Federated Learning

Institute of Computing
Unicamp
www.ic.unicamp.br

Where are we?

s-media-cache-ak0.pinimg.com/

Where are we?

VENEZUELA
GUYANA
SURINAME
FRENCH GUIANA
COLOMBIA
Atlantic Ocean
RORAIMA
AMAPÁ
Equator
ECUADOR
Amazon River
Manaus
Fortaleza
PARÁ
MARANHÃO
CEARÁ
RIO GRANDE DO NORTE
PARAÍBA
AMAZONAS
PIAUÍ
PERNAMBUCO
Recife
ALAGOAS
SERGIPE
PERU
ACRE
BAHIA
Salvador
SÃO JOSÉ DO DO RIO PRETO
RIBEIRÃO PRETO
ARAÇATUBA
CAMPINAS
SÃO JOSÉ DOS CAMPOS
GRANDE SÃO PAULO
SANTA CATARINA
URUGUAY
~2.6 Million People (Metro Region) 9th
~20 Million People (Metro Region) 1st
220 km 0 220 440 km
0 500 1,000 Miles
New York
São Paulo

Campinas

Our home


THINK THE
OUTSIDE


Ciências da


WORK
HARD


hello!


INNOV ATE


H.IAAC
HUB DE INTELIGÊNCIA
ARTIFICIAL E ARQUITETURAS
COGNITIVAS

Viva Bem team

55 people

Institute of Computing (IC)	Institute of Physics "Gleb Wataghin" (IFGW)	Faculty of Physical Education (FEF)	School of Electrical and Computer Engineering (FEEC)

Viva Bem team

Coordinator
Prof. Anderson Rocha

Vice coordinator
Prof. Leandro Villas

Lead Researcher
Prof. Rickson Mesquita

Lead Researcher
Prof. Marco Uchida

Lead Researcher
Prof. Fernando Von Zuben

Associate Researcher
Prof. Nelson Fonseca

Associate Researcher
Prof. Esther Colombini

Associate Researcher
Prof. Heitor Soares Ramos Filho

Associate Researcher
Prof. Marcelo Reis

Collaborating Researcher
Prof. Milton Shoiti Misuta

Collaborating Researcher
Prof. Zanoni Dias

Collaborating Researcher
Prof. Daniel Ludovico Guidoni

Collaborating Researcher
Prof. Breno França

Our Goals

PROPOSE Continuous **monitoring of the health and well-being** of individuals through wearable **devices;**

PROPOSE New **health methods and algorithms** to be **incorporated** into **mobile and wearable devices;**

PROPOSE New **health and well-being services based** on **mobile and wearable technologies**.

Innovative and disruptive research in AI for health and well-being

Research lines

VIVA BEM

HEALTH AND WELL-BEING: NEUROSCIENCE

HEALTH AND WELL-BEING: PHYSICAL EDUCATION

ARTIFICIAL INTELLIGENCE

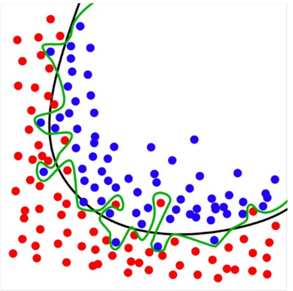
EXPLAINABLE ARTIFICIAL INTELLIGENCE

FEDERATED LEARNING

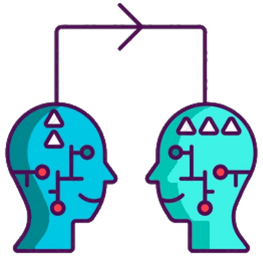
SOFTWARE ENGINEERING

Cutting-edge applications

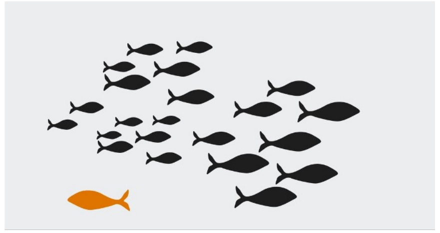
Challenges



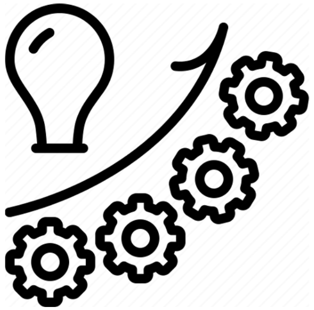
Avoid overfitting and look for accurate forecasts



