Implications of Fairness in Federated Learning in Healthcare

Machine Learning Systems

Navya Annapareddy and Jade Preston

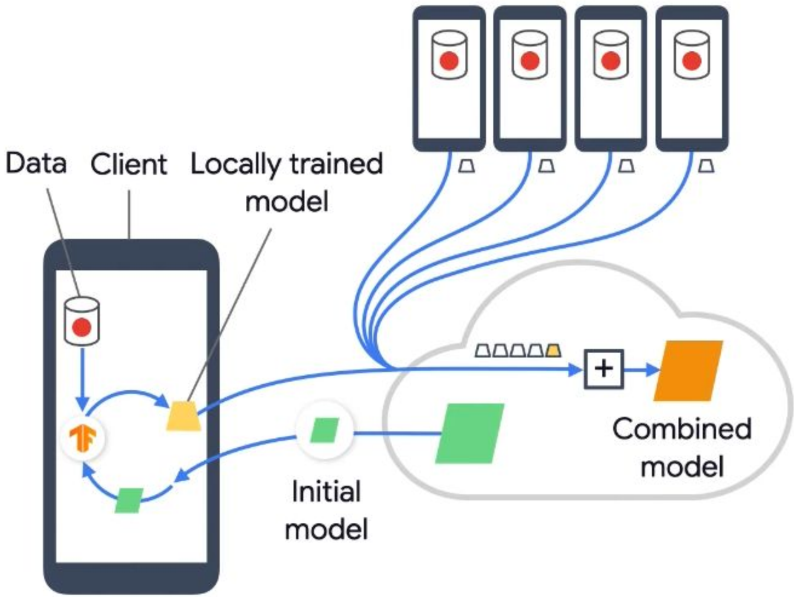
DS 7406

Dec 02, 2022

University of Virginia | School of Data Science

Agenda

- Problem Description
- Potential Research Gap(s)
- Proposed Contribution
- Literature Review
- Methodology: FAFL Survey
- Results
    - FAFL Taxonomy
    - Lifecycle View
    - Healthcare Implications



Problem Description

- **Data sharing** is often difficult or constrained by security and distribution limitations
  - Large sample sizes allow models to generalize for more variability
  - Data is often governed by data-use ordinances such as **HIPAA** and security restrictions

- **Federated learning** is a type of **distributed learning** framework
  - Allows data to be trained decentralized
  - Addresses **data security**, **privacy**, and **vulnerability** considerations
  - Challenges to federated learning include:
    - Node data may not be independent and identically distributed (iid)
    - High levels of communication
    - Heterogeneity in the individual nodes w.r.t bias and size of data samples

Identified Research Gap

1. **Categorization of existing implementations by approach**
    a. Metric based, resource allocation based
2. **Existing fairness surveys focus on tabular data**
    a. Lack of consideration for image and other high dimensional datasets
3. **No comprehensive lifecycle view**
    a. Difficulty in aligning model processes across node and server
        i. Across implementations of metrics/fairness approaches
4. **Healthcare focus**
    a. No existing ties to implications to healthcare

Proposed Contributions

*New contribution

1. **Comprehensive survey according to considerations by fairness approach**
    a. Identify existing text, image, and other high dimensional implementations
        i. Differentiate fairness approach and update w.r.t taxonomy
        ii. Differentiate unsupervised vs. supervised
        iii. **Create discrete model process representation (ie: pre-training vs. post)**
2. **Classify security and scaling considerations in context of FL lifecycle**
    a. **Security of aggregation/model sending***
    b. **Robustness and non IID data***
    c. Scalability (esp. adding peers)
3. **Create focus on implications of FL fairness in healthcare domain**

Related Work - Surveys on FAFL

- **Shi et al.** Categorized **fairness notions** and **fairness approach taxonomy**, assuming a single fairness implementation
  - Accuracy Parity
  - Good Intent Fairness
  - Selection Fairness
  - Contribution Fairness
  - Regret Distribution Fairness
  - Expectation Fairness
- **Quy et al.** examined **bias** and **challenges to fairness** in federated learning datasets in different domains, including healthcare

