Föderiertes Lernen: ein Hilfsmittel zur datenschutzkonformen Forschung in der Biomedizin und darüber hinaus

Von *Jan Baumbach, Mohammad Mahdi Kazemi Majdabadi, Christina Caroline Saak, Mohammad Bakhtiari* und *Niklas Probul*

I. Einleitung

„Big Data" hat das Potenzial, eine neue Ära der Präzisionsmedizin einzuläuten,[1] und der rasche technologische Fortschritt hat zu einer Explosion der verfügbaren Datensätze geführt. So ist beispielsweise die Menge der im *Sequencing Read Archive* des *National Center for Biotechnology Information* (NCBI) verfügbaren DNA-Sequenzen in den letzten zehn Jahren exponentiell angestiegen.[2] Trotz dieser stetig wachsenden Datenmenge steht die Biomedizin vor einem Problem. Wie *Brauneck* und *Schmalhorst* in ihrem Beitrag in diesem Band beschreiben, sind vor allem Daten, die für Fortschritte in der Präzisionsmedizin nützlich sein könnten (genetische, biometrische und Gesundheitsdaten), nach Art. 9 Abs. 1 Datenschutz-Grundverordnung (DSGVO)[3] besonders schutzwürdig und dürfen nach Art. 9 Abs. 2 DSGVO nur in Ausnahmefällen verarbeitet werden.[4] In der Praxis bedeutet dies, dass Daten, die über mehrere Standorte verteilt sind, zum Beispiel über verschiedene Krankenhäuser, nicht zusammengeführt werden können, um mithilfe von künstlicher Intelligenz (KI) Modelle zu lernen. Dies wirkt sich wiederum negativ auf die Qualität der gelernten KI-Modellen aus, da zum Beispiel die volle Heterogenität von Krankheitsbildern nicht abgebildet werden kann. Ein Ausweg aus diesem Dilemma, der auf dem „Privacy-by-Design"-Prinzip aufbaut, ist das föderierte Lernen. Es ermöglicht,

[1] *Tim Hulsen/Saumya Jamuar/Alan Moody/Jason Karnes/Orsolya Varga/Stine Hedensted/Roberto Spreafico/David Hafler/Eoin McKinney*, From Big Data to Precision Medicine, Frontiers in Medicine, 2019, S. 1.

[2] *Kenneth Katz/Oleg Shutov/Richard Lapoint/Michael Kimelman/Rodney Brister/Christopher O'Sullivan,* The Sequence Read Archive: a decade more of explosive growth, Nucleic Acids Res. 2022, S. 387 (388).

[3] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

[4] *A. Brauneck/L. Schmalhorst*, in diesem Band, S. 241, 251 – 252.

DOI https://doi.org/10.3790/978-3-428-58889-3.2024.263 | Generated on 2025-12-11 08:28:45

KI-Modelle auf großen Datenmengen zu trainieren und dabei gleichzeitig die Privatsphäre dieser Daten zu schützen.[5]

Beim föderierten Lernen bleiben die Daten geschützt an ihrem Ursprungsort und werden nicht an einen zentralen Server (z. B. eine Cloud) übertragen. Stattdessen wird das KI-Modell lokal gelernt und nur die Parameter der gelernten Modelle werden mit anderen Teilnehmern des KI-Lernprozesses geteilt, sodass die Rohdaten selbst nie übermittelt werden müssen (Abb. 1 A).[6] Welche Parameter genau übertragen werden, hängt von der jeweils verwendeten KI-Methode ab (Abb. 1B).

Da beim föderierten Lernen keine sensiblen Daten über das Internet ausgetauscht werden müssen und somit das Risiko eines unbefugten Zugriffs auf diese Daten, zum Beispiel durch einen gezielten Cyberangriff, deutlich verringert wird, kann dieser Ansatz dazu beitragen, nicht nur die Anforderungen der DSGVO, sondern auch andere internationale Datenschutzbestimmungen wie die des *California Consumer Privacy Acts* (CCPA)[7] zu erfüllen, die jeweils strenge Kontrollen für die Erfassung, Speicherung und Nutzung personenbezogener Daten vorsehen. Durch die Kombination von Skalierbarkeit und Datenschutz wird das föderierte Lernen zu einer Schlüsseltechnologie für die Bewältigung der ständig wachsenden Datenmengen und der immer strengeren Datenschutzbestimmungen.

In diesem Kapitel wird zunächst ein Überblick über das föderierte Lernen gegeben, einschließlich der Anwendungsbereiche und der wichtigsten aktuellen Herausforderungen. Zudem werden Techniken zur weiteren Verbesserung des Datenschutzes erörtert und verschiedene Plattformen für das föderierte Lernen vorgestellt. Abschließend wird die Plattform FeatureCloud (featurecloud.ai), die vom gleichnamigen Horizon 2020-Konsortium entwickelt wurde, näher beleuchtet und konkrete Anwendungsfälle vorgestellt.

II. Föderiertes Lernen im Überblick

In einer föderierten Lernkonfiguration verfügen die verschiedenen, teilnehmenden Geräte, z. B. Smartphones oder Laptops, jeweils über ihre eigenen lokalen Daten, die sie für das Training eines maschinellen Lernmodells verwenden. Während des föderierten Lernprozesses werden Berechnungen lokal durchgeführt und die resultierenden Modellparameter werden an den Koordinator gesendet, der das Gesamt-

[5] *Alissa Brauneck/Louisa Schmalhorst/Mohammad Kazemi Majdabadi/Mohammad Bakhtiari/Uwe Völker/Christina Saak/Jan Baumbach/Linda Baumbach/Gabriele Buchholtz*, Federated machine learning in data-protection-compliant research, Nature Machine Intelligence, 5 (2023), S. 2.

[6] *Qiang Yang/Yang Liu/Tianjian Chen/Yongxin Tong*, Federated Machine Learning: Concept and Applications, ACM Transactions on Intelligent Systems and Technology, 10 (2019), S. 12 (12:3).

[7] California Consumer Privacy Act (CCPA), abrufbar unter https://oag.ca.gov/privacy/ccpa (zuletzt abgerufen am 2. 12. 2023).

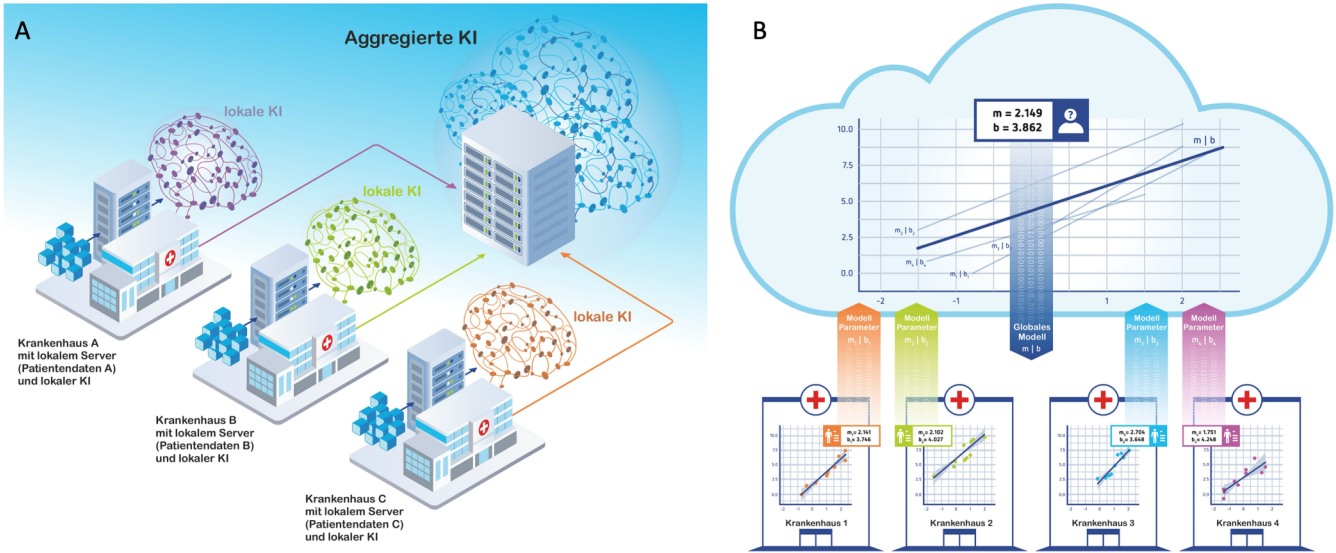

Abb. 1: Föderiertes Lernen im Überblick (© 2023 FeatureCloud).
(A) Beim föderierten Lernen werden KI-Modelle lokal gelernt und nur die Modell-Parameter werden in einem übergreifenden KI-Modell zusammengefasst.
(B) Die ausgetauschten Modell-Parameter hängen hierbei vom Modell ab.
In diesem Beispiel der linearen Regression werden Parameter *m* und *b* ausgetauscht.

modell erstellt. Bei iterativen Ansätzen des föderierten Lernens werden aktuelle Versionen eines Lernmodells an die teilnehmenden Geräte gesendet. Diese Modelle werden anhand der lokalen Daten analysiert und die von den Geräten an den Koordinator zurückgesendeten Modellaktualisierungen werden aggregiert. Für das Lernen der lokalen Modelle können verschiedene Algorithmen verwendet werden. Die Geräte senden dann die aktualisierten Modelle oder Modellparameter, an den zentralen Server zurück. Der zentrale Server aggregiert dann die Modellaktualisierungen aller teilnehmenden Geräte und aktualisiert das globale Modell. Dieser Prozess wird in der Regel mit einer Technik wie der föderierten Mittelwertbildung durchgeführt, bei der der Mittelwert aller von den Geräten empfangenen Modellaktualisierungen gebildet wird. Wie oben beschrieben, verbleiben die Rohdaten während dieses Lernprozesses auf den einzelnen Geräten und werden nicht übertragen oder mit anderen geteilt.