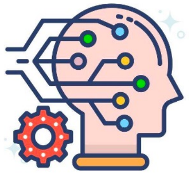
Transfer Learning



Identify and remove outliers to get an accurate model



Data augmentation techniques, so that better deep learning models can be built



Self-supervised learning, extracting useful representations from unlabeled data

One-shot or few-shot learning for building models with extremely limited data

For more information


H.IAAC
HUB DE INTELIGÊNCIA
ARTIFICIAL E ARQUITETURAS
COGNITIVAS

TEAM

Leandro Villas
Coordinator
Distributed Learning

Paula Costa
Cognitive
Architectures

Esther Colombini
Learning in
Cognitive
Architectures

Edson Borin
Knowledge
Representation

Sandra Avila
Natural Language
Processing

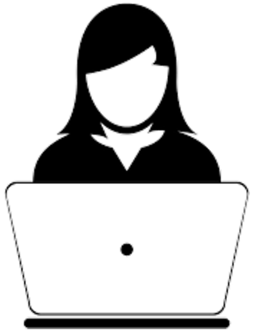
Marcos Raimundo
AI for Finance

Marcelo Reis
AI for Marketing

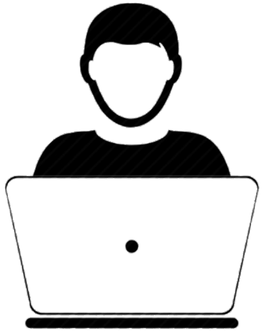
Team of 23 professors who are experts in AI, Cognitive Architectures, Sensors and IoT. Five are listed among the top 2% most influential scientists in the world, according to a study by Stanford University

31
PhD researchers

16
PhD candidate



17
Master's students



24
Undergraduate students

Research Lines

DISTRIBUTED LEARNING

Develop models and algorithms that allow data collected at the edge to be aggregated and processed in a distributed manner.

KNOWLEDGE REPRESENTATION

Find stable, compact and interpretable representations for data coming from input sensors from different domains.

AI FOR MARKETING

Study of automatic ad allocation systems based on behavioral analysis obtained through data from mobile devices.

COGNITIVE ARCHITECTURES

Development and adaptation of architectures for use in the context of mobile devices.

LEARNING IN COGNITIVE ARCHITECTURES

Study of learning algorithms that can be used in the context of cognitive architectures.

AI FOR FINANCES

Study of automatic financial models that promote financial inclusion by ensuring impartiality, data security and privacy.

NATURAL LANGUAGE PROCESSING

Construction of databases in Portuguese and application of ML techniques to find patterns and extract information from data in Portuguese.

Main Objectives

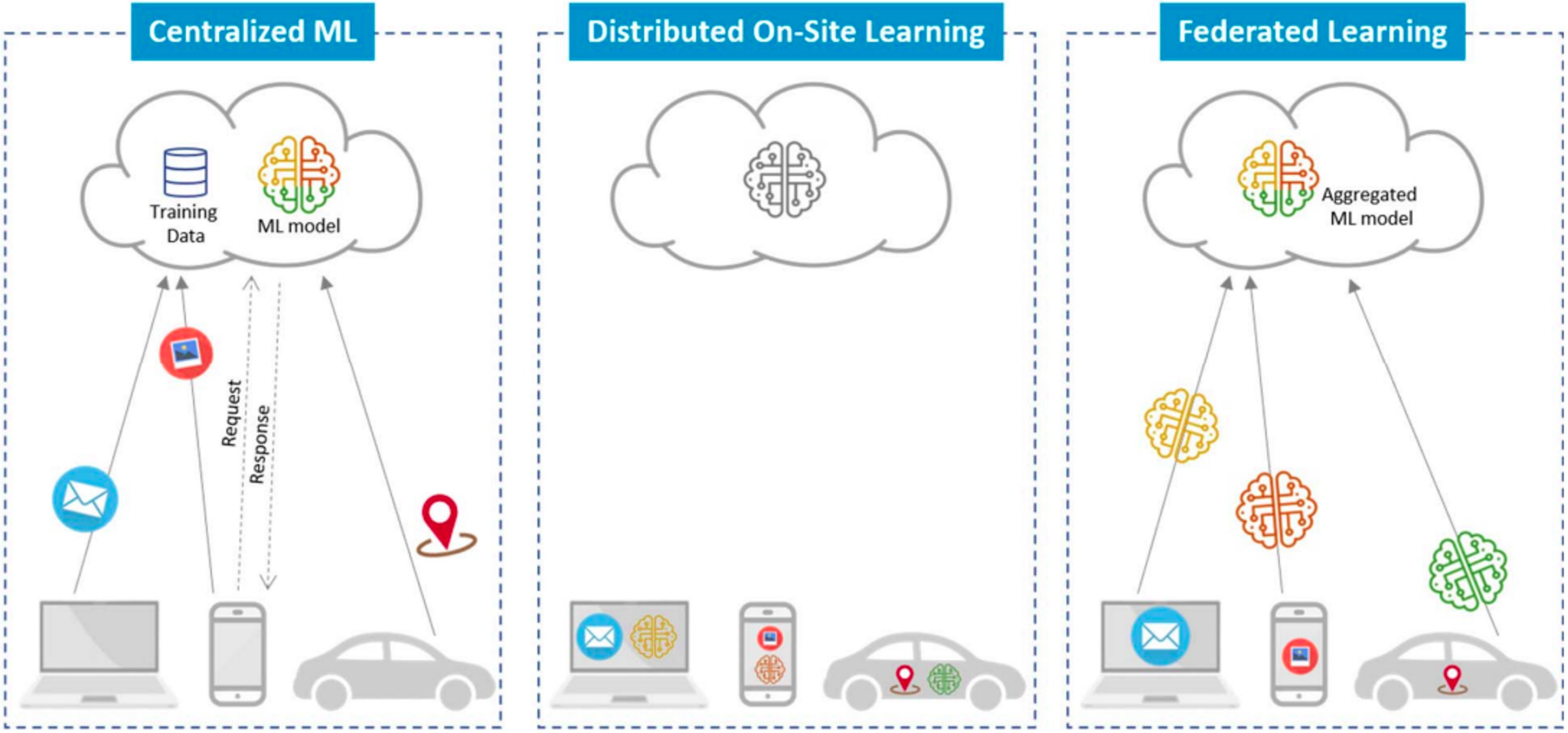
Promote innovative and disruptive research in AI and Cognitive Architectures;

