**How to encrypt the Database variables in AWS Lambda Function using customer KMS key**

1. **To create AWS KMS key**

A screenshot of a computer

Description automatically generated with medium confidence

1. **To create policy for KMS Decrypt Write operation with specific KMS ARN**

A screenshot of a computer

Description automatically generated with medium confidence

1. **To attach KMS policy to Lambda basic execution role**

//By default, lambda basic execution role has permission to create log group and log streams in CloudWatch

A screenshot of a computer

Description automatically generated with medium confidence

1. **To make ensure this role has attached to Lambda Function**

A screenshot of a computer

Description automatically generated with medium confidence

1. **To create an environment variable for Database**

A screenshot of a computer

Description automatically generated

Enable Encryption in transit

Select – Use a customer master key – choose – your KMS key

Then choose – Encrypt button – to encrypt the variable

After encryption – save the environment variables

A screenshot of a computer

Description automatically generated with medium confidence

1. **To execute the below code**

[**https://github.com/kohlidevops/aws-lambda-secure-env-variables/blob/main/lambda.py**](https://github.com/kohlidevops/aws-lambda-secure-env-variables/blob/main/lambda.py)

A screenshot of a computer program

Description automatically generated with medium confidence

//Once code has been placed don’t forget to deploy the code

1. **Test the code with sample event**

//If you select “shareable” then you can share this event to other IAM users (who have permission to access this lambda)

Just Save and Test this event

A screenshot of a computer

Description automatically generated with low confidence

You can see the encrypted & decrypted value for DB\_PASSWORD

A screenshot of a computer

Description automatically generated with medium confidence