Protecting Sensitive Biosignal Data in Model Training: Federated Learning for Healthcare Applications

Kai Malcolm[1], Momona Yamagami[1]
[1]Rice University, Department of Electrical and Computer Engineering

Study Objective: Design and validate privacy-preserving machine learning models capable of quickly personalizing to sensitive biosignal data.

Always-on Personalized Wearable Sensors Will Bolster Human Health and Well-being

Figure 1: Illustration of EMG measuring devices and potential applications.

Wearable sensors have promising applications in:

- Improving health through **continuous tracking** for personalized, preventative medicine.
- Enabling intuitive and accessible device interaction.
- **Ubiquitous rehabilitation**: rehabilitation that harnesses activities of daily life to monitor, train, and improve movement.

Obstacles to Next-generation Wearable Devices:

- Reluctance to adopt always-on medical devices is particularly pronounced among individuals with disabilities, who worry about misuse by insurance providers or the denial of healthcare access, causing invaluable data to be unuseable [5].
- Novel interfaces require long calibration times, and many must be periodically re-calibrated.
- Models are developed to perform well for the "average" user:
  - No user is perfectly "average" [4].
  - Models are biased against individuals far from "average" (e.g. users with disabilities).

Privacy Attacks on Sensitive Biomedical Data

1. **Record Linkage:** Ability to link records from different databases to uniquely identify individuals.

Federated Learning Offers A Privacy-Preserving Solution For Training Over Data From Different Populations

