National College of Ireland

Configuration Manual

MSc Research Project
Cloud Computing

Sanjana Gavhane
Student ID: x23325178

School of Computing
National College of Ireland

Supervisor: Yasantha Samarawickrama

National College of Ireland
Project Submission Sheet
School of Computing

Student Name:	Sanjana Gavhane
Student ID:	x23325178
Programme:	Cloud Computing
Year:	2024-2025
Module:	MSc Research Project
Supervisor:	Yasantha Samarawickrama
Submission Due Date:	11/08/2025
Project Title:	Configuration Manual
Word Count:	1000
Page Count:	7

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:	
Date:	11th August 2025

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

Sanjana Gavhane
x23325178

1 Introduction

This configuration guide shows how to install and use the multimodal deepfake detection system in a step-by-step manner. It will explain both the training stage of the offline model in Google Colab as well as the inference stage in the cloud in real-time with the help of AWS S3, cloud, Lambda, EC2, and DynamoDB. The proposed system uses the Capsule Network with the audio-visual fusion of scores to identify manipulated videos accurately using privacy-preserving, scalable, and automatic detection of manipulations in multiple content sources.

2 System Requirements

1. Cloud Resources:

- Google Colab with GPU runtime (e.g., NVIDIA Tesla T4 provided by Colab) for model training.
- AWS S3 for dataset storage and retrieval.
- AWS Lambda for event-driven inference.
- AWS EC2 (Ubuntu 22.04) for hosting the inference server and preprocessing scripts.
- AWS DynamoDB for result storage.
- AWS CloudWatch for logging and monitoring.

2. Software Environment:

- Python 3.11+ *Welcome to Python.org* (n.d.)
- Required libraries:
  - `boto3` (1.40.4)
  - `facenet-pytorch` (2.6.0)
  - `librosa` (0.11.0)
  - `matplotlib` (3.10.0)
  - `opencv-python` (4.11.0.86)

3 Model Training and Evaluation

1. Access Google Colab

- Open Google Colab. *Google Colab* (n.d.)
- Ensure GPU runtime is enabled: Runtime → Change Runtime Type → GPU.

2. Access Google Colab

- Connect to AWS S3.
- Use AWS temporary session credentials to connect.

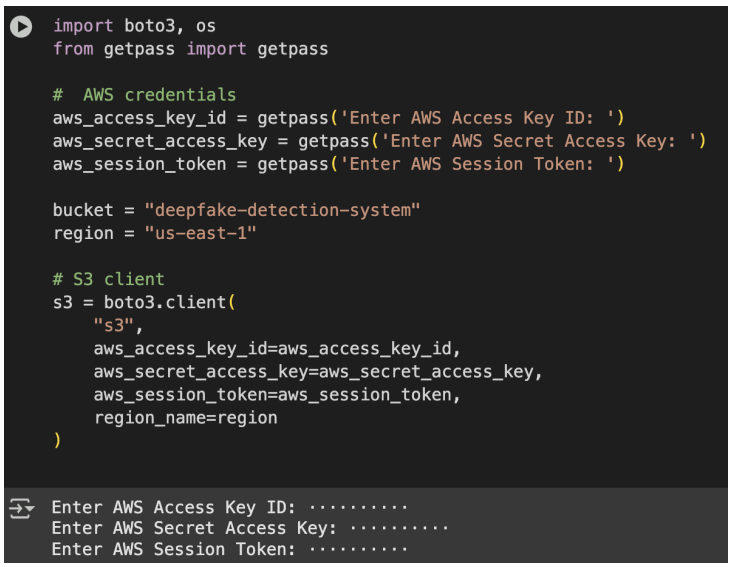

Figure 1: AWS IAM Temporary Credentials Setup in Google Colab

3. Download Dataset from S3

- Bucket name: deepfake-detection-system

Folders:

- FakeVideo-RealAudio/
- RealVideo-FakeAudio/

4. Extract Face Frames & Audio

For each video:

- Extract 1 face frame (*visual modality*).
- Extract audio, convert to WAV, then generate mel spectrogram (*audio modality*).

5. Train Model

- Use Capsule Network + Score Fusion architecture. Muppalla et al. (2023) Kwabena Patrick et al. (2022)
- Dataset split: 80% training / 20% testing.

6. Save Trained Model

- Final model file: `capsule_scorefusion_model.pth`.
- Upload to S3 bucket: `deepfake-detection-system/model/`.

4 Real-Time Cloud Inference

1. Create S3 Bucket

- **Name:** `deepfake-detection-system` *Amazon S3 - Cloud Object Storage - AWS* (n.d.)
- Enable **SSE-KMS encryption** to ensure data is encrypted at rest without manual key management.
- Enable **Versioning** to maintain historical versions of uploaded files for audit and rollback purposes.

Folder Structure:

- `FakeVideo-RealAudio/` – dataset folder
- `RealVideo-FakeAudio/` – dataset folder
- `models/` – stores the trained model file
- `realtime-demo/` – receives videos for real-time inference

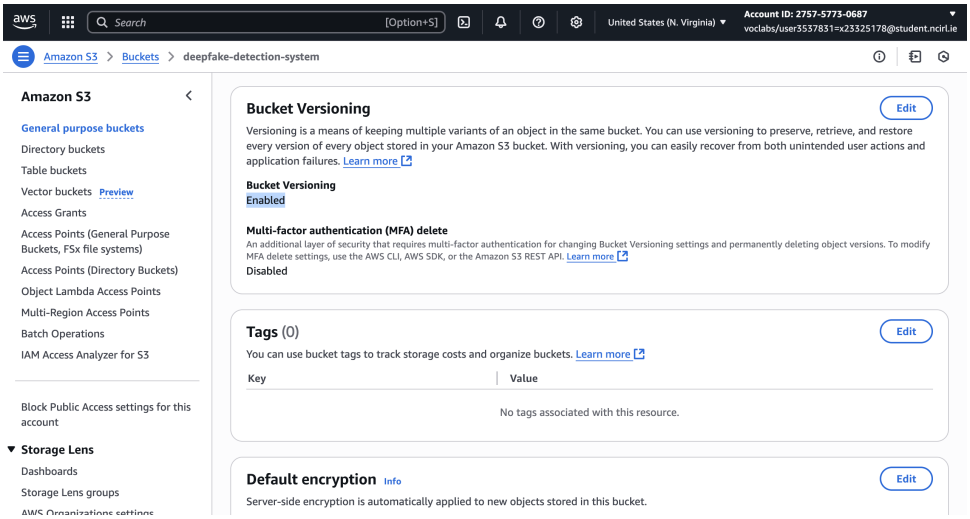

Figure 2: Versioning Enabled

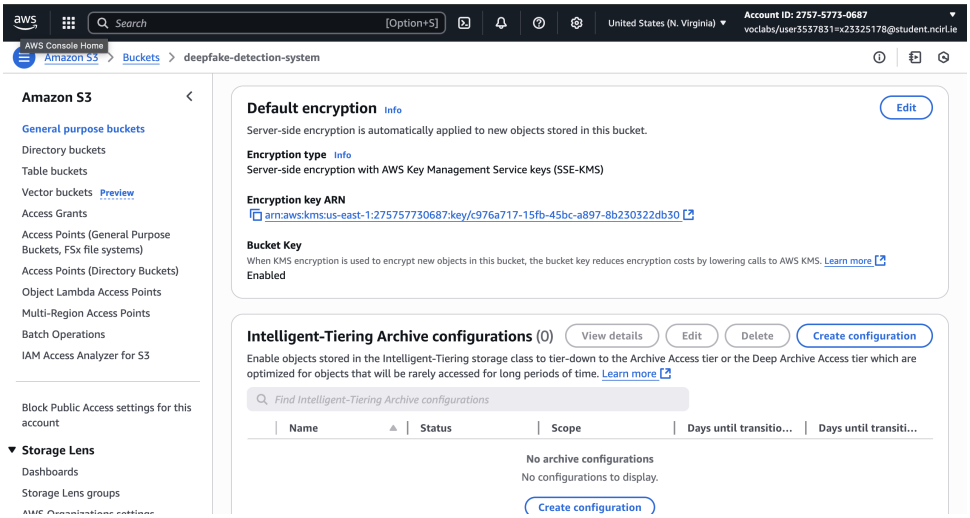

Figure 3: SSE-KMS Encryption Enabled

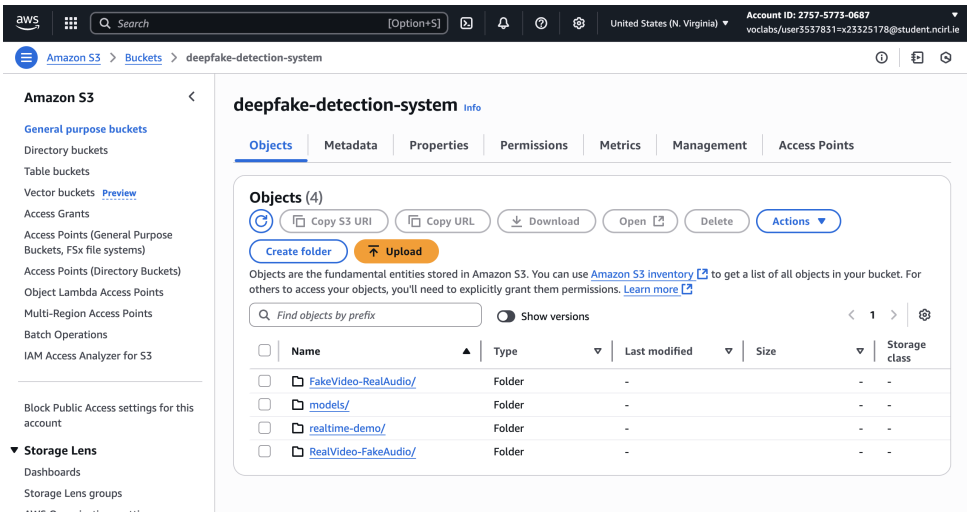

Figure 4: S3 bucket properties showing SSE-S3 and Versioning enabled

2. Set Up DynamoDB Table

- Table name: `DetectionResults`. *Amazon DynamoDB* (n.d.)
- Partition key: `id` (String).

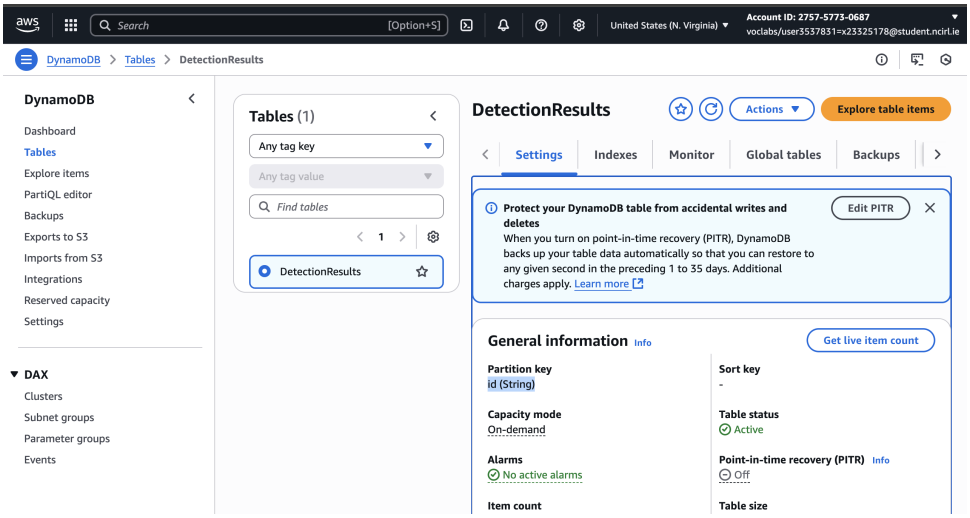

Figure 5: DynamoDB Table Setup

3. Launch EC2 Instance

- OS: Ubuntu 22.04 LTS. *Amazon EC2 - Cloud Compute Capacity - AWS* (n.d.)
- Install required libraries (same as training).

