Configuration Manual

MSc Research Project
Cloud Computing

Dhyanesh Naik
Student ID: X22206124

School of Computing
National College of Ireland

Supervisor: Rashid Mijumbi

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	DHYANESH PRADIP NAIK
Student ID:	X22206124
Programme:	: Cloud Computing **Year:** 2024
Module:	MSc Research Project
Lecturer:	Rashid Mijumbi
Submission Due Date:	12/08/2024
Project Title:	A Serverless Federated Learning Service Ecosystem for Secure and Flexible Model Sharing in Multi-Cloud Environments
Word Count:	527 **Page Count: 4**

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Dhyanesh Pradip Naik

Date: 12th August 2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□

Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

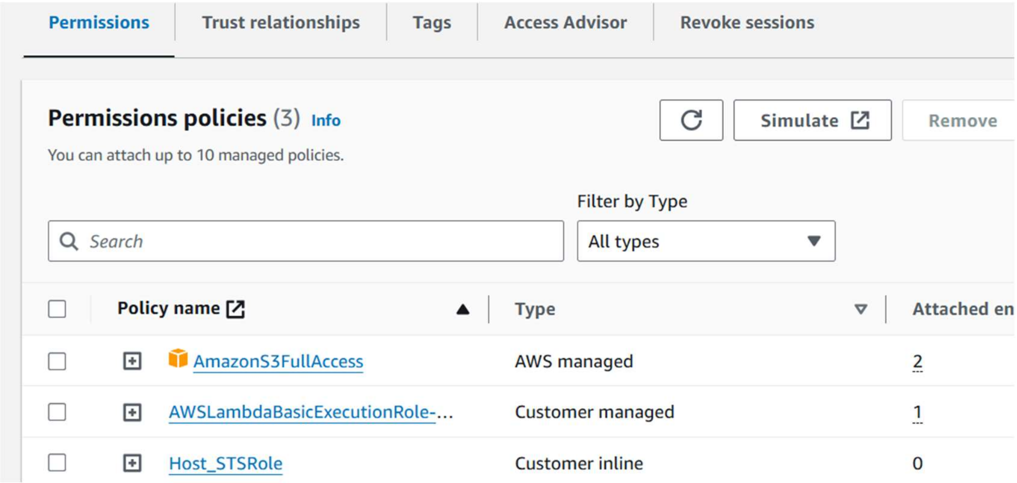
Configuration Manual

Dhyanesh Naik
X22206124

1 Introduction

This Configuration Manual covers all AWS prerequisites for repeating the study and its outcomes. This document covers a synthetically generated dataset, Python ML packages, AWS Lambda, and AWS CloudFormation implementation.

2 AWS Lambda Configuration



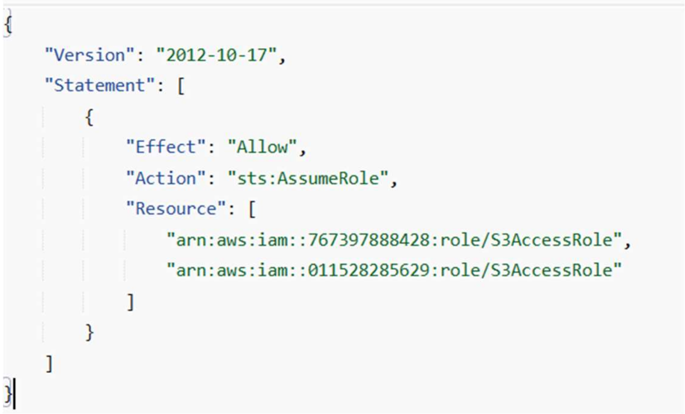
Permissions policies (3) Info

You can attach up to 10 managed policies.

Filter by Type: All types

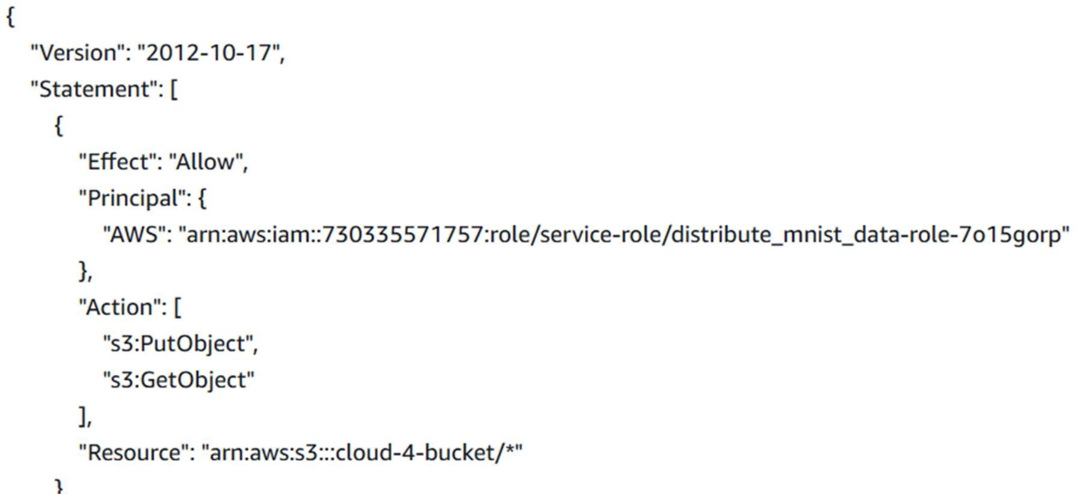
□	Policy name	Type	Attached en
□	AmazonS3FullAccess	AWS managed	2
□	AWSLambdaBasicExecutionRole-...	Customer managed	1
□	Host_STSRole	Customer inline	0

Figure 1: IAM Execution Role for MNIST Distribute Lambda Function



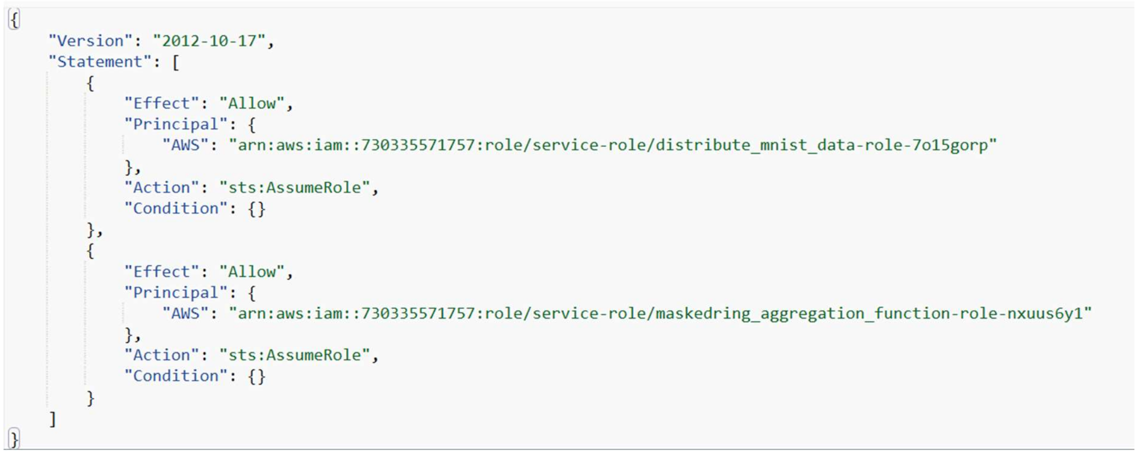
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": [
                "arn:aws:iam::767397888428:role/S3AccessRole",
                "arn:aws:iam::011528285629:role/S3AccessRole"
            ]
        }
    ]
}
```

Figure 2: Security Token Service Role Policy for Cross-cloud Access



```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::730335571757:role/service-role/distribute_mnist_data-role-7o15gorp"
      },
      "Action": [
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource": "arn:aws:s3:::cloud-4-bucket/*"
    }
```

Figure 3: S3 bucket policy to access the client bucket, cloud-4-bucket from host cloud lambda function



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::730335571757:role/service-role/distribute_mnist_data-role-7o15gorp"
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        },
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::730335571757:role/service-role/maskedring_aggregation_function-role-nxuus6y1"
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```

Figure 4: S3AccessRole Trust Relationship for Cross-cloud Access from Host Cloud

3 Data Science Environment and Packages

- Pandas
- Numpy
- Matplotlib
- Scikit-learn
- TensorFlow
- PyTorch
- PyCryptodome
- Imblearn
- Boto3
- Logging
-

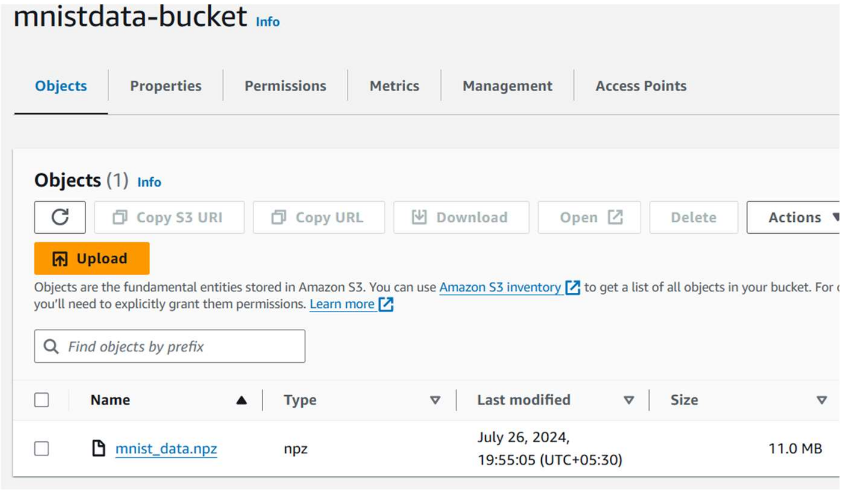
4 Dataset

This work uses MNIST dataset for model aggregation on the host cloud, and distributes the MNIST subsets across client clouds. The MNIST is a database of handwritten digits. It consists of 60,000 training Examples and a Test set with 10,000 examples It is a subset of the larger NIST Special Database 3 and Special Database 1, which contain binary images. NIST originally designated black and white, bilevel images in a (minimum) 20x20 pixel box with aspect ratio preserved.

The MNIST dataset can be download from the link,

https://paperswithcode.com/dataset/mnist

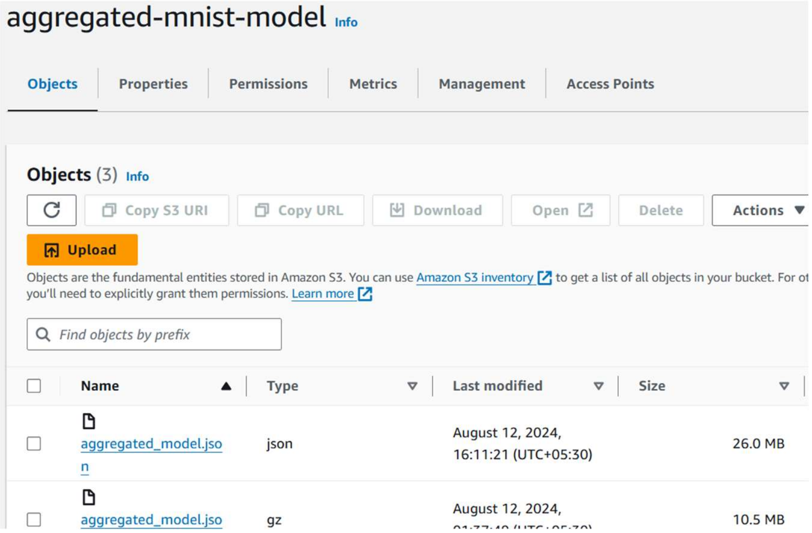
