Federated Learning

Madrid, Dajsinani
RezzyTech Inc.

***Zusammenfassung*—Hier soll die neuartige Methode des Federated Learnings, als Teil der Klasse von Algorithmen im Machine Learning Bereich besprochen werden. Dabei wird besonderer Wert auf die Abgrenzung zu herkömmlichen Machine Learning Algorithmen gelegt, sowie den offenen Fragestellungen in diesem Bereich. Einer Kategoriesierung und Definition der Kernpunkte folgt eine Übersicht der Vor- und Nachteile dieses Ansatzes. Eingehend auf diese Punkte, werden einige Beispiele von bereits umgesetzten und möglichen Anwendungsfeldern für Federated Learning vorgestellt.**

Inhaltsverzeichnis

1. Einleitung

Eine zunehmende Verfügbarkeit von Daten durch das Internet und diffuse Fragestellungen, wie die automatisierte Steuerung von Kraftfahrzeugen, haben in den letzten Jahren zu einer Enormen Entwicklung im Bereich von Machine Learning beigetragen. Alle Algorithmen aus diesem Bereich erstellen aus großen Datenmengen Modelle, die in der Lage sind, ohne explizite Vorgabe eines Lösungsalgorithmus, komplexe Aufgaben zu bewältigen. Sieht man die Daten als Punkte in hochdimensionalen Räumen, wobei jede Eigenschaft eines Eintrages eine Dimension des Raumes ist, kann man Machine Learning Algorithmen daher als Fit-Algorithmen in hochdimensionalen Vektorräumen begreifen.

Die historische Entwicklung von Machine Learning Algorithmen beginnt bereits in den 50er und 60er Jahren, mit der Entdeckung von Baysianischen Methoden, der Weiterentwicklung statistischer Algorithmen, sowie spezialisierten Neuentdeckungen wie dem Nearest Neighbor Algorithmus [16]. Diese Periode folgte der erste "AI Winter", in dem das Vertrauen in die Nützlichkeit von Machine Learning Algorithmen vollständig schwand [23, S. 24]. Viel von dem Mangelnden Vertrauen kann auf fehlende Rechnerleistung zurückgeführt werden. Nach der Wiederentdeckung des Backpropagation Algorithmus zu beginn der 80er Jahre, folgte ein zweiter AI-Winter Ende der 80er Jahre [16]. Dieser hielt bis zu Beginn der 2000er Jahre an. Als Hauptgrund hierfür wird oft der Mangel an großen Datenmengen und das anschließende aufkommen von solchen, durch die Verbreitung des Internets und die Etablierung von Firmen wie Google und Facebook, genannt. Die Bereitstellung dieser Datenmengen hat zu einem enormen Zuwachs an Forschungsergebnissen, besonders im Bereich der Bilderkennung, geführt [16]. Am Phänomen der Ablösung zahlreicher öffentlich zugängiger APIs aus den Frühzeiten des Internets, siehe z.B. Twitter, YouTube, Facebook, sieht man, dass die Segmentierung und Abschottung von Daten voranschreitet [37]. Genau diese Entwicklung zu höherer Datensicherheit und Datenschutz, zeichnet sich auch in der politischen und rechtlichen Entwicklung (siehe DSGVO von 2018, CCPA von 2020) und letztendlich auch der Entwicklung von Machine Learning Algorithmen, ab. Zunehmend komplexe Problemstellungen aus dem Bereich des Machine Learning sorgen dafür, das größere und heterogenere Datensätze benötigt werden. Diese stehen aber nicht mehr einzelnen Entitäten zur Verfügung und können aus Grund des Datenschutzes oder der Wirtschaftlichkeit nicht öffentlich verfügbar gemacht werden [32].

Während ein weiterer "AI Winter" im Moment nicht absehbar ist, sind sich Forscher den Herausforderungen der Anwendung von Algorithmen auf riesige Datenbestände dennoch bewusst. Resultierend daraus wird die Entwicklung und Forschung neuer Ansätze besonders unter den Gesichtspunkten der geänderten Rahmenbedingunen von Datenbeständen diskutiert. Kern dieser neuen Entwicklung bildet das "Federated Learning", welches die Voraussetzung monolithischer Datenbestände, welcher traditionalle Ansätze unterworfen sind, auflöst. Im Folgenden wird zunächst eine Definition und kurze Einführung gegeben. Folgend darauf, werden verschiedene Teilaspekte detailliert besprochen, bevor ein Vergleich von *Federa-*

ted Learning mit traditionellen Algorithmen, sowie eine Übersicht der Chancen, Herausforderungen und potentiellen Anwendungsgebiete gegeben wird.

