

Travail de lecture et de rédaction scientifique sur le  
Federate Learning

Bal Sébastien

3 août 2021

## Remerciements

# TABLE DES MATIÈRES

<b>1</b>	<b>Concepts</b>	<b>1</b>
1.1	Machine Learning . . . . .	1
1.2	Deep Learning . . . . .	3
1.2.1	Modèle d'entraînement . . . . .	4
1.3	Federated Learning . . . . .	5
<b>2</b>	<b>Technologies existantes (Framework)</b>	<b>7</b>
2.0.1	TensorFlow Federated (TFF) . . . . .	7
2.0.2	Federated AI Technology Enabler (FATE) . . . . .	7
<b>3</b>	<b>Catégorisation</b>	<b>8</b>
3.0.1	Horizontal FL . . . . .	8
3.0.2	Vertical FL . . . . .	9
3.0.3	Federated Transfer Learning (FTL) . . . . .	10
<b>4</b>	<b>Exemples d'utilisations</b>	<b>11</b>
4.0.1	La Finance . . . . .	11
4.0.2	La santé . . . . .	12
<b>A</b>	<b>Annexe</b>	<b>15</b>

## 1.1 Machine Learning

Le Machine Learning appelé en Français apprentissage automatique "[...] est un champ d'étude de l'intelligence artificielle qui se fonde sur des approches mathématiques et statistiques pour donner aux ordinateurs la capacité d'apprendre à partir de données[...]". Ceci a pour objectif de traiter l'information afin de lui donner de la valeur ajoutée.

De nos jours, le Machine Learning est présent partout sur la toile, cela va du moteur de recherche comme Google, aux assistants vocaux comme Siri et Alexa, les fil d'actualités des réseaux sociaux comme Facebook et Twitter. Le point commun entre toutes ces plateformes et le stockage massif des données de leur utilisateur appelé Big Data [x : ?]. Le Big Data est une technologie apparue dans les années 1900, a permis l'essor de l'apprentissage automatique, le Machine Learning. En effet, cet imposant volume de données collectées sur les utilisateurs a permis, dans les exemples cités ci dessus, de mieux cibler le comportement des utilisateurs et ainsi améliorer les expériences.

Pour fonctionner, le Machine Learning (ML) a besoin de données à ingérer et d'avoir un modèle appris afin de fournir des données à valeur ajoutée comme des algorithmes de prédiction de bourse et la maintenance prédictive. Il est donc nécessaire d'identifier les approches techniques pour créer ces modèles de ML.

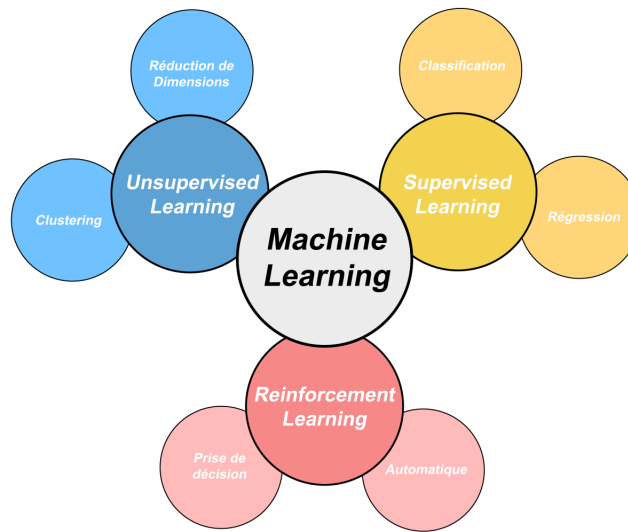


FIGURE 1.1: Familles d'algorithmes les plus utilisés

La première famille, l'apprentissage supervisé (en jaune dans la figure 1.1) consiste à donner des données en entrées, le résultat attendu itéré sur un grand jeu de données afin de trouver le modèle. Pour que le modèle devienne performant, on fournit un grand volume de données dans le but qu'il se rapproche du modèle attendu. Ce type de modèle nécessite donc une bonne connaissance du processus métier vu qu'il est nécessaire de fournir des jeux de données en entrée et le résultat désiré. Ce type d'algorithme est donc souvent utilisé pour simplifier ou optimiser des solutions existantes.

Dans un exemple, en prenant un Input ????????

La deuxième famille, l'apprentissage non-supervisé (en bleu dans la figure 1.1) consiste à apprendre par identification des ressemblances et des différences entre les données fournies. L'algorithme rassemble les données en groupe ce qui permet lors de l'intégration d'une nouvelle information de la classer dans un des groupes existants très rapidement. Ce type d'exemple a souvent pour objectif de créer des arbres de décisions sur base de "clustering".