5 AWS S3 Access



Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For
you'll need to explicitly grant them permissions. Learn more

□	Name ▲	Type	Last modified	Size
□	mnist_data.npz	npz	July 26, 2024, 19:55:05 (UTC+05:30)	11.0 MB

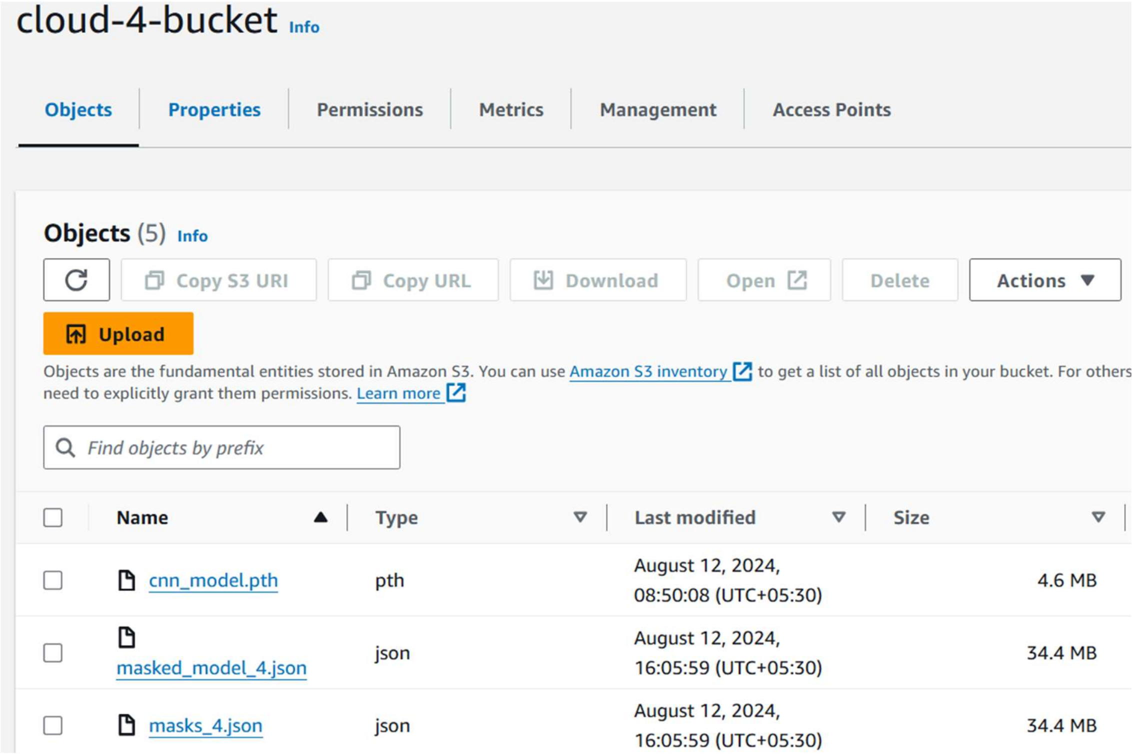
Figure 5. MNIST Host Data Bucket



Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For ot
you'll need to explicitly grant them permissions. Learn more

□	Name ▲	Type	Last modified	Size
□	aggregated_model.json	json	August 12, 2024, 16:11:21 (UTC+05:30)	26.0 MB
□	aggregated_model.jso	gz	August 12, 2024,	10.5 MB

Figure 6. MNIST Host Model Bucket

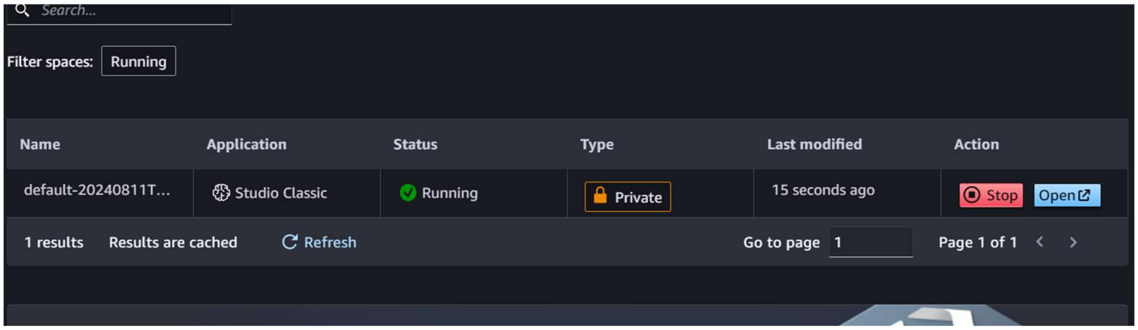


Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others need to explicitly grant them permissions. Learn more

□	Name ▲	Type	Last modified	Size
□	cnn_model.pth	pth	August 12, 2024, 08:50:08 (UTC+05:30)	4.6 MB
□	masked_model_4.json	json	August 12, 2024, 16:05:59 (UTC+05:30)	34.4 MB
□	masks_4.json	json	August 12, 2024, 16:05:59 (UTC+05:30)	34.4 MB

Figure 7. MNIST Client Model and Data Bucket

6 AWS Sagemaker Domain



Name	Application	Status	Type	Last modified	Action
default-20240811T...	Studio Classic	Running	Private	15 seconds ago	Stop Open

1 results Results are cached

Figure 8. SageMaker Domain Access for Local Training

References

Amazon Web Services (2023) What is AWS CloudFormation? Available at: https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/Welcome.html (Accessed: 12 August 2024).
Serverless, Inc. (2023) AWS Lambda: The Ultimate Guide. Available at: https://www.serverless.com/aws-lambda (Accessed: 12 August 2024).