Resilient Federated Learning Framework

Course: “Preparação de Dissertação | Estágio”

Supervisor: Prof. Mário Luís Pinto Antunes
Co-supervisor: Rui Aguiar

21-01-2025

universidade de aveiro
theoria poiesis praxis

Leonardo Almeida 102536

Introduction

- AI is becoming increasingly used daily
- Sensitive/distributed data is a challenge
- **Solution:** Federated Learning
- Robustness and Resilience are critical

Resilience
The ability of the system to maintain its performance and convergence, even in the presence of node failures, delays, and other adversities

Motivation

Challenges in FL:

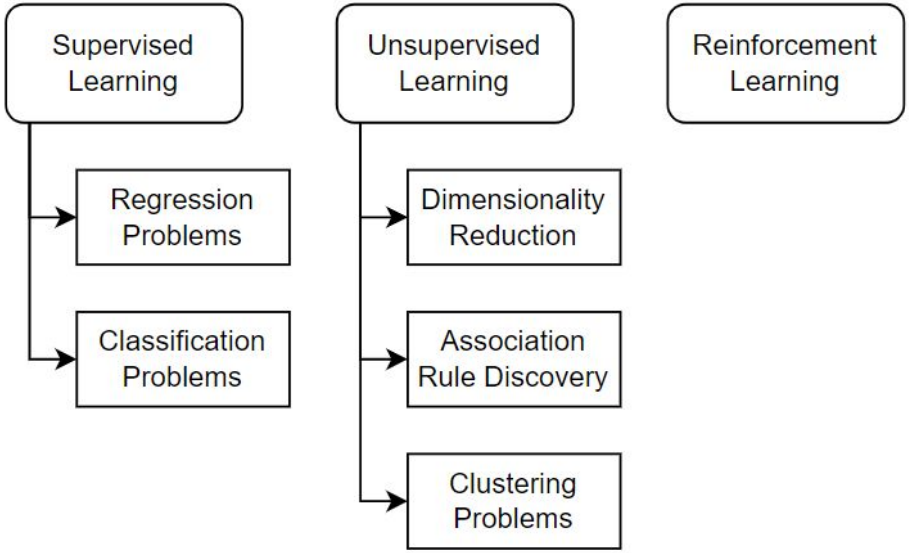
- Node failure and dynamic networks
- Non-iid data, communication overhead and reliable model aggregation
- Existing works lack modularity and resilience

Expected Outcomes:

- Open Source Framework
- Scientific Publication
- Dissertation Document

Background

Centralized Machine Learning



Machine Learning Taxonomy organized by the learning method

Advantages:

- No communication overhead
- Resource efficient
- Easier to implement and monitor

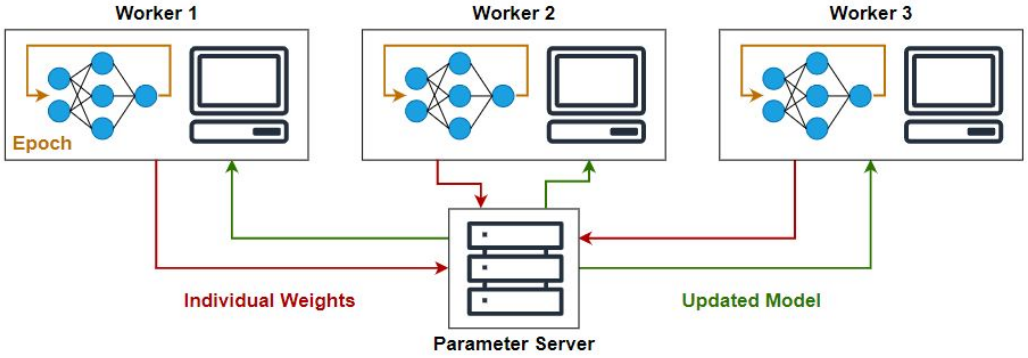
Drawbacks:

- Data privacy concerns
- Single point of failure
- Scalability issues

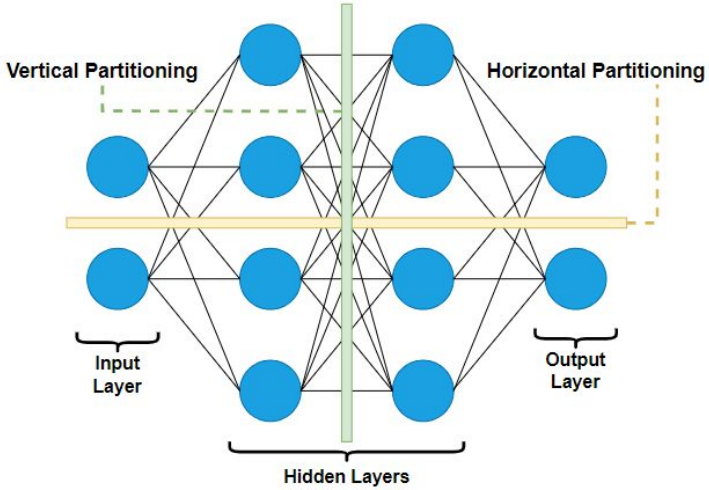
Background

Distributed Machine Learning

- Data vs Model Parallelism
- Centralized vs Decentralized Optimization
- Synchronous vs Asynchronous Scheduling



Decentralized Optimization



Horizontal vs Vertical Model Parallelism

Background

Federated Learning

Subset of Distributed Learning where:

- Data cannot be shared
- Designed to work in a distributed manner
- Can have security mechanisms

Categories of FL:

- Horizontal FL
- Vertical FL
- Federated transfer learning

Background

Communication Protocols

Summary and Comparison

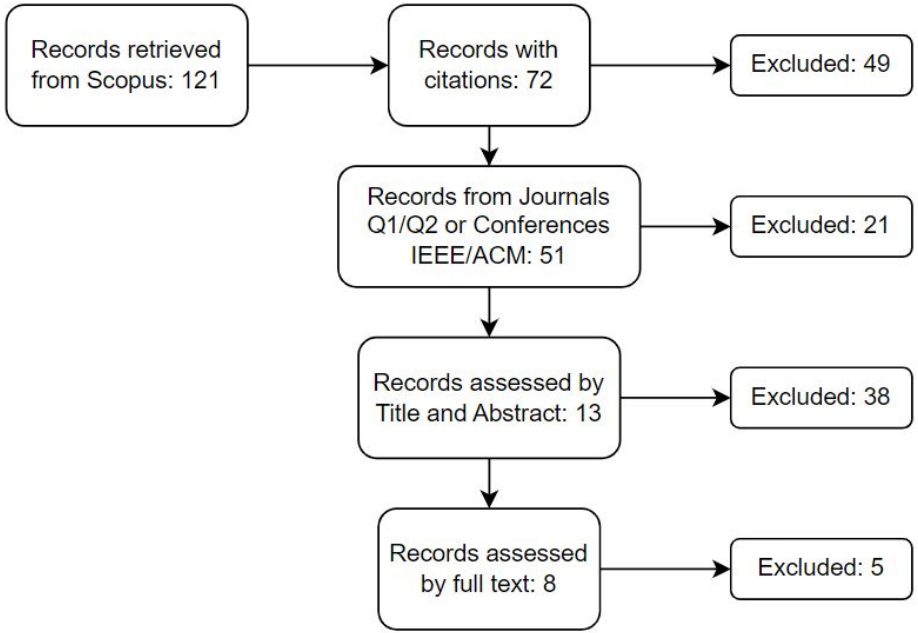
Protocol	Scalability	Fault Tolerance	Security	Suitability
MPI	Limited	No built-in support	None	Low, lacks fault tolerance and scalability
MQTT	Moderate	Moderate	TLS, mTLS, role-based	Moderate, suitable for smaller FL systems
Kafka	High	High	TLS, mTLS, role-based	High, but latency can hinder synchronization
Zenoh	High	High	TLS	High, but limited ecosystem maturity

Related Work

Systematic Literature Review

RQ1
How can Federated Learning frameworks be designed to ensure robustness against node failures across dynamic network environments?

RQ2
What communication layer architectures are most suitable for supporting fault-tolerant and resilient Federated Learning under dynamic network conditions?



