AWS offers a comprehensive security framework for services using IAM and KMS work together. This combination helps protect sensitive information in AWS environments.

In this Cloud Lab, you’ll thoroughly explore the security and identity management services provided by AWS, focusing on IAM and KMS. You’ll learn about different IAM policies, create a user group with different policies, and add a user. Next, you’ll create an S3 bucket and attach a resource-based policy to allow public access. Then, you’ll create an execution role for a Lambda function. After this, you’ll create a customer-managed key for encrypted storage and database. Then, you’ll try to access it with a different user and learn how encryption key access works.

By the end of this Cloud Lab, you’ll have practical experience in using IAM identity-based policy, resource-based policy, and KMS keys for encrypting and decrypting AWS resources.

The following is the high-level architecture diagram of the infrastructure that you’ll create in this Cloud Lab:

