Configuration Manual

MSc Research Project
Cloud Computing

Rajesh Reddy Madduri
Student ID: 23340231

School of Computing
National College of Ireland

Supervisor: Shaguna Gupta

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Rajesh Reddy Madduri
Student ID:	23340231
Programme:	Cloud Computing **Year:** 2024-2025
Module:	MSc Research Project
Lecturer:	Shaguna Gupta
Submission Due Date:	15-09-2025
Project Title:	Cloud-Based Federated Learning System for Financial Fraud Detection
Page Count:	5
Word Count:	637

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 Rajesh Reddy Madduri

Date: 15-09-2025

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

Rajesh Reddy Madduri
Student ID: 23340231

The given manual will give a step-by-step protocol on how to set up the Cloud-Based Federated Learning System that can be used to detect financial fraud. The system integrates privacy preserving federated learning that offers explainable AI (XAI), running on aws infrastructure through Docker containerisation.

1 Environment Requirements

1.1 System Requirements

- OS: Windows/Linux
- RAM: Min 8GB
- Storage: SSD Preferred with no less than 256GB
- Network: Stable Internet for AWS CLI access and package downloads

1.2 Software Dependencies

- Python 3.9+
- Docker 24.0+
- Docker Compose 2.0+
- AWS CLI
- Git

1.3 AWS Services

- S3: Model storage
- CloudWatch: Monitoring and logging

2 Tools and Technologies

2.1 Core Technologies

- TensorFlow: 2.13.0 – for deep learning
- Docker - for Containerization
- Flask - Web dashboard
- boto3 - AWS SDK for Python

2.2 Machine Learning

- scikit-learn: 1.6.1 - ML utilities
- numpy: 1.24.3 - Numerical computing
- pandas: 2.3.1 - Data manipulation

2.3 Explainable AI Tools

- SHAP: 0.48.0 - Model explanations
- LIME: 0.2.0.1 - Local interpretability
- matplotlib: 3.10.3 - Visualization

3 Package Requirements

3.1 Edge Client Packages (docker/edge/requirements.txt)

```
tensorflow==2.13.0
boto3==1.39.4
numpy==1.24.3
pandas==2.3.1
scikit-learn==1.6.1
shap==0.48.0
lime==0.2.0.1
matplotlib==3.10.3
seaborn==0.13.2
cryptography==41.0.7
requests==2.31.0
```

3.2 Dashboard Requirements (docker/dashboard/requirements.txt)

```
Flask==3.1.1
flask-cors==6.0.1
plotly==6.2.0
numpy==1.24.3
pandas==2.3.1
boto3==1.39.4
PyYAML==6.0.2
requests==2.31.0
```

4 Installation Procedure

4.1 Install Docker and AWS CLI

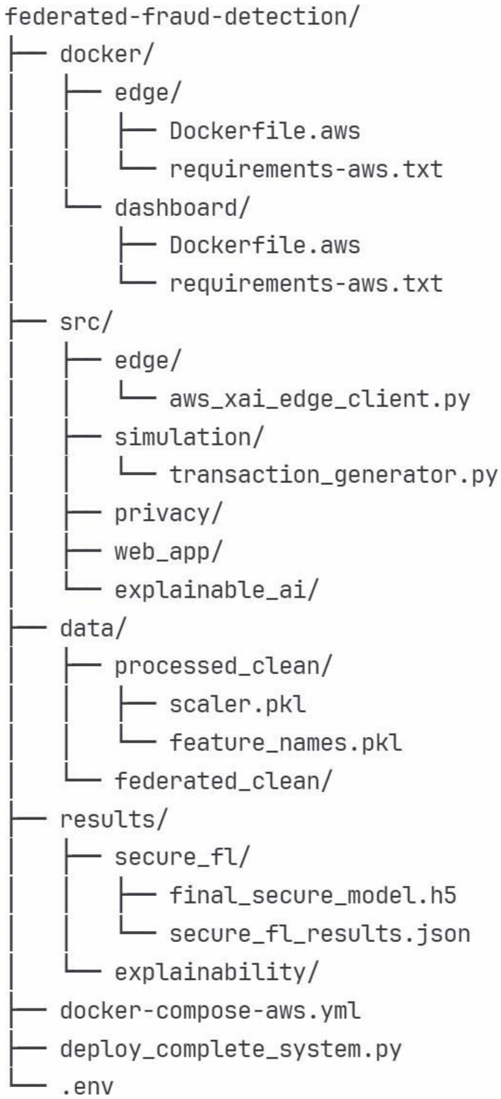
```
# Install Docker (Ubuntu/Debian)
sudo apt-get update
sudo apt-get install docker.io docker-compose

# Install AWS CLI
curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"
unzip awscliv2.zip
sudo ./aws/install
```

4.2 Download Dataset

https://www.kaggle.com/datasets/sgpjesus/bank-account-fraud-dataset-neurips-2022

4.3 Project Directory



```
federated-fraud-detection/
├── docker/
│   ├── edge/
│   │   ├── Dockerfile.aws
│   │   └── requirements-aws.txt
│   └── dashboard/
│       ├── Dockerfile.aws
│       └── requirements-aws.txt
├── src/
│   ├── edge/
│   │   └── aws_xai_edge_client.py
│   ├── simulation/
│   │   └── transaction_generator.py
│   ├── privacy/
│   ├── web_app/
│   └── explainable_ai/
├── data/
│   ├── processed_clean/
│   │   ├── scaler.pkl
│   │   └── feature_names.pkl
│   └── federated_clean/
├── results/
│   ├── secure_fl/
│   │   ├── final_secure_model.h5
│   │   └── secure_fl_results.json
│   └── explainability/
├── docker-compose-aws.yml
├── deploy_complete_system.py
└── .env
```

5 Configuration

5.1 AWS Credentials

```
# AWS Configuration
S3_BUCKET=your-fraud-detection-bucket
AWS_ACCESS_KEY_ID=your-access-key-id
AWS_SECRET_ACCESS_KEY=your-secret-access-key
AWS_SESSION_TOKEN=your-session-token-if-needed
AWS_DEFAULT_REGION=us-east-1

# System Configuration
NUM_CLIENTS=3
NUM_ROUNDS=10
EPSILON=1.0
```

5.2 AWS Bucket

```
# Create S3 bucket
aws s3 mb s3://your-fraud-detection-bucket --region us-east-1

# Set bucket policy for federated learning
aws s3api put-bucket-policy --bucket your-fraud-detection-bucket --policy file://bucket-policy.json
```

6 Execution Steps

6.1 Docker Deployment

```
# Step 1: Build and start Docker services
docker-compose -f docker-compose-aws.yml up -d --build

# Step 2: Monitor service status
docker-compose -f docker-compose-aws.yml ps

# Step 3: View logs
docker-compose -f docker-compose-aws.yml logs -f
```

6.2 Edge Client Deployment

```
# Terminal 1 - Edge Client 0
export CLIENT_ID=0
python aws_edge_client.py

# Terminal 2 - Edge Client 1
export CLIENT_ID=1
python aws_edge_client.py

# Terminal 3 - Edge Client 2
export CLIENT_ID=2
python aws_edge_client.py
```

7 System Monitoring

Dashboard: http://localhost:5000/