2. Was ist Federated Learning?

Ferated Learning ist ein neue Ansatz, der erst vor wenigen Jahren von Google, zur Lösung der oben diskutierten Probleme aus Segmentierung von Daten auf unterschiedliche Anbieter, vorgeschlagen wurde [11]. Ziel ist es, ein Machine Learning Modell zu definieren, dass mit den Rahmenbedingungen aus verteilten Datensätzen und limitiertem Informationsaustausch arbeiten kan. Besonders die Herausforderungen durch heterogene Statistik [26], die sowohl die Datensätze als auch die Netzwerkarchitekturen und Modelle betrifft, als auch die Kommunikationssicherheit [1], stehen dabei im Vordergrund aktueller Forschung [32]. Besonders die Herausforderungen von extremen Unterschieden in der Datenverteilung und Zuverlässigkeit von (oft eingebetteten Systemen) Geräten waren in bisherigen Publikationen zentral. Hier soll es allerdings auch darum gehen Kollaboration zwischen Firmen zu definieren, wie oben beschrieben wurde [32].
Der folgende Abschnitt orientiert sich stark an Q. Yang et al. [32]. Um Federal Learning einzuführen wird zunächst eine Menge aus N Parteien $\{\mathcal{F}_1, \ldots, \mathcal{F}_N\}$ definiert, die jeweils eigene Datensätze $\{\mathcal{D}_1, \ldots, \mathcal{D}_N\}$ besitzen. Das Ziel ist es, ein gemeinsames Modell $\mathcal{M}_{\text{Fed}}$ zu trainieren. Dies unterscheidet sich von traditionellen Machine Learning Modellen dadurch, dass niemandem ein gemeinsamer Datensatz $\mathcal{D} = \bigcup_{1 \leq i \leq N} \mathcal{D}_i$ auf dem ein Modell $\mathcal{M}_{\text{Sum}}$ trainiert wird. Nichtsdestotrotz ist es das Ziel, das neue Modell $\mathcal{M}_{\text{Fed}}$ möglichst nah am traditionellen zu halten. Es wird daher gefordert, dass die Differenz der Performance $\mathcal{V}.$ beider Modelle beschränkt ist:

$$|\mathcal{V}_{\text{Fed}} - \mathcal{V}_{\text{Sum}}| < \delta \tag{1}$$

$\delta \in \mathbb{R}^+$ bezeichnet den δ-Loss (engl. Verlust) des Federal Learning Algorithmus.
Da Datensicherheit von zentraler Bedeutung für Federal Learning ist, werden hier, wie auch in Q. Yang et al. [32], die drei wichtigsten Konzepte dafür kurz vorgestellt. Wichtiger Punkt für alle diese Konzepte ist die Vermeidung von (indirekter) Übertragung persönlicher Daten (also jener Daten, die nicht für den Algorithmus notwendig sind, aber deren Information nicht aus dem Unternehmen gelangen soll). Dies geschieht zum Beispiel, wenn ein bösartiger Teilnehmer j den Datenfluss in einer Weise manipuliert, dass er Zugriff auf die Daten $\mathcal{D}_i$ eines anderen Teilnehmers $i \neq j$ bekommt [32]. Speziell unter dem Ausnutzen von Gradienteninformationen kann dies implizit geschehen [28]. Die drei Punkte, welche zur Datensicherheit beitragen sollen sind:

- *Secure Multi-Party Computation:* Diese Form der Absicherung soll jede Übertragung von sensibler Information verhindern. Dabei ist es notwendig aufwändige Modifikationen an der Kommunikation vorzunehmen und die Sicherheit der Kommunikationsprotokolle zu gewährleisten [6]. Diese Methode ist im Vergleich zu den übrigen aufwändig und eine teilweise Auflösung der vollständigen Absicherung kann sinnvoll sein [32].
- *Differential Privacy:* Hierbei werden sensible Daten, zum Beispiel durch Hinzufügen von Rauschen, oder Generalisierung (Aggregation oder Verschiebung von Datenpunkten) obfuskiert. Die Daten müssen allerdings weiterhin übertragen werden und bleiben damit angreifbar [32].
- *Homomorphic Encryption:* Durch eine homomorphe (also bilderhaltende) Transformation, bleibt die Struktur der Daten gewahrt, während die sensiblen Informationen nurnoch transformiert vorliegen. Durch diese Methode müssen die Daten also nicht länger in der ursprünglichen Form übertragen werden. Diese Transformationen können allerdings, in Abhängigkeit von der Genauigkeit der Transformation, die Performance des Modells negativ beeinflussen [32].

3. Kategorisierung von Federated Learning

In Abhängigkeit von der Verteilung der Daten unter den teilnehmenden Parteien, sowie der Zielsetzung des zu lernenden Modells, gibt es drei verschiedene Kategorien von Federated Learning. Diese sollen nun im Detail diskutiert werden, dazu werden folgende Definitionen benutzt: $\mathcal{X}$ bezeichnet die Menge der Features eines Datensatzes, $\mathcal{Y}$ the zugehörigen Labels und $\mathcal{I}$ die IDs der Samples. Ein gesamter Datensatz wird dementsprechend mit $(\mathcal{I}, \mathcal{X}, \mathcal{Y})$. Die Menge der segmentierten Daten $\{\mathcal{D}_1, \ldots, \mathcal{D}_N\}$ wird wie oben beschrieben verwendet. In der Kategorisierung werden die unterschiedlichen Aufteilung dieser Mengen auf die teilnehmenden Parteien untersucht [32].

3.1. Definition von Sicherheitsaspekten

Im Folgenden wird wiederholt die (Kommunikations-) Sicherheit von Algorithmen eingegangen. Dafür ist es sinnvoll zunächst einige Definitionen zusammenzufassen.

- *honest* - Ehrlicher Teilnehmer, der keine wissentlich falsche Information versendet, Daten manipuliert oder den Versuch unternimmt andere Teilnehmer auszuspähen oder zu beeinflussen,
- *honest-but-curious* - (passiv bösartig) Ehrlicher Teilnehmer, der keine wissentlich falsche Information versendet oder Daten manipuliert, *aber* Daten und Anfragen ausspäht.
- *semi-malicious* - (semi aktiv bösartig) Teilnehmer, der Daten fälscht, sich allerdings an die Kommunikationsprotokolle hält.
- *malicious* - Bösartiger Teilnehmer, der jede technische Möglichkeit nutzt, um das gesamtergebnis negativ zu beeinflussen.