Systematic Literature Review Process

Related Work

Systematic Literature Review

Comparison of the Papers obtained previously

Ref	Fault Tolerance	Elasticity	Scalability	Security	Evaluation	Code	Compliance
[9]	✓	X	Not tested	✓	X	X	33%
[10]	✓	X	1000	✓	✓	X	66%
[13]	✓	✓	10000	X	✓	X	66%
[14]	✓	X	400	✓	X	X	50%
[16]	✓	X	1000	✓	X	✓	66%
[17]	✓	X	600	X	✓	X	50%
[21]	✓	✓	64	X	✓	✓	83%
[22]	✓	X	10	X	✓	✓	66%
Total:	100%	25%	87.5%	50%	62.5%	37.5%	

Related Work

Other Frameworks

Summary of Federated Learning Frameworks

Framework	Key Features	Limitations
HeteroFL	Supports heterogeneous client models Static batch normalization	Lack of customization Focus on heterogeneity
CoCoFL	Partial neural network freezing Quantization	Out of the box solution Lack of flexibility
Flower	Framework agnostic Customizable and scalable	Not a complete solution Requires additional components
TFF	Seamless integration with TensorFlow Supports dynamic client participation	Restricted to TensorFlow Fixed communication layer

Requirements and Architecture

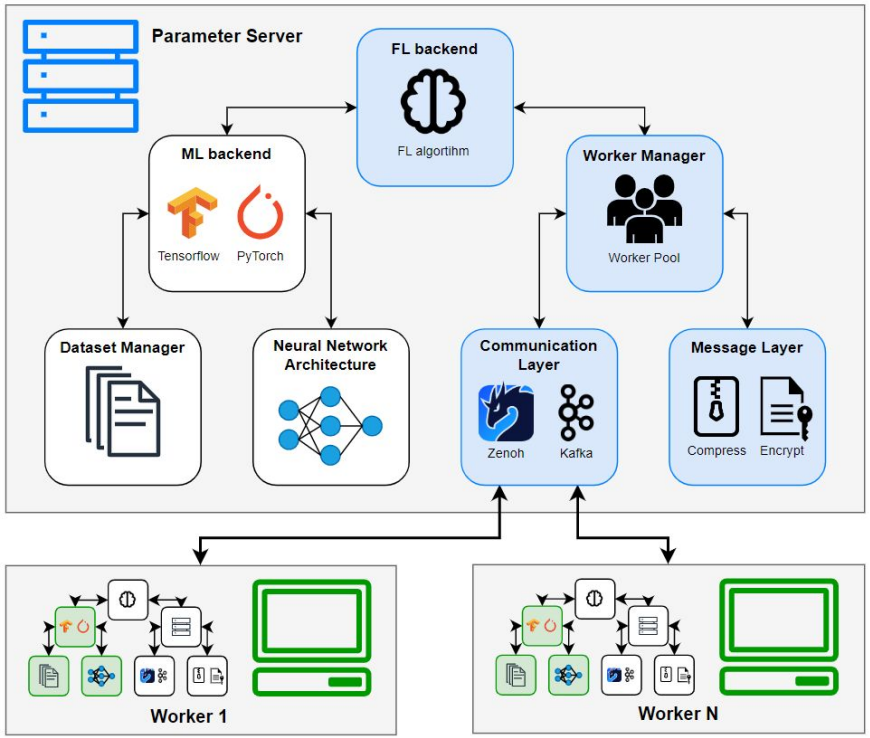
System Analysis and Comparison

Qualitative comparison of the proposed solution with existing solutions

Solution	Resilience	Modularity	Analysis	Code and Documentation	Compliance
[10]	X	X	✓	X	25%
[13]	✓	X	✓	X	50%
[17]	X	X	✓	X	25%
[21]	✓	X	✓	✓	75%
[22]	X	X	✓	✓	50%
HeteroFL	✓	X	✓	✓	75%
CoCoFL	✓	X	✓	✓	75%
Flower	X	✓	X	✓	50%
TTF	✓	X	X	✓	50%
Proposed	✓	✓	✓	✓	100%