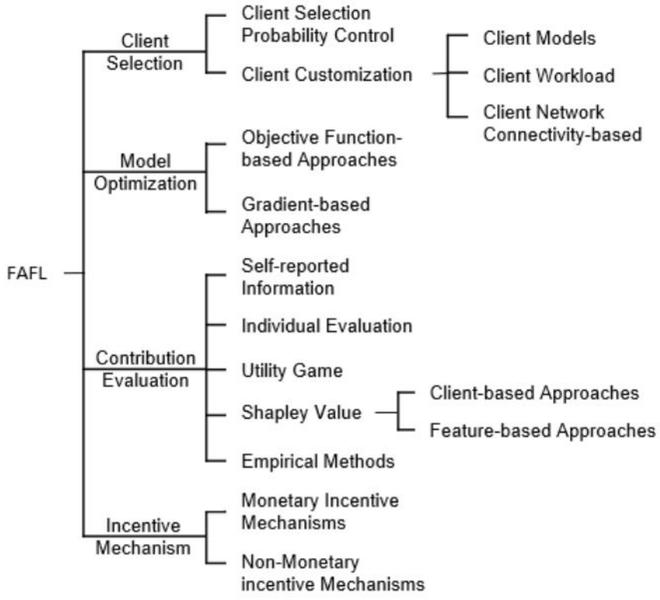
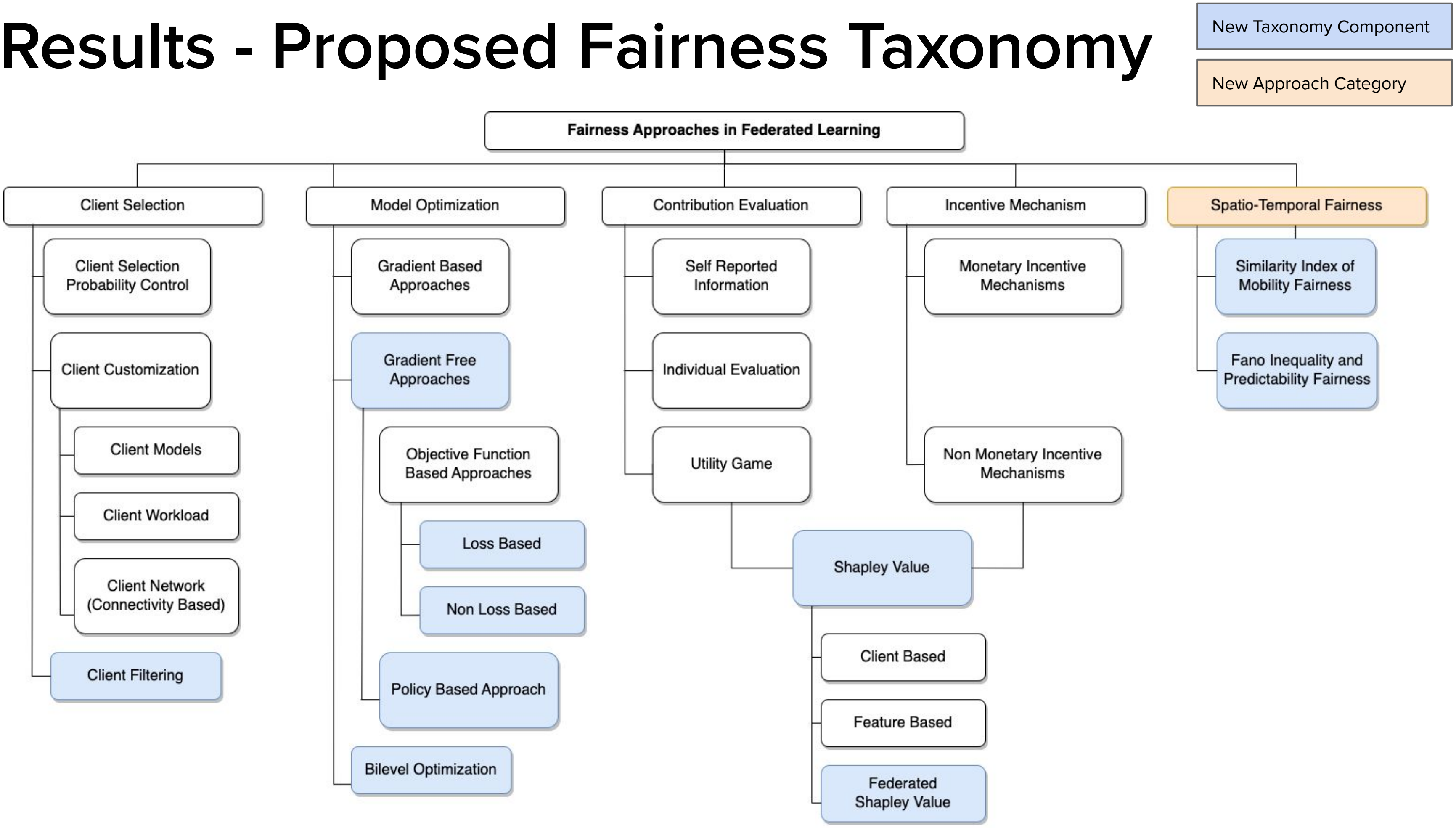


