Privacy-preserving Machine Learning on Distributed Devices

Studiengang: BSc in Elektrotechnik und Informationstechnologie | Vertiefung: Embedded Systems
Betreuer*in: Prof. Dr. Angela Meyer

Im Zentrum von machine learning Applikationen stehen immer Datensätze, in welchen ein statistischer Zusammenhang erkannt werden soll. Deshalb ist das Sammeln von Daten ein grosser Bestandteil jedes Projekts. Je nach Typ der Daten, die gesammelt werden sollen, ist das Verletzen der Privatsphäre von Personen ein grosses Problem. Mithilfe von federated learning kann dieses Problem umgangen werden.

Ausgangslage

Machine learning Lösungen werden immer häufiger für das Lösen verschiedenster Probleme eingesetzt. Mit der heute zur Verfügung stehenden Rechenleistung und der grossen Anzahl generierter Daten, findet ein Konzept, das ursprünglich in den 60er Jahren entwickelt wurde, grossen Anklang. Die Einsatzmöglichkeiten sind fast unbegrenzt. Im Zentrum stehen aber immer gesammelte Daten, aus welchen ein statistischer Zusammenhang erkannt werden soll. Somit ist der erste Schritt eines machine learning Projekts üblicherweise das Sammeln von Daten. Ein Ansatz die Privatsphäre der Daten nicht zu verletzen ist das sogenannte federated learning (Föderales Lernen). Damit kann ein machine learning Modell trainiert werden, ohne die Trainingsdaten an einem zentralen Ort zu verarbeiten. Somit bleiben die privaten Daten auf den Geräten der Benutzer und die Privatsphäre ist gewährleistet. Die Schwierigkeit besteht in der Heterogenität der Daten. Konventionellen machine learning Algorithmen, welche dezentral lernen gehen von identisch verteilten und homogenen Datensätzen aus. Dies ist aber nur gewährleistet, wenn ein globales Datenset erstellt und auf die dezentralen Geräte verteilt werden kann. Wenn die Daten das Gerät des Benutzers nicht verlassen sollen, muss der Algorithmus heterogenen Datensätze verarbeiten können.

Konzept

Ein proof of concept eines federated learning Modell wird mithilfe der Tensorflow Bibliothek realisiert. Es wird ein neuronales Netzwerk entwickelt, welches aus einem Datensatz von Windkraftanlagen das Erstellen einer typischen power curve lernt. Die power curve beschreibt das Verhältnis zwischen der Windgeschwindigkeit und der Leistungsabgabe einer Windkraftturbine. Der Datensatz beinhaltet Messungen von 40 Windkraftturbinen über einen Zeitraum von 2 Jahren. Die Daten werden behandelt als würden sie nur auf jeder der einzelnen Turbinen lokal zur Verfügung stehen. Der federated Leraning Algorithmus läuft folgendermassen ab:

- Ein zentraler Server verteilt das aktuelle Modell an die Clients.
- Die Clients trainieren das Modell mit ihren lokalen Daten.
- Sie senden das trainierte Modell zurück an den Server.
- Der Server fügt alle trainierten Modelle zu einem zusammen und verteilt dieses wieder an die Clients.

Dieser Ablauf wird wiederholt, bis das Modell die gewünschte Funktion gelernt hat. Zur Analyse der federated learning Technologie wird auch ein konventionelles zentrales Modell aufgebaut, welchen mit Daten von nur einer Turbine trainiert wird. So kann ein direkter Vergleich der Technologien gemacht werden.

Resultate

Ein Modell wurde zuerst mithilfe von konventionellen Technologien und anschliessend mit der federated learning Technologie trainiert. In beiden Fällen konnte die power curve trainiert und rekonstruiert werden.

Vergleich

Weil die dezentralen Geräte nur simuliert sind, werden die Berechnungen zentral und seriell ausgeführt. Deshalb dauert das Trainieren mit der federated Learning Technologie bedeutend länger. Um die Vorteile des federated learning aufzuzeigen, wurde das Datenset verkleinert, indem nur Daten von einer Woche verwendet wurden. In diesem Fall ist das Datenset des konventionellen Modells zu klein und die power curve kann nicht rekonstruiert werden. Mit der federated learning Technologie stehen aber die Datensätze aller Turbinen zur Verfügung und die power curve konnte rekonstruiert werden.

Lorin Alexander Jenkel