New methods and algorithms to be incorporated into mobile and wearable devices;

Creation of databases for machine learning algorithms for all research areas.

Dissemination of knowledge and training of specialized professionals in an area of very high demand.

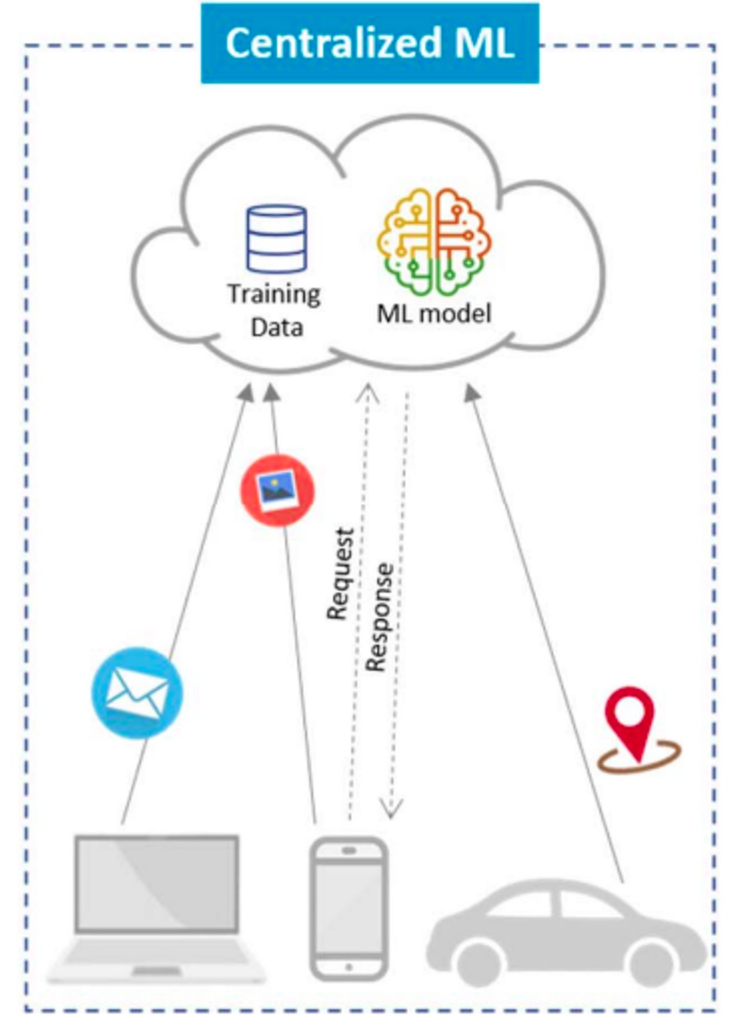
ARCHITECTURES FOR ML



Sawsan Abdulrahman, et al. A survey on federated learning: The journey from centralized to distributed on-site learning and beyond. IEEE Internet of Things Journal, 8(7):5476–5497, 2021.