Fig. 1. The proposed taxonomy of FAFL approaches.

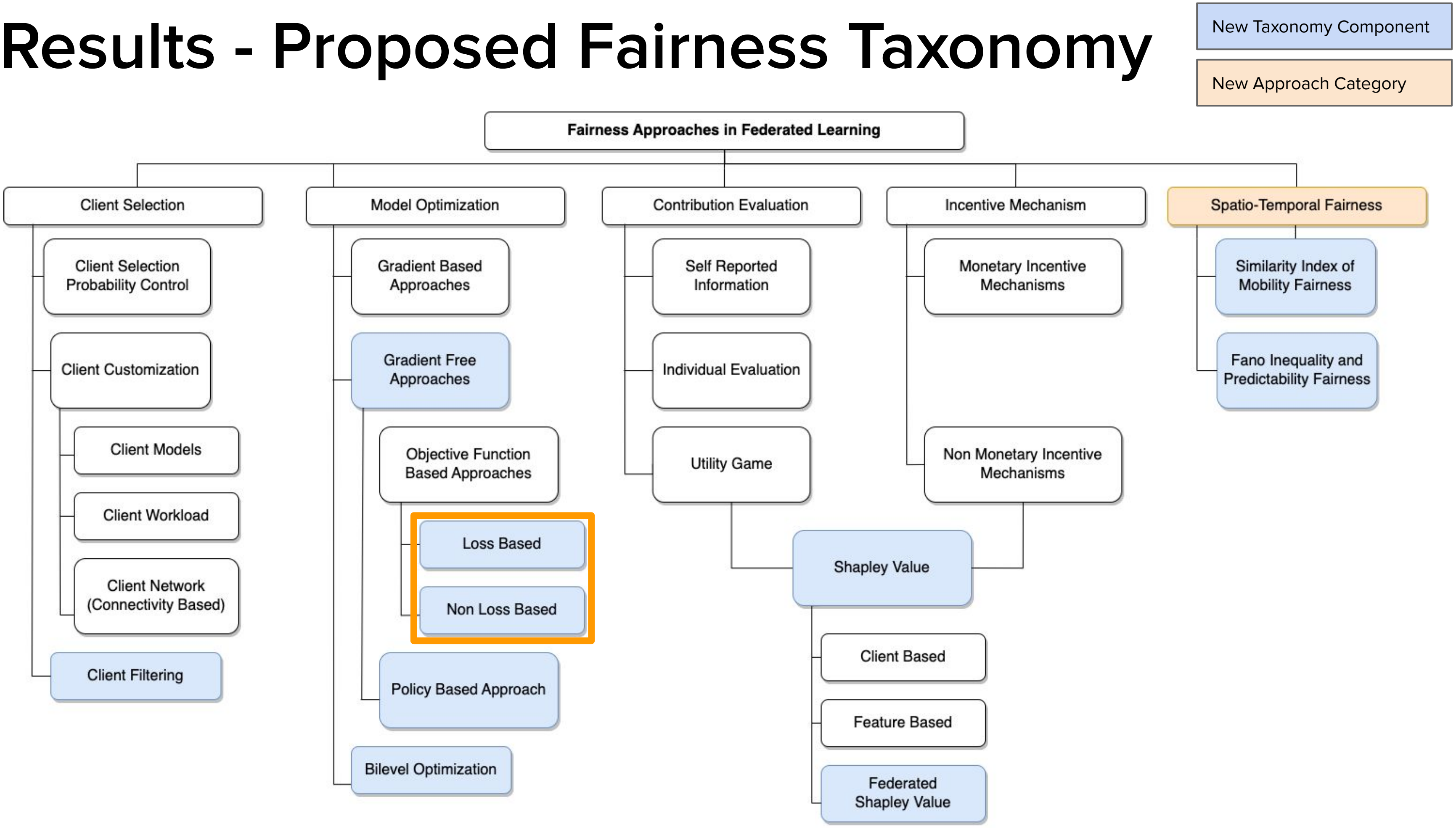
Methodology - Surveyed Implementations

Implementation Papers	
FedScale: Benchmarking Model and System Performance of Federated Learning at Scale	Resource Management and and Model Personalization for Federated Learning over Wireless Edge Networks
Federated Learning on Clinical Benchmark Data: Performance Assessment	Fairness and Accuracy in Horizontal Federated Learning
Fair Federated Learning via Bounded Group Loss	Fairness Aware Incentive Scheme for Federated Learning
Fairness in Federated Learning for Spatial-Temporal Applications	Fairness and Accuracy in Federated Learning
A Reputation Mechanism Is All You Need: Collaborative Fairness and Adversarial Robustness in Federated Learning	Federated Optimization In Heterogeneous Networks
Ditto: Fair and Robust Federated Learning Through Personalization	Fairness-aware Agnostic Federated Learning
Utility Fairness for the Differentially Private Federated Learning	An Efficiency-boosting Client Selection Scheme for Federated Learning with Fairness Guarantee