3.2. Horizontal Federated Learning

Das Lernen auf Datensätze mit verteilten Samples nennt man “Horizontal Federated Learning”. Alle Teilnehmer verfügen also über Datensätze mit der selben Feature- und Labelmenge, allerdings nur über einen Teil der Samples:

$$\forall \mathcal{D}_i, \mathcal{D}_j,\ i \neq j: \quad \mathcal{I}_i \neq \mathcal{I}_j, \mathcal{X}_i = \mathcal{X}_j, \mathcal{Y}_i = \mathcal{Y}_j$$

Ein Schema für die Segmentierung der Daten für zwei Parteien ist in Abbildung 1 gegeben. Diese Aufteilung wird beispielsweise von Firmen Dependancen mit unterschiedlichen Kunden auftreten. Die erfassten Daten sind in jeder Niederlassung identisch, allerdings unterscheiden sich die erfassten Nutzer. Auch unter konkurrierenden

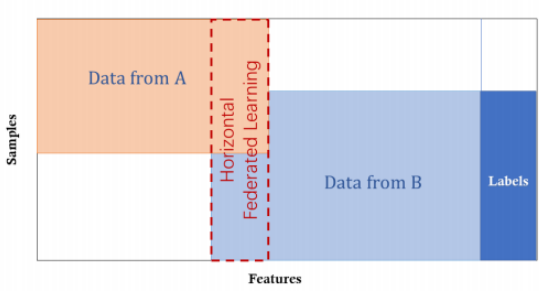

Abbildung 1. Horizontal Federated Learning

Unternehmen in dem selben Sektor kann diese Situation auftreten.
Die Annahme unter diesem Modell ist typischerweise, dass alle Teilnehmer *honest* und der koordinierende Server *honest-but-curious* ist [2, 32]. Dies stellt eine relativ starke Einschränkung der Sicherheit dar, da kein Schutz vor *semi-malicious* oder *malicious* Teilnehmern gegeben ist. In der aktuellen Forschung wird dieses Problem bereits diskutiert und es kann für zukünftige Verbesserungen dieser Modelle werden aller Erwartung nach resistenter gegen diese Art von Teilnehmern sein. Ein Beispiel für die möglichen Verbesserungen ist die Zuhilfenahme von statistischem Rauschen unter homomorpher Verschlüsselung [15].
Zukünfigte Verbesserungen zielen auch auf die Reduktion von Kommunikation zwischen den Teilnehmern [18]. Dies ist besonders im Kontext von eingebetteten Geräten ohne ständigen Internetzugang eine wichtige Entwicklung.

3.3. Vertical Federated Learning

"Vertical Federated Learning" ist invers zum horizontal Federated Learning. Statt einer Segmentierung in Samples, besteht eine solche in den Features, bei identischen Samples. Denkbar ist diese Situation bei Firmen, die in unterschiedlichen Sektoren operieren, aber über eine gemeinsame Kundenbasis verfügen.

$$\forall \mathcal{D}_i, \mathcal{D}_j,\ i \neq j: \quad \mathcal{I}_i = \mathcal{I}_j, \mathcal{X}_i \neq \mathcal{X}_j, \mathcal{Y}_i \neq \mathcal{Y}_j$$

Ein vollständigis Kundenprofil aus Zahlungswürigkeit, Einkaufsverhalten, Interessen, kann von großem Wert für Firmen sein. Diese Informationen sind jedoch typischerweise nicht einer Firma gemeinsam zugänglich und die Weitergabe in vielen Ländern durt Datenschutz-Regelungen geschützt. Daher ist dieses Machine-Learning-Modell besonders durch die, bereits oben diskutierten, verschärften gesetzlichen Rahmenbedingungen zunehmend interessant. Ein Schema für die Segmentierung der Daten für zwei Parteien ist in Abbildung 2 gegeben.
Durch den segmentierten Feature-Space im Vertical Federated Learning, besteht die Möglichkeit eine höhere Sicherheit zu gewährleisten. Daher ist es möglich

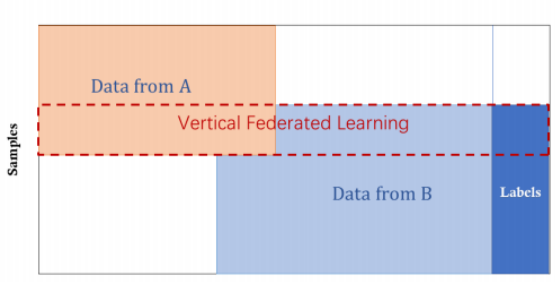

Abbildung 2. Vertical Federated Learning

honest-but-curious Teilnehmer vorauszusetzen. Für den Kommunikationsaspekt des Algorithmus können sogar *semi-malicious* Teilnehmer angenommen werden, die allerdings nicht zusammenarbeiten dürfen, um die Sicherheit weiterhin zu gewährleisten [32].
Die Anwendungsgebiete für diese Kategorie sind im Bereich von kollaborativer Statistik [5]. Also speziell dem Erstellen quantitativer, statistischer Deskriptoren auf Datensätzen, deren voller Feature-Space nicht bekannt ist. Konkret, kann dies eine gemeinsame lineare Regression sein, obwohl jedem Teilnehmer nur ein Teil jedes Vektors im Entsprechenden Raum zur Verfügung steht [10].