CENTRALIZED ARCHITECTURE

- **Overview:** *end-users (i.e., clients) send their data to a central server (i.e., cloud) to train a machine learning model*
- **Advantage:** *more efficient and robust models due to the access of the whole dataset*
- **Limitation:** *problems related to data privacy*



DISTRIBUTED ARCHITECTURE

- **Overview:** *end-users train a local model with their local data without any data sharing between users and the central server*

- **Advantage:** *ensure data privacy, since no information is shared with anyone*

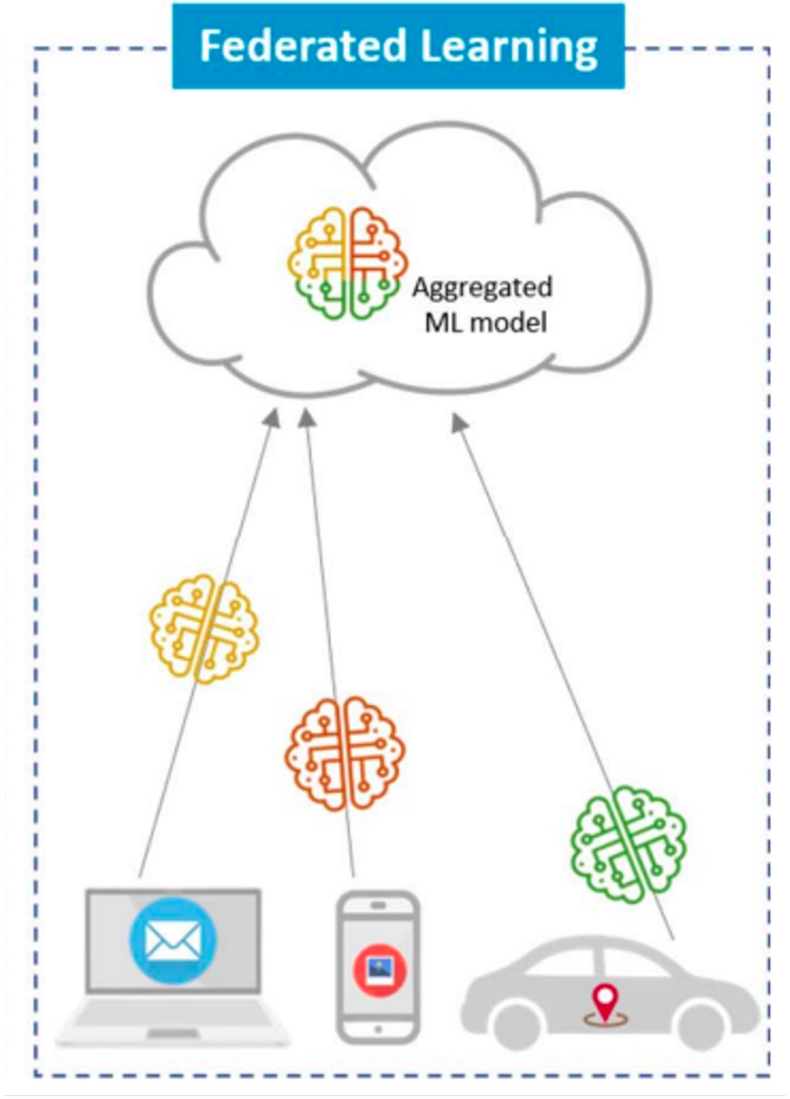
- **Limitation:** *limited model's performance since it just relies on the data of a particular user; no generalization is provided*

FEDERATED LEARNING ARCHITECTURE

- ***Overview:*** *end-users train the model with their local data, then their trained model are shared with a central server to be aggregated and updated.*

