Resilient Federated Learning Framework
Sprint 2

Student: Leonardo Almeida

Supervisor: Mario Luis Pinto Antunes

Co-supervisors: Rui Aguiar

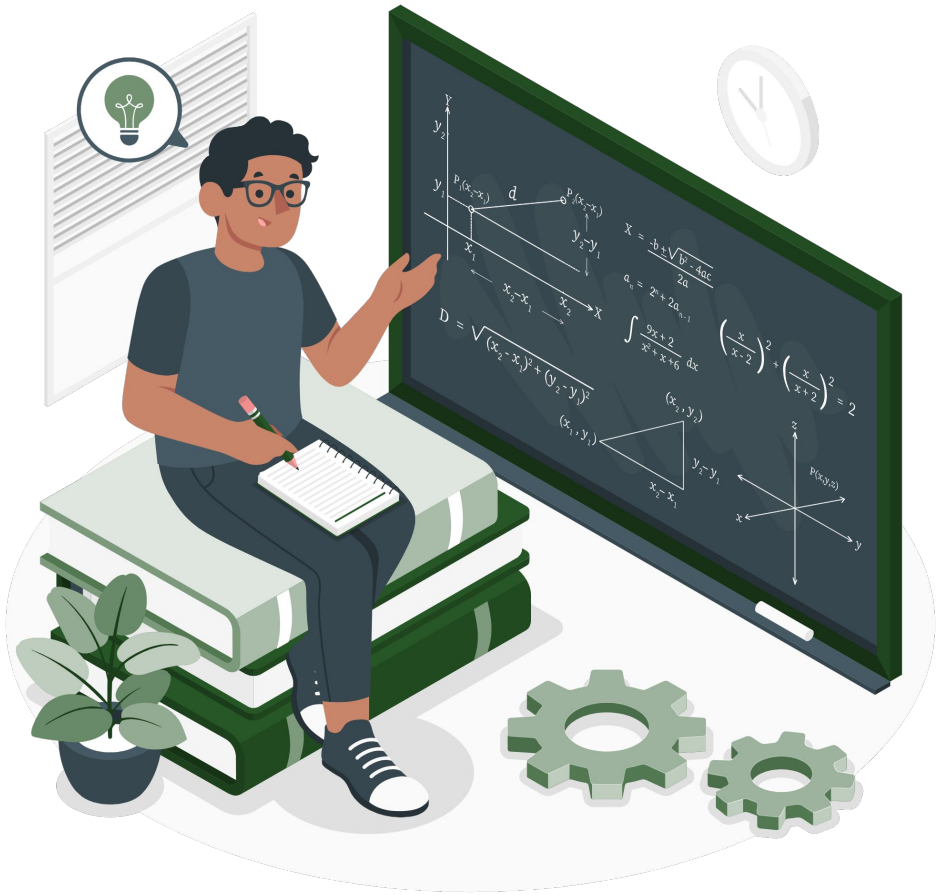
Summary: Federated Learning (FL) offers a promising approach to training machine learning models collaboratively across distributed devices while preserving data privacy. However, the performance and robustness of FL systems are heavily influenced by the underlying communication infrastructure. The proposed 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 - Background

Review of papers about FL

Key concepts:

- Data vs Model Parallelism
- Centralized vs Decentralized Optimization
- Synchronous vs Asynchronous Scheduling
- Distributed vs Federated Learning
- When to apply Federated Learning



Work done / results - PRISMA

Research questions:

- How can **Federated Learning** frameworks be designed to ensure robustness across **dynamic network** environments?
- What **communication** layer architectures are most suitable for supporting **resilient** Federated Learning under dynamic network conditions?

