# Securing Data with AWS KMS and OpenSSL on EC2

Objective

The objective of this practical exercise is to demonstrate how to securely encrypt and decrypt data using AWS Key Management Service (KMS) and OpenSSL on an Amazon EC2 instance. This process involves generating encryption keys with KMS, encrypting data locally on EC2, and safely handling encryption keys to ensure data confidentiality.
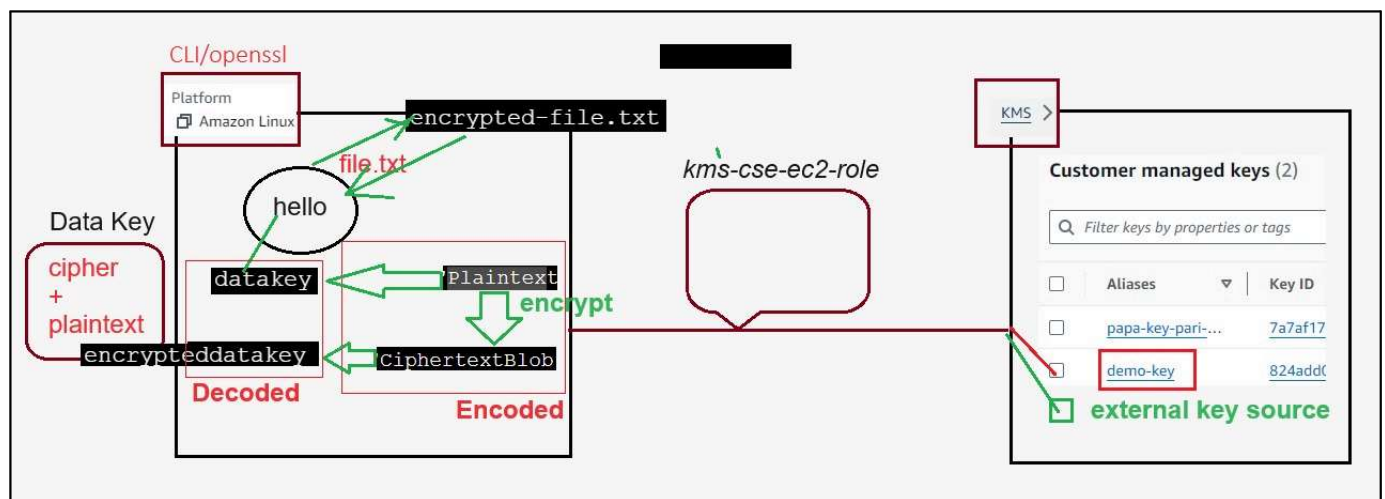
Steps to Implement

1. **Create a Customer Master Key (CMK) in AWS KMS:**
   - Navigate to the AWS Management Console.
   - Access the KMS service to create a new CMK for data encryption purposes.