

Configuration Manual

MSc Research Project
MSc Cyber Security

Ramani Katale
Student ID:23320834

School of Computing
National College of Ireland

Supervisor: Prof. Joel Aleburu

National College of Ireland
MSc Project Submission Sheet



School of Computing

Student Name: Ramani Tukaram Katale

Student ID: X23320834

Programme: MSc Cybersecurity

Year: 2024-2025

Module: Research Project

Lecturer: Prof. Joel Aleburu

Submission Due Date:

11-08-2025

Project Title: Privacy-Preserving Poisoning Attack Detection in Federated Learning for IDS Using CKKS Homomorphic Encryption and Hybrid Approach.

Word Count: 544

Page Count: 3

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: Ramani Tukaram Katale.

Date: 11-08-2025

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

"Privacy-Preserving Poisoning Attack Detection in Federated Learning for IDS Using CKKS Homomorphic Encryption and Hybrid Approach"

Environment: Jupyter notebook
Main Components: CKKS Encryption, hybrid approach, Autoencoder

1. What This Project Does

This research project implements a **privacy-preserving Intrusion Detection System (IDS)** using **Federated Learning (FL)**.

The system integrates **CKKS homomorphic encryption** to protect client model updates, and **Krum** robust aggregation to defend against poisoning attacks.

The IDS uses a **hybrid anomaly detection** approach (Autoencoder + Clustering) and evaluates performance under different malicious client ratios (5%, 20%, 40%) using **NSL-KDD** and **CICIDS-2018** datasets.

Key capabilities:

- **Train federated IDS models** with real-world intrusion datasets.
- **Encrypt client updates** using CKKS to preserve data privacy.
- **Detect and mitigate poisoning attacks** using Krum aggregation.
- **Simulate varying attack intensities** to test robustness.
- **Log performance metrics** (Precision, Recall, F1-score, Accuracy) for each attack scenario.
- **Generate comparative bar plots** for Plain vs Encrypted FL performance.

2. Tools & Technologies Used

Component	Tool / Library
Programming Language	Python 3.10+
FL Framework	Custom implementation in Jupyter Notebook
Encryption	TenSEAL (CKKS scheme)
ML/DL Libraries	TensorFlow / Keras, Scikit-learn
Data Handling	Pandas, NumPy
Visualization	Matplotlib
Robust Aggregation	Custom Krum implementation
Dataset	NSL-KDD, CICIDS-2018
Environment	Jupyter Notebook
Attack Simulation	Custom Python functions

3. Project Folder Structure

```
federated_ids_project/
|
|— data/
|   |— nsl_kdd.csv
|   |— cicids.csv
|
|— models/
|   |— autoencoder_model.h5
|   |— clustering_model.pkl
|
|— encryption/
|   |— ckks_context.tenseal
|
```

```
├── scripts/
│   ├── federated_training.py
│   ├── attack_simulation.py
│   └── krum_aggregation.py
├── results/
│   ├── metrics_logs.csv
│   └── bar_plots.png
└── notebooks/
    └── thesis_final.ipynb
```

4. Requirements & Installation

Python Version: Use Python 3.10+ (3.11 recommended)

Install Dependencies:

bash

pip install pandas numpy scikit-learn tensorflow matplotlib tenseal

5. Configuration Details

- **Datasets:** Place nsl_kdd.csv and cicids.csv inside the data/ folder.
- **Models:** Pre-trained autoencoder and clustering models go in models/.
- **Encryption Context:** ckks_context.tenseal must be in the encryption/ folder for encrypted FL runs.
- **Logs:** Performance metrics are stored in:

bash

CopyEdit

results/metrics_logs.csv

- **Plots:** Generated comparison graphs are saved in:

bash

CopyEdit

results/bar_plots.png

6. How to Run

1. Open **Jupyter Notebook** in the project folder

jupyter notebook

2. Open thesis_final.ipynb
3. Run all cells sequentially to:
 - Load datasets.
 - Train and evaluate Plain FL.
 - Train and evaluate Encrypted FL with CKKS.
 - Apply Krum aggregation and log metrics.
 - Generate bar plots for performance comparison.

7. Main Functions & Scripts

File	Purpose
federated_training.py	Main training loop for federated learning
attack_simulation.py	Simulates poisoning attacks
krum_aggregation.py	Implements Krum robust aggregation
main_federated_learning.ipynb	Jupyter Notebook for experiments

8. Common Problems & Fixes

Problem	Cause	Fix
TenSEAL error "context not	Missing ckks_context.tenseal	Place the file in encryption/ folder

found"	file	
Krum aggregation fails	Incorrect data shape in updates	Ensure model updates are consistent
Long runtime	Large dataset size	Use smaller dataset samples for testing
CICIDS dataset not loading	File not in expected folder	Place dataset in data/ folder
