IEEE DCOSS – IoT 2024

International Conference on Distributed Computing In Smart Systems and the Internet of Things

Advancements in Federated Learning for Health Applications: A Concise Survey

V. Stamatis, P. Radoglou-Grammatikis, A. Sarigiannidis, N. Pitropakis, T. Lagkas, V. Argyriou, E. K. Markakis and P. Sarigiannidis

Introduction

Telemedicine and Remote Care
Telemedicine has seen significant expansion, allowing patients to access healthcare remotely through virtual appointments, teleconsultations, and remote monitoring

Wearables & Remote Monitoring
Wearable devices such as fitness trackers, smartwatches, and medical-grade sensors enable continuous monitoring of vital signs, activity levels, and health metrics

Health Information Exchange and Interoperability
Health information exchange (HIE) initiatives and interoperability standards facilitate the seamless sharing of patient data across healthcare systems, providers, and organizations. Interoperable health IT systems enable comprehensive patient care coordination, data-driven decision-making, and population health management.

Artificial Intelligence
AI and machine learning technologies are transforming healthcare by enabling predictive analytics, clinical decision support, and personalized treatment recommendations.

Lack of Privacy
Privacy issues still remain

Advancements of Federated Learning in Health

C1 – State of the Art Analysis: We conduct an analysis and comparison of various research works that have applied FL in the healthcare domain.

C2 – Trends and Gaps: We discuss potential future directions and identify gaps in the current research before concluding our paper.

Under TRUSTEE

Authors & Contributors

K3Y Ltd

https://k3ylabs.com/

Vasileios Stamatis

Panagiotis Radoglou Grammatikis

Antonios Sarigiannidis

Edinburg Napier University

https://www.napier.ac.uk/

Nikolaos Pitropakis

Democritus University of Thrace

https://www.cs.duth.gr/

Thomas Lagkas

Kingston University London

https://www.kingston.ac.uk/

Vasileios Argyriou

Hellenic Mediterranean University

https://hmu.gr/en/home/

Evangelos K. Markakis

University of Western Macedonia

https://www.uowm.gr/

Panagiotis Sarigiannidis

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101070214 (TRUSTEE). Disclaimer: Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the European Commission can be held responsible for them.

What is the Problem?

Why federated learning in the health domain?

Data Privacy
Federated learning allows for model training across decentralized data sources without the need to share raw data.

Data Localization
Maybe the data cannot leave original locations due to regulatory constraints.

Communication Overhead
Federated learning reduces the need for large-scale data transfers