Eine effektive Kommunikation zwischen den teilnehmenden Geräten und dem zentralen Server ist entscheidend für den Erfolg eines föderierten Lernsystems. Dies beinhaltet in der Regel das Senden und Empfangen von Modellparametern zwischen den Geräten und dem Server, was auf sichere und effiziente Weise erfolgen muss. Nachdem das Modell mit immer mehr Daten von den Geräten trainiert wurde, sollte es zu einem globalen Modell konvergieren, das die Gesamtheit aller lokalen Daten repräsentiert. Die Geschwindigkeit dieser Konvergenz hängt von Faktoren wie der Größe des Modells, der Qualität der Daten und der Effizienz der Kommunikation zwischen den Geräten und dem Server ab.

Innerhalb des föderierten Lernens haben sich verschiedene Arten herausgebildet, um verschiedene Datenverteilungsszenarien anzugehen. Dazu gehören horizontales föderiertes Lernen, vertikales föderiertes Lernen und hybrides föderiertes Lernen.[8]

Horizontales föderiertes Lernen bezieht sich auf Szenarien, in denen die Teilnehmer über Datensätze mit denselben gemessenen Merkmalen, aber unterschiedlichen Stichproben verfügen. Die Daten werden horizontal zwischen den Teilnehmern aufgeteilt, und jeder Teilnehmer trainiert an seinen eigenen Daten, während ein gemeinsamer Satz von Attributen geteilt wird. Beispielsweise würden in einer Adipositasstudie für alle Probanden dieselben Ernährungs- und Bewegungsdaten erhoben und die Teilnehmer am Modell-Lernprozess würden jeweils die Daten für einen Teil der Studienteilnehmer erhalten. Diese Art des föderierten Lernens bewältigt Herausforderungen wie die Heterogenität der Daten und zielt darauf ab, trotz der Unterschiede in den Teilnehmerdaten eine genaue Modellleistung zu erzielen.

Vertikales föderiertes Lernen hingegen ist anwendbar, wenn die Teilnehmerdatensätze die gleichen Stichproben, aber unterschiedliche gemessene Merkmale enthalten. Die Daten werden auf der Grundlage der Merkmale vertikal partitioniert, und die Teilnehmer arbeiten zusammen, um Modelle zu trainieren, die ihre jeweiligen Merkmalsrepräsentationen berücksichtigen. Im Beispiel der Adipositasstudie würde ein

[8] *Hangyu Zhu/Haoyu Zhang/Yauchu Jin*, From federated learning to federated neural architecture search: a survey, Complex & Intelligent Systems, 7 (2021), S. 639 (640, 642, 643).

Teilnehmer des Modell-Lernprozesses Bewegungsdaten, ein anderer Ernährungsdaten derselben Studienteilnehmer erhalten. Dieser Ansatz ermöglicht die effiziente Nutzung verschiedener Datenquellen unter Wahrung des Datenschutzes und eignet sich für Szenarien, in denen Teilnehmer zwar über unterschiedliche Sätze von Merkmalen, aber überlappende Stichproben verfügen. Dies ist zum Beispiel der Fall, wenn Organisationen über verschiedene Daten von denselben Verbraucher*innen/ Kund*innen verfügen.

Hybrides föderiertes Lernen berücksichtigt Szenarien, in denen die Datensätze verschiedener Teilnehmer nicht nur unterschiedliche Stichproben, sondern auch unterschiedliche Merkmale enthalten. Für das Beispiel der Adipositas-Studie bedeutet dies, dass die Teilnehmer am Modell-Lernprozess eine weniger als 100 %-ige Überlappung von Teilnehmern und Datentypen haben. Diese Art des föderierten Lernens erfordert die gemeinsame Nutzung von Datenidentitätsinformationen, um die Schnittmenge der Datensätze für das gemeinsame Training zu finden. Die Herausforderung besteht darin, die Privatsphäre zu wahren und gleichzeitig eine effektive Zusammenarbeit zwischen Teilnehmern mit unterschiedlichen Datenmerkmalen zu erreichen.

Durch das Verständnis der Besonderheiten und Herausforderungen des horizontalen, vertikalen und hybriden föderierten Lernens können Forscher und Praktiker maßgeschneiderte Lösungen entwickeln, um die Leistungsfähigkeit des föderierten Lernens in verschiedenen Datenverteilungsszenarien zu nutzen und gleichzeitig den Datenschutz und die Modellleistung zu gewährleisten.

Darüber hinaus kann das föderierte Lernen in Bezug auf die Teilnehmer am Lernprozess der KI-Modelle in zwei Kategorien unterteilt werden: Föderiertes Lernen auf Edge-Geräten und Silo-übergreifendes föderiertes Lernen. Beim föderierten Lernen auf Edge-Geräten findet der Lernprozess der Modelle direkt auf den Geräten, wie zum Beispiel Smartphones, statt. Bei dieser Art des föderierten Lernens ist eine der größten Herausforderungen die Verwaltung einer sehr großen Anzahl von Geräten. Föderiertes Lernen auf Edge-Geräten wird hauptsächlich im Kontext von Verbraucheranwendungen eingesetzt, da es ein großes Potenzial für Skalierbarkeit bietet. Im Gegensatz dazu, ist beim Silo-übergreifenden föderierten Lernen die Teilnehmeranzahl wesentlich geringer, aber jeder Teilnehmer verfügt über einen großen Teil der Datensätze und über leistungsstarke Rechenressourcen. Bei dieser Art des föderierten Lernens besteht eine der größten Herausforderungen darin, die Vertraulichkeit einer großen Menge von Daten für die jeweiligen Teilnehmer des Lernprozesses zu wahren. Siloübergreifendes föderiertes Lernen wird hauptsächlich für die Zusammenarbeit zwischen Organisationen, wie z. B. medizinischen Einrichtungen, verwendet.

DOI https://doi.org/10.3790/978-3-428-58889-3.2024.263 | Generated on 2025-12-11 08:28:45

III. Anwendungsbereiche des föderierten Lernens

Föderiertes Lernen findet in vielen Bereichen der Wissenschaft und Wirtschaft Anwendung. Als häufige Anwendungsbereiche wurden mobile Anwendungen, Industrietechnik und das Gesundheitswesen identifiziert.[9] Auch in der biomedizinischen Forschung und im Finanzwesen findet das föderierte Lernen zunehmend Anwendung. Im Folgenden werden einige Anwendungsbereiche näher beleuchtet.

1. Mobile Anwendungen

Föderiertes Lernen wird zum Beispiel bei der automatischen Vorhersage von Tastatureingaben,[10] einschließlich der Vorhersage von Emojis,[11] eingesetzt.[12] Föderiertes Lernen spielt auch eine Rolle bei der Vorhersage menschlicher Bewegungen und Verhaltensweisen durch mobile Anwendungen, z. B. bei der Vorhersage der Nachfrage nach öffentlichen Verkehrsmitteln zu verschiedenen Tageszeiten.[13] In einem weiteren Beispiel wird föderiertes Lernen mit *Deep Reinforcement Learning* kombiniert, das sogenannte „*In-Edge AI*“,[14] das zum Beispiel für das Training von KI-Modellen für Computerspiele oder auch für die Optimierung der Ressourcennutzung eingesetzt werden kann. Die Einsparung von Ressourcen wird durch das föderierte Lernen ermöglicht, da unter anderem der Bedarf an umfangreichen Datenübertragungen deutlich reduziert wird und die Verarbeitungslast auf mehrere Geräte verteilt wird. Die dezentrale Natur des föderierten Lernens erleichtert auch die Kommunikation, da

[9] *Roseline Ogundokun/Sanjay Misra/Rytis Maskeliunas/Robertas Damasevicius*, A Review on Federated Learning and Machine Learning Approaches: Categorization, Application Areas, and Blockchain Technology, Information, 13 (2022), S. 1 (15 – 17).

[10] *Qinbin Li/Zeyi Wen/Zhaomin Wu/Sixu Hu/Naibo Wang/Yuan Li/Xu Liu/Bingsheng He,* A survey on federated learning systems: Vision, hype and reality for data privacy and protection, arXiv, 2021, S. 1 (10); *Mingqing Chen/Rajiv Mathews/Tom Ouyang/Françoise Beaufays,* Federated Learning Of Out-Of-Vocabulary Words, arXiv, 2019, S. 1; *Andrew Hard/Kanishka Rao/Rajiv Mathews/Swaroop Ramaswamy/Françoise Beaufays/Sean Augenstein/Hubert Eichner/Chloé Kiddon/Daniel Ramage,* Federated Learning for Mobile Keyboard Prediction, arXiv, 2019, S. 1.