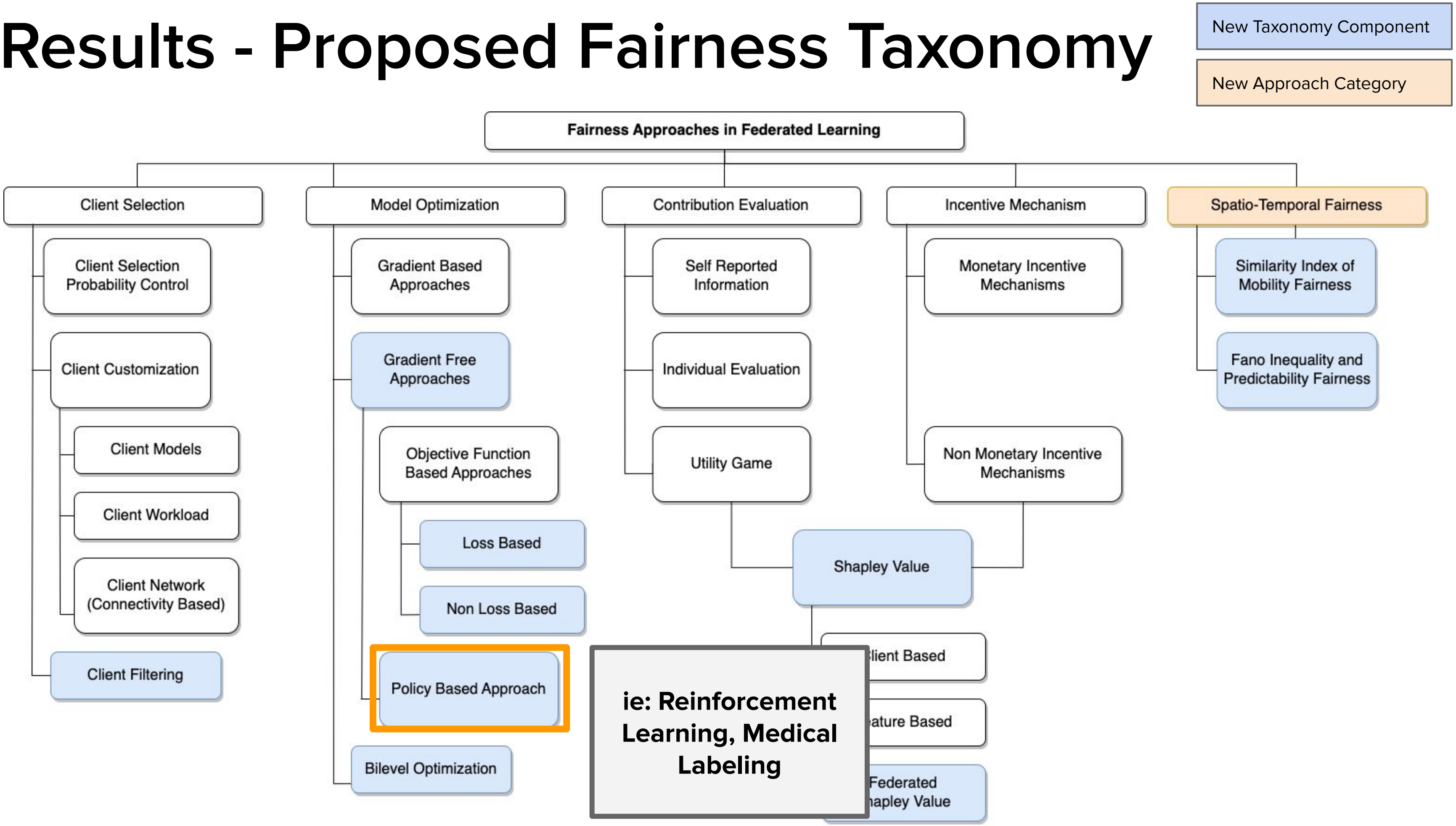
Results - Proposed Fairness Taxonomy



Results - Proposed Fairness Taxonomy

