Performance Analysis of Architectural Patterns for Federated Learning Systems

Ivan Compagnucci[a], Riccardo Pinciroli[b], Catia Trubiani[a]

Gran Sasso Science Institute (GSSI), L'Aquila, Italy[a]
Zimmer Biomet, Milan, Italy[b]

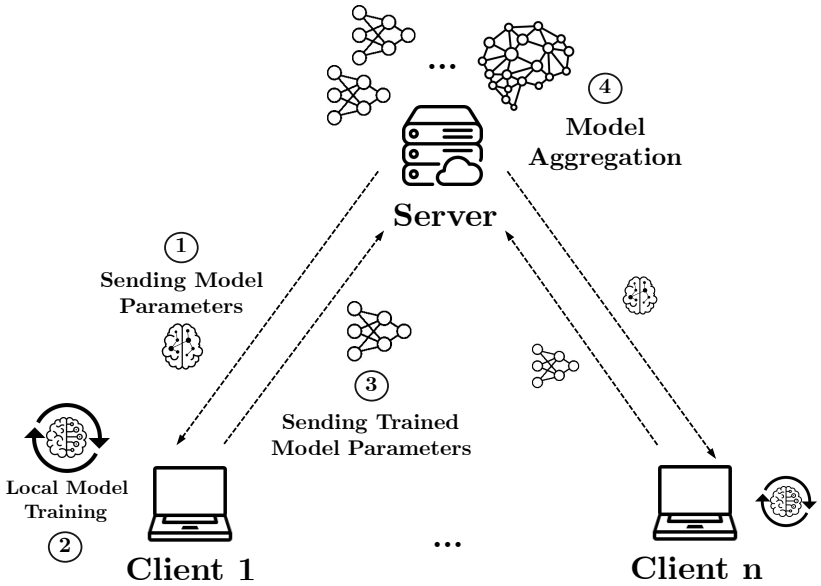
Setting the Scene

Federated Learning

Allows multiple clients to **collaboratively train a global model without sharing the local data** used for the training.

Federated Learning round

① Sending Model Parameters
② Local Model Training
③ Sending Trained Model Parameters
④ Model Aggregation



Goal: Train a Machine Learning model while **preserving Data Privacy.**

This Paper in a Nutshell

State of the Art

[1] S. K. Lo, Q. Lu, L. Zhu, H.-Y. Paik, X. Xu, and C. Wang, **"Architectural Patterns for the Design of Federated Learning Systems"** Journal of Systems and Software, vol. 191, p. 111357, 2022.

What is missing?

Lack of evidence on how **Architectural Patterns impact Federated Learning system performance.**

Our Contribution

1. Development of a **Federated Learning Benchmarking Framework**;
2. **Implementation of 4 Architectural Patterns** [1] within the Framework;
3. **Performance Analysis** of the Architectural Patterns.

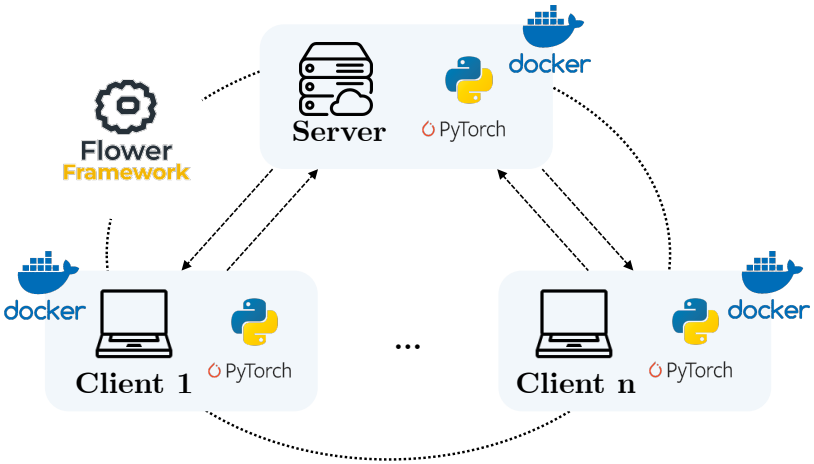
Overview of our Benchmarking Platform

AP4Fed

It allows to **dynamically integrate Architectural Patterns and monitor Performance Metrics** during the Federated Learning process.

