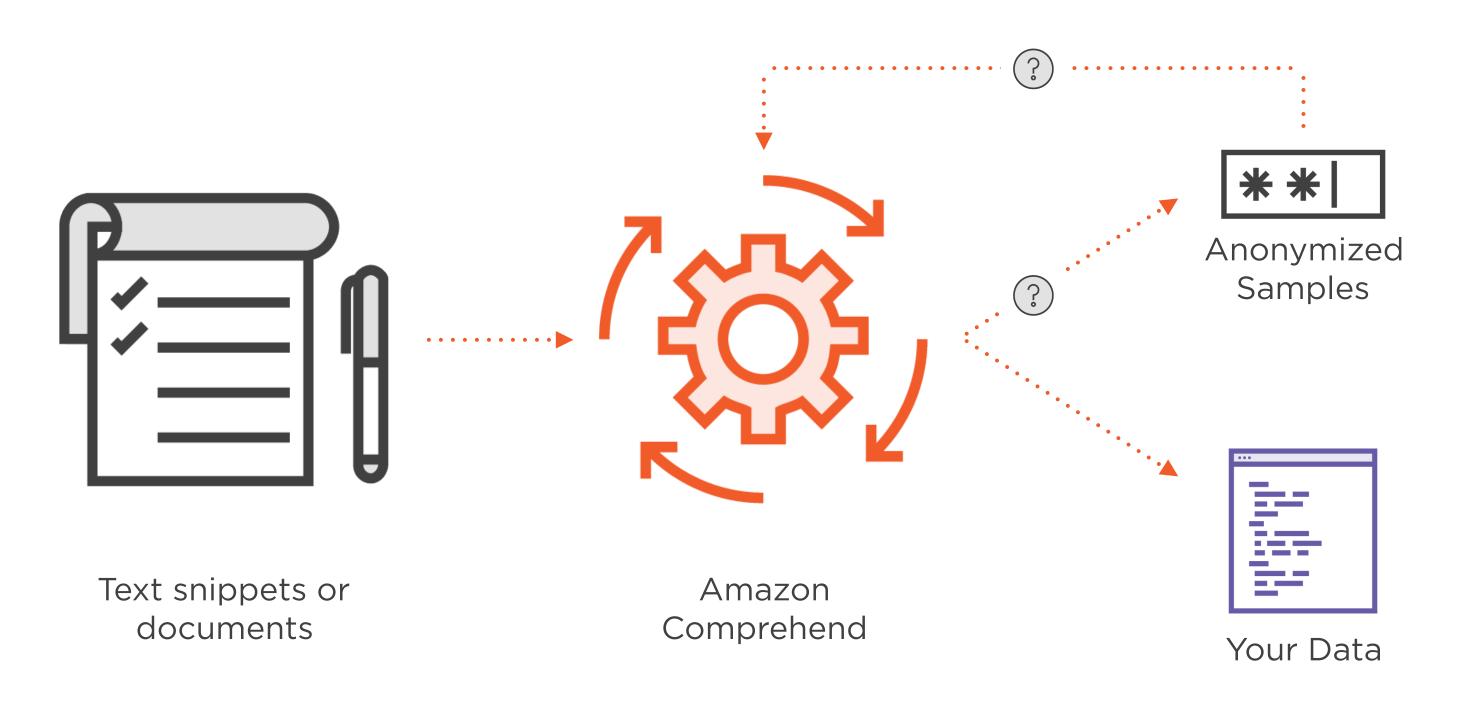
Overview

Examine the possible risk of natural language processing in the cloud

Understand how managed encryption can help reduce that risk

The Security and Privacy Risks of Analysis

Amazon Comprehend Workflow



Anonymized samples **may** be used to train the global models. This **may** pose a risk depending on data sensitivity

Principle of Least Privilege

Users and systems should only have the permissions required to complete their assigned tasks and nothing more