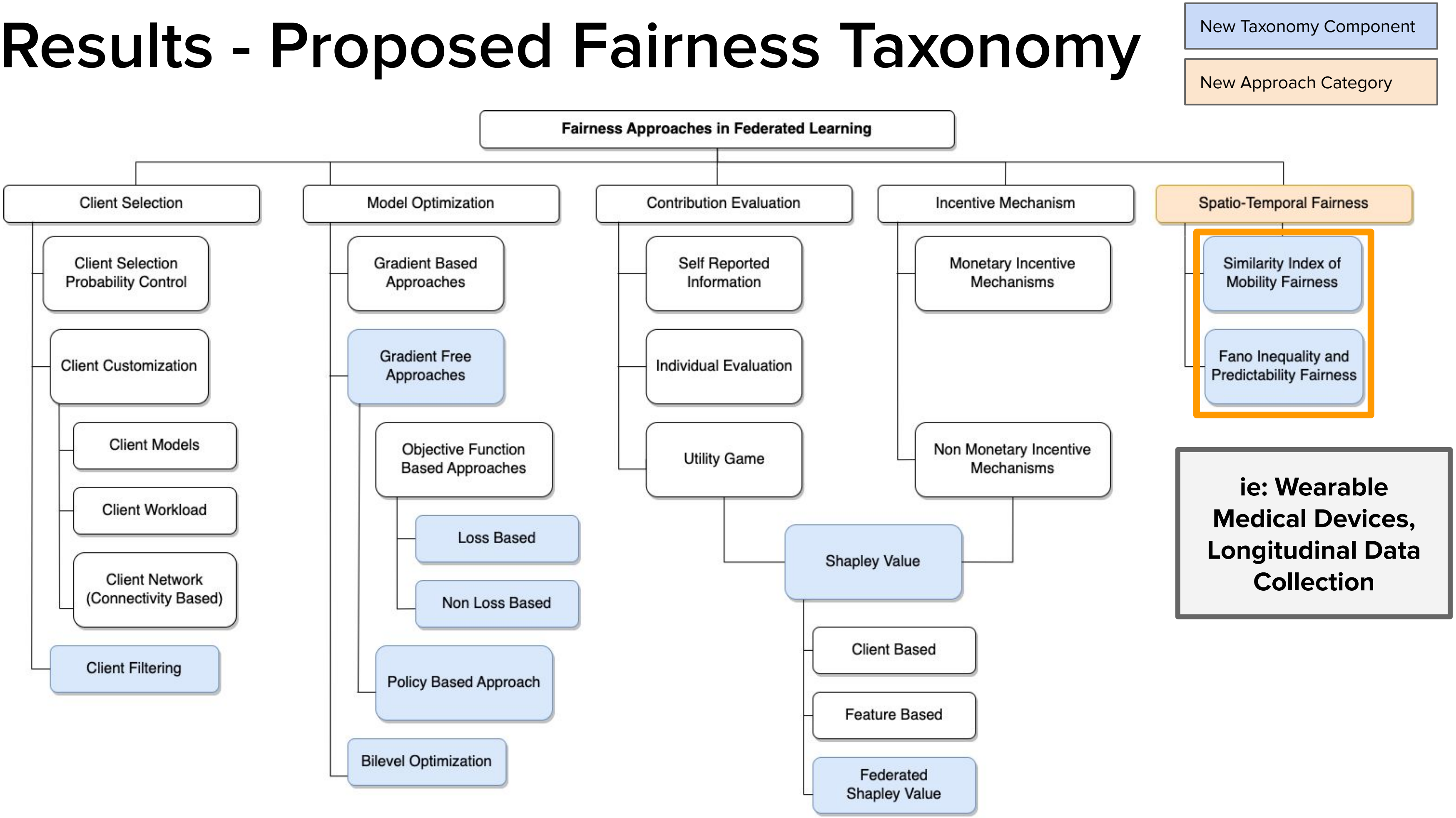


Results - Proposed Fairness Taxonomy



