inovex

Machine Learning ohne Preisgabe privater Daten mit Federated Learning

Christian Becker

Karlsruhe, 11. März 2020

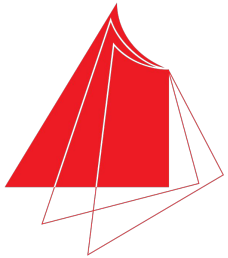
Christian Becker

Informatikstudent an der Hochschule Karlsruhe:

2019/02 Werkstudent inovex

2019/2020 Bachelorthesis bei inovex

2020 Master in Informatik an der Hochschule Karlsruhe



Hochschule Karlsruhe
Technik und Wirtschaft
UNIVERSITY OF APPLIED SCIENCES

Roadmap

1. Was ist Federated Learning
2. Worauf muss man in Federated Learning achten
3. Differential Privacy & Secure Aggregation
4. Evaluation
5. Ergebnisse
6. Zusammenfassung

Overview Federated Learning

- Spezialfall von verteiltem Machine Learning mit mehreren Teilnehmern
- Ermöglicht das Training ohne Herausgabe der Trainingsdaten
- Schützt die Privatsphäre der Daten durch Differential Privacy

Machine Learning

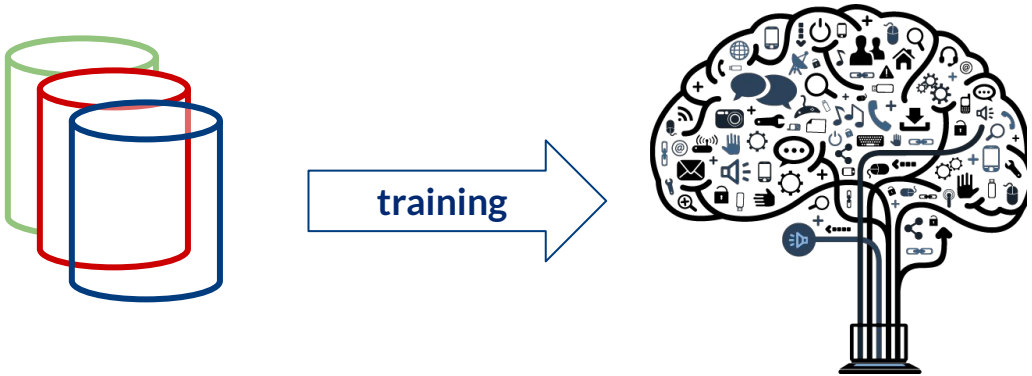
Modell lernt Muster und Gesetzmäßigkeiten von Daten

Training: Optimierungsprozess der wiederholt mit den Daten durchgeführt wird

inovex

Federated Learning

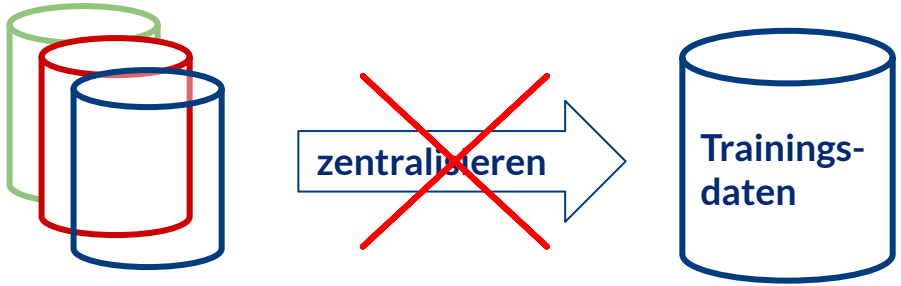
- Ermöglicht das Lernen mit privaten dezentralen Daten
- Daten verbleiben bei den Besitzern
- Eine Art von verteilten maschinellem Lernen