3.4. Federated Transfer Learning

Ein letzter wichtiger Fall ist gegeben, wenn gar kein Überlapp der Daten garantiert werden kann.

$$\forall \mathcal{D}_i, \mathcal{D}_j,\ i \neq j: \quad \mathcal{I}_i \neq \mathcal{I}_j, \mathcal{X}_i \neq \mathcal{X}_j, \mathcal{Y}_i \neq \mathcal{Y}_j$$

Trotz der unterschiedlichen Datenlage, kann es dennoch sinnvoll sein, ein gemeinsames Machine Learning Modell zu nutzen. Dies ist zum Beispiel für ähnliche Unternehmen in unterschiedlichen kulturellen Regionen[1] relevant. Der Ausdruck "Transfer" steht daher für den Transfer von Wissen aus einem Bereich in einen anderen (speziell geschieht dies durch Übertragung von Modellparametern). Zwar sind die erfassten Daten strukturell anders und ein Überlapp der gemeinsamen Kunden gering, allerdings müssen zum Verkauf eines identischen Produktes, dennoch ähnliche Modelle gelten. Zu dem Lernprozess muss also auch das Finden einer gemeinsamen Repäsentation der Daten gehören [20]. Ein Schema für die Segmen-

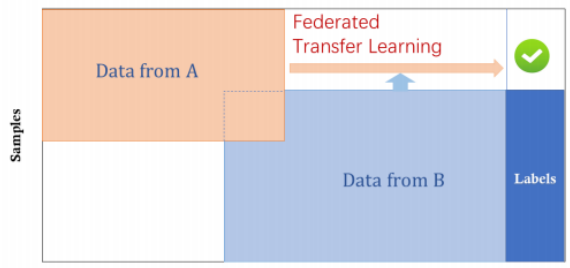

Abbildung 3. Federated Transfer Learning

tierung der Daten im Federated Transfer Learning Fall,

1. Beispielsweise kann es vorkommen, dass eine Person aus Ägypten keinen Nachnamen besitzt, dieses Feld für einen Entrag in einer Datenbank aus Deutschland aber vorgesehen wäre.

für zwei Parteien, ist in Abbildung 3 gegeben. Im Detail gibt es in dieser Form der Modellierung zahlreiche Unterkategorien. Eine Übersicht ist in Abbildung 4 gegeben. Statt hier auf die Details dieses Ansatzes eingehen, wird

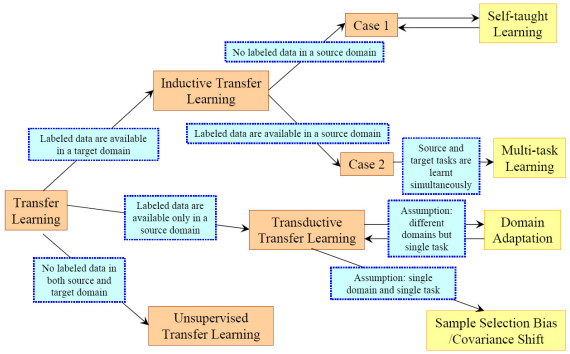

Abbildung 4. Übersicht Transfer Federated Learning. Aus [20]

in der Diskussion der Vor- und Nachteile von Federated Learning auf die vielfältigen Einsatzmöglichkeiten Bezug genommen.
Durch den mangelnden Überlapp an Features, ähnelt die Sicherheit, der des Vertical Federated Learning [32].
Beispiele für eine Anwendung von Federated Transfer Learning wurden mit der Klassifikation von Text in Stimmungskategorien und Bild-Klassifikationen bereits geliefert [20, 30, 36]. Speziell der zweite Anwendungsfall ist interessant, da hier ein Modell, dass zur Texterkennung trainiert wurde, für Bildklassifikationen weiterverwendet wird. Durch die größere Menge an beschrifteten Textdaten, kann hier ein wesentlich präzieseres Modell trainiert werden.

4. Vorteile des Federated Learnings

Nach der Einführung in die konkreten Aspekte von Federated Learning, können nun die speziellen Vorteile diskutiert werden, die diesen Ansatz von anderen Machine Learning Modellen abheben.

4.1. Datensicherheit und Datenschutz

Alle Algorithmen, die sich unter Federated Learning einordnen, enthalten die Kommunikation der Teilinformation als Kernbestandteil. Die bietet die Möglichkeit, Datensicherheit als Teil des Algorithmus zu verstehen. Nicht in jedem Fall ist die Information allerdings vollständig dezentralisiert. Einer der erprobten Algorithmen, ein dezentralisierter Back-Propagation Algorithmus, benötigt eine zentrale vertrauenswürdige Instanz (im Folgenden wird diese *Trusted Authority* - TA genannt) [34]. Die TA ist für die Schlüsselvergabe notwendig und weitere Verschlüsselugnsschichten ergänzen das Konzept. Im Fall des dezentralisierten Back-Propagation Algorithmus, liegt eine zusätzliche homomorphische Verschlüsselung vor [34]. Dies ist im Fall von horizontalem Federated Learning und der Linearität von Operationen im Lernprozess neuronaler Netzwerke möglich, aber nicht zwingend auf alle Kategorien erweiterbar. Das dabei beschrittene Vorgehen wird auch als *Gradienten Aggregation* bezeichnet.

4.2. Gradienten Aggregation

Um einen solchen verteilten Algorithmus zu konkretisieren, wird hier den Kern des *Unbiased Gradienten Aggregation* Algorithmus diskutiert [33]. Sei $\mathcal{B}_t^{k(i)} \subset \mathcal{D}_k$ der Batch für die t-te Runde und den i-ten Schritt eines Gradienten-basierten Verfahrens mit Gewichten $\omega_t^{k(i-1)}$. Man kann für das Modell $\mathcal{L}$ den neuen Gradient $g_t^{k(i)}$ auf jedem der k Teilnehmer berechnen lassen:

$$g_t^{k(i)} = \nabla_{\omega_t^{k(i-1)}} \mathcal{L}(\omega_t^{k(i-1)}, \mathcal{B}_t^{k(i)})$$

