Resilient Federated Learning Framework
Sprint 3

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

Table 3.1: Categorization of Papers based on Topics

Ref	Fault Tolerance	Elasticity	Scalability	Security	Evaluation	Code
[1]	✓	X	Not tested	✓	X	X
[2]	✓	X	1000	✓	✓	X
[5]	✓	✓	10000	X	✓	X
[6]	✓	X	400	✓	X	X
[8]	✓	X	1000	✓	X	✓
[9]	✓	X	600	X	✓	X
[13]	✓	✓	64	X	✓	✓
[14]	✓	X	10	X	✓	✓
Results:	100%	25%	-	50%	62.5%	37.5%

Work done / results

Table 4.1: Qualitative comparison of the proposed solution with existing solutions

Solution	Resilience	Modularity	Analysis	Code and Documentation	Compliance
[2]	X	X	✓	X	25%
[5]	✓	X	✓	X	50%
[9]	X	X	✓	X	25%
[13]	✓	X	✓	✓	75%
[14]	X	X	✓	✓	50%
HeteroFL	✓	X	✓	✓	75%
CoCoFL	✓	X	✓	✓	75%
Flower	X	✓	X	✓	50%
TTF	✓	X	X	✓	50%
Proposed	✓	✓	✓	✓	100%

Work done / results

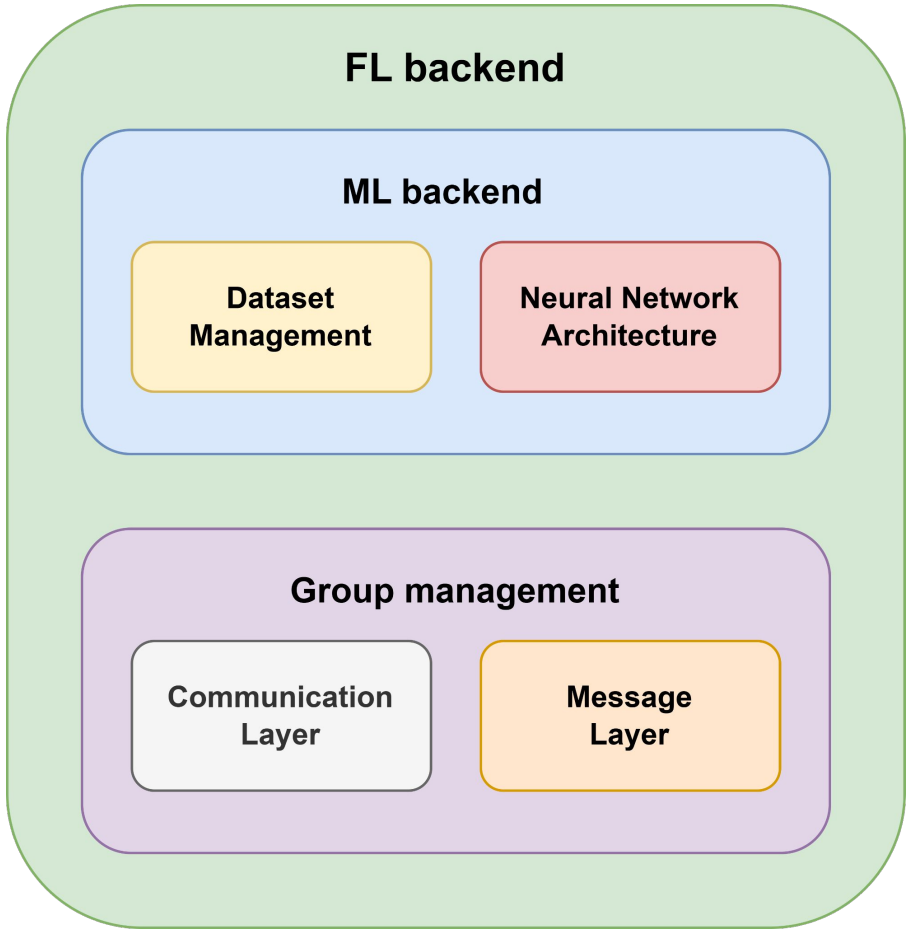

Figure 4.1: Proposed system architecture

Table 4.2: SWOT analysis of the proposed solution

	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

Future work / challenges