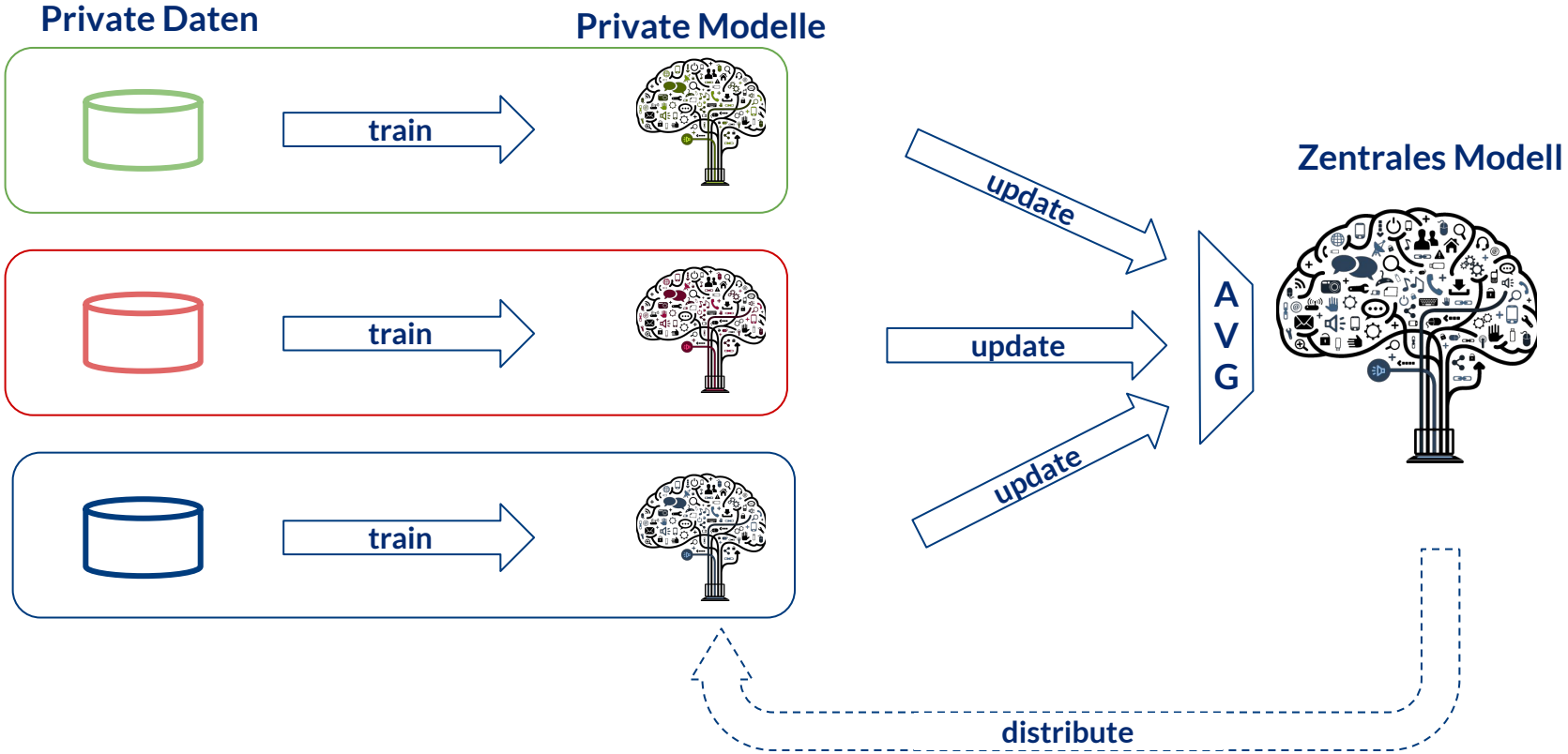
inovex

Beispiele für Private Daten

- MRT Bilder aus mehreren Krankenhäusern zur Tumorerkennung
- Sensordaten aus autonomen Autos zu Verbesserung der Gefahrenerkennung
- Tastatureingabe von Smartphones zum Trainieren einer Autovervollständigung



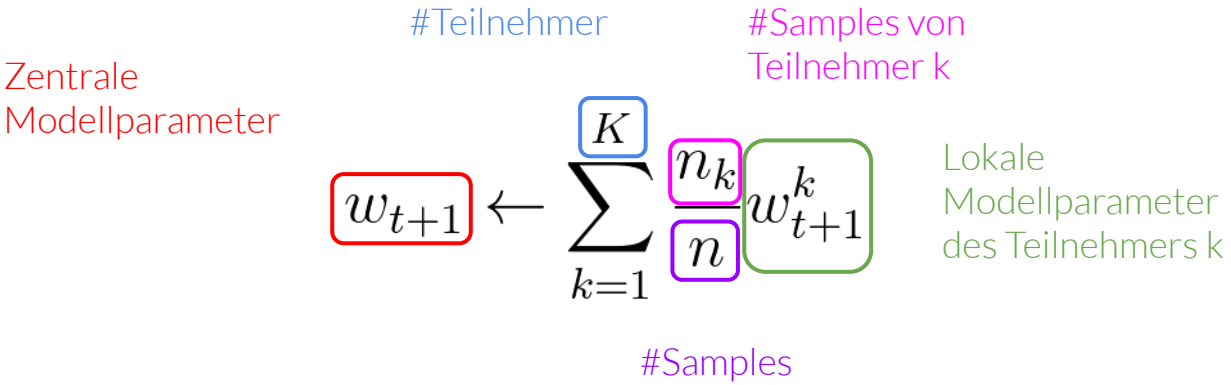
Federated Learning mit privaten Daten



inovex

Aggregierung in Federated Learning

Gewichteter Mittelwert über die Modellparameter:



Brendan McMahan, H., Moore, E., Ramage, D., Hampson, S., & Agüera y Arcas, B. (2017). Communication-efficient learning of deep networks from decentralized data

inovex

Privacy in Machine Learning

extrahieren

Trainingsdaten können aus dem Modell extrahiert werden:

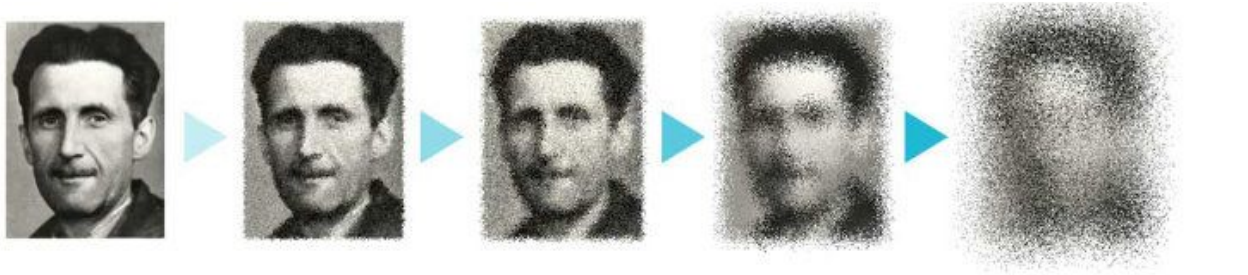
"Meine Kreditkartennummer ist **4567-4321-8932-0973** "

Sanitizer können nicht alle personenbezogenen Informationen entfernen.

Quelle: Carlini, N., Liu, C., Erlingsson, Ú., Kos, J., & Song, D. (2018). The Secret Sharer: Evaluating and Testing Unintended Memorization in Neural Networks.

Differential Privacy

- Differential Privacy verhindert, dass Trainingsdaten aus den Modellen generiert werden können
- Verrauscht Gradienten im lokalen Optimierungsprozess des SGD
- Beeinflusst durch das Rauschen die Qualität des Modells
- Begrenzt die Anzahl der Möglichen Trainingsepochen