[11] *Swaroop Ramaswamy/Rajiv Mathews/Kanishka Rao/Françoise Beaufays*, Federated Learning for Emoji Prediction in a Mobile Keyboard, arXiv, 2019, S. 1.

[12] *Ogundokun/Misra/Maskeliunas/Damasevicius* (Fn. 9), S. 4.

[13] *Jie Feng/Can Rong/Funing Sun/Diansheng Guo/Yong Li*, PMF: A Privacy-preserving Human Mobility Prediction Framework via Federated Learning, Proceedings of the ACM on In teractive Mobile Wearable and Ubiquitous Technologies, 4 (2020), S. 10 (10:2)*; Konstantin Sozinov/Vladimir Vlassov/Sarunas Girdzijauskas*, Human Activity Recognition Using Federated Learning. 2018 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications (ISPA/IUCC/BDCloud/SocialCom/SustainCom)*,* 2018, S. 1103.

[14] *Xiaofei Wang/Yiwen Han/Chenyang Wang/Qiyang Zhao/Xu Chen/Min Chen*, In-Edge AI: Intelligentizing Mobile Edge Computing, Caching and Communication by Federated Learning. IEEE Network *,* 33 (2019), S. 156 (159).

die Abhängigkeit von einer ständigen Verbindung zu zentralen Servern minimiert wird.

2. Industrietechnik

Föderiertes Lernen wird zunehmend auch in der Industrie eingesetzt.[15] Zum Beispiel haben Forscher auf föderiertem Lernen basierende Methoden zur Energieprognose entwickelt, um Überlastungsprobleme an Ladestationen für Elektrofahrzeuge zu lösen, indem Energie für Spitzenzeiten im Voraus gespeichert und nicht erst bei akutem Bedarf abgerufen wird.[16]

3. Gesundheitswesen und biomedizinische Forschung

In der biomedizinischen Forschung und im Gesundheitswesen spielt föderiertes Lernen eine besondere Rolle, da Gesundheitsdaten nach Art. 9 Abs. 1 DSGVO besonders schutzwürdig sind. Hier findet föderiertes Lernen Anwendung bei der Auswertung von elektronischen Gesundheitsakten,[17] bei der Interpretation von MRT-Bildgebungsdaten[18] und bei der Klassifikation von EEG-Daten[19].[20]

Auch in der biomedizinischen Forschung spielt föderiertes Lernen eine besondere Rolle. Denn es ermöglicht, personenbezogene Daten, wie beispielsweise Genetikdaten, welche per se personenbezogen sind, unter Wahrung der Privatsphäre zu analy-

---

[15] *Ogundokun/Misra/Maskeliunas/Damasevicius* (Fn. 9), S. 4.

[16] Yuris *Saputra/Dinh Hoang/Diep Nguyen/Eryk Dutkiewicz/Markus Mueck/Srikathyayani Srikanteswara*, Energy Demand Prediction with Federated Learning for Electric Vehicle Net works, 2019 IEEE Global Communications Conference (GLOBECOM), 2019, S. 1.

[17] Li *Huang/Yifeng Yin/Zeng Fu/Shifa Zhang/Hao Deng/Dianbo Liu*, LoAdaBoost: Loss-based AdaBoost federated machine learning with reduced computational complexity on IID and non-IID intensive care data, PLoS One, 15 (2020), S. 1 (14); *Theodora Brisimi/Ruidi Chen/Theofani Mela/Alex Olshevsky/Ioannis Paschalidis/Wei Shi*, Federated learning of predictive models from federated Electronic Health Records, International Journal of Medical In formation, 112 (2018), S. 59 (59 – 60); *Junghye Lee/Jimeng Sun/Fei Wang/Shuang Wang/Chi-Hyuck Jun/Xiaoqian Jiang*, Privacy-Preserving Patient Similarity Learning in a Federated Environment: Development and Analysis, JMIR Med Inform, 6 (2018), S. 1 (2); *Dianbo Liu/Dmitriy Dligach/Timothy Miller*, Two-stage Federated Phenotyping and Patient Representation Learning, *Proc Conf Assoc Comput Linguist Meet* 2019, S. 283.

[18] *Santiago Silva/Boris Gutman/Eduardo Romero/Paul Thompson/Andre Altmann/Marco Lorenzi*, Federated Learning in Distributed Medical Databases: Meta-Analysis of Large-Scale Subcortical Brain Data, 2019 IEEE 16th International Symposium on Biomedical Imaging, 2019, S. 270.

[19] *Dashan Gao/Ce Ju/Xiguang Wei/Yang Liu/Tianjian Chen/Qiang Yang*, HHHFL: Hierarchical Heterogeneous Horizontal Federated Learning for Electroencephalography, arXiv, 2020, S. 1.

[20] *Ogundokun/Misra/Maskeliunas/Damasevicius* (Fn. 9), S. 4.

sieren und präzise KI-Modelle zu entwickeln. *Flimma*[21] ist zum Beispiel ein Werkzeug für die differenzielle Genexpressionsanalyse. Durch die Integration föderierter Techniken und die Gewährleistung des Datenschutzes ermöglicht es *Flimma* den Forschern, wertvolle Einblicke in Genexpressionsmuster zu gewinnen und gleichzeitig die Vertraulichkeit sensibler genomischer Daten zu wahren. Ein weiteres Beispiel für die Anwendung von föderiertem Lernen in der Biomedizin ist *sPLINK*.[22] *sPLINK* ist ein hybrides, föderiertes computergestütztes Werkzeug, das datenschutzgerechte genomweite Assoziationsstudien (GWAS) zur Identifizierung von krankheitsassoziierten Genomvarianten in verteilten Datensätzen ermöglicht und genaue Ergebnisse gewährleistet. Mit seiner benutzerfreundlichen Oberfläche ermöglicht *sPLINK* Forschern die Durchführung von GWAS unter Wahrung des Datenschutzes und der Integrität der Analyse. *Partea*,[23] ein drittes Beispiel für föderiertes Lernen in der Biomedizin, bietet eine kollaborative Lösung für *Time-to-Event*-Studien zur statistischen Analyse der Zeit bis zum Eintreten eines vorherbestimmten Ereignisses, die es ermöglicht, mit anderen Institutionen zusammenzuarbeiten, ohne Daten zu zentralisieren. Benutzerfreundliche Funktionen ermöglichen es, Projekte zu erstellen, andere Teilnehmer einzuladen und große Datenmengen zu nutzen, ohne den Datenschutz zu gefährden. Die föderierte Implementierung modernster Algorithmen für die Analyse der Zeit bis zum Ereignis ermöglicht sichere und effiziente gemeinsame Studien, während die Daten für maximale Vertraulichkeit lokal gespeichert bleiben.

4. Finanzwesen

Im Finanzwesen spielt föderiertes Lernen zum Beispiel bei der Bewertung der Kreditwürdigkeit eine wichtige Rolle. In diesem Fall können Finanzinstitute und E-Commerce-Unternehmen mit Hilfe von föderiertem Lernen zusammenarbeiten, um KI-Modelle zur Risikobewertung auf der Grundlage einer größeren Anzahl von Faktoren zu erstellen.[24]

---

[21] *Olga Zolotareva/Reza Nasirigerdeh/Julian Matschinske/Reihaneh Torkzadehmahani/Mohammad Bakhtiari/Tobias Frisch/Julian Späth/David Blumenthal/Amir Abbasinejad/Paolo Tieri/Georgios Kaissis/Daniel Rückert/Nina Wenke/Markus List/Jan Baumbach*, Flimma: a federated and privacy-aware tool for differential gene expression analysis, Genome Biology, 22 (2021), S. 1.

[22] *Reza Nasirigerdeh/Reihaneh Torkzadehmahani/Julian Matschinske/Tobias Frisch/Markus List/Julian Späth/Stefan Weiss/Uwe Völker/Esa Pitkänen/Dominik Heider/Nina Wenke/Georgios Kaissis/Daniel Rueckert/Tim Kacprowski/Jan Baumbach*, sPLINK: a hybrid federated tool as a robust alternative to meta-analysis in genome-wide association studies, Genome Biology, 23 (2022), S. 1.

[23] *Julian Späth/Julian Matschinske/Frederick Kamanu/Sabina Murphy/Olga Zolotareva/Mohammad Bakhtiari/Eliott Atman/Joseph Loscalzo/Alissa Brauneck/Louisa Schmalhorst/Gabriele Buchholtz/Jan Baumbach,* Privacy-aware multi-institutional time-to-event studies, PLOS Digital Health, 1 (2022), S. 1.

[24] *Priyanka Mammen*, Federated Learning: Opportunities and Challenges, arXiv, 2021, S. 1 (3).

IV. Herausforderungen des föderierten Lernens

Föderiertes Lernen bringt eine Reihe von Herausforderungen mit sich. Im Folgenden werden zunächst diese Herausforderungen untersucht und anschließend mögliche Lösungsansätze diskutiert, die den Weg für eine breite Akzeptanz ebnen können.