Requirements and Architecture

Proposed Solution



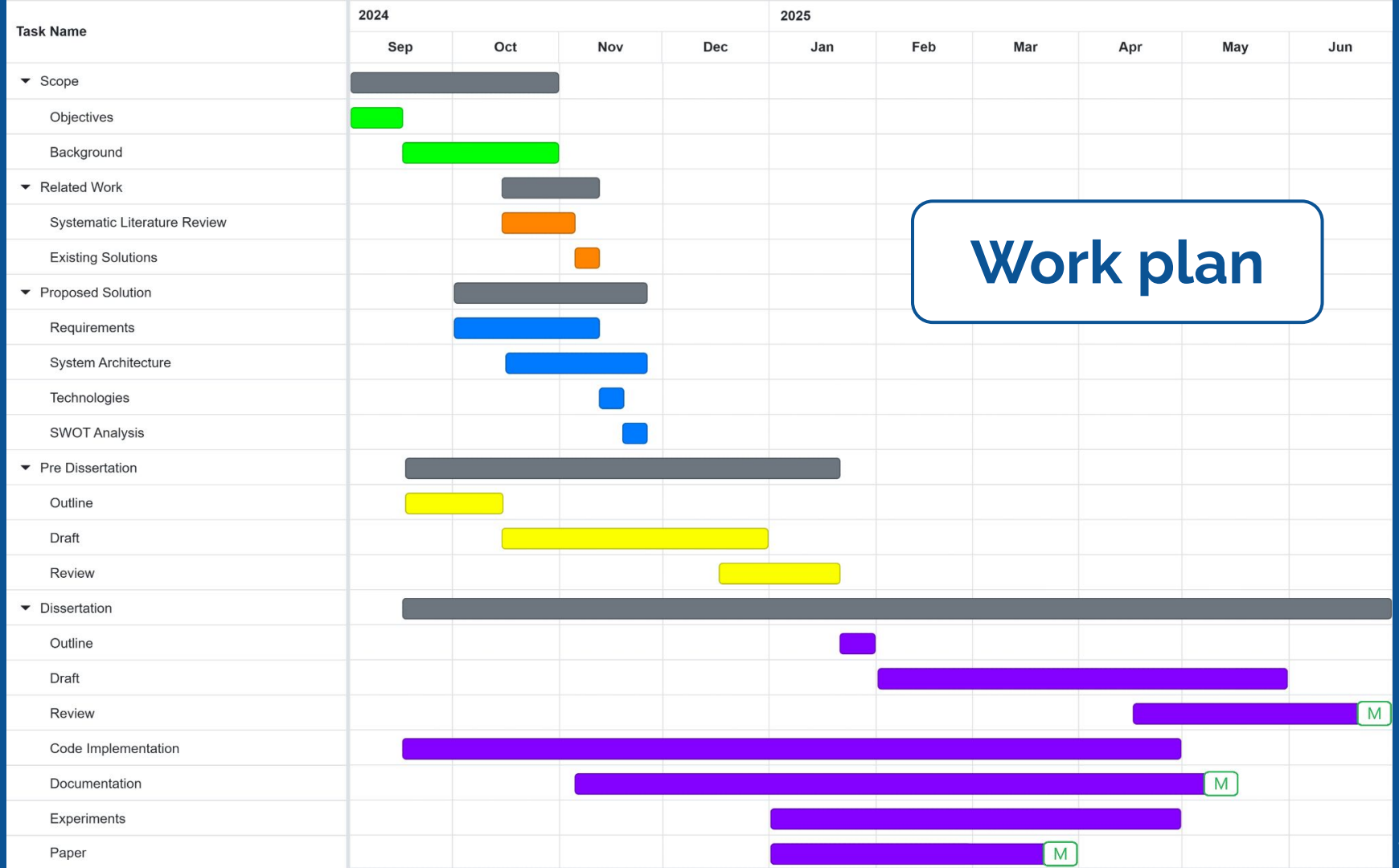
Proposed system architecture

SWOT analysis

	Helpful	Harmful
Internal	**Strengths** Resilient, highly modular and easy to use	**Weaknesses** Validation is limited to the simulation environment
External	**Opportunities** Easy to extend and integrate with other systems	**Threats** Scalability may be limited

Communication Layer is critical to ensure Resilience

Work plan


Task Name
2024
2025
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Scope
Objectives
Background
Related Work
Systematic Literature Review
Existing Solutions
Proposed Solution
Requirements
System Architecture
Technologies
SWOT Analysis
Pre Dissertation
Outline
Draft
Review
Dissertation
Outline
Draft
Review
Code Implementation
Documentation
Experiments
Paper
M
M
M

Conclusion

Work done:

- Motivation, objectives, and preliminary progress toward a resilient and modular FL framework
- Work plan outlined with tasks and milestones

Future work:

- Respect the timeline and achieve the milestones outlined in the work plan

Impact:

- Enhance FL applicability in diverse scenarios
- Promote innovation in privacy-preserving distributed learning