Main Steps

1. System Emulation
2. Docker Environment Setting
3. FL Simulation and Benchmarking



Parameter	Description
NUM_ROUNDS	# of Federated Learning Rounds
nS	# of Server Container Instances
nC	# of Client Container Instances
n_CPU	# of CPUs allocated to each Container
RAM	RAM allocated to each Container

Input Parameters Summary.

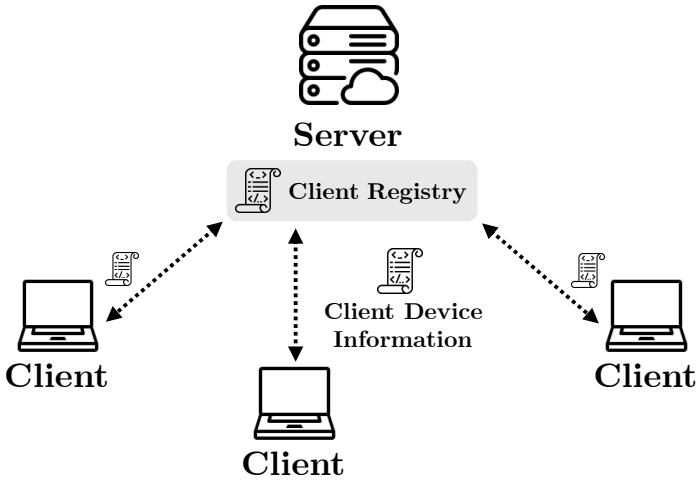
Parameter	Description
Training Time	Time Spent on Local Training
Communication Time	Time for Client-Server Communication
Total Round Time	Total Time for each FL Round
F1 Score	F1 score of the global model

Output Metrics.

Architectural Pattern: Client Registry

Definition

It is designed to **store relevant information of each client** device participating in an Federated Learning process.



Parameter	Description
`cID`	Client Unique Identifier
`n_CPU`	# of Container CPU
`cluster_Type`	Cluster associated to the Client
`training_time`	Client Training Time
`communication_time`	Client Communication Time
`total_round_time`	Client Total Round Time

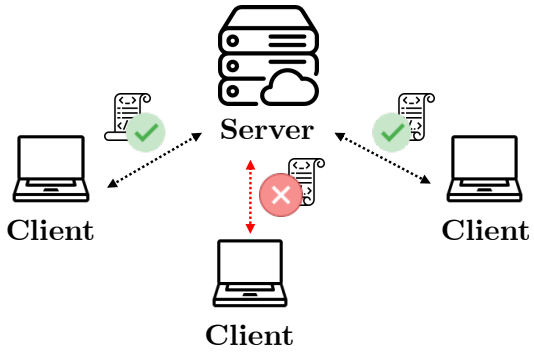
Extended Parameters for Client Registry.

It primarily serves to **provide relevant client information used by other patterns**.

Architectural Pattern: Client Selector

Definition

It introduces a mechanism for **selecting/excluding Clients to participate in the Federated Learning round** according to specific criteria.