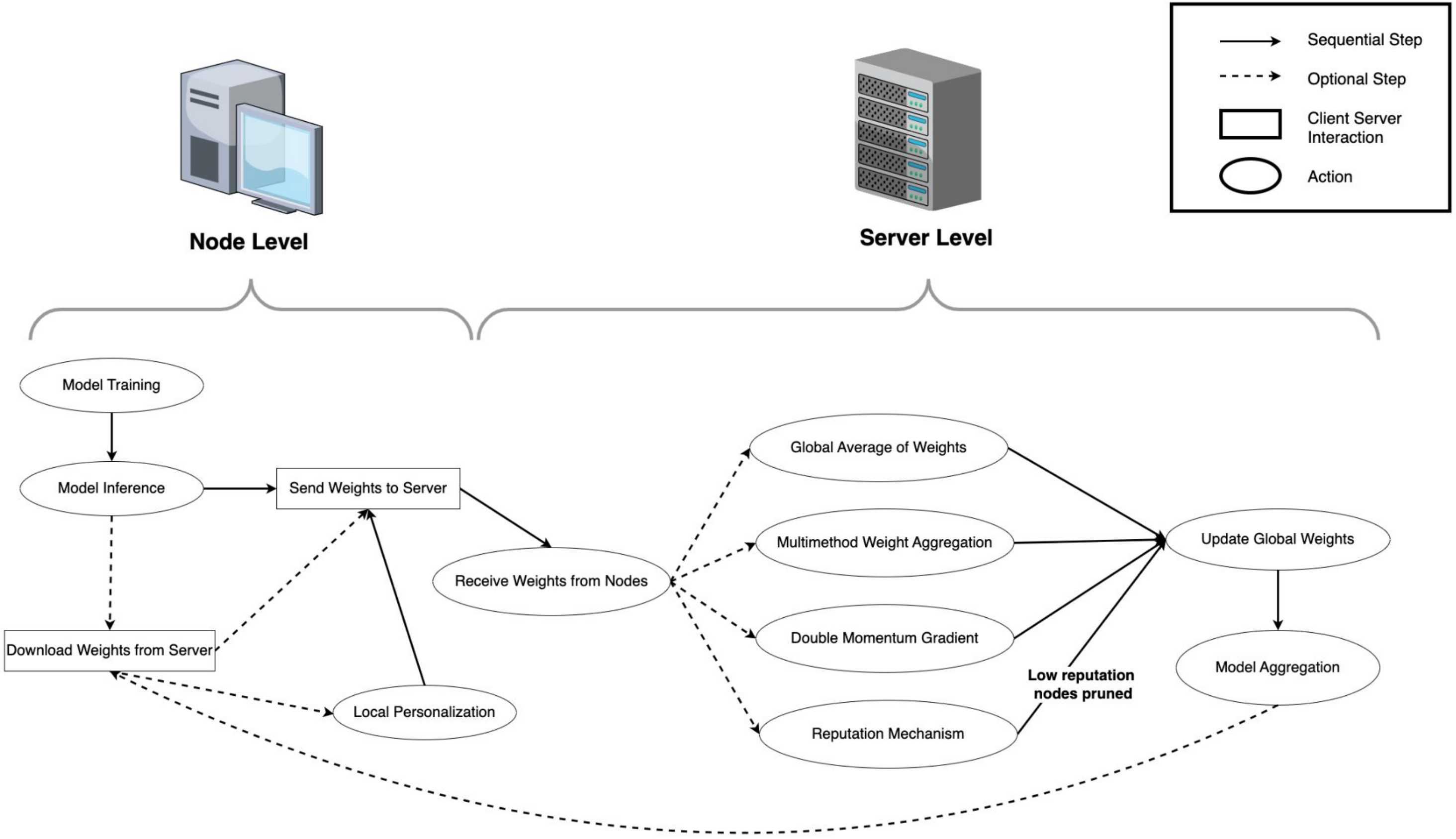
ie: Reinforcement Learning, Medical Labeling

Results - Proposed Fairness Taxonomy