Die Herausforderungen lassen sich in folgende Kategorien einteilen:

1. Heterogenität der Geräte und Daten

Die Teilnehmer an einem föderierten Lernprozess können über verschiedene Geräte mit unterschiedlichen Hardwarekonfigurationen und Betriebssystemen verfügen. Es ist von entscheidender Bedeutung, Systeme für föderiertes Lernen zu entwickeln, die auf dieser Vielzahl von Geräten effektiv funktionieren. Darüber hinaus sind die Daten oft heterogen unter den Teilnehmern verteilt. Dieses Szenario wird auch als nicht-IID (*independent and identically distributed*) Datenverteilung bezeichnet und stellt eine große Herausforderung für das föderierte Lernen dar.[25]

Eine mögliche Lösung für dieses Problems ist, die Anzahl der lokalen Trainingsepisoden zwischen den zentralen Aggregationsschritten zu begrenzen. Dieser Ansatz verlangsamt jedoch die Konvergenzgeschwindigkeit des föderierten Lernsystems erheblich und erfordert viele Kommunikationsrunden, um eine zufriedenstellende Leistung zu erreichen. Die längere Konvergenzzeit und der erhebliche Kommunikationsaufwand, die mit diesem Ansatz verbunden sind, sind für reale verteilte Systeme oft nicht praktikabel.

Eine weitere Lösung zur Bewältigung der Datenheterogenität beim föderierten Lernen besteht darin, Datenaugmentation zu nutzen.[26] Hierbei werden anhand eines bestehenden Datensatzes neue Daten generiert.

---

[25] *Qinbin Li/Yiqun Diao/Quan Chen/Bingsheng He*, Federated Learning on Non-IID Data Silos: An Experimental Study, arXiv, 2021, S. 1.

[26] *Artur de Luca/Guojun Zhang/Xi Chen/Yaoliang Yu*, Mitigating Data Heterogeneity in Federated Learning with Data Augmentation, arXiv, S. 2 (4); *Peter Kairouz/Brendan McMahan/Brendan Avent/Aurélien Bellet/Mehdi Bennis/Arjun Nitin Bhagoji/Kallista Bonawitz/Zachary Charles/Graham Cormode/Rachel Cummings/Rafael D'Oliveira/Hubert Eichner/Salim El Rouayheb/David Evans/Josh Gardner/Zachary Garrett/Adrià Gascón/Badih Ghazi/Phillip Gibbons/Marco Gruteser/Zaid Harchaoui/Chaoyang He/Lie He/Zhouyuan Huo/Ben Hutchinson/Justin Hsu/Martin Jaggi/Tara Javidi/Gauri Joshi/Mikhail Khodak/Jakub Konečný/Aleksandra Korolova/Farinaz Koushanfar/Sanmi Koyejo/Tancrède Lepoint/Yang Liu/Prateek Mittal/Mehryar Mohri/Richard Nock/Ayfer Özgür/Rasmus Pagh/Mariana Raykova/Hang Qi/Daniel Ramage/Ramesh Raskar/Dawn Song/Weikang Song/Sebastian Stich/Ziteng Sun/Ananda Theertha Suresh/Florian Tramèr/Praneeth Vepakomma/Jianyu Wang/Li Xiong/Zheng Xu/Qiang Yang/Felix Yu/Han Yu/Sen Zhao*, Advances and Open Problems in Federated Learning, Foundations and Trends in Machine Learning, 14 (2021), S. 1 (20).

2. Modellsynchronisation

Da das Training auf den lokalen Geräten stattfindet, müssen die Modellupdates effizient synchronisiert werden, um ein kohärentes Modell aufzubauen. Die Herausforderung besteht darin, Mechanismen zu entwickeln, die die Modellaktualisierungen effizient zusammenführen, insbesondere bei variablen Netzwerkbedingungen und unterschiedlichen Trainingszeiten. Um diese Herausforderung zu bewältigen können zum Beispiel Strategien zur Modellkomprimierung angewendet werden, wie zum Beispiel die Verringerung der Genauigkeit der Modellgewichte oder das sogenannte *Pruning*, bei dem weniger wichtige Modellgewichte eliminiert werden. Diese Techniken verringern die Gesamtgröße eines Modells, ohne die Vorhersagekraft übermäßig zu beeinträchtigen.[27]

3. Skalierbarkeit

Das föderierte Lernen sollte auf große verteilte Systeme angewendet werden können, etwa um eine höhere Rechenleistung und einen besseren Schutz der Privatsphäre zu gewährleisten. Je mehr Geräte am Netz teilnehmen, desto größer werden die kollektiven Rechenressourcen, was eine robustere und vielfältigere Datenverarbeitung ohne Beeinträchtigung des Datenschutzes ermöglicht.

Allerdings ist Skalierbarkeit nicht nur eine wichtige Eigenschaft des föderierten Lernens, sondern auch eine ernstzunehmende Herausforderung in der Sicherstellung, dass das Training auch mit einer großen Anzahl von Teilnehmern und umfangreichen Datensätzen effektiv funktioniert. Die Herausforderung liegt hier vor allem in der Aggregation von Parametern aus einer großen Anzahl von teilnehmenden Geräten. Mit zunehmender Größe des Netzes steigt die Komplexität der Aggregation, was häufig zu netzbedingten Verzögerungen führt. Um diese Probleme zu lösen, müssen effiziente Mechanismen implementiert werden, die den erhöhten Netzwerkverkehr bewältigen und eine rechtzeitige und effektive Aggregation von Parametern gewährleisten können. Diese Mechanismen sind entscheidend für die Aufrechterhaltung der Leistung und Zuverlässigkeit des föderierten Lernsystems, auch wenn es skaliert.

4. Kommunikationseffizienz

Da die Daten auf verschiedene Geräte verteilt sind, ist die Kommunikation zwischen den Geräten ein wichtiger Aspekt des föderierten Lernens. Effiziente Kommunikationsprotokolle und -mechanismen müssen entwickelt werden, um den Austausch von Modellparametern und Aggregationsergebnissen zu optimieren. Zur Steigerung der Kommunikationseffizienz können Datenkompressionstechniken einge-

[27] *Tingting Wu/Chunhe Song/Peng Zeng*, Efficient federated learning on resource-constrained edge devices based on model pruning, Complex & Intelligent Systems, 2023, 9, S. 6999.

setzt werden, um die zu übertragende Datenmenge zu reduzieren.[28] Eine weitere Lösungsmöglichkeit besteht in der Priorisierung der Übertragung von Parametern an den zentralen Server. Bei diesem Ansatz werden die Rechenressourcen zunächst auf die für das Modell einflussreichsten Parameter konzentriert, um einen effizienteren und schnelleren Umwandlungsprozess zu gewährleisten.[29]

5. Datenschutz und Sicherheit

Da beim föderierten Lernen verschiedene Teilnehmer mit unterschiedlichen Interessen und Absichten zusammenkommen, besteht eine weitere Herausforderung darin, Mechanismen zu entwickeln, um Manipulationsversuche oder Angriffe auf das Modell oder die Daten zu erkennen und zu verhindern. Darüber hinaus müssen die Daten vor Angriffen von außen geschützt werden. In den folgenden Abschnitten werden sowohl die potenziellen Datenschutzrisiken des föderierten Lernens als auch mögliche Abwehrmechanismen näher beleuchtet.

Insgesamt erfordern diese Herausforderungen kontinuierliche Forschung und Entwicklung, um die Wirksamkeit und Praktikabilität des föderierten Lernens in verschiedenen Anwendungsbereichen zu verbessern.

V. Potenzielle datenschutzrechtliche Gefahren beim föderierten Lernen

Eine Datenschutzverletzung ist die versehentliche oder absichtliche Freigabe sensibler Informationen über Personen oder Organisationen als Ergebnis von Datenverarbeitungsaktivitäten, wie z. B. maschinellem Lernen. Im Kontext des föderierten Lernens können Datenschutzverletzungen durch verschiedene Angriffe ausgelöst werden (Abb. 2).

Bei Model-Inversion-Angriffen (engl. *‚model inversion attack‘*)[30] verwendet ein Angreifer ein maschinelles Lernmodell, um die Daten, mit denen es trainiert wurde, wiederzugewinnen und so sensible Informationen zu erlangen, die im Training des Lernmodells verwendet wurden. Beim föderierten Lernen kann diese Art von Angriff erfolgen, wenn der Angreifer Zugriff auf das globale Modell hat oder die von den

[28] *Jakub Konečný/Brendan McMahan/Felix Yu/Peter Richtárik/Ananda Suresh/Dave Bacon*, Federated Learning: Strategies for Improving Communication Efficiency, arXiv, 2017, S. 1 (2).

[29] *Kevin Hsieh/Aaron Harlap/Nandita Vijaykumar/Dimitris Konomis/Gregory Ganger/Philip Gibbons*, Gaia: Geo-distributed machine learning approaching LAN speeds, Proceedings of the 14th USENIX Symposium on Networked Systems Design and Implementation, 2017, S. 629 (640); *Luping Wang/Wei Wang/Bo Li*, CMFL: Mitigating Communication Overhead for Federated Learning, 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), 2019, S. 954 (956).

[30] *Matt Fredrikson/Somesh Jha/Thomas Ristenpart*, Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures, Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security 2019, S. 1322.

teilnehmenden Geräten an den zentralen Server gesendeten Aktualisierungen nicht ausreichend geschützt sind.