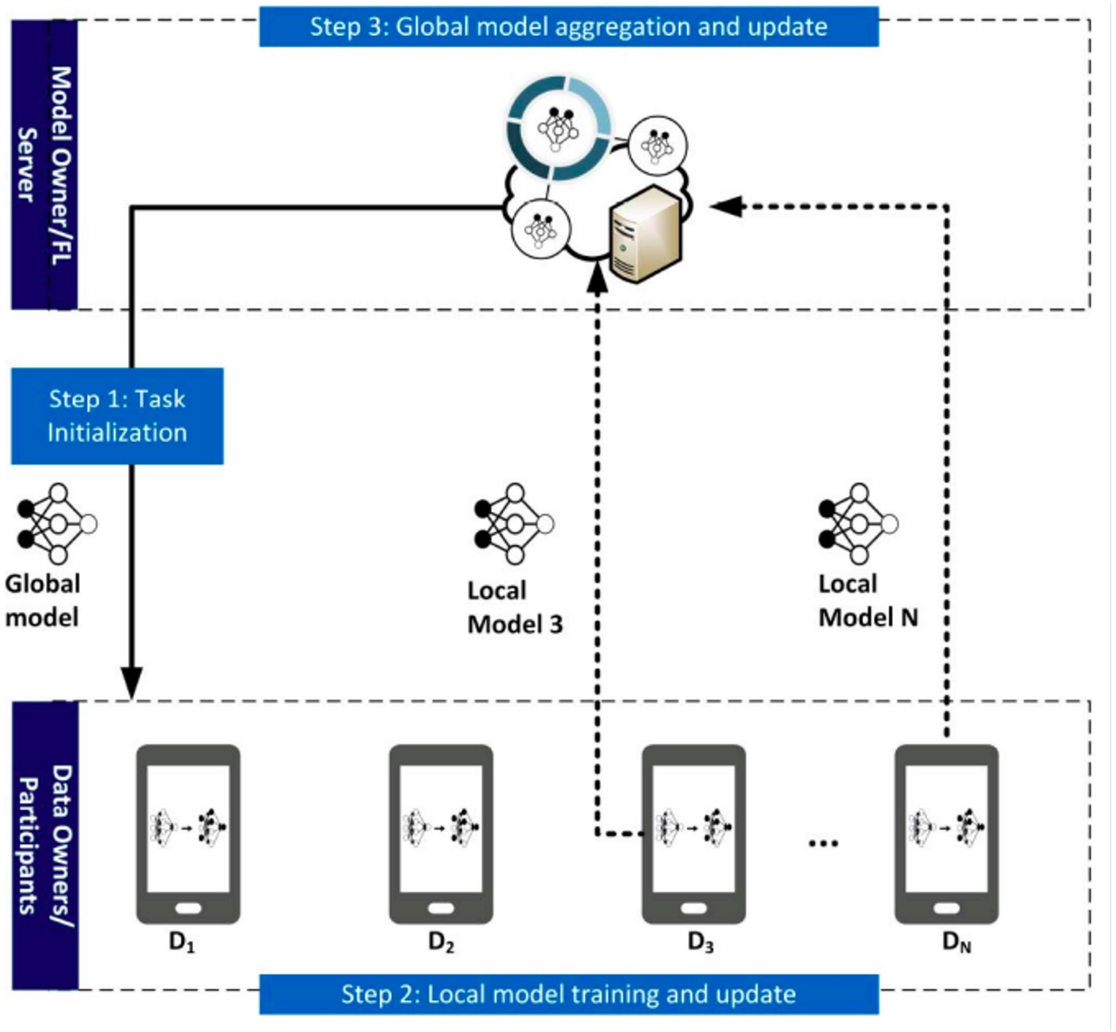
- ***Advantage:*** *ensures privacy and keeps an efficient performance due to the model sharing of each user*

- ***Limitation:*** *needs robust aggregation algorithms and communication protocols to enable an efficient collaborative learning without increasing the communication overhead*



FEDERATED LEARNING

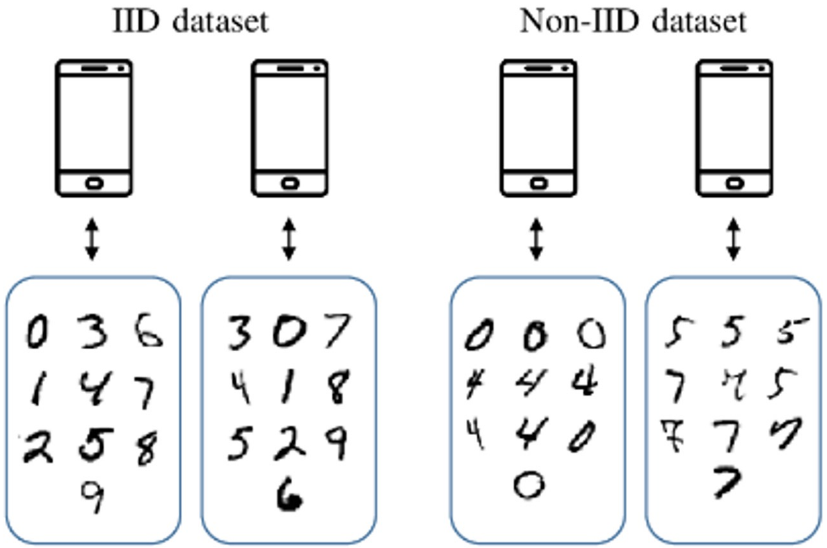
- **Step 1: Initialization**
  - *Server sends the machine learning model to clients*
- **Step 2: Local training**
  - *Clients who received the model train it using their local data*
- **Step 3: *Model aggregation and update***
  - *Clients send the trained model to the server to be aggregated*



Wei Yang et al. Federated learning in mobile edge networks: A comprehensive survey. IEEE Communications Surveys Tutorials, 22(3):2031–2063, 2020.