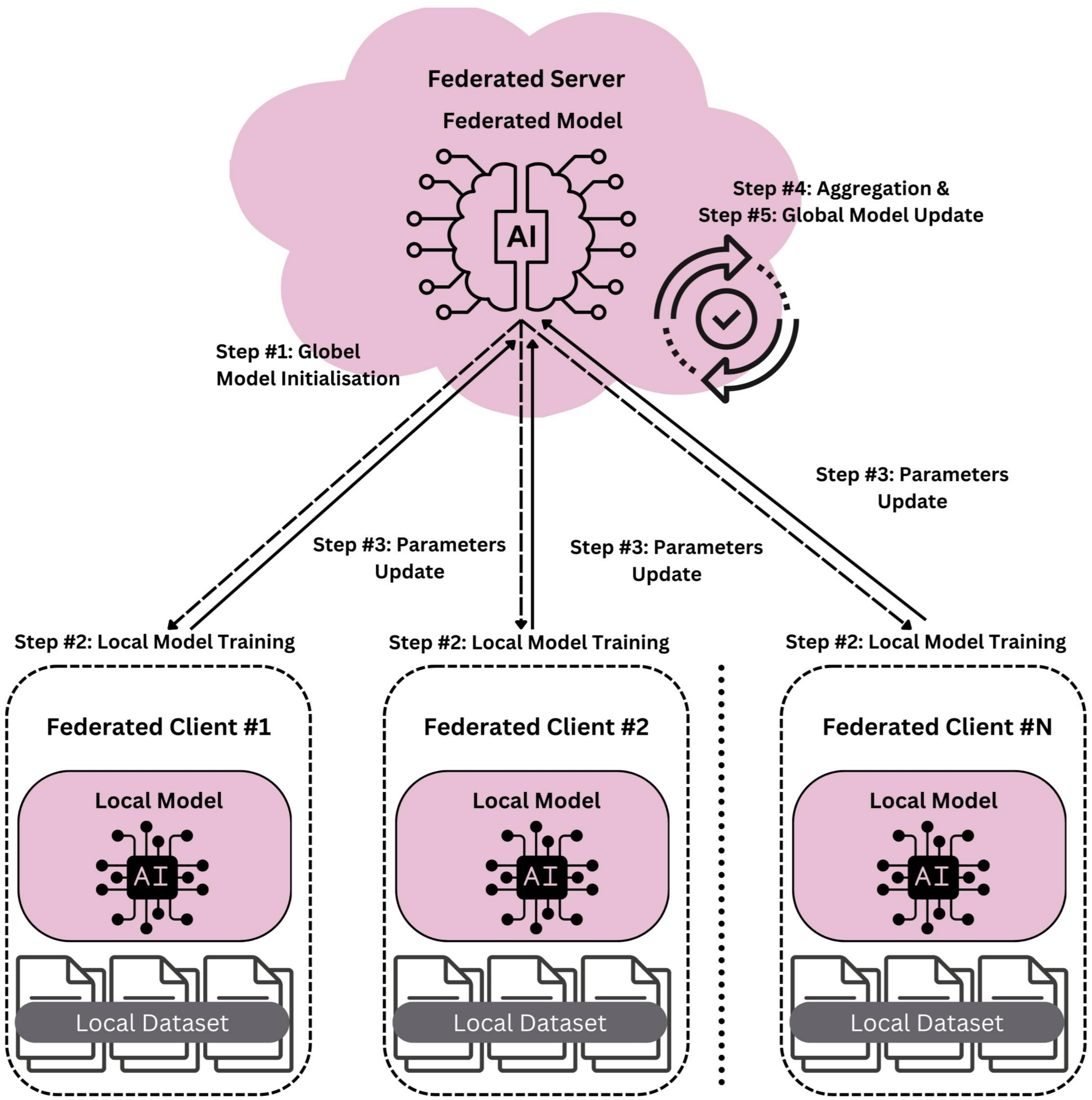
Scalability Issues
Federated learning can scale to large number of clients

Data Distribution Shift
Changes in the data distribution across clients

Data breaches
Federated learning reduces the risk of data breaches since sensitive data remains on the clients

Federated Learning Lifecycle

Why federated learning?



Global Model Initialisation

A global model is initialized on a central server. This model serves as the starting point for training.

Local Model Training

Each selected client independently trains a local model using its own data. This training process can involve multiple iterations (epochs) of training using standard machine learning algorithms, such as gradient descent.

Parameters Update

After local training, each client computes a model update, typically in the form of gradients, based on the difference between its local model and the global model.

Aggregation & Global Model Update

The model updates from all participating clients are aggregated or combined on the central server to generate a new global model.

Model Distribution

The updated global model is then distributed back to the clients, replacing their local models. This step ensures that all clients benefit from the collective knowledge learned across the federated network.