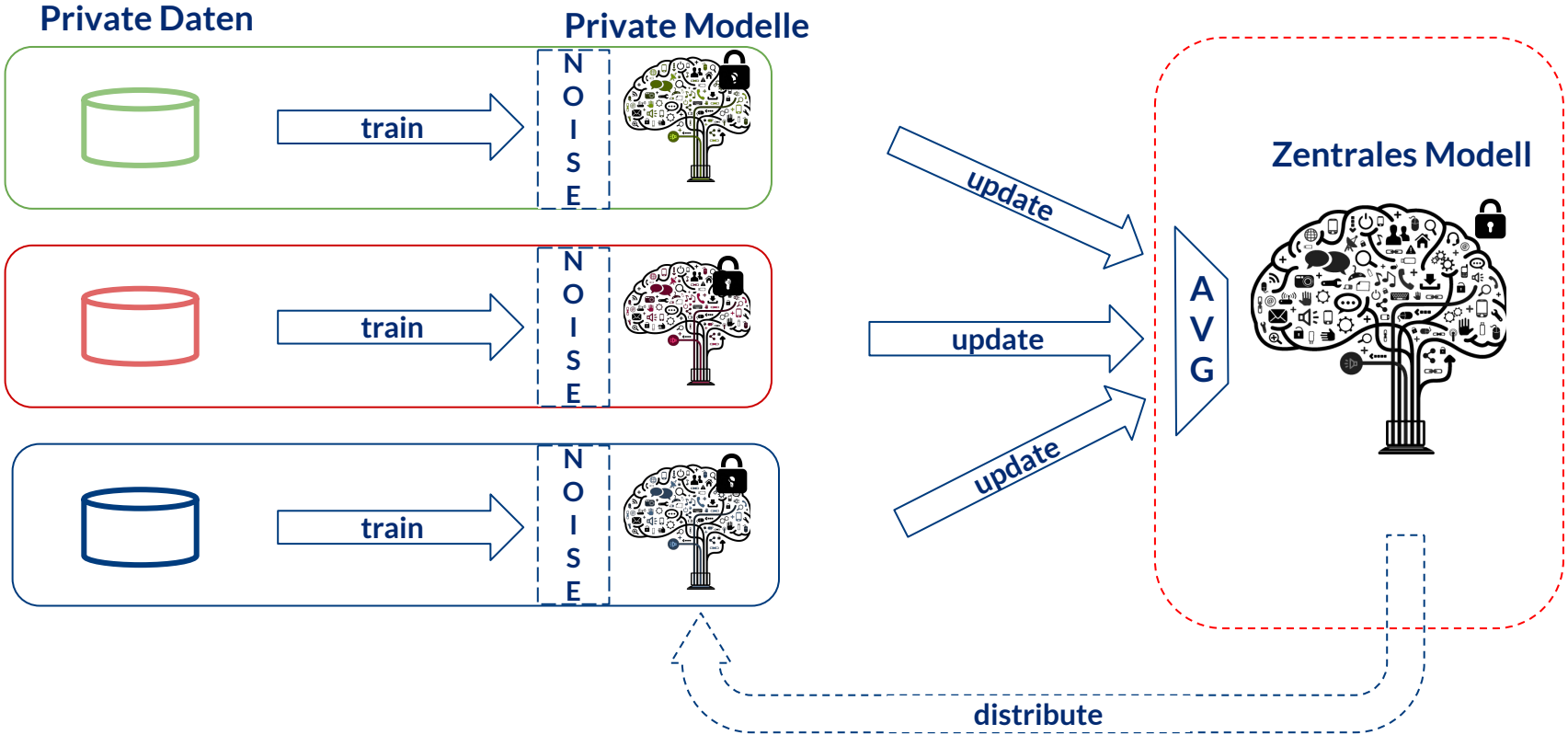


high utility
no privacy

high privacy
no utility

Quelle: https://aircloak.com/explaining-differential-privacy/

Differential Private - SGD



inovex

Secure Multi-Party Computation (SMPC)

- Ermöglicht das Rechnen mit verschlüsselten Zahlen!
- Beschränkt auf ganze Zahlen, Addition und Multiplikation

