Federated Learning

Konzepte und Begriffe

- **Server**: Der Server ist eine **zentrale** (oder auch **dezentrale**) Instanz, die die Clients und das Machine Learning Modell verwaltet
- **Client**: Ein Client ist eine Instanz, die das Modell trainiert und die Daten lokal besitzt (z.B. ein *Smartphone* oder *Krankenhaus*)
- **Datenvertraulichkeit**: Die Daten der Clients sind **vertraulich** und dürfen nicht an den Server übertragen werden
- **Heterogene / Homogene Daten**: Daten können starke Bias und Unterschiede besitzen, welche die Konvergenz des Modells beeinflussen können
  - Heterogen Daten → Underfitting
  - Homogene Daten → Overfitting
- **Konvergenz**: Abhängig von den Daten kann ein Model konvergieren oder sogar divergieren, besonders wenn Biases in den Daten vorhanden sind

Funktionsweise (Centralized Federated Learning)

Zunächst wollen wir uns den *Centralized Federated Learning* Ansatz anschauen. Des Weiteren gibt es noch den *Decentralized Federated Learning* und *Heterogeneous Federated Learning* Ansatz.

1. **Server wählt** ein Machine Learning **Modell** aus und **verteilt** (distributed) es an die **Clients**
   - z.B. Lineare Regression, neuronale Netze, Boosting
2. Clients **trainieren** das Modell mit ihren **lokalen** Daten
   - *Records*, *Epochen* und *Batches*
3. Die Gradienten / Gewichte des Models werden vom Server **aggregiert**
   - Es können auch einzelne Layer eines Models upgedatet werden
   - Federated Stochastic Gradient Descent (*FedSGD*): Clients senden nur die Gradienten an den Server und dieser bildet den gewichteten Durchschnitt
   - Federated Averaging (*FedAvg*): Clients berechnet die Gradienten und gewichtet das Modell neu und sendet dieses an den Server
   - Hybrid Federated Dual Coordinate Ascent (*HyFDCA*)
4. Sobald der Server ein neues Modell gebildet hat, wird es an die Clients verteilt und eine neue *Epoche* beginnt
5. Sobald die **gewünschte Anzahl an Epochen** (oder ein anderes Kriterium) erreicht ist, wird das **finale Modell** erstellt und ausgegeben
   - Zusätzlich werden Metriken wie *Accuracy* und *Loss* berechnet

> **Note:** Gewisse Ähnlichkeit zu *Parameter Server*