Bei einem Modelldiebstahl (engl. ‚*model stealing attack*') kopiert ein Angreifer ein maschinelles Lernmodell und verwendet es für seine eigenen Zwecke, wodurch die Vertraulichkeit und Sicherheit der zum Trainieren des Modells verwendeten Daten beeinträchtigt werden kann.[31] Beim föderierten Lernen kann diese Art von Angriff erfolgen, wenn der Angreifer Zugriff auf den zentralen Server hat und in der Lage ist, das globale Modell einzusehen.

Darüber hinaus stellen Seitenkanalangriffe (engl. ‚*side channel attacks*') eine weitere Bedrohung für die Privatsphäre dar.[32] Ein Seitenkanalangriff ist ein Angriff, bei dem Informationen über ein System genutzt werden, die nicht Teil der normalen Kommunikations- oder Berechnungskanäle sein sollten. Beim föderierten Lernen können Seitenkanalangriffe auftreten, wenn der Angreifer in der Lage ist, Informationen über die Trainingsdaten oder die Modellaktualisierungen zu erhalten, die zwischen den teilnehmenden Geräten und dem zentralen Server übertragen werden.

Eine weitere Bedrohung für die Privatsphäre sind *Data-Poisoning*-Angriffe, bei denen ein Angreifer absichtlich falsche oder bösartige Daten in den Trainingssatz einspeist, um die Qualität und Genauigkeit des Modells zu beeinträchtigen.[33] Beim föderierten Lernen kann diese Art von Angriffen erfolgen, wenn der Angreifer in der Lage ist, die lokalen Daten auf einem oder mehreren teilnehmenden Geräten zu verändern oder sich als Teilnehmer einzuschleusen.

Dies sind nur einige Beispiele für die Arten von Angriffen, die beim föderierten Lernen auftreten können. Es ist wichtig, sich dieser und anderer potenzieller Risiken für die Privatsphäre bewusst zu sein und geeignete Gegenmaßnahmen und Sicherheitsvorkehrungen zu treffen, um sich vor dem Verlust der Privatsphäre in föderierten Lernumgebungen zu schützen. Einige dieser Maßnahmen werden im folgenden Abschnitt beschrieben.

[31] *Sanjay Kariyappa/Atul Prakash/Moinuddin Qureshi*, MAZE: Data-free model stealing at tack using zeroth-order gradient estimation, 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) 2021, S. 13809 (13814).

[32] *François-Xavier Standaert*, Introduction to Side-Channel Attacks, in: Verbauwhede, Secure Integrated Circuits and Systems, 2021, S. 27 (28).

[33] *Vale Tolpegin/Stacey Truex/Mehmet Gursoy/Ling Liu*, Data Poisoning Attacks Against Federated Learning Systems, Computer Security – ESORICS, 2020, S. 480 (483).

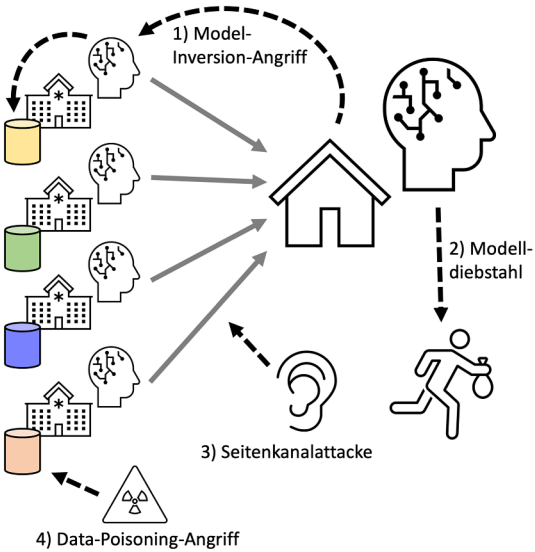

Abb. 2: Potenzielle Angriffe auf Infrastrukturen des föderierten Lernens.

VI. Techniken zur Verbesserung der Privatsphäre

Es gibt verschiedene Datenschutztechniken, die beim föderierten Lernen eingesetzt werden können, um die Privatsphäre der für das Modelltraining verwendeten Daten zu schützen.[34] Einige der gängigsten Techniken werden im Folgenden beschrieben:

1. Differential Privacy

Differential Privacy ist ein mathematisches Modell für den Schutz der Privatsphäre einzelner Datensätze, wobei die Daten dennoch für statistische Analysen verwendet werden können.[35] Diese Technik beruht auf dem Einspeisen von statistischem Rauschen, um die Identifizierung einzelner Dateneinträge unmöglich zu machen. Beim föderierten Lernen kann *Differential Privacy* verwendet werden, um den Modellaktualisierungen, die von den Client-Geräten an den zentralen Server gesendet werden, statistisches Rauschen hinzuzufügen, um die Beziehung zwischen den Daten und dem Modell zu verschleiern. *Differential Privacy* wurde zum Beispiel

[34] *Reihaneh Torkzadehmahani/Reza Nasirigerdeh/David Blumenthal/Tim Kacprowski/Markus List/Julian Matschinske/Julian Spaeth/Nina Wenke/Jan Baumbach,* Privacy-Preserving Artificial Intelligence Techniques in Biomedicine, Methods of Information in Medicine, 2022, S. e12 (e16).

[35] *Cynthia Dwork*, Differential Privacy, Automata, Languages and Programming, 2006, S. 1.

DOI https://doi.org/10.3790/978-3-428-58889-3.2024.263 | Generated on 2025-12-11 08:28:45

in einer Studie mit Daten von funktionellen Magnetresonanztomographien mehrerer klinischer Standorte verwendet.[36]

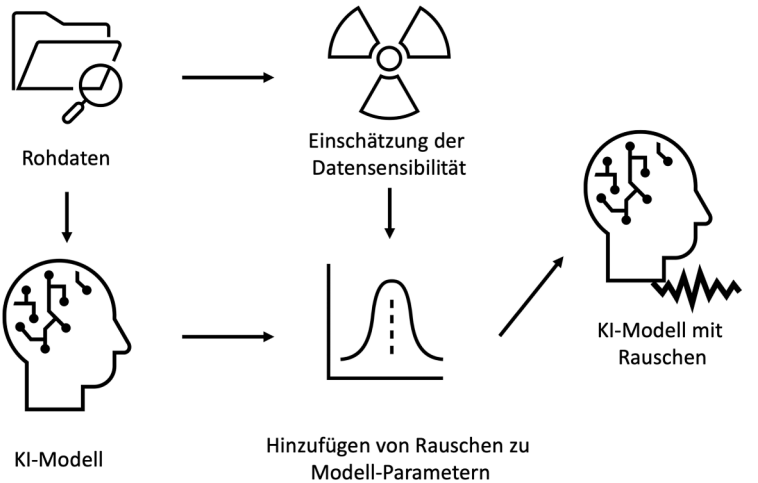

Abb. 3: Prinzip der Differential Privacy.

2. Secure Multiparty Computation (SMPC)

SMPC ist eine Technik, die es mehreren Parteien ermöglicht, gemeinsam eine Funktion mithilfe ihrer privaten Daten zu berechnen, ohne sich gegenseitig Rohdaten preiszugeben.[37] Hierzu werden beispielsweise einzelne Summanden einer Summe in mehreren Teilen (engl. '*shards*') über mehrere andere Teilnehmer zum zentralen Aggregator weitergeleitet. Dies sorgt dafür, dass der Aggregator keinen Summanden einer Partei zuordnen kann. Beim föderierten Lernen kann SMPC verwendet werden, um das Modelltraining und die Aggregationsprozesse auf sichere und datenschutzfreundliche Weise durchzuführen, selbst in Fällen, in denen der zentrale Server nicht uneingeschränkt vertrauenswürdig ist. Diese Methode wurde zum Beispiel im Zusammenhang mit genomweiten Assoziierungsstudien (GWAS) angewandt.[38] Diese

[36] *Xiaoxiao Li/Yufeng Gu/Nicha Dvornek/Lawrence Staib/Pamela Ventola/James Duncan.,* Multi-site fMRI analysis using privacy-preserving federated learning and domain adaptation: ABIDE results, Medical Image Analysis, 65 (2020), S. 1 (4).

[37] *Chuan Zhao/Shengnan Zhao/Minghao Zhao/Zhenxiang Chen/Chong-Zhi Gao/Hongwei Li/Yu-an Tan,* Secure Multi-Party Computation: Theory, practice and applications, Information Sciences, 476 (2019), S. 357.

[38] *Scott Constable/Yuzhe Tang/Shuang Wang/Xiaoqian Jiang/Steve Chapin,* Privacy-preserving GWAS analysis on federated genomic datasets, BMC Medical Information Decision Making, 15 (2015), S. 1 (2).

Art von Studien werden in der Biomedizin verwendet, um krankheitsspezifische Mutationen zu identifizieren.

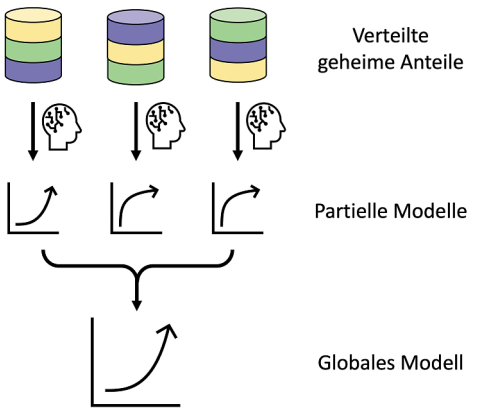

Abb. 4: Prinzip der Secure Multiparty Computation.