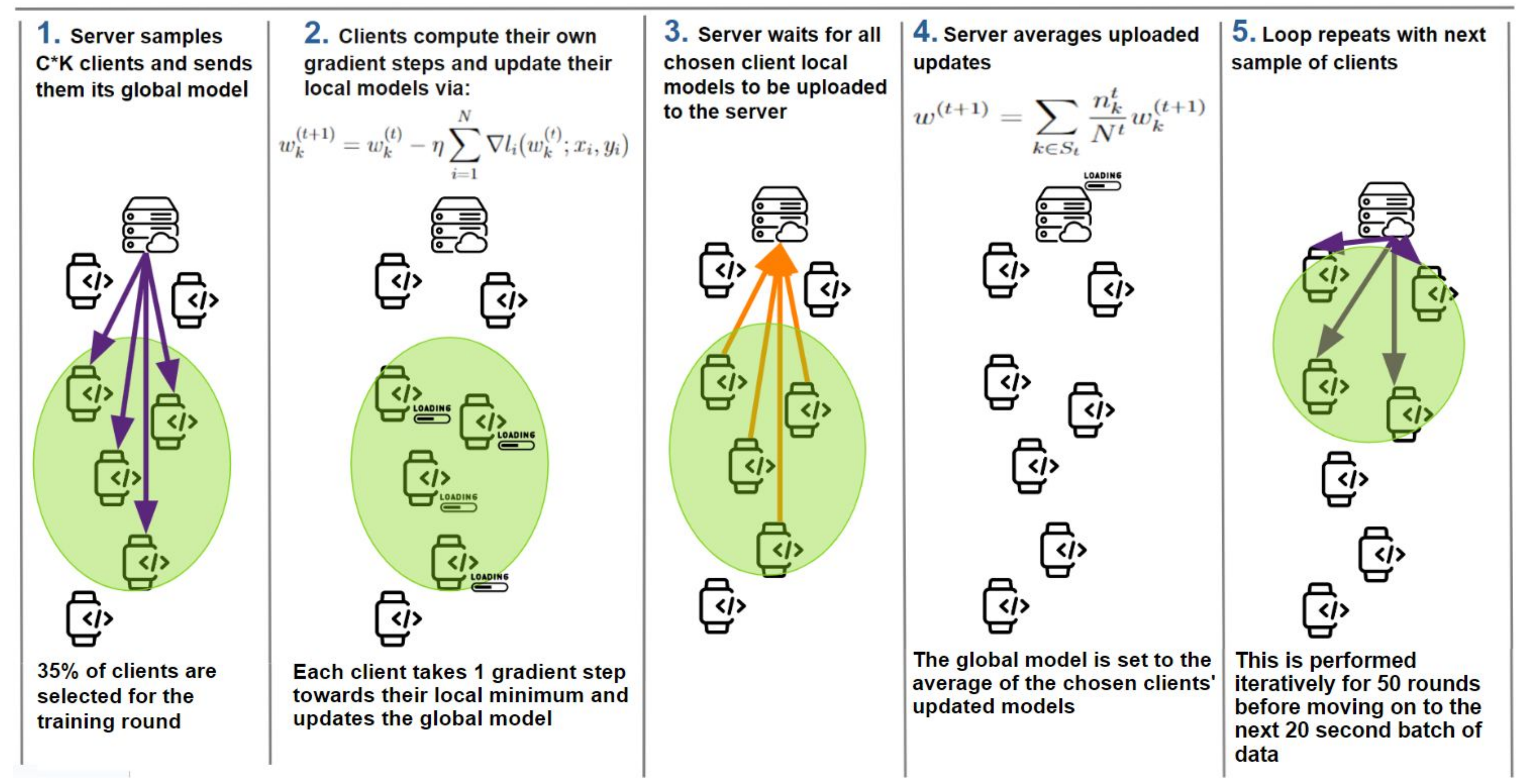

Figure 2: Illustration of the FedAvg Algorithm in the synchronous wearable setting.

Federated learning is well-suited for applications with the following properties:

1. Training Data Is Not Independent and Identically Distributed (**Non-IID**)
2. Clients' Training Dataset Sizes Are **Unbalanced**
3. **Communication** Is More Expensive Than Computation

Our work extends FedAvg [3], shown in Fig.2, which is typically run in simulations on popular image classification datasets (i.e. CIFAR-10), to a real-world biosignal dataset, and incorporates the necessary streaming-based data processing pipeline (Fig. 4).

Method: Secondary Data Analysis Simulating EMG Biosignal Interface Trained Via Federated Learning

Secondary data analysis of trajectory tracking task [2]

- 14 participants using a forearm EMG input to complete a trajectory-tracking task (Fig. 3).
- 5 minute trials with the decoder model updated every 20 seconds.
- The primary analysis [2] sought to optimize a decoder model through co-adaption of the user and the model.
  - Co-adaptation models both the learning of the user and the model.
- **We want to enable higher initial performing models**
  - Randomly initialized models (as used in [2] for each new trial) are unusable for roughly the first minute of the 5 minute trials.
  - This can be **frustrating** for users, and additionally can **increase fatigue**, especially for users with disabilities.

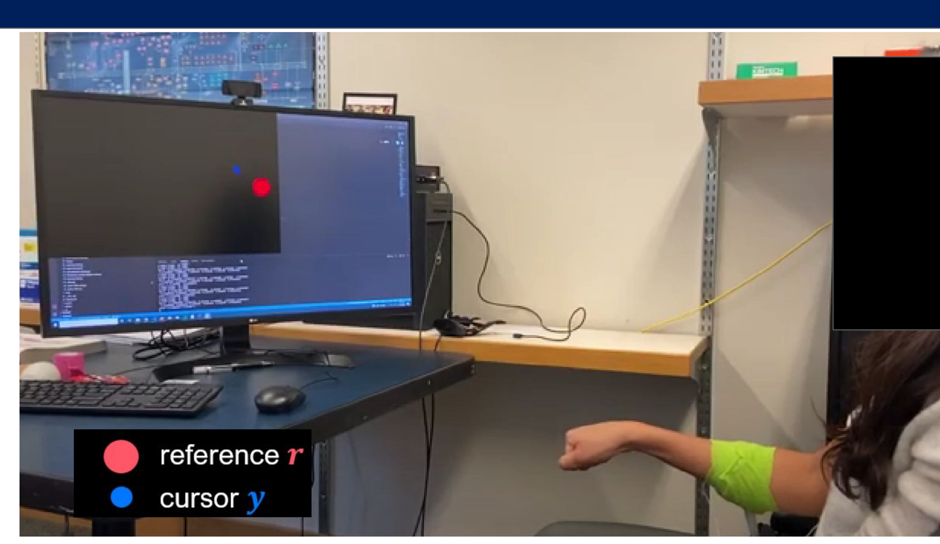

Figure 3: Experimental setup from primary work's data collection.