Der letzte Schritt auf dem Teilnehmer k, für Runde t, bezeichnet man mit (Da alle Batches benutzt wurden, hängt das Modell jetzt von dem gesamten Teildatensatz $\mathcal{D}_k$ ab):

$$g_t^k = \nabla_{\omega_t^k} \mathcal{L}(\omega_t^k, \mathcal{D}_k)$$

Der gemeinsame Gradient für den nächsten Schritt $t+1$ kann nun wie folgt berechnet werden:

$$\omega_{t+1} = \omega_t - \eta_g \sum k \in S_t \frac{n_k}{n_{S_t}} g_t^k$$

Hierbei bezeichnet n_k die Verteilungsfunktion der Daten für den k-ten Teilnehmer und n_{S_t} die Verteilungsfunktion der Daten in der t-ten Runde auf einer zufälligen Teilmenge aller Teilnehmer[2]. η_g ist die übliche Lernrate.
Diese Klasse an Algorithmen findet zum Beispiel in der Erstellung stark verteilter Systeme (zum Beispiel im Internet of Things (IoT)) Anwendung. Dabei ist von einer Restriktion in Performance und Netzwerkbandbreite auszugehen [25]. Beide Probleme, werden durch die Auswahl von Teilmengen aller Teilnehmer S_t und einer entsprechenden Verteilung der Daten n_{S_t} gelöst.

4.3. Minimale Infrastruktur

Man sieht hier auch, dass die Infrastruktur wesentlich flexibler und kostensparender gestaltet werden kann, als für große Machine Learning Modelle sonst üblich. Zum Beispiel wurde für AlphaGo, das erste Machine Learning Modell, dass einen Go-Großmeister schlagen konnte, spezialisierte Hardware entwickelt [9]. Die Skalierbarkeit und Funktionsweise unter heterogenität der Teilnehmer, ist dabei durch die Verteilungsfunktionen der Daten abgesichert. Diese Flexibilität kann auch dazu genutzt werden, um Stromverbrauch und Auslastung zu optimieren.

4.4. Latenzzeiten

Durch die Denzentralisierung des Trainingsvorgangs ist es möglich, Vorhersagen mit deutlich geringerer Latenz und sogar ohne Verbindung zu einem Server zu ermöglichen. Diese, besonders für integrierte Geräte und Smartphones nützliche Eigenschaft, ist eine direkte Konsequenz aus den dezentral trainierten Gewichten. Auch ohne unmittelbare Verbindung zu den anderen Geräten, steht allen Teilnehmern ein Modell zur Verfügung, dass die letzten gemeinsamen Gewichte enthählt und einen Gradienten, der aus der kollaborativen Berechnung stammt.

2. Es nehmen also nicht alle Teilnehmer an jeder Trainingsrunde teil.

Dies ermöglicht Modell-Performace, auf den Niveau eines Großrechners auf integrierten Geräten, welche nicht Permanent an das Internet gekoppelt sind. Der Vorteil wird zum Beispiel and der enormen Fähigkeit des Google-Keyboards deutlich. Hier ist es auf eingebetteten Geräten ohne herausragende Rechenkapazität möglich "state-of-the-art" Machine Learning Voraussagen zu tätigen [17].

4.5. Modell-Leistung

Besonders durch die im Abschnitt 3.4 besprochenen Transfermodelle, ist es möglich wesentlich präziesere Modelle zu liefern, als dies für isolierte oder naive kombinierte Modelle der Fall wäre. Die Kombination aus bekannten Kombinationsmodellen, wie Hierarchischen Bayesianischen Modellen und Federated Learning stellt dabei eine spannende Option dar, durch die die Übertragung und Kombination von Wissen aus unterschiedlichen Teilaspekten eine überlegene Leistung gegenüber einzelnen Modellen liefert [4, 35]. Diese Kombination kann in einigen Bereichen sogar erreicht werden, ohne die hier vorgestellten Kommunikationsprotokolle zu modifizieren [4].
Auch die bereits besprochene Leistungsakkumulation von vielen Leistungs-Heterogenen Teilnehmern, liefert dabei einen Beitrag. Diese Beiträge stellen eine Kombination aus unterschiedlichen Forschungsbereichen dar, die zunehmend an Bedeutung gewinnen [19].

5. Herausforderungen

Die Neuartigkeit des hier diskutierten Ansatzes führt dazu, dass eine Reihe von offenen Problemen existieren. Auch einige konzeptionelle Herausforderungen liefern eine Eingrenzung des Anwendungsgebietes. Die konkreten Punkte sollen in diesem Abschnitt kurz diskutiert werden.

5.1. Datensicherheit und Datenschutz

Durch die Neuartigkeit des Ansatzes, werden für Federated Learning immer wieder neue Angriffsvektoren bekannt [15]. Wir haben in Abschnitt 3 bereits gesehen, dass alle Kategorien von Federated Learning anfällig gegen kollaborierende bïosartige Angreifer sind.
Die Kategorien an Angriffen umfassen interne (aus dem Kreis der Trainierenden Teilnehmer) und externe (also lauschende Angreifer) Angriffe [14]. Auch der Zeitpunkte des Angriffs kann entscheidend sein. So kann nur während dem Training ein aktiver Angreifer die Manipulation der Daten vornehmen. Nach dem Training ist möglicherweise allerdings weiterhin ein Ausspähen der Modell-Parameter und Feature-Beschriftungen durchführbar [14].
Eine zentrale Unterscheidung der Sicherheitsaspekte ist dabei zwischen Angriffen auf die Leistung des Modells (etwa durch gefälsche Daten) und Angriffen auf die Privatsspähre (auch *privacy leakage*) [14]. Während eine Verifikation von korrekten Daten schwierig ist, ohne signifikante Steigerung des Kommunikationsaufwandes, ist ein Schutz der privaten Daten leichter denkbar und wünschenswert. Dies ist nicht zuletzt deswegen ein wichtiges Ziel, weil Federated Learning genau hier einen Vorteil verspricht, indem keiner zentralen Instanz, die ein Modell mit allen Daten trainiert, vertraut werden muss.