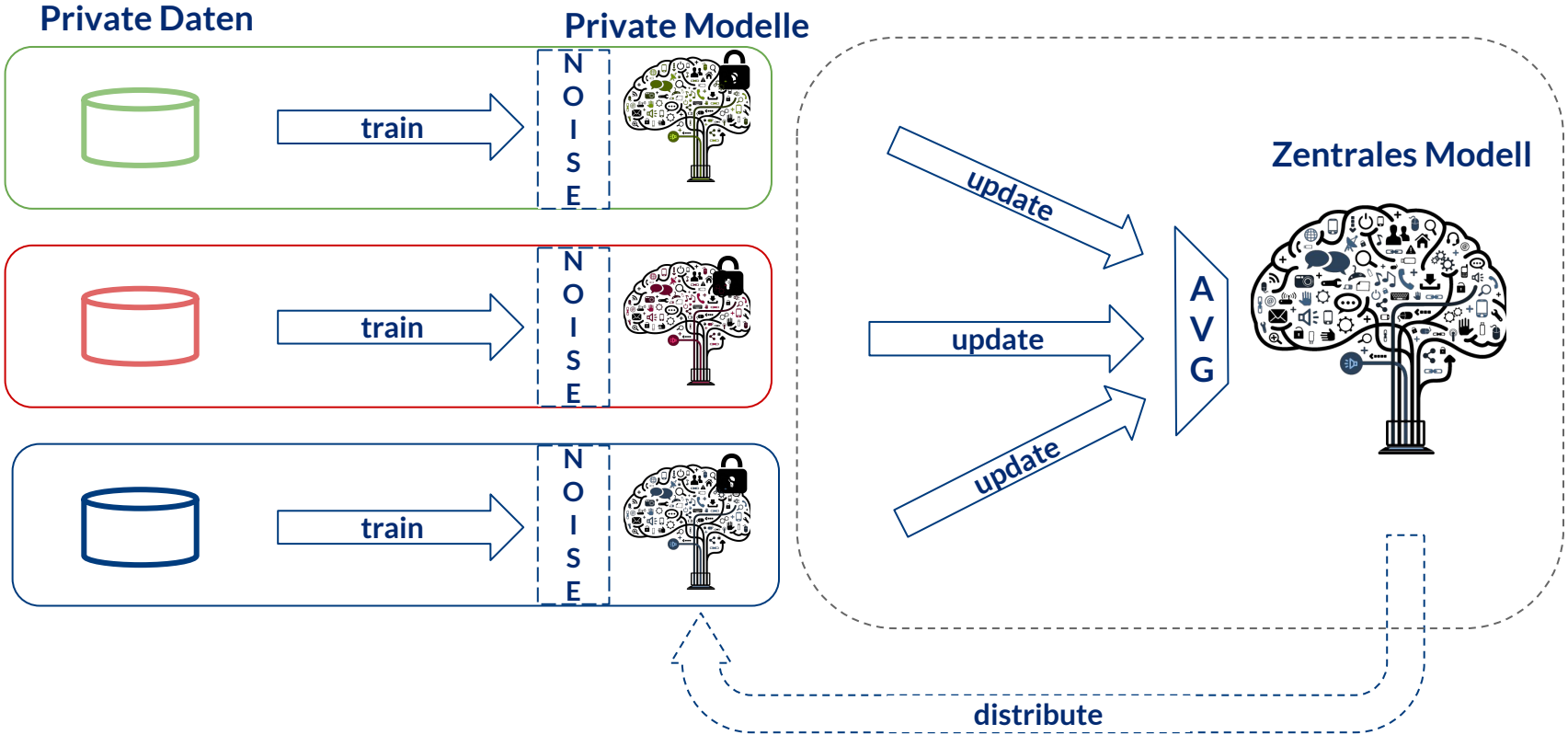
Lokal bei den Teilnehmer

Dezentral mit SMPC

$$w_{t+1} \leftarrow \sum_{k=1}^{K} \frac{n_k}{n} w_{t+1}^k \longrightarrow w_{t+1} \leftarrow \frac{1}{n} \sum_{k=1}^{K} n_k w_{t+1}^k$$

Lokal beim Teilnehmer k

Federated Learning mit SMPC



inovex

Evaluation

PySyft Framework

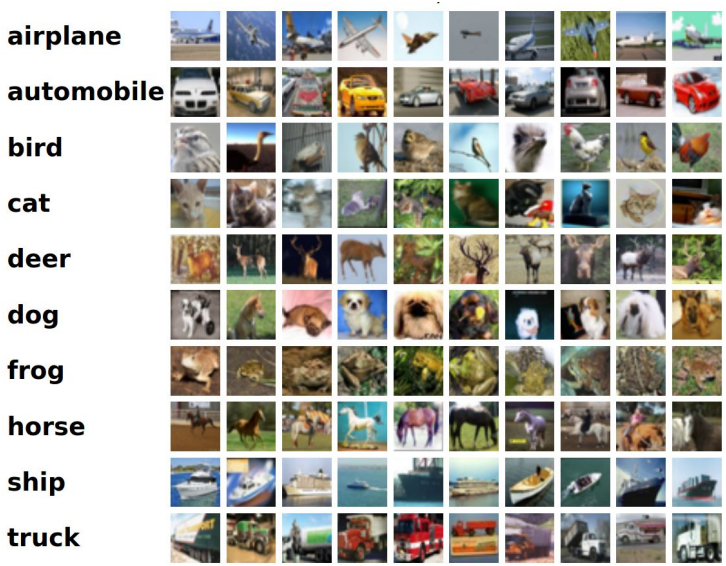
PySyft ermöglicht Federated Learning mit PyTorch:

- Worker sind passive Einheiten die private Daten vorhalten
- Trainingsprozess wird zentral gesteuert (mit hook auf PyTorch)
- Training nur auf der CPU nicht auf der GPU möglich
- Noch keine Verschlüsselung der Kommunikation
- Keine Differential Privacy implementierung

Datensätze

MNIST-10:

CIFAR-10:



inovex

Evaluationsaufbau

- Vergleich verschiedener Federated Learning Training Setups:

Parameter	**Optionen**
Worker type	virtual or docker
Number of workers	2 to N workers
Amount of samples	up to 50.000 samples
Klassenverteilung	Percent per worker
SMPC	Activate or Deactivate