3. Homomorphe Verschlüsselung (engl. ‚homomorphic encryption')

Homomorphe Verschlüsselung ist eine Art der Verschlüsselung, die es ermöglicht, Berechnungen mit verschlüsselten Daten durchzuführen, ohne die Daten vorher entschlüsseln zu müssen.[39] Beim föderierten Lernen kann homomorphe Verschlüsselung verwendet werden, um die Modelltrainings- und Aggregationsprozesse auf verschlüsselten Daten durchzuführen, was dazu beiträgt, die Vertraulichkeit der Daten zu wahren, selbst wenn sie ohne weitere Sicherheitsmaßnahmen für das Modelltraining verwendet werden. Homomorphe Verschlüsselung wurde zum Beispiel benutzt, um ähnliche Patienten in verschiedenen Krankenhäusern zu identifizieren.[40]

Dies sind nur einige Beispiele für Techniken, die beim föderierten Lernen zum Schutz personenbezogener Daten eingesetzt werden können. Welche Techniken im Einzelnen zum Einsatz kommen, hängt von den Anforderungen und Beschränkungen des jeweiligen Szenarios ab, einschließlich der Art der verwendeten Daten, der beteiligten Parteien und des rechtlichen und regulatorischen Umfelds.

[39] *Abbas Acar/Hidayet Aksu/Selcuk Uluagac/Mauro Conti*, A Survey on Homomorphic Encryption Schemes: Theory and Implementation, ACM Computing Surveys, 51 (2018), S. 1.

[40] *Lee/Sun/ Wang/Wang/Jun/ Jiang* (Fn. 17), S. 6.

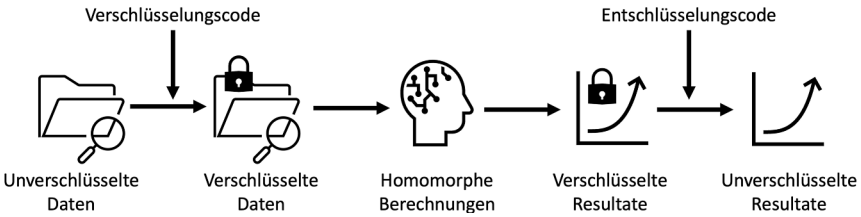

Abb. 5: Homomorphe Verschlüsselung.

VII. Föderierte Plattformen

Derzeit gibt es mehrere Plattformen, die für die Umsetzung föderierter Anwendungen geeignet sind. Zu den wichtigsten Beispielen gehören:

1. TensorFlow Federated

TensorFlow Federated ist eine Open-Source-Plattform für föderiertes Lernen, die von Google entwickelt wurde und eine flexible und skalierbare Infrastruktur für die Erstellung und den Einsatz von föderierten Lernmodellen bietet.[41] Sie ist mit dem *TensorFlow-Framework* für maschinelles Lernen integriert und bietet Werkzeuge und Bibliotheken für die Implementierung von föderierten Lernalgorithmen sowie für die Simulation von föderierten Lernszenarien. *Tensorflow* wird zum Beispiel benutzt, um mit Hilfe von durch Android-Benutzer aufgenommenen Bildern den Luftqualitätsindex zu schätzen.[42]

2. PySyft

PySyft ist eine weitere *Open-Source*-Plattform für föderiertes Lernen und baut auf der Open-source-Programmbibliothek *PyTorch* auf.[43] *PySyft* bietet eine umfassende Auswahl von Tools und Bibliotheken für die Erstellung und den Einsatz von föderierten Lernmodellen. Sie unterstützt eine breite Palette von Techniken zur Wahrung der Privatsphäre, darunter *Differential Privacy*, *Secure Multiparty Computation* und homomorphe Verschlüsselung. *PySyft* hat eine Reihe von Anwendungsfällen, wie zum Beispiel im Bereich der autonomen Fahrzeuge.

[41] *TensorFlow,* TensorFlow federated, https://www.tensorflow.org/federated (29. 06. 2023).

[42] *VisionAir,* https://vision-air.github.io/ (29. 06. 2023).

[43] *Alexander Ziller/Andrew Trask/Antonia Lopardo/Benjamin Szymkow/Bobby Wagner/Emma Bluemke/Jean-Mickael Nounahon/Jonathan Passerat-Palmbach/Kritika Prakash/Nick Rose/Théo Ryffel/Zarreen Naowal Reza/Georgios Kaissis*, PySyft: A Library for Easy Federated Learning, in: Rehman/Gaber, Federated Learning Systems: Towards Next-Generation AI, 2021, S. 111 (119).

In autonomen Fahrzeugen wird eine große Menge an Daten von verschiedenen Sensoren wie Kameras, LiDAR und Radar erzeugt. Diese Daten sind entscheidend für Aufgaben wie Objekterkennung, Kollisionsvermeidung und Routenoptimierung. Die Übermittlung all dieser Daten an einen zentralen Server zur Verarbeitung ist jedoch aufgrund von Bandbreitenbeschränkungen und Datenschutzbedenken nicht möglich.

Föderiertes Lernen ermöglicht den autonomen Fahrzeugen, kollektiv zu lernen und dabei die Daten lokal zu halten. Jedes Fahrzeug fungiert als Edge-Gerät, das Daten verarbeitet und lokal Modelle lernt. Diese Modelle werden dann durch föderiertes Lernen aggregiert, wodurch sichergestellt wird, dass jedes Fahrzeug von den kollektiven Lernerfahrungen der anderen profitiert, ohne sensible Rohdaten zu teilen.[44]

3. FATE (Federated AI Technology Enabler)

FATE ist eine von *Webank* entwickelte Open-Source-Plattform für föderiertes Lernen, die eine skalierbare und sichere Infrastruktur für die Entwicklung und den Einsatz von Modellen für föderiertes Lernen bietet.[45] Sie unterstützt eine breite Palette von Algorithmen für maschinelles Lernen und bietet Tools und Bibliotheken für die Implementierung von föderierten Lernen und datenschutzfreundlichen Techniken. Auch FATE bietet eine Reihe von Anwendungsmöglichkeiten, wie zum Beispiel die Erfassung von Geldwäsche oder die Einschätzung von Kreditrisiken.[46]

4. NVIDIA Clara

Dies ist eine Plattform für die Entwicklung und den Einsatz von KI-Anwendungen im Gesundheitswesen und in den Biowissenschaften.[47] Sie bietet Tools und Bibliotheken für die Erstellung und Bereitstellung von föderierten Lernmodellen sowie Hardware-Beschleunigung und Leistungsoptimierung für das Lernen von Deep-Learning-Modellen. *NVIDIA Clara* findet zum Beispiel Anwendung in der Entwicklung von medizinischen Geräten, von Arzneimitteln und intelligenten Krankenhäusern.

---

[44] *OpenMined,* https://blog.openmined.org/tag/use-cases/ (29. 06. 2023).

[45] *Yang Liu/Tao Fan/Tianjian Chen/Qian Xu/Qiang Yang*, FATE: an industrial grade platform for collaborative learning with data protection, Journal of Machine Learning Research, 22 (2021), S. 1.

[46] *FedAI*, https://www.fedai.org/cases/ (29. 06. 2023).

[47] *NVIDIA Developer,* Healthcare developer resources, https://developer.nvidia.com/industries/healthcare (29. 06. 2023).

5. FeatureCloud

Das Horizon 2020-geförderte FeatureCloud-Projekt entwickelt Mechanismen für föderiertes maschinelles Lernen, insbesondere im Gesundheitswesen. Ein zentrales Ergebnis dieses Projekts ist die Schaffung von featurecloud.ai, einem App Store für föderierte Anwendungen. Was featurecloud.ai auszeichnet, ist der Open-Source-Charakter, der es jedem ermöglicht, seine eigenen Apps zu entwickeln und beizusteuern. Diese Inklusivität erstreckt sich auch auf die Nutzer, da jeder frei auf die auf der Plattform verfügbaren Apps zugreifen und sie nutzen kann. Darüber hinaus bietet featurecloud.ai robuste Workflow-Management-Funktionen, die eine nahtlose und effiziente Ausführung von föderierten Lern-Workflows gewährleisten.

Welche Plattform für einen bestimmten Anwendungsfall am besten geeignet ist, hängt von den Anforderungen und Einschränkungen der jeweiligen Situation ab, einschließlich der Art der verwendeten Daten, der beteiligten Parteien und des rechtlichen und regulatorischen Umfelds. Im folgenden Abschnitt wird die *FeatureCloud* Plattform näher beleuchtet.