5.2. Kommunikation zwischen Nodes

Auf Grund der Tatsache, dass im Federated Learning oft eingebettete und mobile Geräte zum Einsatz kommen, ist die Kommunikation zwischen Teilnehmern besonders relevant. Diese kann durch limitierte Bandbreiten beschränkt sein oder wegen mobilen Verbindungen zeitweise unterbrochen sein. Auf diese Situation müssen sich traditionelle Machine Learning Modelle nicht einstellen. Daher ist dieser Bereich der Algorithmenentwicklung neuartig und Gegenstand aktueller Forschung [11]. Anders als bei vielen traditionellen Machine Learning Modellen muss hier eine sorgfältige Evaluation der Hardwarearchitektur für den Einsatz vorgenommen werden. Dies beeinflusst dann nicht nur die Kommunikation von Modellparametern und Modellparametern während dem Training, sondern auch die Speicherung und Auswertung des Modells zum Vorhersagezeitpunkt [11]. Im Kontext von Datensicherheit entsteht hier ebenfalls eine Einsatzspeziefische Abwägung. Wie bereits zuvor diskutiert, kann das Hinzufügen von statistischem Rauschen zum Schutz der privaten daten beitragen. Dies stellt aber typischerweise einen Mehraufwand an Kommunikation da, der gegen die Verfügbarkeit von Bandbreite zu stellen ist.
Letztendlich ist auch einer Leistungsfähigkeit einzelner Teilnehmer Sorge zu tragen. So können bestimmte, sonst übliche, mathematische Operationen (wie das Berechnen einer Vektornorm) auf bestimmten Geräten unerschwinglich aufwändig sein [11].

5.3. Heterogene Datensätze

Das Vorhandensein von heterogenen Daten ist keine inhärente Einschränkung von Federated Learning Algorithmen, sondern erwächst aus dem Einsatzgebiet. Durch den Fokus auf stark verteilte Datensätze ist es unumgänglich, dass diese in ihrer Struktur nicht homogen sind. Daher ist es für die Entwicklung von Algorithmen in diesem Bereich notwendig auch Methoden für den Umgang mit derartigen Datenbeständen zu finden. Weiterhin können Fehler in Daten auch aus (möglicherweise unabsichtlichem) Fehlerverhalten von Teilnehmern im Trainignsprozess oder der Kommunikation erwachsen. Liefert eine Berechnung auf unterschiedlichen Teilnehmern widersprüchliche Resultate, spricht man von einem Byzantinischen Fehler. Algorithmen, die unter diesem Fehler weiterhin operieren können sind von besonderem Interesse für Federated Learning. Sie laufen unter der Bezeichnung *Byzantine tolerant Algorithms*. Mit Hilfe von Fehlerschranken kann auch unter diesen Voraussetzungen eine Modell-Performance in einem gewissen Intervall garantiert werden [7]. Nichtsdestotrotz bleibt dieser Bereich eine Herausforderung für die Entwicklung von neuen Algorithmen.

6. Anwendungen von Federated Learning

Es gibt bereits zahlreiche Anwendungen im Bereich vom Federated Learning. Personalisierte Produkte erfordern die Auswertung von privaten Daten, zum Beispiel Messdaten der Herzfrequenz einer Smartwatch. Technologische Anwendungen dieser Art bilden das "Internet of things" und umfassen unter anderem smart homes,

wearable devices, autonome Fahrzeuge (all preprints) [21, 24]. Smartphones bieten immer häufiger komplexe Bedienhilfen wie "next work prediction", Gesichtserkennung und Stimmerkennung. Dies sind einfach zu bediendende Operationen, die durch die heterogene Datenlage komplexe Machine Learning Modelle erfordern. In genau diesen Fällen verspricht Federated Learning in der Zukunft mehr Anwendung finden zu finden [3, 8, 22]. All diesen Produkten unterliegt eine delikate Handhabung der persönlichen Kundendaten, Federated Learning bildet demnach eine solide Basis für deren Nutzung.

6.1. GBoard

Speziell die Eingabedaten von Smartphone-Tastaturen haben in den letzten Jahren an Funktionalität gewonnen. Gleichzeitig ist es (rechtlich und technisch) nicht möglich die Rohdaten zu sammeln. Am Beispiel der Google Eingabehilfe, GBoard, kann der erfolgreiche Einsatz von Federated Learning besonders gut beobachtet werden [8]. Die interne Umstellung eines "finite state transducers" auf ein "long term short term memory recurrent neural nerwork", also eine wesentlich moderne und mächtigere Alternative, erforderte hier gleichzeitig mehr Trainignsdaten, als durch einen einzelnen Nutzer möglich wäre. Um trotzdem auf aktuelle Trends in den Eingaben reagieren zu können, bietet sich hier allerdings kein zentral vortrainiertes Netzwerk an. Im Fall von GBoard kann die Sicherheit der persönlichen Daten dabei gewahrt bleiben, indem lokale Modelle trainiert werden, während ein zentraler Server die Kombination, unter Berücksichtigung der heterogenen Eingabedaten, vornimmt [8].