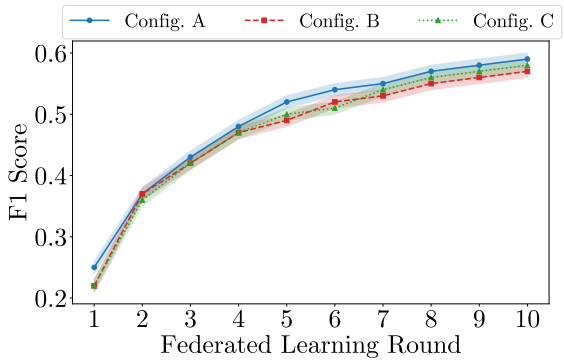


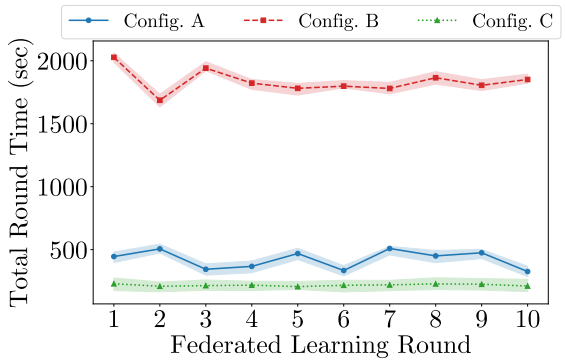
Parameter	Value
NUM_ROUNDS	10
nS	1
nC	4
n_CPU	1 *for Low-Spec Clients*; 2 *for High-Spec Clients*
RAM	2GB
Selection Strategy	Resource-based
Selection Criteria	# of CPU >1

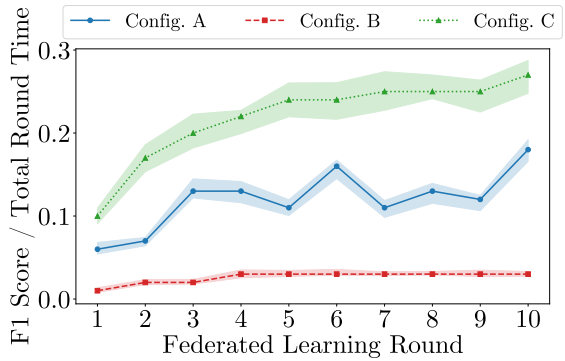
Input parameters.

	A	B	C
Pattern	×	×	✓
# of High-Spec Clients	4	3	3
# of Low-Spec Clients	-	1	-
Total Clients	4	4	4 → 3

Experiment Configurations.



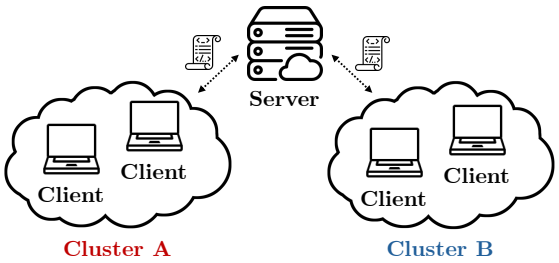




Architectural Pattern: Client Cluster

Definition

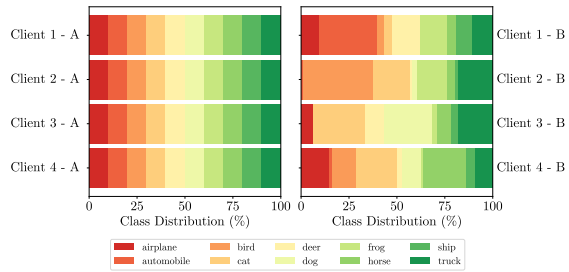
It is designed to **groups client devices based on the similarity** of their characteristics.



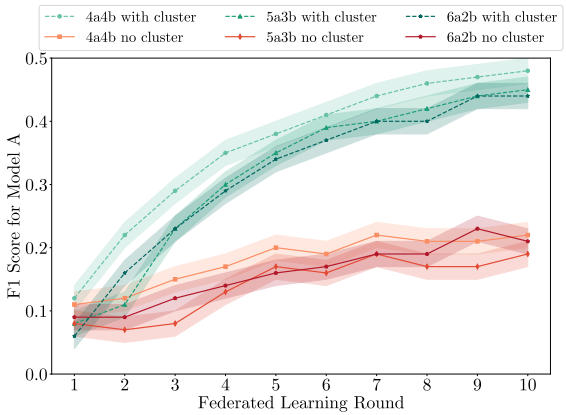
Parameter	Value
NUM_ROUNDS	10
nS	1
nC	8
n_CPU	1
RAM	2GB
Training Samples	$50,000 \rightarrow 25,000$
Cluster Strategy	Data Partitioning Type
Cluster Criteria	IID vs non-IID

