This document explains how to setup a lambda function that gets data from AWS IoT Core and store it in DynamoDB

* The lambda function can be created through the console and a rule can be created in AWS IoT Core to send whatever is received in a topic directly to the AWS Lambda function that has been created.
* The lambda function created is IoTtoDynamoDB.
* For users and applications in your account that use Lambda, you manage permissions in a permissions policy that you can apply to IAM users, groups, or roles.
* To grant permissions to other accounts or AWS services that use your Lambda resources, you use a policy that applies to the resource itself.
* A Lambda function also has a policy, called an execution role, that grants it permission to access AWS services and resources. If your function accesses services with the AWS SDK, you grant it permission to call them in the execution role.
* Use resource-based policies to give other accounts and AWS services permission to use your Lambda resources. Lambda resources include functions, versions, aliases, and layer versions. Each of these resources has a permissions policy that applies when the resource is accessed, in addition to any policies that apply to the user. When an AWS service like Amazon S3 calls your Lambda function, the resource-based policy gives it access.
* So, for a lambda function to access another AWS resource, we use an execution role to grant it permission. If the lambda function is called by some other resources, then that permission must be specified in the resource-based policy.
* Explanation in detail is provided here: <https://docs.aws.amazon.com/lambda/latest/dg/lambda-permissions.html>

Including explanations about execution role and resource based policies.

* To provide this lambda function with the read and write permission to DynamoDB, the following policy must be added: <https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_lambda-access-dynamodb.html>

A role for this function will already exist, inside which there will be a policy to allow this function to write to CloudWatch logs. This is done as a default when creating the function.

* To add the rea, write permission, we go into the role that the function is using (in this case[, MyLambdaRole](https://console.aws.amazon.com/iam/home?region=us-east-2#/roles/MyLambdaRole)).Inside the role, under Permissions, we can attach a policy. We create a new policy and copy the policy in the json format (link above) and paste it here and change the db name.
* The code to write data to dynamoDB using python can be found here under “Creating a new item”:

<https://boto3.amazonaws.com/v1/documentation/api/latest/guide/dynamodb.html>

* The handler function is invoked by AWS Lambda when the code is run. Any data sent to this function is passed to the event parameter. So, the sensor data that we send will be in this parameter. For more info about the handler, check here: <https://docs.aws.amazon.com/lambda/latest/dg/python-handler.html>