Pour finir, il existe une catégorie qui gère sa propre expérience. En effet, l'apprentissage par renforcement (en rouge dans la figure 1.1) consiste à générer ses propres expériences. On se rapproche de l'automobile autonome, la machine change ses états suivant les actions qu'elle entreprend de faire. Un système de récompense positive et négative est mis en place pour constituer une nouvelle expérience et rendre la machine attentive pour maximiser ses chances de réussite. Ce type d'approche est la plus générique, elle

convient aussi bien pour optimiser des solutions existantes que pour classer des données. En règle générale, cette approche est souvent utilisée pour des recherches exploratoires. L'inconvénient principal de cette approche scientifique est son besoin de ressources. En effet, les combinaisons peuvent très vite être importantes et par conséquent, l'exploration aura besoin de temps ou de ressources physiques pour les tester.

Pour conclure, le ML est une technologie qui vise à trouver des modèles, comprendre des comportements afin de prédire les besoins d'une application suivant un besoin.

On peut constater que ce type de besoin se focalise sur une application spécifique cependant, le ML connaît des limites au niveau des complexités combinatoire [x : ], or certaines applications nécessitent des applications plus complexes avec plus d'entrées, tels que le traitement des images. Pour palier aux limites du ML, le Deep Learning a vu son essor [x : lien vers essor DL]

## 1.2 Deep Learning

Le Deep Learning(DL) est représentatif d'un système neuronal comme notre système cérébral, il est conçu de plusieurs neurones qui interagissent entre eux. Pour rendre performant tous ces neurones, il est nécessaire d'avoir une grande quantité de données, un Data Lake. Celui-ci fournit au système plusieurs informations afin de lui constituer une "mémoire". Cette mémoire lui permet de reconnaître des éléments bien particuliers suivant l'entraînement qu'il aura suivi. Cet entraînement est supervisé par des développeurs qui vérifient que le DL ne sort pas de son modèle défini. Si il s'en éloigne, ils corrigent son algorithme mathématique pour le rendre plus performant et le remettre sur le droit chemin. Pour que le modèle mathématique devienne performant, il faudra l'entraîner à reconnaître une donnée en particulier. C'est le sujet de notre prochaine section.

### 1.2.1 Modèle d'entraînement

Pour entraîner le DL, il lui faut un algorithme mathématique et un grand flux de données afin d'affiner ses recherches et prendre de l'expérience. Dans notre situation, on décide de prendre la reconnaissance d'une image, en particulier celle d'un chat. On fournit à l'algorithme un flux d'images de plusieurs espèces d'animaux, on définit les paramètres qui permettent d'affirmer que l'image que l'on soumet soit bien un chat. Ainsi avec ces critères, l'algorithme devient plus précis car on le guide un peu sur l'objectif qu'il doit atteindre.

Voici un schéma pour l'exemple du fonctionnement du DL, [fig2.1], les boules vertes représentent le bon chemin que le système va prendre pour arriver à vérifier le modèle qui était demandé. Les boules bleues sont celles qui ont des caractéristiques avec le modèle mais ne correspondra pas exactement au modèle qui était demandé. Les boules rouges quand à elles, représentent les erreurs que le système a exclu pour pouvoir apprendre le modèle exacte. Les erreurs sont par la suite renvoyées en amont du système pour que le système ajuste son modèle mathématique

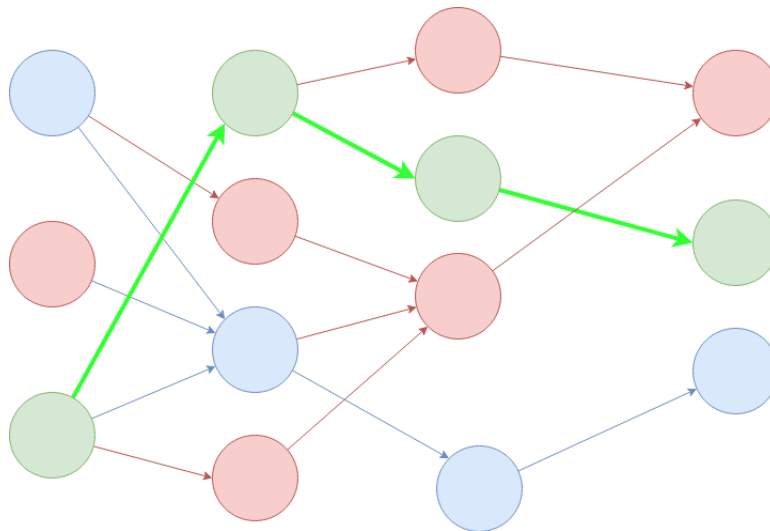


FIGURE 1.2: Autoapprentissage Deep Learning

On peut constater que ce type d'algorithme peut être très vite devenir énergivore. De plus, le DL se focalise principalement sur une application. Or, il peut être intéressant d'étudier plusieurs applications similaires afin d'identifier des modèles plus poussés. C'est dans ce contexte que nous allons introduire le Federated Learning.