$$c_{L2} = \min_D f(D)$$

$$= \lambda_E \underbrace{||DF - \frac{d}{dt}(p_{ref} - \int_0^t D_{prev} F dt)||_2^2}_{c_{perf} = ||V_{user} - V_{target}||_2^2} + \lambda_D ||D||_2^2 + \lambda_F ||F||_2^2$$

Secondary Data Processing

- Batch gradient descent was computed on each 20 second update, subject to a local update threshold.
- Updates presented to the model in sequential fashion to simulate real-time streaming.
- EMG input was normalized, then passed through PCA to reduce reliance on channel alignment

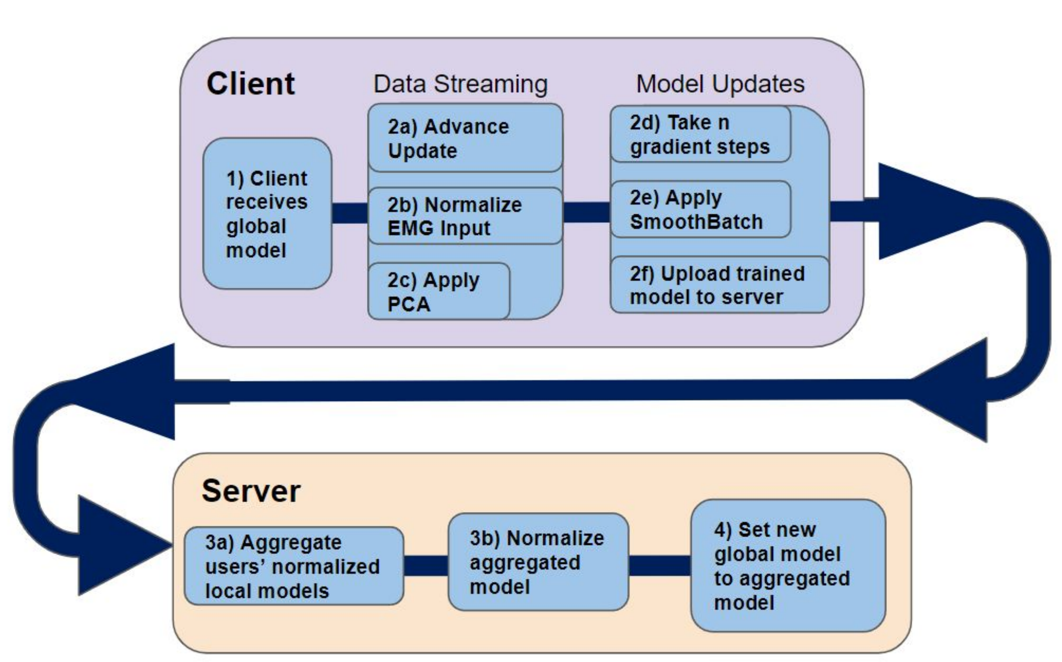

Figure 4: Data streaming and processing pipeline added to FedAvg.

Three Learning Algorithms In Model Training

Non-Federated Models

1. **Local models:** Client-specific models, trained exclusively on the data from a given client (this is the training scheme used in the primary analysis [2]).

Federated Models

2. **Global model:** A single shared model across all clients, trained via the FedAvg algorithm.
3. **Fine-tuned models:** Client-specific extensions to the global model, trained for a few gradient steps on said client's local data. Personalized to each client's data distribution according to the optimization below:

$$\min_{w \in \mathbb{R}^d} F(w) = \frac{1}{K} \sum_{i=1}^{K} f_i(w - \alpha \nabla f_i(w))$$

Evaluating Learning Algorithms for Performance and Privacy Linkage

Comparing Performance of Federated vs Non-federated Models

- All models start from the same random initialization.
- Local model: Minimizes the closed-form cost function for each 20 second batch, then advances to the next 20 second batch, same as in the trials of the primary analysis.
- Federated models: model updates iteratively on each 20 second batch as shown in Fig. 2 for a set number of training iterations before advancing to the next 20 second batch.