Challenges in FL

- Different clients might have different data distributions
- Overfitting model at clients, consequently decreasing its overall performance



- **How to address such a problem?**
  - Improving data representation at clients (*i.e., data sharing and data augmentation*)
  - Developing robust model aggregation algorithms
  - Designing efficient systems and protocols (*i.e., clustering similar clients, etc*)

Challenges in FL

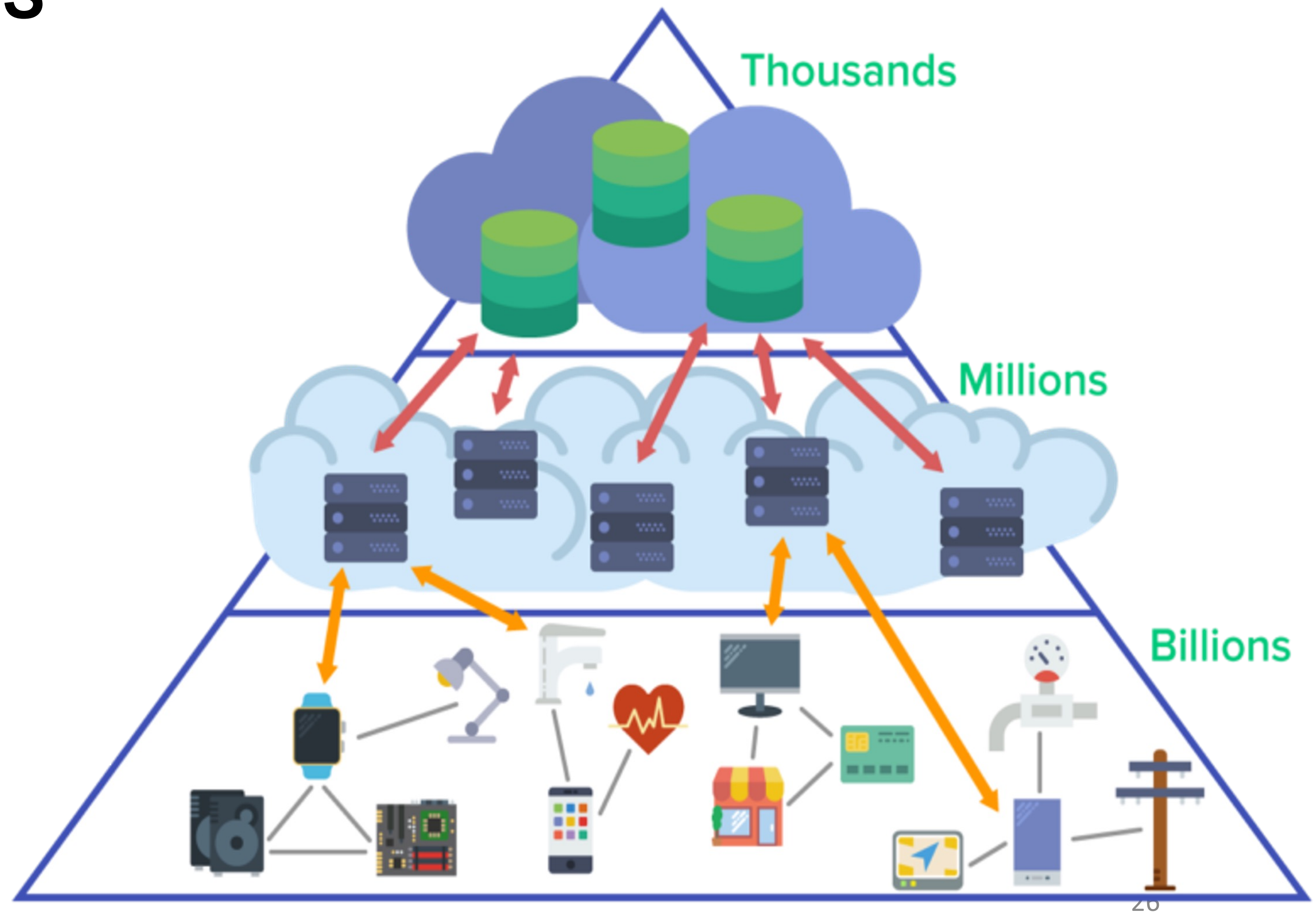
HETEROGENEOUS DEVICES

Device characteristics:

- Processing power
- Memory
- Communication
- Mobility
- Sensors

Problems

- *Energy constraints*
- *Introduce latency*
- *No reliable model updates*
- *Heterogeneous models*



Challenges in FL

COMMUNICATION COSTS AND OVERHEAD

- **Client selection**

  The goal is to selects the clients properly to increase the convergence of the model while reducing the number of model transmissions

- **Number of communication rounds**

  The goal is to reduce the number of iterations between server and clients to achieve model convergence

- **Model representation**

  The goal is to reduce size needed to represent the model without decreasing its performance