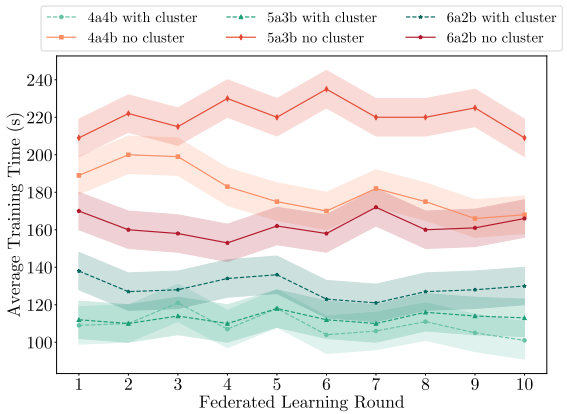
Input parameters.

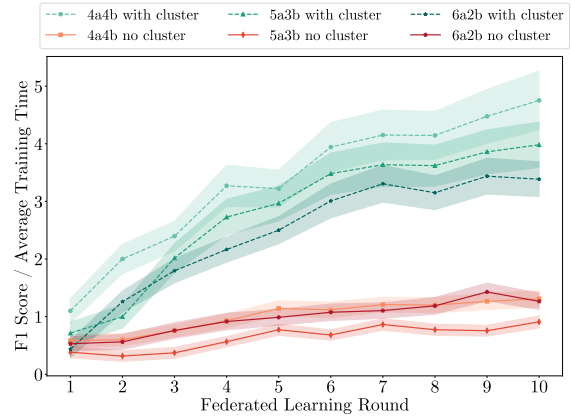
	4a4b	5a3b	6a2b
Pattern	✓, ×	✓, ×	✓, ×
Total Clients	4A+4B	5A+3B	6A+2B



Experiment Configurations.



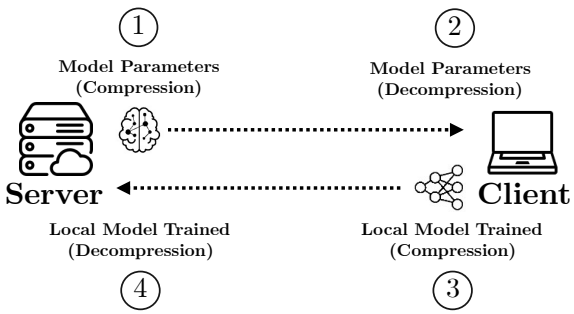




Architectural Pattern: Message Compressor

Definition

It is designed to **reduce the size of message data exchanged** between the central Server and the Clients in an Federated Learning environment.