6.2. Gesundheitswesen

Organisationen/Institutionen wie beispielsweise Krankenhäuser erfordern die Speicherung und eventuell Auswertung größer Datenmengen an privater Patienteninformationen. Letztere unterliegen "strict privacy practices". Auch hier ist Federal learning gut mit den lokalen Speicherrestriktionen vereinbar [12]. Weiterhin liegen zunehmend lokalisierte Messdaten aus Smartwatches, Smartphones und anderen Geräten mit entsprechender Sensorik vor. Erste Versuche mit Daten aus Smartwatches, die dezentralisiert trainiert wurden, gibt es bereits [27].
Neben dem Einsatz auf schwachen, lokalen Geräten, gibt es auch das Feld der kooperierenden Unternehmen. Im Vereinigten Königreich laufen bereits erste Tests, in denen Krankenhäuser national kooperieren [17]. Dies ermöglicht im Rahmen der Diagnose, für die IBM bereits seit einigen Jahren Watson im "klassischen" Machine Learning Sektor etabliert hat [29], einen enormen Zuwachs an Daten, die anderweitig auf Grund von Datenschutz nicht zugänglich wären.

6.3. Autonomes Fahren

Das vielleicht offensichtlichste Beispiel für ein Anwendungsfeld von Federated Learning ist das, von selbstfahrenden Autos. Diese, ohnehin schon durch Machine Learning geprägte, Industrie, hat nicht nur die Forschungskapazitäten und ingenieurtechnischen Umsetzungsmöglichkeiten, sondern die eingesetzen Autos verfügen auch über Rechenressourcen, die optimal Anwendungs finden können. Modelle für autonome Bewegung gehören zu den komplexesten Machine Learning Modellen, da sie viele komplizierte Einzelaufgaben vereinen. Dazu gehört Bild- und Bewegungserkennung, Entfernungsmessung, überwachung von interner Sensorik und Kommunikation mit der Umwelt [31]. Es ist nicht möglich auch nur Teile dieser Modelle in einem einzelnen Fahrzeug zu trainieren. Gleichzeitig liegen aber zahlreiche individuelle Datenpunkte vor, die ungenutzt verfallen, wenn die Messdaten von Fahrzeugen nicht in das Gesamtmodell einfließen. Weiterhin sollten die Bewegungsdaten von Personen in keinem Fall ableitbar sein, es liegt also auch, der bereits vielfach diskutierte Datenschutzaspekt vor [31].
Wie auch die gesamte Forschung in Bezug auf autonomes Fahren, befindet sich auch die Anwendung von Federated Learning auf diesen Bereich noch in der Anfangsphase. Zahlreiche Fortschritte in der Forschung lassen allerdings die Vermutung zu, dass Federated Learning in diesem Industriesektor eine zentrale Rolle spielen wird [13].

Literatur

[1] Keith Bonawitz u.a. „Practical Secure Aggregation for Privacy-Preserving Machine Learning". In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. CCS '17. Dallas, Texas, USA: Association for Computing Machinery, 2017, 1175–1191. ISBN: 9781450349468. DOI: 10.1145/3133956.3133982. URL: https://doi.org/10.1145/3133956.3133982.

[2] Keith Bonawitz u.a. „Practical Secure Aggregation for Privacy-Preserving Machine Learning". In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. CCS '17. New York, NY, USA: Association for Computing Machinery, 2017, 1175–1191. ISBN: 9781450349468. DOI: 10.1145/3133956.3133982. URL: https://doi.org/10.1145/3133956.3133982.

[3] Keith Bonawitz u.a. „Towards federated learning at scale: System design". In: *arXiv preprint arXiv:1902.01046* (2019).

[4] Christopher Briggs, Zhong Fan und Peter Andras. *Federated learning with hierarchical clustering of local updates to improve training on non-IID data*. 2020. arXiv: 2004.11791v2 [cs.LG].

[5] W. Du und M. Atallah. „Privacy-Preserving Cooperative Statistical Analysis". In: *Proceedings of the 17th Annual Computer Security Applications Conference*. ACSAC '01. USA: IEEE Computer Society, 2001, S. 102. ISBN: 0769514057.

[6] Wenliang Du, Yunghsiang S. Han und Shigang Chen. „Privacy-Preserving Multivariate Statistical Analysis: Linear Regression and Classification". In: *Proceedings of the 2004 SIAM International Conference on Data Mining*. Society for Industrial und Applied Mathematics, Apr. 2004. DOI: 10.1137/1.9781611972740.21. URL: https://doi.org/10.1137/1.9781611972740.21.

[7] Avishek Ghosh u.a. *Robust Federated Learning in a Heterogeneous Environment*. 2019. arXiv: 1906.06629 [cs.LG]. (Besucht am 23. 05. 2020).

[8] Andrew Hard u.a. „Federated learning for mobile keyboard prediction“. In: *arXiv preprint arXiv:1811.03604* (2018). (Besucht am 20. 05. 2020).

[9] Norm Jouppi. *Google supercharges machine learning tasks with TPU custom chip*. Juni 2017. URL: https://cloud.google.com/blog/products/gcp/google-supercharges-machine-learning-tasks-with-custom-chip (besucht am 25. 05. 2020).

[10] Alan F. Karr u.a. „Privacy-preserving analysis of vertically partitioned data using secure matrix products“. In: *J. Official Statistics* (2009).

[11] Jakub Konečný u.a. „Federated Learning: Strategies for Improving Communication Efficiency“. In: *NIPS Workshop on Private Multi-Party Machine Learning*. 2016. URL: https://arxiv.org/abs/1610.05492 (besucht am 28. 05. 2020).

[12] Tian Li u.a. „Federated learning: Challenges, methods, and future directions“. In: *arXiv preprint arXiv:1908.07873* (2019). (Besucht am 29. 05. 2020).

[13] Xinle Liang u.a. *Federated Transfer Reinforcement Learning for Autonomous Driving*. 2019. arXiv: 1910.06001 [cs.LG]. (Besucht am 29. 05. 2020).