Methodology

Systematic literature review

✓ **Step #1**
Definition of the overall study

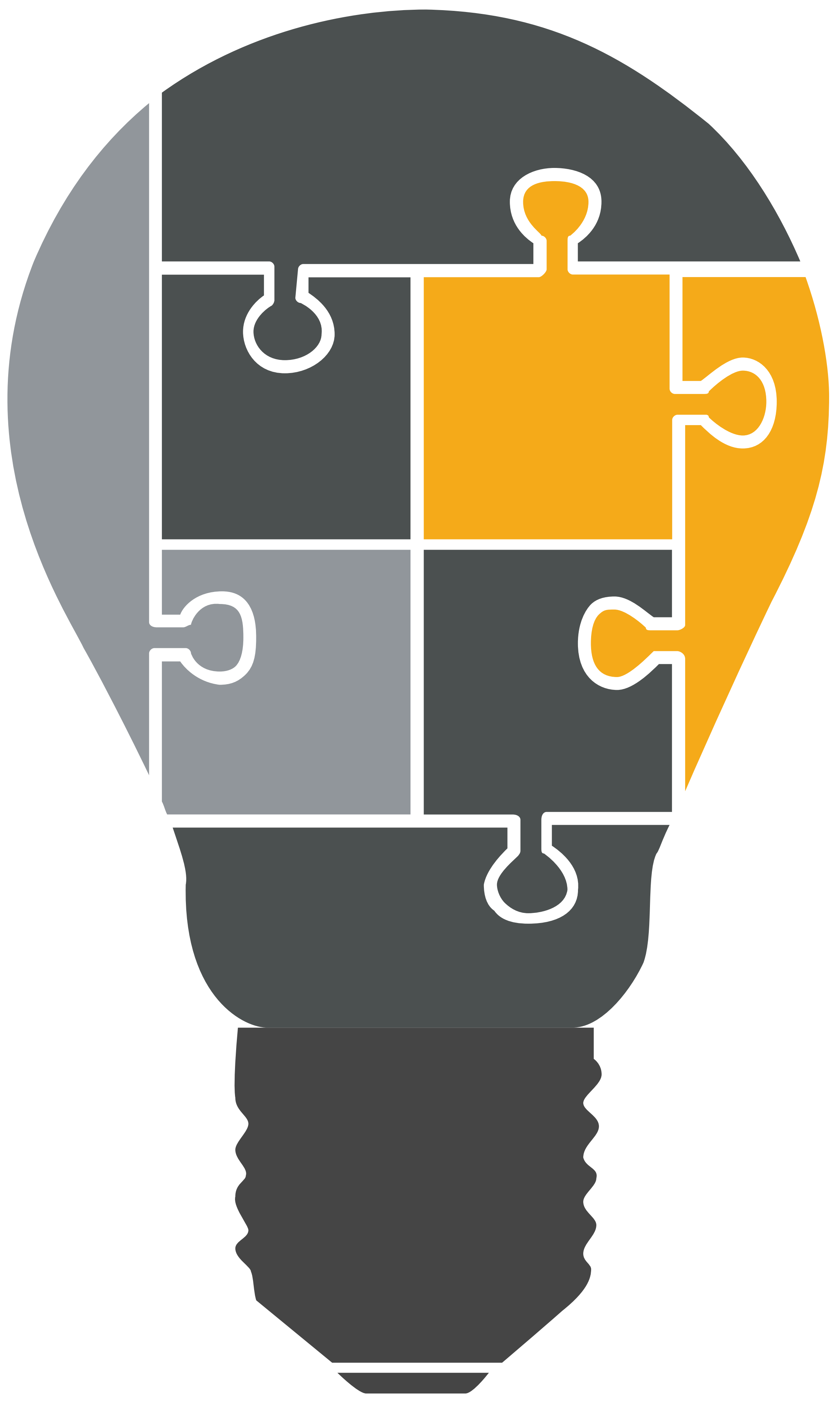
✓ **Step #2**
Selection Criteria

✓ **Step #3**
Thorough Analysis

✓ **Step #4**
Conclusions & Research Directions

Concise State of the Art Analysis

Federated learning in the health domain



Problem Statement
First, the problem is studied in terms of how federated learning can benefit

Data Type
Special attention is paid to data types, such as text data, numerical data, images, etc.

Aggregation
The aggregation strategies were investigated, paying attention to custom methods

Privacy and Security Measures
Privacy and security measures, such as additional anonymization methods were further investigated