Evaluating Adversarial Record Linkage Capabilities

- Want to demonstrate the extent to which model parameters can be linked to specific subjects
- Trained popular ML models (Logistic Regression, Support Vector Classifier, Random Forest, etc.) by giving them (decoder, subject ID) pairs, one 20 second batch at a time, to predict future subject ID pairs from new models.

Result: Personalization Is Required For High Performing Models

- **Local** and **fine-tuned** models outperform **global** model
  - This makes sense because EMG biosignals are personal to each individual
- **Global** model has larger variance in cost as updates increase
  - 35% client inclusion rate per round results in apparent stochasticity
- Using the final **global** model below as the initialization for a new client can result in better initial performance, but this is highly dependent on the final model and can be inconsistent.
- The **global** model is optimized to perform well for the average cost function (Fig. 2), and thus the performance is biased towards the average user as opposed to any existing users.

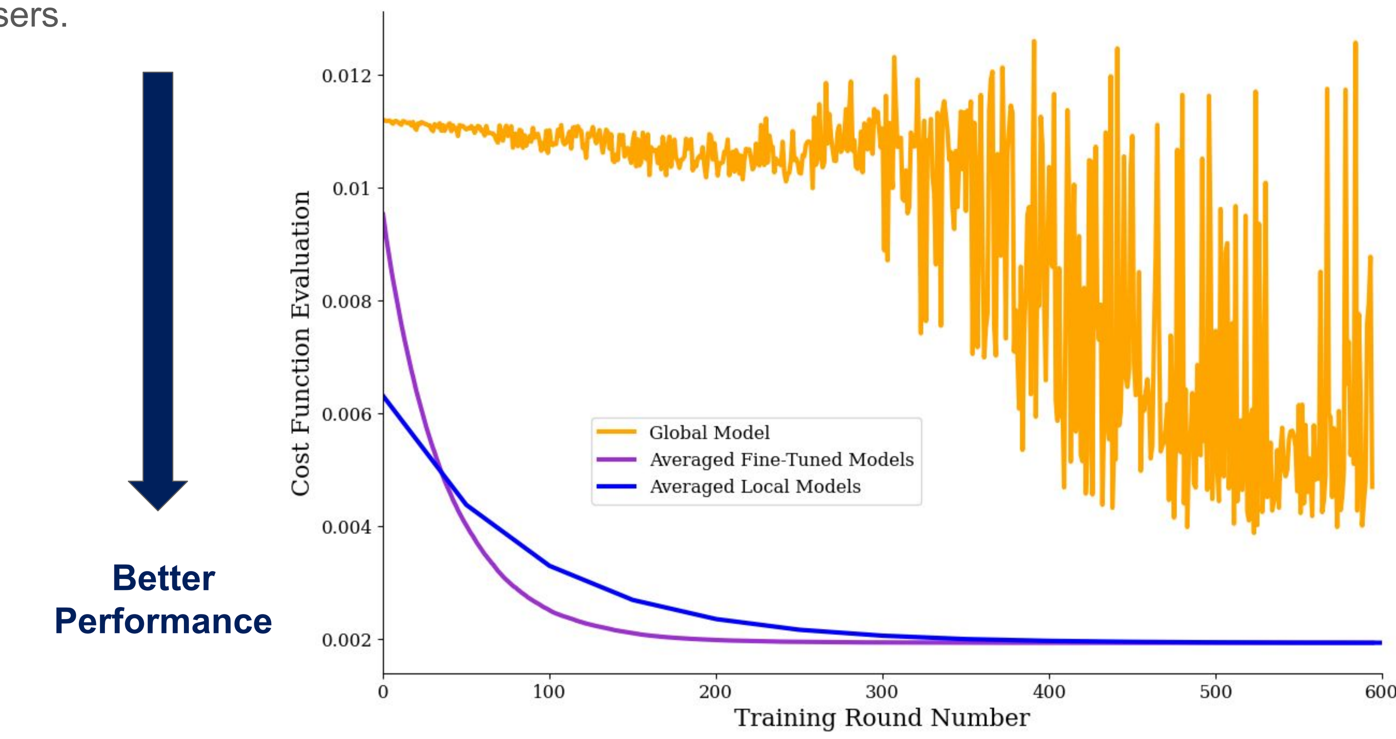

Figure 5: Comparison of EMG decoder model testing error.