Query:

- "federated learning" AND "fault tole*"
- Published between 2019 and 2024
- Journals and Conferences

Work done / results - PRISMA

Final query was a result of iterations with different keywords

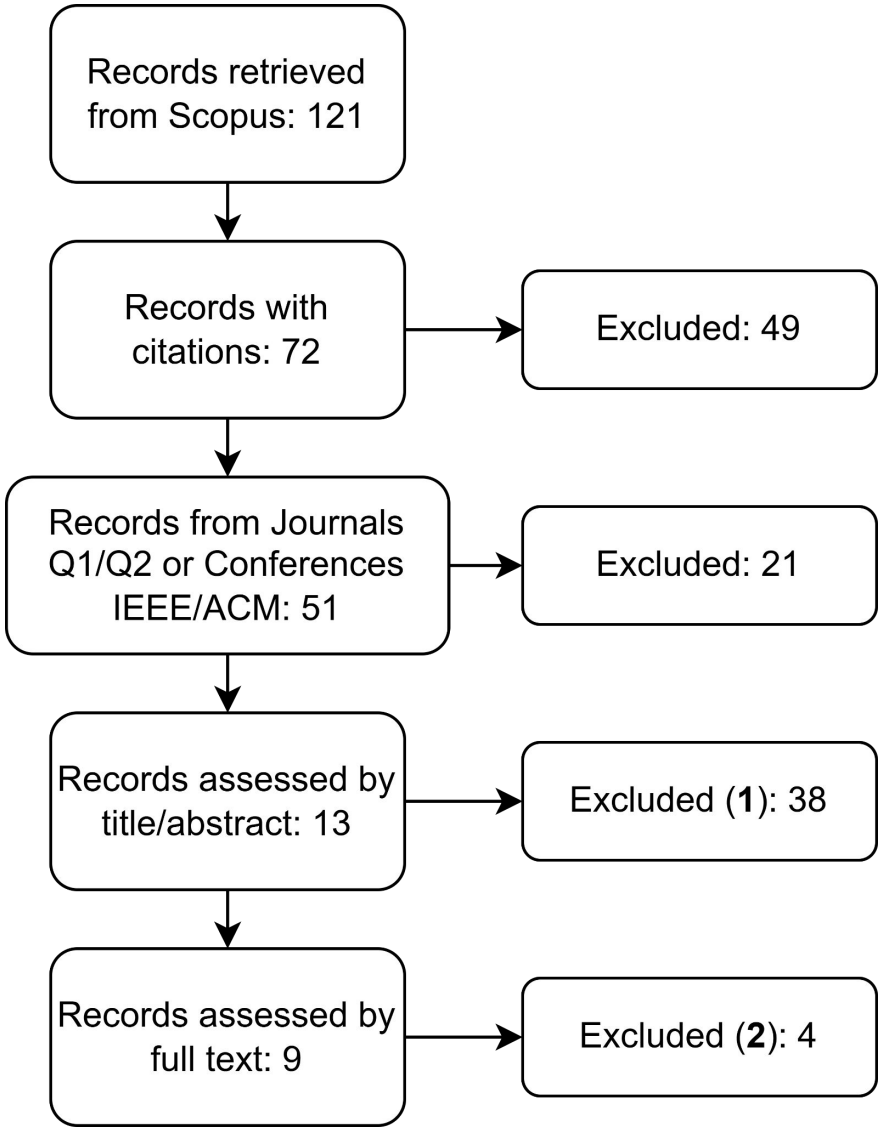
Problems with "communication":

- Costs
- Efficiency
- Analysis

Problems with "resilient":

- Attacks
- Data poisoning
- Convergence

Work done / results - PRISMA



Done programmatically to register each step

Reasons for exclusion in (1):

- Implementation in blockchain
- Focus on data privacy
- Problems shown before

Reasons for exclusion in (2):

- Don’t specify the communication layer
- Don’t specify node failure handling
- Focus on security

Future work / challenges

Compare the methods shown in the papers obtained with PRISMA:

- Advantages/Disadvantages
- Requirements

Consolidate background section

Investigate and compare communication frameworks:

- MPI, Zenoh, Kafka, MQTT, etc…