Datasets & Technologies
Special emphasis to open datasets

Performance Evaluation
Methodologies, metrics, scores

Ref	Problem Statement	Data Type	Aggregation Techniques	Privacy and Security Mechanisms	Datasets	Tools	Performance Evaluation
[1]	Predicting COVID-19 patient outcomes while safeguarding patient privacy through the application of federated learning.	Images, Numerical	Federated averaging	Differential privacy	Data from 20 medical institutes.	Tensorlflow	ROC curve, Confusion Matrix
[2]	Federated learning strategies for cancer diagnosis, while optimizing model parameter exchange and enhancing federated learning training efficiency.	Images	Federated averaging, Consensus-driven federated averaging	Differential privacy, Authentication	BraTS 2018, BraTS 2020, Athens dataset	N/A	Dice Similarity Coefficient over time
[3]	Predicting oxygen needs in COVID-19 patients using federated learning.	Images, Numerical	Federated averaging	Secure sockets layer (SSL) Encryption, Differential privacy	Data from 20 medical institutes.	Tensorflow	ROC curve, Confusion Matrix
[4]	Leveraging federated learning and blockchain to securely collaborate on healthcare data.	All types	Federated averaging	Blockchain, Differential privacy, Homomorphic encryption	Patient-related data (blood pressure, glucose meter, insulin pump, and others)	N/A	Overheads (ms)
[5]	Addressing the privacy vulnerabilities inherent in federated learning.	Numerical	Sum of weighted parameters	Ring signatures	Collected physiological data from users	JPBC library	Signature time, Verification time
[6]	Federated learning-enabled person movement identification using wearable device data for personalized health monitoring.	Numerical, Text	Federated averaging	Blockchain	UniMiB SHAR, Human activity recognition	N/A	Accuracy, Precision, Recall, and F1-score
[7]	Predicting the level of user depression using federated learning.	Text	Federated averaging	N/A	The Global Sentiment Dictionary	Tensorflow	Accuracy, Precision, Recall, and F1-score
[8]	Addressing the data privacy and efficiency challenges of mental health monitoring systems using federated learning.	Numerical	Federated averaging	Encrypted communication	Collected data from devices.	CoreML	Average memory usage (KB), Average power consumption (%)
[9]	Using user-generated data for healthcare data analytics utilizing the federated learning approach.	Numerical	Federated averaging	Homomorphic encryption	Health-related data from wearable devices	N/A	N/A
[10]	Federated learning for chronic kidney disease prediction.	Images, Numerical	Federated averaging	N/A	Image dataset collected from kaggle	Tophat for image enhancement	Sensitivity, Specificity, Accuracy, Efficiency
[11]	Addressing the non-IID data distribution challenge in the healthcare domain using a clustered federated learning approach.	Numerical	Federated averaging	N/A	HRV dataset (Gathered for research at Samsung Medical Center Department of Psychiatry).	Tensorflow (Keras)	Accuracy
[12]	Privacy-preserving federated learning framework tailored for IoT-driven SmartHealth Systems.	Images	Federated averaging	Differential privacy	MNIST, CIFAR10, STL10, COVID19 Chest X-RAY	Pysift, Pytorch	MAE, Accuracy, Computation time.

Problem Statement

Four main applications of federated learning in health domain

Predicting COVID-19 patient outcomes while safeguarding patient privacy through the application of federated learning.

01

02

Federated learning strategies for cancer diagnosis, while optimizing model parameter exchange and enhancing federated learning training efficiencyIt includes advertising, selling and delivering products to people.

Predicting oxygen needs in COVID-19 patients using federated learning.

03

04

Federated learning-enabled person movement identification using wearable device data for personalized health monitoring.

Data Types & Datasets

Five key categories of data

EHR

Electronic Health Records - medical history, diagnoses, medications, laboratory results, and treatment plans

Mixed

Medical Imaging Data

Medical imaging data, such as X-rays, MRIs, CT scans, and ultrasounds

Image

Genomic Data

DNA sequences, genetic variations, and gene expression profiles

Numerical

Clinical Trials

demographics, treatment protocols, and outcomes

Mixed

Medical Sensor Data

electrocardiograms (ECGs), blood glucose monitors, and blood pressure cuffs

Numerical

What kind of Data

In the health domain, federated learning utilizes diverse data types including electronic health records (EHRs) containing mixed textual, numerical, and categorical information, medical imaging data comprising images such as X-rays and MRIs, and genomic data consisting of sequences and numerical genetic variations.

Aggregation Strategies

FedAvg is the most used strategy

FedSGD – Federated Stochastic Gradient Descent

- Each client calculates the average gradient of global model
- The server aggregates these averages and perform the update
- Client performs only one step of gradient descent
- Requires large number of rounds training due to single batch gradient calculation

FedAvg – Federated Averaging

- Each client makes multiple steps of Gradient Descent locally
- The Server calculates the Weighted Average of the resulting Models
- Robustness to Unbalanced and non-IID data
- Reduces number of rounds of Communication
- It drops the clients that fail to perform their work within a time window.