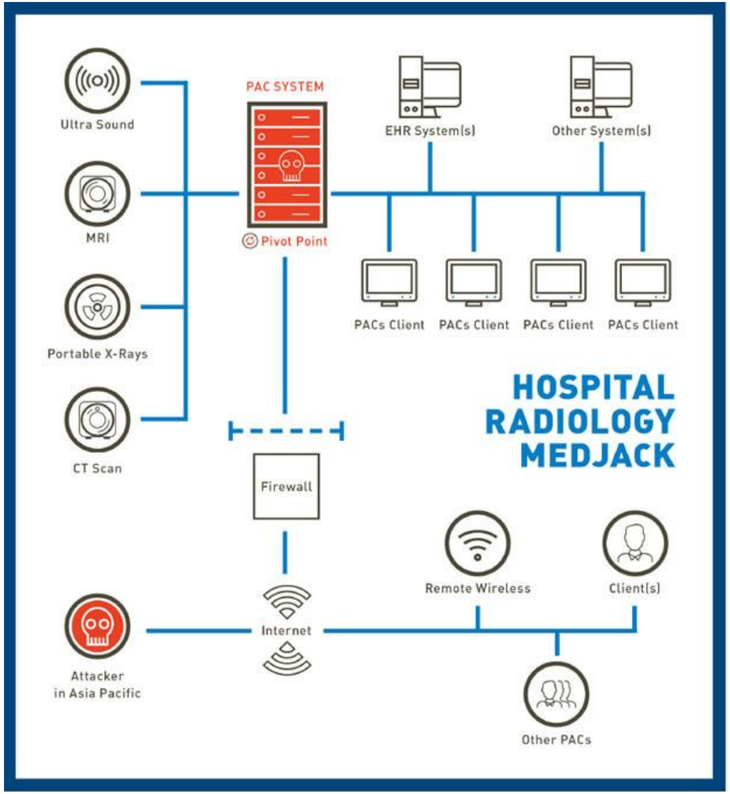
ie: Wearable Medical Devices, Longitudinal Data Collection