6. FeatureCloud

FeatureCloud (featurecloud.ai)[48] ist eine speziell für föderiertes maschinelles Lernen entwickelt Plattform, die biomedizinischen Wissenschaftlern eine nutzerfreundliche, einheitliche Infrastruktur für die Erstellung, Ausführung und Verwaltung föderierter maschineller Lernmodelle bietet. *FeatureCloud* stellt eine Vielzahl von Methoden des maschinellen Lernens und zur Präprozessierung und Visualisierung von Daten und Ergebnissen zur sofortigen Anwendung bereit. Neben der Bereitstellung einer Reihe von existierenden Algorithmen und Ansätzen für föderiertes Lernen konzentriert sich *FeatureCloud* auf die Minimierung der Komplexität, die mit dem Training von Modellen innerhalb einer föderierten Umgebung verbunden ist. Durch die Bereitstellung einer benutzerfreundlichen und effizienten Plattform ermöglicht *FeatureCloud* Forschern und Entwicklern die Nutzung von Techniken des föderierten Lernens, ohne dass eine umfangreiche IT-Infrastruktur eingerichtet werden muss und beschleunigt so die Einführung und Umsetzung von föderiertem Lernen. Der *FeatureCloud App Store* enthält eine Vielzahl von föderierten Anwendungen für

[48] *Julian Matschinske/Julian Späth/Mohammad Bakhtiari/Niklas Probul/Mohammad Kazemi Majdabadi/Reza Nasirigerdeh/Reihaneh Torkzadehmahani/Anne Hartebrodt/Balazs-Attila Orban/Sándor-József Fejér/Olga Zolotareva/Supratim Das/Linda Baumbach/Josch Pauling/Olivera Tomašević/Béla Bihari/Marcus Bloice/Nina Donner/Walid Fdhila/Tobias Frisch/Anne-Christin Hauschild/Dominik Heider/Andreas Holzinger/Walter Hötzendorfer/Jan Hospes/Tim Kacprowski/Markus Kastelitz/Markus List/Rudolf Mayer/Mónika Moga/Heimo Müller/Anastasia Pustozerova/Richard Röttger/Christina Saak/Anna Saranti/Harald Schmidt/Christof Tschohl/Nina Wenke/Jan Baumbach*, The FeatureCloud Platform for Federated Learning in Biome-dicine: Unified Approach, Journal of Medical Internet Research, 2023, 25, S. e42621.

die Biomedizin und hat aufgrund seiner Flexibilität das Potenzial, auch in verschiedenen Bereichen außerhalb der Biomedizin eingesetzt zu werden.

7. Nutzen und App-Entwicklung

Durch Containerisierung, also einer Bündelung aller notwendigen Software, kann *FeatureCloud* nahtlos auf jeder Plattform ausgeführt werden. Über die *Controller Application* können Nutzer auf den *App Store* zugreifen und Arbeitsabläufe über die benutzerfreundliche webbasierte Schnittstelle ausführen. Für die Entwicklung föderierter Anwendungen wird ein Python-Paket angeboten, das Kernfunktionen wie Kommunikationsprotokolle und Techniken zur Verbesserung des Datenschutzes wie *Secure Multiparty Computing* (SMPC) bereitstellt. Darüber hinaus gibt es eine *Command Line Interface* (CLI), um die Erstellung, das Testen und die Veröffentlichung von Anwendungen zu optimieren.

Mit dem *FeatureCloud* Python-Paket können Benutzer schnell föderierte Anwendungen entwickeln, die auf der *FeatureCloud*-Plattform ausgeführt werden können. Voraussetzungen hierfür sind lediglich Python, die *FeatureCloud*-Bibliothek und *Docker*, ein Containerisierungsprogramm zur sicheren Ausführung von Apps unabhängig von der Computerumgebung. Dies bedeutet, dass die App in einem in sich geschlossenen System (*Docker-Container*) ausgeführt wird und nur über *FeatureCloud* kommunizieren kann. Für die Erstellung von Apps sollte man die *FeatureCloud* App-Vorlage verwenden, die über das *FeatureCloud* GitHub Repositorium, in welchem Code, Dateien und der Revisionsverlauf der Dateien hinterlegt sind, oder das *FeatureCloud* Python-Paket verfügbar ist. Um die Entwicklung und das Testen von Anwendungen zu erleichtern, beinhaltet die Plattform zudem eine Testumgebung, mit der ein föderiertes Szenario auf einem lokalen Computer simuliert werden kann, um Anwendungen während der Entwicklungsphase zu evaluieren und zu verfeinern. Hierbei können entwickelte Apps auch im Zusammenspiel mit bereits im App-Store verfügbaren Apps getestet werden.

8. Veröffentlichung von Apps

Sobald Entwickler ihre App implementiert und erfolgreich getestet haben, können sie sie der *FeatureCloud*-Community zur Verfügung stellen. Um die Veröffentlichung von Apps und den Zugang für Entwickler und Endnutzer zu erleichtern, bietet *FeatureCloud* den App Store, in dem Apps kategorisiert, geprüft und zertifiziert werden.

Jede App verfügt über ihre individuelle Seite im App-Store, in der Informationen angezeigt werden, die von App-Entwicklern, Endnutzern und dem *FeatureCloud*-Zertifizierungsteam bereitgestellt werden. Diese Seite kann vom jeweiligen App-Entwickler bearbeitet werden und enthält typischerweise den Namen der App, eine detaillierte Beschreibung mit Hinweis auf entsprechend implementierte Algo-

rithmen, Tags zum Kategorisieren der App und eine Verlinkung zum Quellcode der App. Solange es mit den datenschutzrechtlichen Gegebenheiten vereinbar ist, können die trainierten KIs öffentlich zugänglich gemacht werden, wie zum Beispiel im AIMe (*Artificial Intelligence in Biomedical research*)-Register, eine von der Forschungsgemeinschaft betriebene Plattform für die standardisierte Meldung biomedizinischer KI-Systeme.[49] Beispiele von veröffentlichten Apps sind zum Beispiel *Flimma*[50] zur föderierten Analyse von differenziellen Genexpressionsdaten sowie *sPlink*,[51] ein hybrides föderiertes Lernwerkzeug zur Analyse von Daten aus genomweiten Assoziationsstudien.

Apps werden im Allgemeinen in Präprozessierungs-, Analyse- und Auswertungs-Apps kategorisiert. Um das Bewusstsein für den Schutz der Privatsphäre in föderierten Apps zu verbessern, ermöglicht *FeatureCloud* zusätzliche Mechanismen zur Wahrung der Privatsphäre wie *Secure Multiparty Computation* und *Differential Privacy.* Die Bereitstellung dieser Funktionalitäten erleichtert die Entwicklung von Apps und vermeidet Probleme bezüglich des Datenschutzes durch unsaubere Implementierung. Für Endnutzer gibt es die Möglichkeit, Apps nach angewandten Techniken zur Wahrung der Privatsphäre zu filtern. Gleichzeitig können *FeatureCloud*-Nutzer Apps mit bis zu fünf Sternen bewerten, um auf die Stärken und Schwächen der App hinzuweisen. Eine Kommentarfunktion erlaubt es Benutzern, weiteres Feedback zu geben. Auf Grundlage der Bewertungen können die Endnutzer zwischen unterschiedlichen Apps wählen.

Die App-Zertifizierung zur Sicherstellung von korrekter Funktionsweise und der Wahrung des Datenschutzes der App ist ein weiterer wichtiger Baustein in der *FeatureCloud*-Plattform. Sie ist die Grundlage für das Vertrauen der Anwender und die Qualitätssicherung der Plattform. Hierzu steht eine gesonderte Zertifizierungsfunktion bereit. Zertifizierer spielen eine entscheidende Rolle bei der Untersuchung und Bewertung der in den Apps implementierten Sicherheitsmaßnahmen sowie bei der Identifizierung und Behebung möglicher Fehler. In einem umfassenden Zertifizierungsprozess werden die Anwendungen auf der Grundlage ihrer verwendeten Sicherheitsstandards bewertet und zertifiziert. Die Endnutzer können dann fundierte Entscheidungen über die von ihnen verwendeten Anwendungen treffen. Endnutzer können nicht zertifizierte Apps auf eigenes Risiko verwenden, es wird aber dazu geraten, den App-Code vorher eigenständig zu prüfen.

---

[49] *Julian Matschinske/Nicolas Alcaraz/Arriel Benis/Martin Golebiewski/Dominik Grimm/Lukas Heumos/Tim Kacprowski/Olga Lazareva/Markus List/Zakaria Louadi/Josch Pauling/Nico Pfeifer/Richard Röttger/Veit Schwämmle/Gregor Sturm/Alberto Traverso/Kristel Van Steen/Martiela Vaz de Freitas/Gerda Cristal Villalba Silva/Leonard Wee/Nina Wenke/Massimiliano Zanin/Olga Zolotareva/Jan Baumbach/David Blumenthal*, The AIMe registry for artificial intelligence in biomedical research, Nature Methods, 18 (2021), S. 1128.

[50] *Zolotareva/Nasirigerdeh/Matschinske/Torkzadehmahani/Bakhtiari/Frisch/Späth/Blumenthal/Abbasinejad/Tieri/Kaissis/Rückert/Wenke/List/Baumbach* (Fn. 21), S. 5.

[51] *Nasirigerdeh/Torkzadehmahani/Matschinske/Frisch/List/Späth/Weiss/Völker/Pitkänen/Heider/Wenke/Kaissis/Rueckert/Kacprowski/ Baumbach* (Fn. 22), S. 6.