FedOpt – Federated Optimisation

- Promotion of Communication Efficiency and Privacy
- Uses Sparse Compression Algorithm (SCA) which is based in Sparse top-k algorithm, to reduce the amount of Communication
- Adopts a lightweight homomorphic encryption with differential privacy for efficient and secure aggregation of gradients

Security Measures

Differential privacy is the most used security mechanism

Encryption

SSL/TLS

Differential Privacy

Differential privacy techniques add noise to model updates to prevent the leakage of individual contributions.

Secure Aggregation

Secure Multi-party Computation (SMPC) or homomorphic encryption, enable secure aggregation of model updates without revealing the raw contributions from individual clients.

Byzantine Robustness

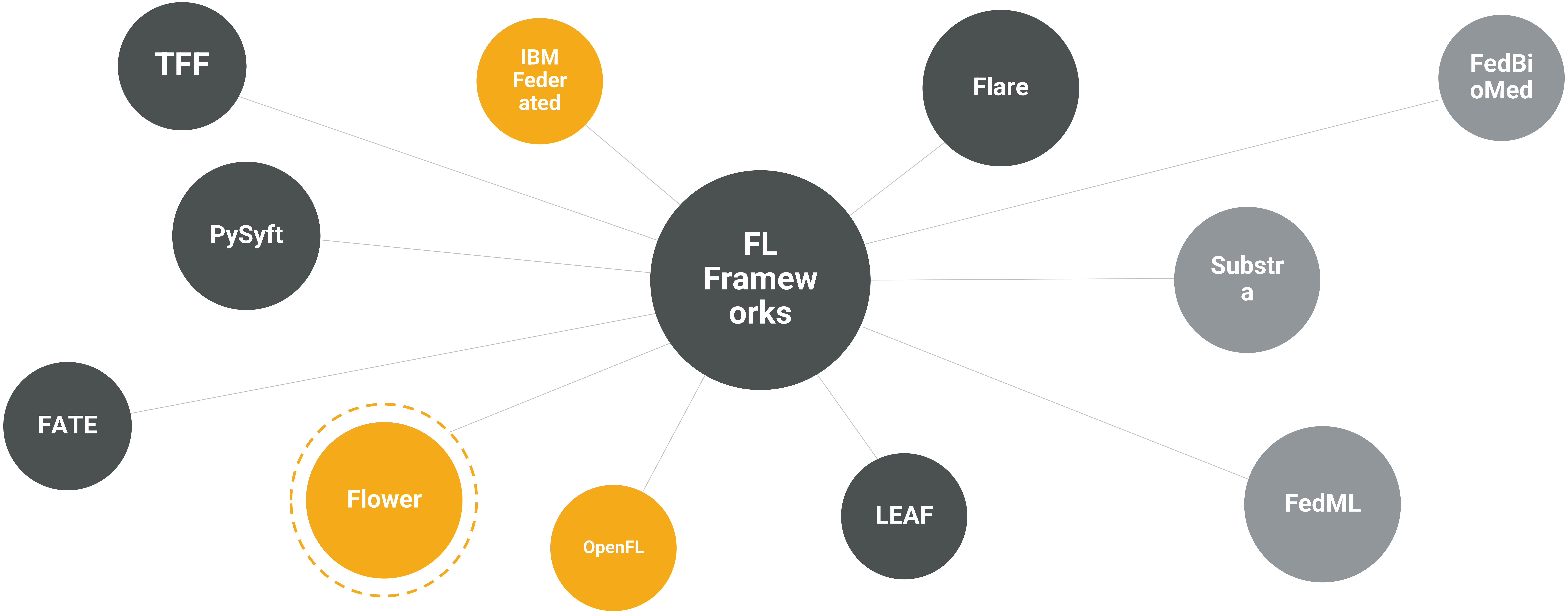
Byzantine fault tolerance (BFT) or robust aggregation methods can detect and mitigate the influence of malicious or faulty clients in federated learning.

Poisoning Detection

Mechanisms for detecting and mitigating model poisoning attacks, where malicious clients attempt to manipulate the global model by submitting malicious updates, are crucial for maintaining model integrity.