Result: FL Global Model Mitigates Adversarial Linkability

- While the **global** model offers the lowest performance, it offers nearly complete user privacy.
- When using **personalized models** (**fine-tuned** / **local**), we can achieve higher performance but incur higher privacy risks.
- **Fine-tuned** models learn the quickest but carry the greatest privacy risk.
- By only communicating the model parameters, FL can bolster user trust by allowing users to retain custody of their data while reaping the benefits of collaborative model training.
- FL is still vulnerable to more complex attacks, but encrypted communication can help.

Key Takeaway: We must make a tradeoff between privacy risk and performance.

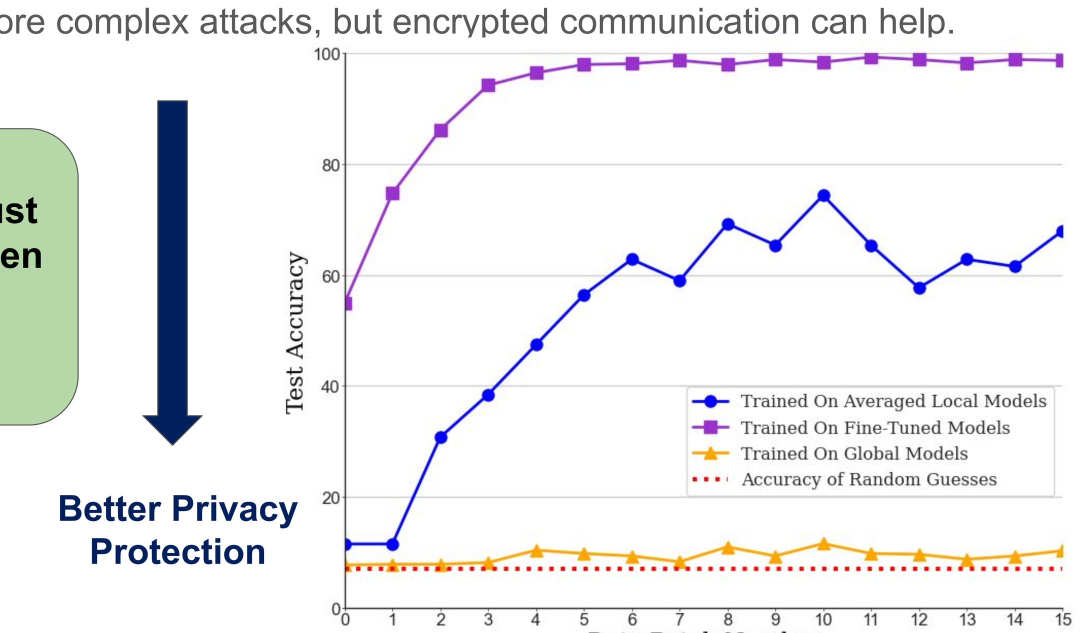

Figure 6: Adversarial model accuracy when linking different model weights back to the subject ID.

Future Work: Translating Simulation Results to Real-time User Applications for Healthcare and Beyond

- Overarching goal of personalized models into the home for ubiquitous rehabilitation in a privacy-preserving manner.
- Transitioning from open-loop simulations to closed-loop user studies to account for co-adaptivity and potentially influence user learning.
- Addressing sequential online learning problem inherent to single-user-at-a-time studies.

References

- [1] Madduri et. al., "A Game-Theoretic Model for Co-Adaptive Brain-Machine Interfaces", 2021
- [2] Madduri et. al., "Co-Adaptive Myoelectric Interface for Continuous Control", 2022
- [3] McMahan et. al., "Communication-Efficient Learning of Deep Networks from Decentralized Data", 2017
- [4] Wobbrock et. al., "Ability-Based Design: Concept, Principles, adn Examples", 2011
- [5] Yamagami et. al., "'I'm Just Overwhelmed': Investigating Physical Therapy Accessibility and Technology Interventions for People with Disabilities and/or Chronic Conditions", 2022