VIII. Schlussbemerkungen

Insgesamt stellt das föderierte Lernen eine attraktive Möglichkeit dar, KI in verschiedenen Bereichen unter Wahrung der Vertraulichkeit personenbezogener Daten einzusetzen, insbesondere in Kombination mit anderen Maßnahmen zum Schutz der Privatsphäre. Bei richtiger Anwendung können so die Anforderungen der Art. 24, 25 und 32 DSGVO erfüllt werden, die den Einsatz geeigneter Schutzmaßnahmen für die Verarbeitung personenbezogener Daten vorsehen. Föderiertes Lernen ist aktuell der Stand der Technik und erfüllt somit weiterhin die Voraussetzungen gemäß Art. 32 Abs. 1 DSGVO, wonach „unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für Rechte und Freiheiten natürlicher Personen […] geeignete technische und organisatorische Maßnahmen" zu treffen sind.

Literatur

Brauneck, Alissa/*Schmalhorst*, Louisa/*Kazemi Majdabadi*, Mohammad Mahdi/*Bakhtiari*, Mohammad/*Völker*, Uwe/*Saak*, Christina Caroline /*Baumbach*, Jan/*Baumbach*, Linda/*Buchholtz,* Gabriele: Federated machine learning in data-protection-compliant research, Nature Machine Intelligence, 5 (2023), S. 2.

Hao, Meng/*Li,* Hongwei/*Xu*, Guowen/*Liu*, Sen/*Yang*, Haomiao: Towards Efficient and Privacy-Preserving Federated Deep Learning, ICC 2019 – 2019 IEEE International Conference on Communications (ICC), 2019, S. 1.

Hulsen, Tim/*Jamuar,* Saumya/*Moody,* Alan R./*Karnes*, Jason H./*Varga*, Orsolya/*Hedensted*, Stine/*Spreafico*, Roberto/*Hafler*, David A./*McKinney*, Eoin F.: From Big Data to Precision Medicine, Frontiers Medicine, 6 (2019), S. 34.

Kairouz, Peter/*McMahan*, Brendan/*Avent*, Brendan/*Bellet*, Aurelien/*Bennis*, Mehdi/*Bhagoji*, Arjun Nitin/*Bonawitz*, Kallista/*Charles*, Zachary/*Cormode*, Graham/*Cummings*, Rachel/*D'Oliveira*, Rafael/*Eichner*, Hubert/*Rouayheb*, Salim El/*Evans*, David/*Gardner*, Josh/*Garrett*, Zachary/*Gascón*, Adria/*Ghazi*, Badih/*Gibbons*, Phillip B./*Gruteser*, Marco/*Harchaoui*, Zaid/*He*, Chaoyang/*He*, Lie/*Huo*, Zhouyuan/*Hutchinson*, Ben/*Hsu*, Justin/*Jaggi*, Martin/*Javidi*, Tara/*Joshi*, Gauri/*Khodak*, Mikhail/*Konecný*, Jakub/*Korolova*, Aleksandra/*Koushanfar*, Farinaz/*Koyejo*, Sanmi/*Lepoint*, Tancrede/*Liu*, Yang/*Mittal*, Prateek/*Mohri*, Mehryar/*Nock*, Richard/*Özgür*, Ayfer/*Pagh*, Ayfer/*Qi*, Hang/*Ramage*, Daniel/*Raskar*, Ramesh/*Raykova*, Mariana/*Song*, Dawn/*Song*, Weikang/*Stich*, Sebastian U./*Sun*, Ziteng/*Suresh*, Ananda Theertha/*Tramèr*, Florian/*Vepakomma*, Praneeth/*Wang*, Juanyu/*Xiong*, Li/*Xu*, Zheng/*Yang*, Qiang/*Yu*, Felix X./*Yu*, Han/*Zhao*, Sen: Advances and Open Problems in Federated Learning, Foundations and Trends in Machine Learning, 14 (2021), S. 1.

Matschinske, Julian/*Späth*, Julian/*Bakhtiair*, Mohammad/*Probul*, Niklas/*Majdabadi*, Mohammad M.K./*Nasirigerdeh*, Reza/*Torkzadehmahani*, Reihaneh/*Hartebrodt*, Anne/*Orbán*, Balazs-Attila/*Fejér*, Sándor-József/*Zolotareva*, Olga/*Das,* Supratim/*Baumbach,* Linda/*Pauling,* Josch K./*Tomašević,* Olivera/*Bihari*, Béla/*Bloice*, Marcus/*Donner*, Nina C./*Fdhila*, Walid/*Frisch*, Tobias/*Hauschild*, Anne-Christin/*Heider*, Dominik/*Holzinger*, Andreas/*Hötzendor-*

fer, Walter/*Hospes*, Jan/*Kacprowski*, Tim/*Kastelitz*, Markus/*List*, Markus/*Mayer*, Rudolf/*Moga*, Mónika/*Müller*, Heimo/*Pustozerova*, Anastasia/*Röttger*, Richard/*Saak*, Christina C./*Saranti*, Anna/*Schmidt*, Harald H./*Tschohl*, Christof/*Wenke*, Nina K./*Baumbach*, Jan: The FeatureCloud Platform for Federated Learning in Biomedicine: Unifired Approach, Journal of Medical Internet Research, 25 *(*2023), e42621.

McMahan, Brendan/*Moore*, Eider/*Ramage*, Daniel/*Hampson*, Seth/*Arcas*, Blaise Aguera y: Communication-Efficient Learning of Deep Networks from Decentralized Data, Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, 54 (2017), S. 1273.

Nasirigerdeh, Reza/*Torkzadehmahani*, Reihaneh/*Matschinske*, Julian/*Frisch*, Tobias/*List*, Markus/*Späth*, Julian/*Weiss*, Stefan/*Völker*, Uwe/*Pitkänen*, Esa/*Heider*, Esa/*Wenke*, Nina K./*Kaissis*, Georgios/*Rueckert*, Daniel/*Kacprowski*, Tim/*Baumbach*, Jan: sPLINK: a hybrid federated tool as a robust alternative to meta-analysis in genome-wide association studies, Genome Biology, 23 (2022), S. 1.

Ogundokun, Roseline Oluwaseun/*Misra*, Sanjay/*Maskeliunas*, Rytis/*Damasevicius*, Robertas: A Review on Federated Learning and Machine Learning Approaches: Categorization, Application Areas, and Blockchain Technology, Information, 13 (2022), S. 263.

Silva, Santiago/*Gutman*, Boris/*Romero*, Eduardo/*Thompson*, Paul M./*Altmann*, Andre/*Lorenzi*, Marco/*ADNI*/*PPMI*/*UK Biobank*: Federated Learning in Distributed Medical Databases: Meta-Analysis of Large-Scale Subcortical Brain Data, 2019 IEEE 16th International Symposium on Biomedical Imaging (ISBI 2019), 2019, S. 270.

Späth, Julian/*Matschinske*, Julian/*Kamanu*, Frederick K./*Murphy*, Sabina A./*Zolotareva*, Olga/*Bakhtiari*, Mohammad/*Antman*, Elliott M./*Loscalzo*, Joseph/*Brauneck*, Alissa/*Schmalhorst*, Louisa/*Buchholtz*, Gabriele/*Baumbach*, Jan: Privacy-aware multi-institutional time-to-event studies, PLOS Digit Health, 1 (2022), S. 1.

Torkzadehmahani, Reihaneh/*Nasirigerdeh*, Reza/*Blumenthal*, David B./*Kacprowski*, Tim/*List*, Markus/*Matschinske*, Julian/*Späth*, Julian/*Wenke*, Nina Kerstin/*Baumbach*, Jan: Privacy-Preserving Artificial Intelligence Techniques in Biomedicine, Methods of Information in Medicine, 61 (2022), S. e12.

Yang, Qiang/*Liu*, Yang/*Chen*, Tianjian/*Tong*, Yongxin: Federated Machine Learning: Concept and Applications, ACM Transactions on Intelligent Systems and Technology, 10 (2019), S. 1.

Zhao, Chuan/*Zhao*, Shengnan/*Zhao*, Minghao/*Chen*, Zhenxiang/*Gao*, Chong-Zhi/*Li*, Hongwei/*Tan*, Yu-an: Secure Multi-Party Computation: Theory, practice and applications, Information Sciences, 476 (2019), S. 357.

Ziller, Alexander/*Trask*, Andrew/*Lopardo*, Antonio/*Szymkow*, Benjamin/*Wagner*, Bobby/*Bluemke*, Emma/*Nounahon*, Jean-Mickael: PySyft: A Library for Easy Federated Learning, in: Rehman/Gaber, Federated Learning Systems: Towards Next-Generation AI, 2021, S. 111.

Zolotareva, Olga/*Nasirigerdeh*, Reza/*Matschinske*, Julian/*Torkzadehmahani*, Reihaneh/*Bakhtiari*, Mohammad/*Frisch*, Tobias/*Späth*, Julian/*Blumenthal*, David B./*Abbasinejad*, Amir/*Tieri*, Paolo/*Kaissis*, Georgios/*Rückert*, Daniel/*Wenke*, Nina K./*List*, Markus/*Baumbach*, Jan: Flimma: a federated and privacy-aware tool for differential gene expression analysis, Genome Biology, 22 (2021), S. 1.