01413.4_Project_Plan – Evaluating Federated Learning Infrastructures and Security Mechanisms

Team: QCIF Applied AI and Quantum Algorithms | Secure Federated Learning Team

Project Duration: 2025-09-30 to 2025-12-06 (10 weeks, ~10 hours per week)

1. Introduction

The project focuses on evaluating the Flower Federated Learning (FL) framework within the National Infrastructure for Secure Federated Learning (NINA).
The intern will set up a local test environment, run sample federated learning workflows, and evaluate security and operational mechanisms such as VPN connections, mTLS certificates, and role-based authentication (Keycloak).

The goal is to provide insights into infrastructure readiness and security risks when scaling to multiple organisations and sensitive health datasets.

2. Project Justification

Secure federated learning allows machine learning models to be trained on sensitive medical data without transferring the data outside institutional boundaries.
QCIF is deploying a production-grade FL environment, and this internship will:

- Validate deployment steps and documentation.
- Identify risks in security and operational procedures.
- Provide reproducible local setup instructions for development and testing.

3. Objectives

- Install and configure a local Flower federated learning environment (server + clients).
- Run initial federated learning experiments using synthetic datasets.
- Test VPN, certificate management, and authentication mechanisms.
- Identify performance and security bottlenecks.
- Recommend improvements for deployment workflows and documentation.

4. Deliverables

- Working local Flower test setup with documentation.
- Scripts and configuration files for automated setup.
- Report on security evaluation (VPN, certificates, Keycloak).

- Recommendations for production deployment improvements.
- Final presentation and handover to QCIF team.

5. Stakeholders

Internal:
- Moji Ghadimi – Head of Applied AI & Quantum Algorithms (Supervisor)
- Peter Marendy – Head of Data and Software Development
- QCIF Data and Software Development Team

External:
- Queensland Digital Health Center
- ARDC
- Partner health organisations providing sensitive datasets (future integration)

6. Benefits

- QCIF: Improved readiness for production FL deployments, validated documentation.
- Partners: Clearer onboarding and security guidelines.
- Intern: Hands-on experience with federated learning, and secure systems.

7. Scope

In scope:
- Flower local setup and testing.
- VPN and mTLS certificate configuration.
- Simulated data experiments.
- Documentation review and improvement.

Out of scope:
- Integration with live medical datasets.
- Full production automation.
- Organisation-specific security audits.

8. Timeline (with Dates)

Week	Dates	Focus Area	Key Tasks

Week 1	15 Sep	Orientation & Learning	• Orientation to QCIF systems and secure FL project. • Review FL_FLWR_OPS manual and documentation. • Set up accounts and access (SharePoint, 1Password). • Initial reading and tutorials on Flower and federated learning concepts.
Week 2	22 Sep	Local Environment Setup	• Set up local Python environment. • Install Flower and dependencies. • Run basic local Python test scripts.
Week 3	29 Sep	Local Flower Deployment	• Configure Flower server (superlink) locally. • Deploy at least two Flower clients (supernodes). • Run a basic federated learning job with synthetic data.
Week 4	6 Oct	Security Foundations	• Set up local certificate authority (EasyRSA). • Configure mutual TLS between server and clients. • Document key generation process.
Week 5	13 Oct	VPN Setup & Testing	• Configure OpenVPN server and client connections. • Test secure

			connectivity between federated nodes. • Validate firewall rules and port access (e.g., 9091-9099).
Week 6	20 Oct	Keycloak Integration	• Install Keycloak and configure realms for user access. • Integrate Flower server with Keycloak for OIDC authentication.
Week 7	27 Oct	Scaling & Performance Testing	• Add additional simulated clients. • Document scaling challenges.
Week 8	3 Nov	Security Evaluation	• Identify gaps in current security controls. • Draft preliminary recommendations.
Week 9	10 Nov	Draft Documentation	• Update QCIF documentation on setup and testing. • Prepare initial report for feedback.
Week 10	17 Nov	Finalisation	• Finalise report and recommendations. • Deliver handover presentation. • Share final scripts and documentation.

9. Risks and Considerations

- VPN connectivity issues may block multi-node testing.
- Certificate misconfigurations causing failed connections.
- Limited hours (10 hrs/week) may restrict advanced testing.

10. Success Measures

- Fully functional local Flower test environment with server and multiple clients.
- Documented procedures for VPN, certificates, and authentication setup.
- Clear recommendations for production rollout.
- Final report and presentation accepted by QCIF.