Evaluations Metriken

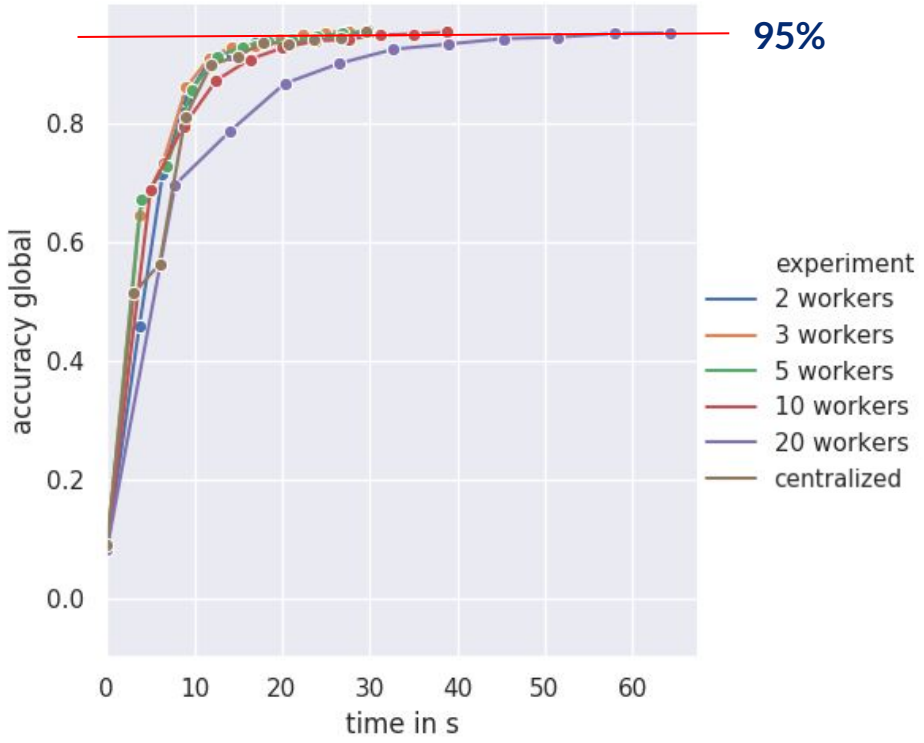
- Vergleichen von folgenden Metriken:
  - Accuracy des Zentralen Modells
  - Accuracy pro Klasse
  - Anzahl an gesendeten Nachrichten
  - Trainingszeit

Evaluations Experimente

- Zentralisiertes vs Federated Learning
- Ungleichmäßige Verteilung der Klassen auf die worker
- Unbalancierte Klassenverteilung

Zentralisiertes vs Federated Training

- 2 bis 20 worker
- 10k samples
- 10 epochs
- gleichmäßige Klassenverteilung



Anzahl der Worker beeinflusst Accuracy nicht

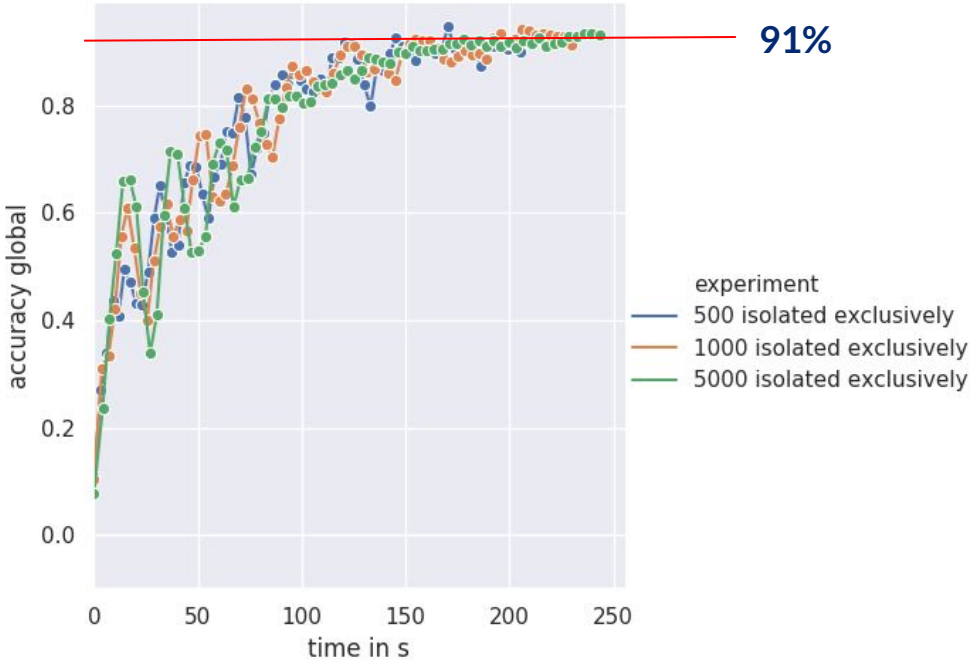
Je mehr worker je länger ist die Trainingszeit