Federated Learning Programmable Frameworks

Flower is the most used framework



Performance Evaluation

Still typical AI evaluation metrics are used

		Predicted condition			
	Total population $= \mathrm{P} + \mathrm{N}$	**Predicted Positive (PP)**	**Predicted Negative (PN)**	Informedness, bookmaker informedness (BM) $= \mathrm{TPR} + \mathrm{TNR} - 1$	Prevalence threshold (PT) $= \frac{\sqrt{\mathrm{TPR} \times \mathrm{FPR}} - \mathrm{FPR}}{\mathrm{TPR} - \mathrm{FPR}}$
Actual condition	**Positive (P)** [a]	**True positive** (TP), hit[b]	**False negative** (FN), miss, underestimation	True positive rate (TPR), recall, sensitivity (SEN), probability of detection, hit rate, power $= \frac{\mathrm{TP}}{\mathrm{P}} = 1 - \mathrm{FNR}$	False negative rate (FNR), miss rate type II error [c] $= \frac{\mathrm{FN}}{\mathrm{P}} = 1 - \mathrm{TPR}$
Actual condition	**Negative (N)**[d]	**False positive** (FP), false alarm, overestimation	**True negative** (TN), correct rejection[e]	False positive rate (FPR), probability of false alarm, fall-out type I error [f] $= \frac{\mathrm{FP}}{\mathrm{N}} = 1 - \mathrm{TNR}$	True negative rate (TNR), specificity (SPC), selectivity $= \frac{\mathrm{TN}}{\mathrm{N}} = 1 - \mathrm{FPR}$
	Prevalence $= \frac{\mathrm{P}}{\mathrm{P} + \mathrm{N}}$	Positive predictive value (PPV), precision $= \frac{\mathrm{TP}}{\mathrm{PP}} = 1 - \mathrm{FDR}$	False omission rate (FOR) $= \frac{\mathrm{FN}}{\mathrm{PN}} = 1 - \mathrm{NPV}$	Positive likelihood ratio (LR+) $= \frac{\mathrm{TPR}}{\mathrm{FPR}}$	Negative likelihood ratio (LR−) $= \frac{\mathrm{FNR}}{\mathrm{TNR}}$
	Accuracy (ACC) $= \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{P} + \mathrm{N}}$	False discovery rate (FDR) $= \frac{\mathrm{FP}}{\mathrm{PP}} = 1 - \mathrm{PPV}$	Negative predictive value (NPV) $= \frac{\mathrm{TN}}{\mathrm{PN}} = 1 - \mathrm{FOR}$	Markedness (MK), deltaP (Δp) $= \mathrm{PPV} + \mathrm{NPV} - 1$	Diagnostic odds ratio (DOR) $= \frac{\mathrm{LR+}}{\mathrm{LR-}}$
	Balanced accuracy (BA) $= \frac{\mathrm{TPR} + \mathrm{TNR}}{2}$	F_1 score $= \frac{2\,\mathrm{PPV} \times \mathrm{TPR}}{\mathrm{PPV} + \mathrm{TPR}} = \frac{2\,\mathrm{TP}}{2\,\mathrm{TP} + \mathrm{FP} + \mathrm{FN}}$	Fowlkes–Mallows index (FM) $= \sqrt{\mathrm{PPV} \times \mathrm{TPR}}$	Matthews correlation coefficient (MCC) $= \sqrt{\mathrm{TPR} \times \mathrm{TNR} \times \mathrm{PPV} \times \mathrm{NPV}} - \sqrt{\mathrm{FNR} \times \mathrm{FPR} \times \mathrm{FOR} \times \mathrm{FDR}}$	Threat score (TS), critical success index (CSI), Jaccard index $= \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN} + \mathrm{FP}}$