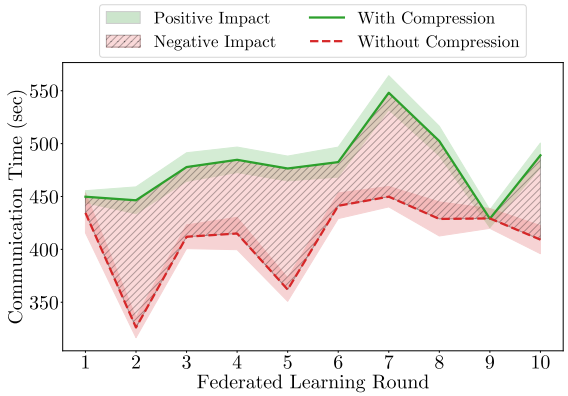


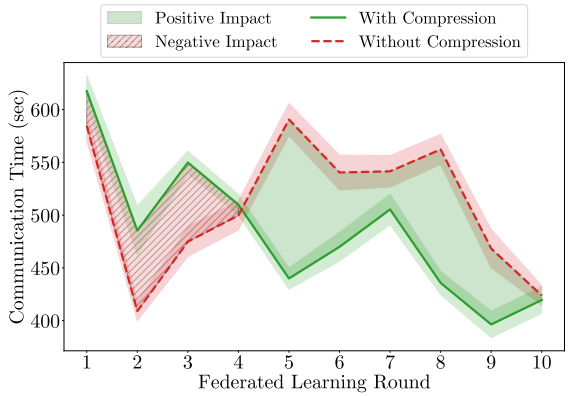
Parameter	Value
NUM_ROUNDS	10
nS	1
nC	8
CPU	1
RAM	2GB
Compression Library	zlib

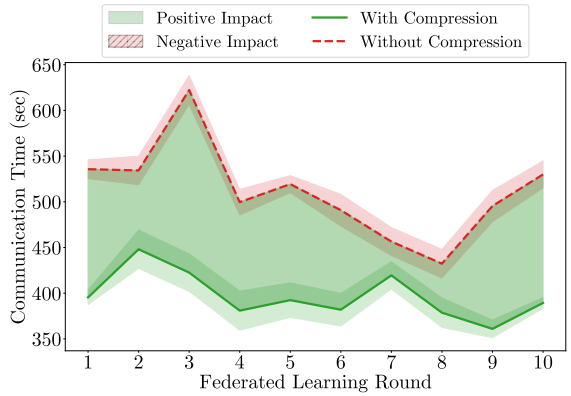
Input parameters.

	n/2	n	n*2
Pattern	✓, ×	✓, ×	✓, ×
Model Params	14 028	28 056	56 112
Batch Size	32	32	32
Learning Rate	0.001	0.001	0.001
Optimizer	SGD	SGD	SGD

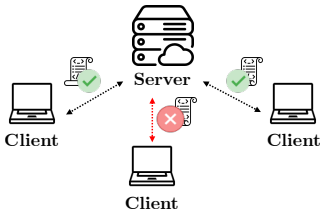
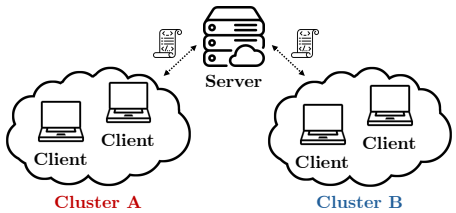
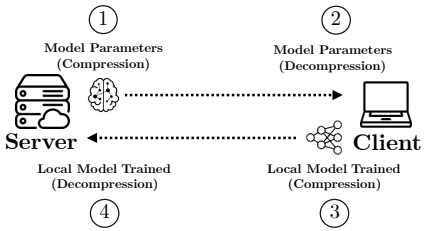
Experiment Configurations.







Conclusion & Future Work

	Client Selector	Client Cluster	Message Compressor
			
Pros	• **Total Round Time** ↓	• **Training Round Time** ↓ • **Model Accuracy** ↑	• **Commun. Round Time** ↓
Cons	• Excluding clients may **impact Model Accuracy.**	• Clustering increases **Data Privacy risks.**	• **Compression overhead** can outweigh benefits.

Future Work

- Implement **Additional ML Models and Testing Dataset** in `AP4Fed`;
- Implement **Additional Architectural Patterns** in `AP4Fed`;
- Performance Analysis of **Combined Architectural Patterns**.

Thank you for the Attention

Ivan Compagnucci[a], Riccardo Pinciroli[b], Catia Trubiani[a]

Gran Sasso Science Institute, L'Aquila, Italy[a]
Zimmer Biomet, Milan, Italy[b]