inovex

Ungleichmäßige Klassenverteilung

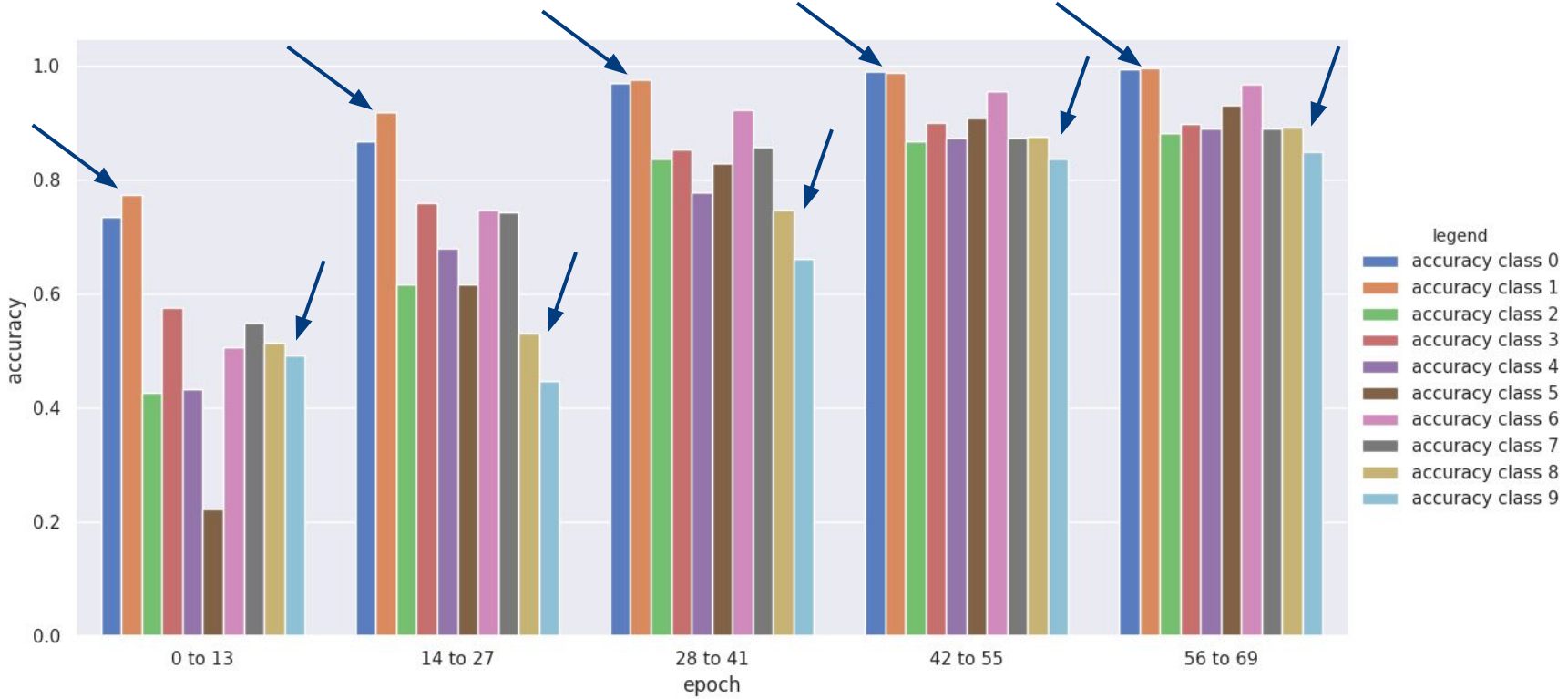
- 10 worker
- 500, 1.000 und 5.000 samples
- 70 epochs
- Jede Klasse isoliert auf einen worker