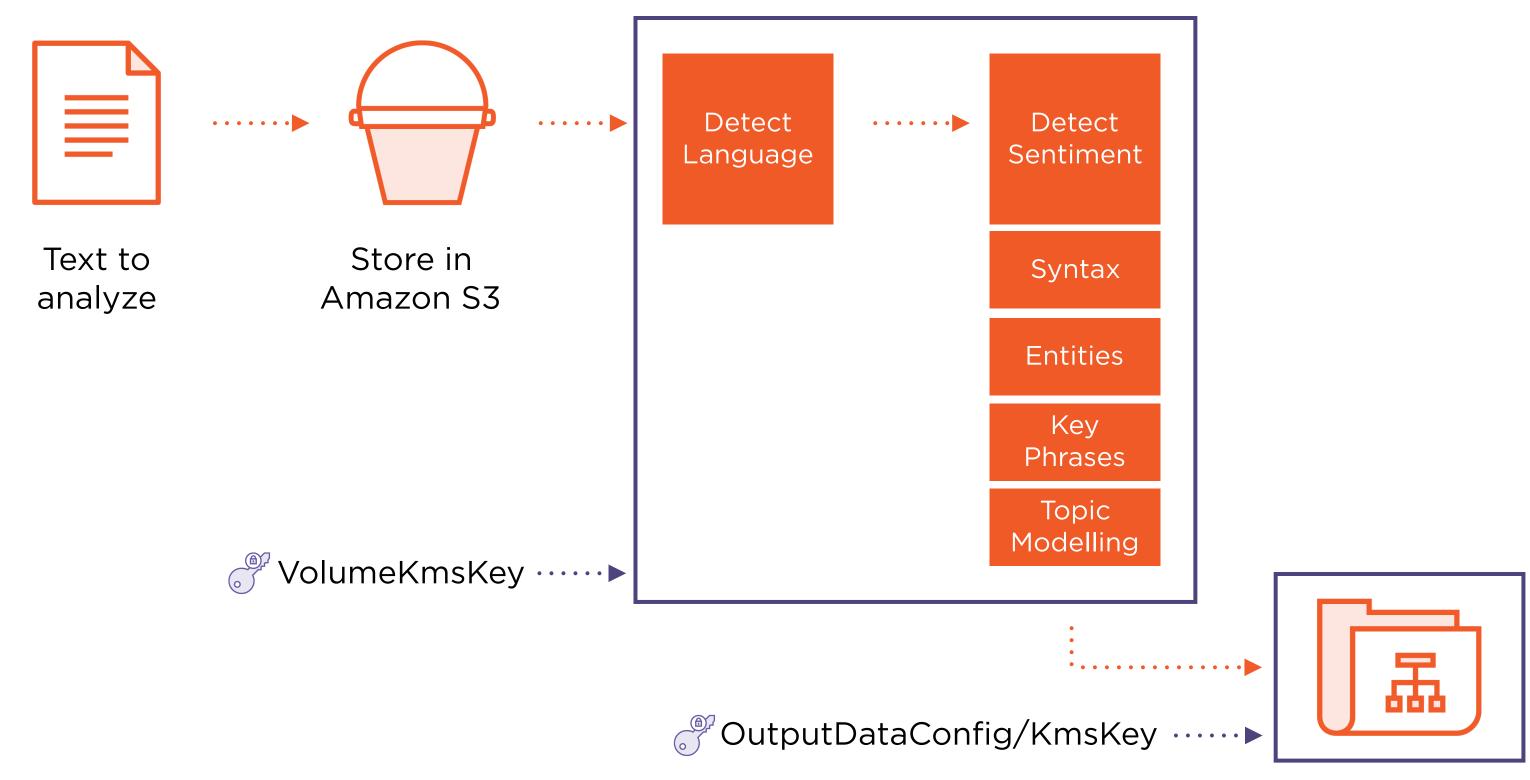


"DataAccessRole" should have read permissions to input documents and write permission to output documents

Restrict access to comprehend:*

Use KMS to encrypt data at rest

Document Analysis



Demo

Create two encryption key pairs in KMS for Amazon Comprehend

Process a classification job using KMS

View the change in results

Review



As with any AWS Machine Learning service, your data is safe and stays under your control exception small, anonymized samples that are used to tune to general model



Amazon Comprehend supports encryption via KMS for data processing and encrypting the output of any classifier



Leverage the principle of "least privilege" to reduce the potential risks associated with use of the service