4. Set Up AWS Lambda Function

- Trigger: S3 PUT event on realtime-demo/. *Serverless Computing Service - Free AWS Lambda - AWS* (n.d.)

Function process:

- Download uploaded video from S3.
- Extract face + spectrogram.
- Load trained model from S3.
- Run inference and generate prediction.
- Store results in DynamoDB.

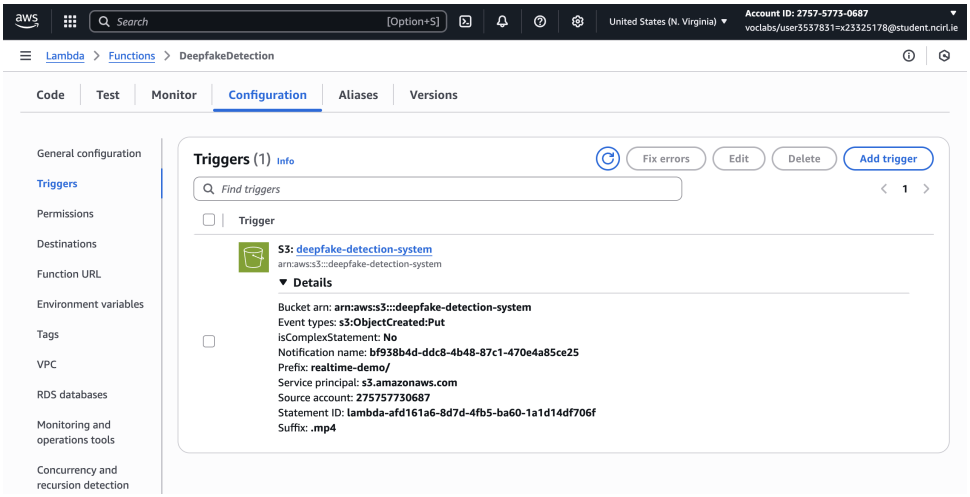

Figure 6: S3 Event Trigger

5. Enable CloudWatch Logging

- Monitor Lambda execution logs for errors or metrics. *APM Tool - Amazon CloudWatch - AWS* (n.d.)

6. Test the Pipeline

- Upload test videos to realtime-demo/.
- Verify results in DynamoDB table.

References

Amazon DynamoDB (n.d.).
URL: *https://aws.amazon.com/dynamodb/*

Amazon EC2 - Cloud Compute Capacity - AWS (n.d.).
URL: *https://aws.amazon.com/ec2/*

Amazon S3 - Cloud Object Storage - AWS (n.d.).
URL: *https://aws.amazon.com/s3/*

APM Tool - Amazon CloudWatch - AWS (n.d.).
URL: *https://aws.amazon.com/cloudwatch/*

Google Colab (n.d.).
URL: *https://colab.research.google.com/*

Kwabena Patrick, M., Felix Adekoya, A., Abra Mighty, A. and Edward, B. Y. (2022). Capsule Networks – A survey, *Journal of King Saud University - Computer and Information Sciences* **34**(1): 1295–1310.
URL: *https://www.sciencedirect.com/science/article/pii/S1319157819309322*

Muppalla, S., Jia, S. and Lyu, S. (2023). Integrating Audio-Visual Features For Multimodal Deepfake Detection, *2023 IEEE MIT Undergraduate Research Technology Conference (URTC)*, pp. 1–5.
URL: *https://ieeexplore.ieee.org/document/10534969*

Serverless Computing Service - Free AWS Lambda - AWS (n.d.).
URL: *https://aws.amazon.com/pm/lambda/*

Welcome to Python.org (n.d.).
URL: *https://www.python.org/doc/*