[14] Lingjuan Lyu, Han Yu und Qiang Yang. *Threats to Federated Learning: A Survey*. 2020. arXiv: 2003.02133 [cs.CR]. (Besucht am 15. 05. 2020).

[15] C. Ma u.a. „On Safeguarding Privacy and Security in the Framework of Federated Learning“. In: *IEEE Network* (2020), S. 1–7.

[16] Bernard Marr. *forbes.com*. Feb. 2016. URL: https://www.forbes.com/sites/bernardmarr/2016/02/19/a-short-history-of-machine-learning-every-manager-should-read/#4fd175cc15e7 (besucht am 19. 05. 2020).

[17] Brendan McMahan und Daniel Ramage. *Federated Learning: Collaborative Machine Learning without Centralized Training Data*. Apr. 2017. URL: https://ai.googleblog.com/2017/04/federated-learning-collaborative.html (besucht am 16. 05. 2020).

[18] Brendan McMahan u.a. „Communication-Efficient Learning of Deep Networks from Decentralized Data“. In: *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, AISTATS 2017, 20-22 April 2017, Fort Lauderdale, FL, USA*. Hrsg. von Aarti Singh und Xiaojin (Jerry) Zhu. Bd. 54. Proceedings of Machine Learning Research. PMLR, 2017, S. 1273–1282. URL: http://proceedings.mlr.press/v54/mcmahan17a.html.

[19] T. Nishio und R. Yonetani. „Client Selection for Federated Learning with Heterogeneous Resources in Mobile Edge“. In: *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*. 2019, S. 1–7.

[20] S. J. Pan und Q. Yang. „A Survey on Transfer Learning“. In: *IEEE Transactions on Knowledge and Data Engineering* 22.10 (2010), S. 1345–1359.

[21] Alexandros Pantelopoulos und Nikolaos G Bourbakis. „A survey on wearable sensor-based systems for health monitoring and prognosis“. In: *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)* 40.1 (2009), S. 1–12.

[22] Swaroop Ramaswamy u.a. „Federated learning for emoji prediction in a mobile keyboard“. In: *arXiv preprint arXiv:1906.04329* (2019). (Besucht am 20. 05. 2020).

[23] Stuart Russell und Peter Norvig. *Artificial Intelligence: A Modern Approach*. 3rd. USA: Prentice Hall Press, 2009. ISBN: 0136042597.

[24] Sumudu Samarakoon u.a. „Distributed federated learning for ultra-reliable low-latency vehicular communications“. In: *IEEE Transactions on Communications* (2019).

[25] S. Savazzi, M. Nicoli und V. Rampa. „Federated Learning With Cooperating Devices: A Consensus Approach for Massive IoT Networks“. In: *IEEE Internet of Things Journal* 7.5 (2020), S. 4641–4654.

[26] Virginia Smith u.a. „Federated Multi-Task Learning“. In: *CoRR* abs/1705.10467 (2017). arXiv: 1705.10467. URL: http://arxiv.org/abs/1705.10467 (besucht am 29. 05. 2020).

[27] Fabian Stieler, Fabian Rabe und Bernhard Bauer. „Federated medical data - how much can deep learning models benefit?“ In: *AMIA 2020 Virtual Clinical Informatics Converence, May 19-21*. 2020.

[28] Lili Su und Jiaming Xu. „Securing Distributed Machine Learning in High Dimensions“. In: *CoRR* abs/1804.10140 (2018). arXiv: 1804.10140. URL: http://arxiv.org/abs/1804.10140 (besucht am 29. 05. 2020).

[29] Clive Thompson. *What Is I.B.M.'s Watson?* Juni 2010. URL: https://www.nytimes.com/2010/06/20/magazine/20Computer-t.html (besucht am 01. 06. 2020).

[30] Chang Wang und Sridhar Mahadevan. „Heterogeneous Domain Adaptation Using Manifold Alignment“. In: *Proceedings of the Twenty-Second International Joint Conference on Artificial Intelligence - Volume Volume Two*. IJCAI'11. Barcelona, Catalonia, Spain: AAAI Press, 2011, 1541–1546. ISBN: 9781577355144.

[31] Simon Fabian Wolf. *Federated Learning*. März 2019. URL: https://blog.mi.hdm-stuttgart.de/index.php/2019/02/28/federated-learning/ (besucht am 03. 06. 2020).

[32] Qiang Yang u.a. *Federated Machine Learning: Concept and Applications*. Jan. 2019. DOI: 10.1145/3298981.

[33] Xin Yao u.a. *Federated Learning with Unbiased Gradient Aggregation and Controllable Meta Updating*. 2019. arXiv: 1910.08234 [cs.LG]. (Besucht am 15. 05. 2020).

[34] J. Yuan und S. Yu. „Privacy Preserving Back-Propagation Neural Network Learning Made Practical with Cloud Computing“. In: *IEEE Transactions on Parallel and Distributed Systems* 25.1 (2014), S. 212–221.

[35] Mikhail Yurochkin u.a. *Bayesian Nonparametric Federated Learning of Neural Networks*. 2019. arXiv: 1905.12022 [stat.ML]. (Besucht am 28. 05. 2020).

[36] Yin Zhu u.a. „Heterogeneous Transfer Learning for Image Classification“. In: *Proceedings of the Twenty-Fifth AAAI Conference on Artificial Intelligence*. AAAI'11. San Francisco, California: AAAI Press, 2011, 1304–1309.

[37] Rolin Zumeran. *openlegacy.com*. Juni 2017. URL: https://www.openlegacy.com/blog/the-history-of-apis-and-how-they-impact-your-future (besucht am 23. 05. 2020).