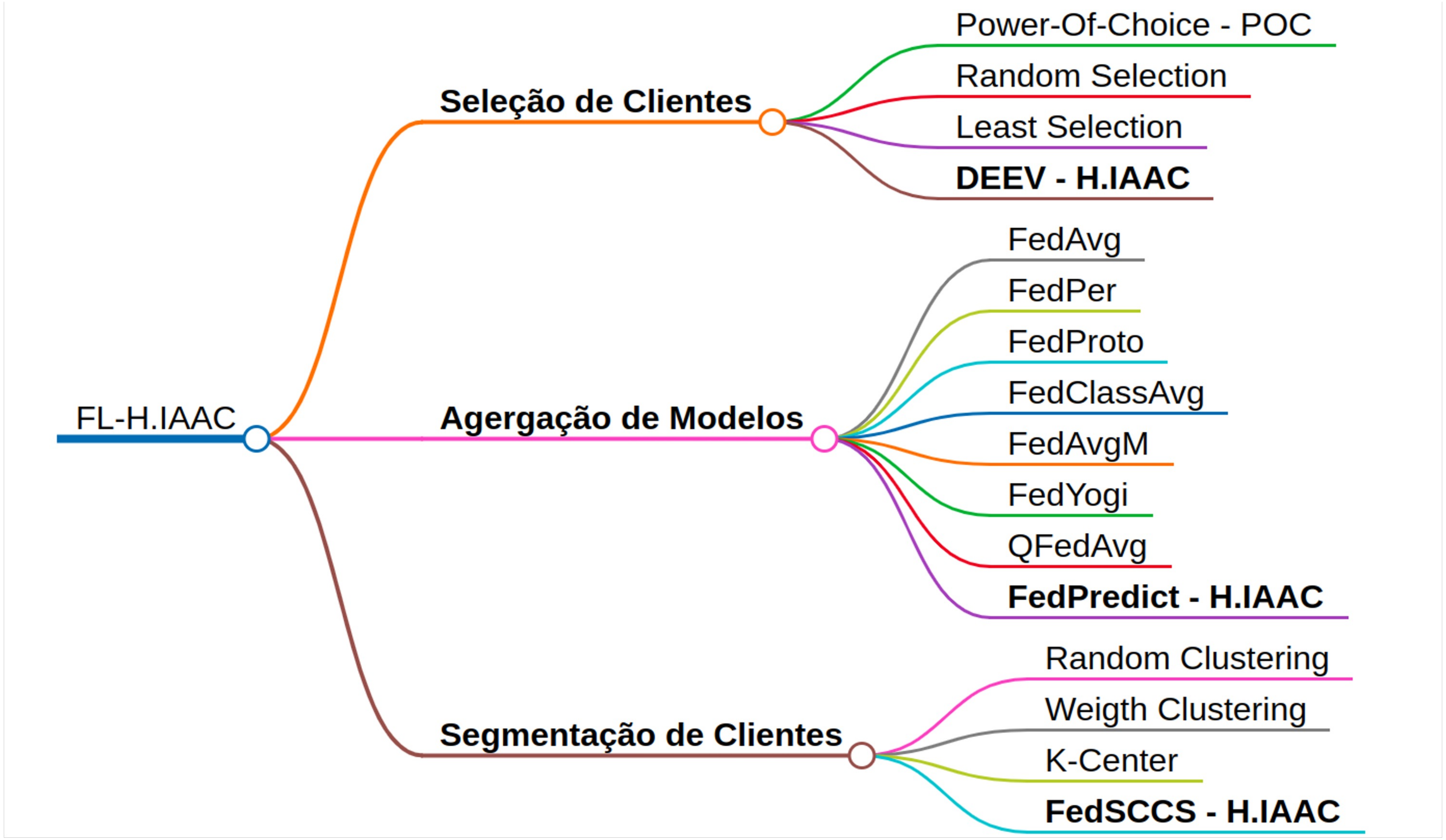
Main Contributions

- **Framework for Developing and Evaluating Federated Learning solutions**
  - *A framework that allows both the development and implementation of federated learning solutions. Such framework is the development basis for all solutions implemented developed by our group.*

- **Adaptive Client Selection Algorithm for Federated Learning**
  - *Client selection is an essential step in federated learning. Therefore, an adaptive solution was developed to improve not only the model performance (i.e., convergence) but also the communication overhead generated by federated learning.*

- **Efficient Model Aggregation Algorithm for non-identically balanced and distributed data**
  - *Non-IID data, is a key challenge in federated learning that needs to be addressed. Therefore, an efficient algorithm was developed to allow good model performance even in scenarios with non-IID data*

FL-H.IAAC - Implemented Solutions



Current Activities

- Algorithm for Clustering Clientes based on Model Similarity
- Context-aware Client Selection for Resource Constraints Devices
- Federated learning with Model Heterogeneity
- A Testbed for Federated Learning with heterogeneous devices

Testbed Overview (Early Stage)

- 5 Raspberry Pi 3 Model B and 1 Notebook acting as the orchestrator.
- Each Raspberry Pi is equipped with a Docker installation and connects via WiFi to a local network, enabling the loading of containers at any time.
- The entire Federation system can be managed using the Flower Framework directly from the orchestrator notebook.
- Parameters such as the model to be used, client selection method, and number of rounds **can be adjusted.**
- Additionally, a dashboard offers real-time visualization of key Federated Training characteristics: Latency, bandwidth usage, selected clients, and training accuracy.