Results - Generalized FL Lifecycle View



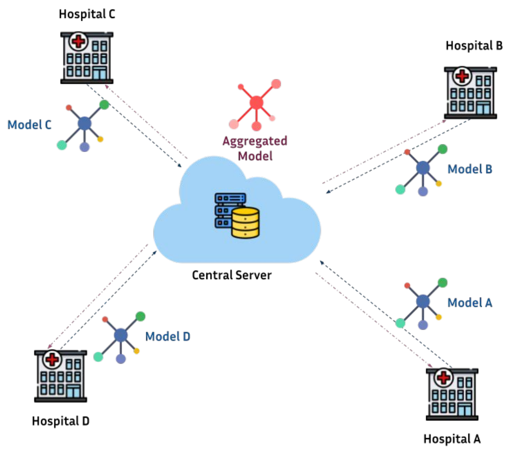
Results - Implications to Healthcare

1. FL in healthcare has unique security and privacy considerations at each step of life cycle
   - TEEs in healthcare
   - Network security/attack considerations
   - **Medical devices, split learning, and IOT**
2. **Differential privacy** is highly relevant
3. Medical imaging considerations
   - High dimensional
   - Alternative encryption methods
4. Data storage and retention
5. Data lifecycle management



Conclusion

- Fairness in federated learning is **not zero-sum**, we consider notions that existing taxonomies do not:
    - Implementations utilize multiple categories
    - High level implementation groups (ie: bilevel)
- **FAFL and Healthcare** require unique considerations and benefit from the FL lifecycle view of to understand execution environment security
- Healthcare also brings **challenges to federated learning** including **high dimensionality**, **high communication overhead and complexity**, and **enforced security standards**



Researchers Assess Federated Learning Models for COVID-19 Diagnostics

Researchers from the University of Minnesota are evaluating how federated learning models may be used for COVID-19 diagnosis through chest X-rays.

Questions?

References

- https://arxiv.org/pdf/2110.00530.pdf
- https://arxiv.org/pdf/2111.01872.pdf
- https://arxiv.org/pdf/2105.11367.pdf
- https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7652692/
- https://arxiv.org/pdf/2203.10190
- https://arxiv.org/pdf/2012.10069
- https://arxiv.org/pdf/2011.10464
- http://proceedings.mlr.press/v139/li21h/li21h.pdf
- https://arxiv.org/pdf/2109.05267
- https://www.mdpi.com/2224-2708/10/1/17/pdf?version=1616039824

References

- https://arxiv.org/abs/1812.06127
- https://zhangjunbo.org/pdf/2022_InsSci_FedFa.pdf
- https://arxiv.org/pdf/2201.06598
- https://dl.acm.org/doi/pdf/10.1145/3375627.3375840?casa_token=eDBBCTTTc88AAAAA:RMn3_v5Yz0Dc4uroUezdB27QHx08ivy1vsGJ4fqU9ctFgc7w9m7GxcIFCUuwRip2NYgyqSZP1-sG
- https://arxiv.org/abs/2010.05057
- https://ieeexplore.ieee.org/document/9797864