Training mit ungleichmäßiger Klassenverteilung ist möglich



inovex

Ungleichmäßige Klassenverteilung



inovex

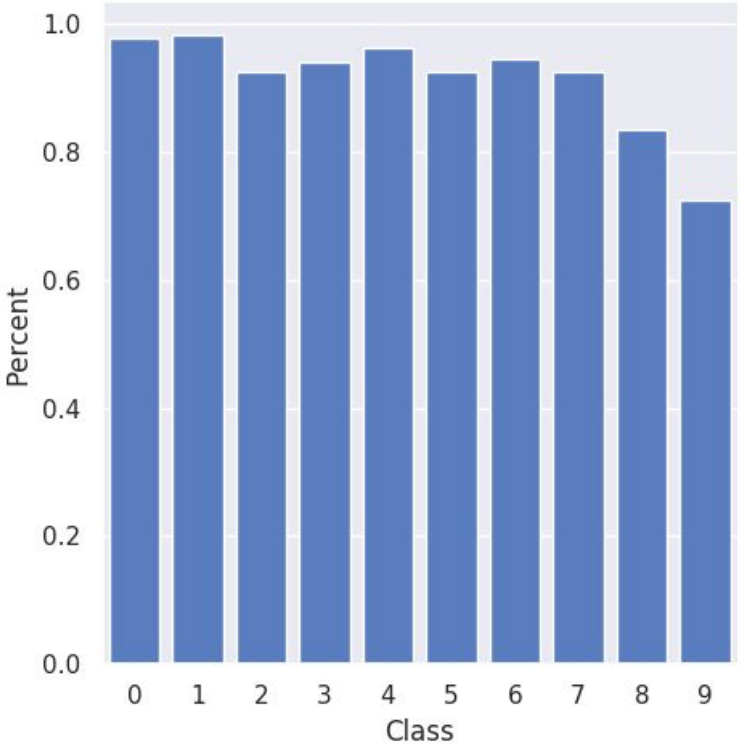
Unbalancierte Klassenverteilung

- Alle Klassen sind exklusive auf einem Worker verfügbar

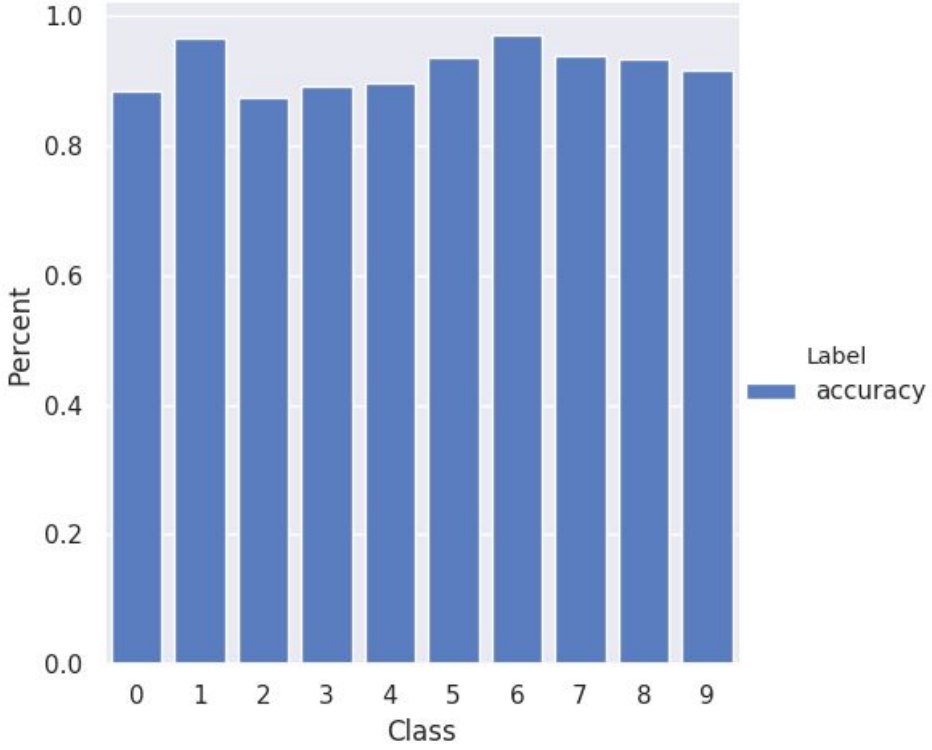
Klasse	0	1	2	3	4	5	6	7	8	9
decreasing ↓	500	450	400	350	300	250	200	150	100	50
increasing ↑	50	100	150	200	250	300	350	400	450	500

- 100 epochs
- Erreichen eine Accuracy von 91%

Unbalancierte Klassenverteilung



decreasing ↓



increasing ↑

inovex

Zusammenfassung

Federated Learning ermöglicht das:

- Trainieren mit privaten Daten durch Differential Privacy
- Verteiltes Lernen auf vielen Endgeräten
- Skalieren auf den Use Case

Ergebnisse aus meiner Evaluation:

- Federated Learning mit ungleichmäßiger Klassenverteilung ist möglich
- Verteilung der Klassen ist relevant für die Accuracy ist
- Für die Anwendbarkeit muss Differential Privacy als Technik leichter zugänglich werden

Vielen Dank

Christian Becker
working student
@ Team DMA

inovex GmbH
Ludwig-Erhard-Allee 6
76131 Karlsruhe

cbecker@inovex.de