Teste inicial FL-H.IAAC

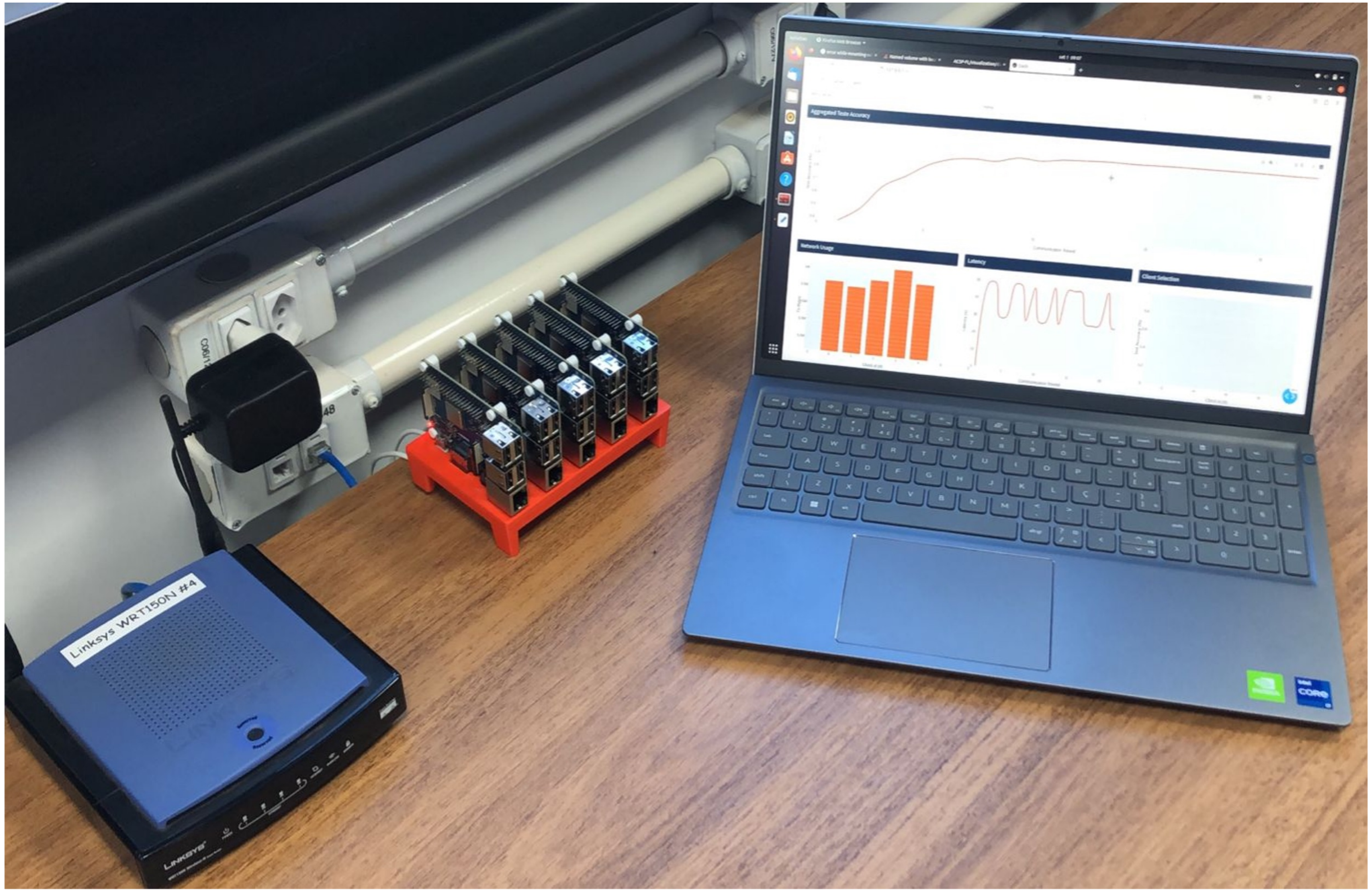
FL-H.IAAC - Testbed (Early Stage)

Deployment of solutions on heterogeneous devices.

Orchestrator to distribute clients across available devices.

- Smartphones
- Wearables
- Notebooks
- IoT Devices

Interface for real-time analysis and visualization



Next Activities

- Open the testbed for collaborators to evaluate their solutions
- Improve the scalability of the testbed including more devices with different computing resources
- Development of more efficient solutions for federated learning, including:
    - Model compression
    - Solutions based on heterogeneous models
    - Fairness and balance in client selection
    - Context-aware solutions (computational and communication resources of devices)
- Explore multi-task federated learning and also deep reinforcement federated learning

Grazie!

Thank you!