

# Resilient Federated Learning Framework

## Sprint 4

Student: Leonardo Almeida

Supervisor: Mario Luis Pinto Antunes

Co-supervisors: Rui Aguiar

**Summary:** Federated Learning (FL) offers a promising approach to training machine learning models collaboratively across distributed devices while preserving data privacy. However, the performance and robustness of FL systems are heavily influenced by the underlying communication infrastructure. The proposed framework will incorporate mechanisms to gracefully handle the addition and removal of worker nodes, minimizing disruptions to the training process and maintaining model quality.

# Work done / results

## 1 Introduction

- 1.1 Motivation . . . . .
- 1.2 Objectives and Expected Outcomes . . . . .
- 1.3 Document Outline . . . . .

Sprint 1

## 2 Background

- 2.1 Centralized Machine Learning . . . . .
- 2.2 Distributed Machine Learning . . . . .
  - 2.2.1 Model vs Data Parallelism . . . . .
  - 2.2.2 Centralized vs Decentralized Optimization
  - 2.2.3 Synchronous vs Asynchronous Scheduling
- 2.3 Federated Learning . . . . .
- 2.4 Communication Protocols . . . . .

Sprint 2

## 3 Related Work

- 3.1 Systematic Literature Review . . . . .
- 3.2 Other Frameworks . . . . .

## 4 Requirements and Architecture

- 4.1 System Analysis and Comparison . . . . .
- 4.2 Proposed Solution . . . . .

Sprint 3

## 5 Work Plan

Previous sprints:

- Understanding concepts
- Highlight important ideias
- Drawing diagrams and tables
- Write blocks of text

Sprint 4:

- Putting these blocks together
- Writing more text
- Chapters 1-4 are written

# Future work / challenges

- Finish chapter 5
- Review with supervisor
- Consolidate the text
- Finish portfolio
- Conclude the document
- Prepare final presentation
- Continue developing the FL framework