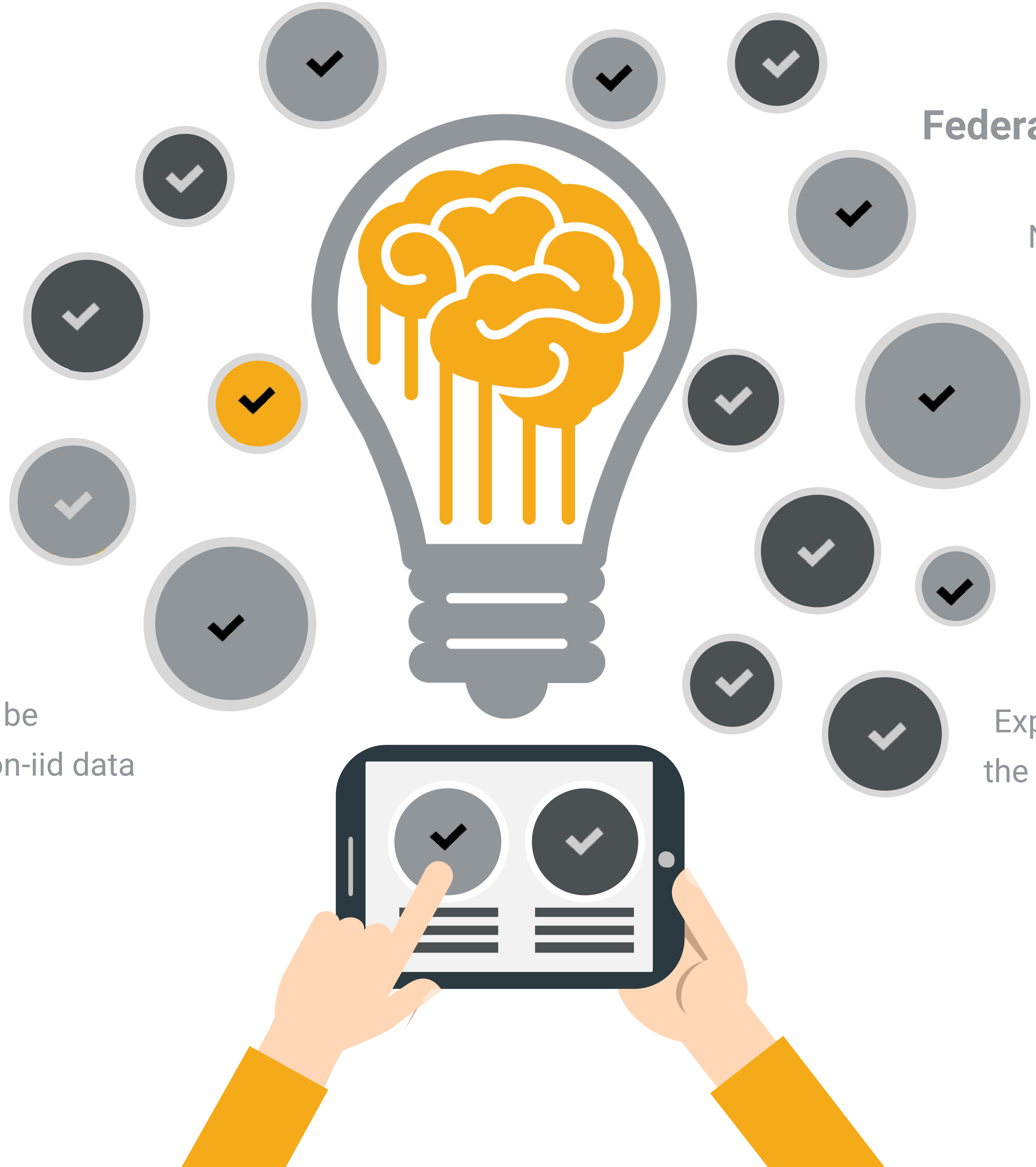
Conclusions & Research Directions

Outcomes and directions for future research

More health applications
Federated learning has the potential to benefit multiple health applications

Multimodal FL for Health
Multimodal FL applications can benefit significantly the health sector

Data Heterogeneity
Custom aggregation methods can be investigated in order to address non-iid data



Federated Learning Trustworthy Evaluation Framework
Need for an evaluation framework investigating each step of the federated learning lifecycle

Adversarial Attacks
Security measures and custom aggregation techniques should counter the impact of adversarial attacks

Explainability Issues
Explainability functions should allow the end-user to fully understand each step during the federated training process

Thank You & Q/A

Contact us

pradoglou@k3y.bg

https://k3ylabs.com/

https://www.linkedin.com/company/k3y/?originalSubdomain=bg

Thank You

Q/A ?

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101070214 (TRUSTEE). Disclaimer: Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the European Commission can be held responsible for them.