Datentreuhand Kompetenz Netzwerk DaT Net


# TreuMed – Entwicklung und Erprobung von Datentreuhandmodellen am Beispiel der verteilten künstlichen Intelligenz in der Medizin

**Kategorien:**
**Workflows:** iterativer Loop
**Architekturen:** verteilte künstliche Intelligenz
**Tools:** Privacy Enhancing Technologies (PET), Feature Cloud

Dr. Lisa Eggerichs (wiss. MA, DaTNet, TU Dresden)

**Kurzbeschreibung des Projekts:** Wirtschaft und Forschung benötigen einen reibungslosen Datenaustausch, stehen jedoch im Spannungsfeld zur Datenhoheit der Datengebenden. TreuMed entwickelt und erprobt am Beispiel der „verteilten künstlichen Intelligenz" in der Medizin Datentreuhandmodelle und entsprechende Geschäftskonzepte und liefert eine technische Lösung für dieses Dilemma. Durch die Nutzung eines iterativen Loops in Kombination mit *Privacy Enhancing Technologies (PET)* wird dem Prinzip *privacy by design* Rechnung getragen und in der *Feature Cloud* umgesetzt (Bauer o.J.).

**Privacy by Design:** Artikel 25 der DSGVO betont, dass Privatsphäre im digitalen Zeitalter nur mit *Privacy by Design* möglich ist. Datenschutz muss daher von Beginn an in Technologien integriert werden – etwa durch *Privacy Enhancing Technologies (PET)* (Brauneck et al. 2023a).

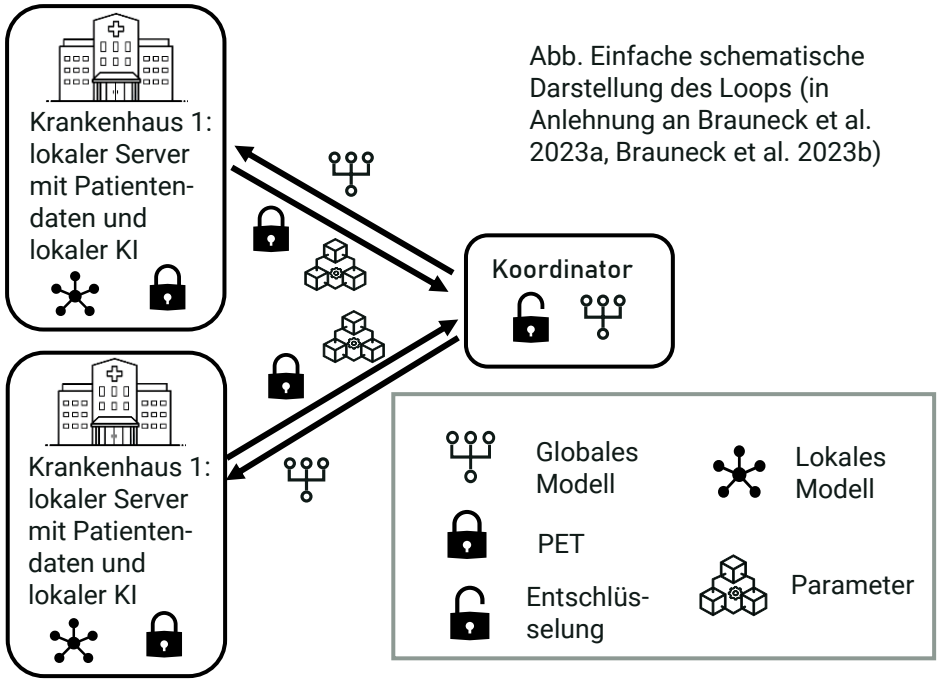


Abb. Einfache schematische Darstellung des Loops (in Anlehnung an Brauneck et al. 2023a, Brauneck et al. 2023b)

**Privacy Enhancing Technologies (PETs):**
- sichere Berechnungen mit mehreren Parteien verhindern Datenzugriff durch zentralen Koordinator
- Identifizierung von Datensubjekten im Training durch z. B. differenziellen Datenschutz verhindern
- Schutz des Modells durch homophorbic encryption

**4 Schritte im iterativen Loop**

**1. Training des lokalen Modells**
Jedes Krankenhaus (KH) trainiert ein lokales Modell mit lokalen Daten. Hier können PETs hinzugefügt werden (z.B. Differential Privacy (DP) oder sichere Mulit-Party-Berechnung).

**2. Sichere Übermittlung des lokalen Modells an den Koordinator**
Die KHs verschlüsseln das (nun trainierte) lokale Modell und senden es an den Koordinator oder einen Teilnehmer, der vorübergehend als Koordinator gewählt wurde.

**3. Zusammenführung lokaler Modelle zum globalen Modell**
Der Koordinator entschlüsselt die lokalen Modelle der KHs und fasst die Parameter der einzelnen lokalen Modelle zu einem globalen Modell zusammen.

**4. Rückgabe des Gesamtmodells**
Der Koordinator verschlüsselt das globale Modell und sendet es an jedes KH. Das globale Modell, das die Aktualisierungen aus der vorherigen Trainingsrunde enthält, wird zum „Basismodell" für die neue Trainingsrunde, wenn die Schleife zu Schritt 1 übergeht.
(Brauneck et al. 2023a)

Literatur

Bauer, C. n.d. *TreuMed. Entwicklung und Erprobung von Datentreuhandmodellen am Beispiel der verteilten künstlichen Intelligenz in der Medizin.*www.hsba.de/forschung/forschungsprojekte/treumed.

Brauneck, Alissa, Louisa Schmalhorst, Mohammad Mahdi Kazemi Majdabadi, Mohammad Bakhtiari, Uwe Völker, Jan Baumbach, Linda Baumbach, and Gabriele Buchholtz. 2023a. "Federated Machine Learning, Privacy-Enhancing Technologies, and Data Protection Laws in Medical Research: Scoping Review." *Journal of Medical Internet Research* 25: e41588. https://doi.org/10.2196/41588.

Brauneck, Alissa, Louisa Schmalhorst, Mohammad Mahdi Kazemi Majdabadi, Mohammad Bakhtiari, Uwe Völker, Christina Caroline Saak, Jan Baumbach, Linda Baumbach, and Gabriele Buchholtz. 2023b. "Federated Machine Learning in Data-Protection-Compliant Research." *Nature Machine Intelligence* 5: 2–4. https://doi.org/10.1038/s42256-022-00601-5.

Matschinske, J., J. Späth, M. Bakhtiari, N. Probul, M. M. Kazemi Majdabadi, R. Nasirigerdeh, R. Torkzadehmahani, et al. 2023. "The FeatureCloud Platform for Federated Learning in Biomedicine: Unified Approach." *Journal of Medical Internet Research* 25: e42621. https://doi.org/10.2196/42621.

Gefördert durch:
Bundesministerium für Forschung, Technologie und Raumfahrt
Finanziert von der Europäischen Union NextGenerationEU
TECHNISCHE UNIVERSITÄT DARMSTADT
TECHNISCHE UNIVERSITÄT DRESDEN
RWTH AACHEN UNIVERSITY
Universität Marburg