## 1.3 Federated Learning

Notre époque fait face à deux défis importants en terme d'avancer technologique :

1- les respects de la vie privée. L'une des plus importantes est celle de la privatisation de ces données sur le web. Avec la protection des données (RGPD) promulgué en 2018, les données privées font entièrement partie de l'utilisateur, ces données ne peuvent pas être utilisés sans son accord.

2- L'union fait la force, or, le traitement en silo des données de chaque entreprise freine énormément l'évolution des apprentissages de machine learning. En effet, en partageant les données entre différents secteurs, les algorithmes pourraient s'enrichir d'autre contexte afin de prendre de meilleures décisions en fonction du besoin de chaque application.

3- « Sans connaissance de son audience, et sans hypothèses préalables solides, la Big data ne sert à rien. » Benjamin Mercier, Responsable Digital Analytics, met en avant l'importance de la collecte des données. La masse d'information nécessaire pour obtenir des apprentissages de qualité demande beaucoup de rigueur et d'expérience dans le domaine ciblé. Par exemple, comme précise l'article BLABLABLA, le secteur de BLABLABLA ne dispose pas de BLABLABLA

C'est grâce au Federated Learning (FL) que l'essor de l'industrie a relevé ces défis. Le FL est un processus d'apprentissage automatique qui vise à exploiter les îlots de données tout en gardant la sécurité des données. Des clients sont coordonnés avec un ou plusieurs serveurs pour faciliter une décentralisation d'un apprentissage automatique tel une architecture étoile.

Le FL est basé sur les deux concepts que nous avons vu précédemment le Machine Learning et le Deep Learning.

Les différents algos de ML et le DL effectuent des calculs basés sur leurs données de leur application. L'objectif du FL est de pouvoir agréger des informations de diverses applications, ou de différents acteurs afin de générer un modèle plus abouti. Cette centralisation des données se fait généralement à l'aide d'un serveur centralisé comme le présente le schéma XXX de l'architecture des téléphones fig 4 avec comme exemple la collecte de données de smartphone :-D SCHEMA!!!

La pseudonymisation est donc un élément crucial pour le FL. L'article XXX met en avant telle ou telle techno avec tel ou tel avantage (BON CHANCE!!!)

Le traitement distribué met en place plusieurs appareils connectés à différents endroits via un réseau de communication sous la surveillance d'un serveur central afin d'effectuer une partie de la même tâche pour l'accom-



plir. Le modèle distribué vise à améliorer l'étape de traitement comparé au FL qui lui se base sur un modèle collaboratif afin d'éviter des fuites de confidentialité.

Pour mieux comprendre son fonctionnement, le FL se déroule en plusieurs étapes, la formation fédérée est celle qui est la plus courante. Pour commencer, un appareil mobile se procure un modèle afin d'acquérir les données et les traiter en local. En second lieu, le modèle est mis à jour de multiples fois à jours régulières en local afin d'être amélioré, celles-ci contiennent des données locales qui appartiennent à différents appareils séparés. Ensuite, les appareils mobiles téléchargent des informations d'un champ de vecteurs présent dans un cloud. En troisième lieu, les modèles locaux effectuent une mise à jour moyenne au sein du cloud et est envoyé à un appareil défini comme le modèle mondial renouvelé. Pour finir, ces étapes précédentes se répètent afin d'arriver à un modèle avec une certaine performance ou qu'une date limite soit atteinte.

Le FL est capable de traiter des données partitionnées horizontalement suivant des échantillons mais aussi de façon verticale suivant les caractéristiques du modèle d'apprentissage.

En quelques mots, c'est un apprentissage automatique distribué qui permet d'entraîner un modèle mathématique avec un large groupe de données décentralisées qui se trouvent sur des appareils distants.

## TECHNOLOGIES EXISTANTES (FRAMEWORK)

### **2.0.1 TensorFlow Federated (TFF)**

Les frameworks ne manquent pas pour manipuler des modèles mathématique et les implémenter pour du ML. Le framework TensorFlow Federated en est un qui est totalement openSource. Il permet aux développeurs de simuler des algorithmes d'apprentissage sur leur modèles et bien entendu tester de nouveau algorithmes. Le TFF est constitué d'un environnement d'exécution de simulation dans lequel on peut simulé nos algorithmes, celle ci est utilisée par une seule machine dédiée aux tests.

### **2.0.2 Federated AI Technology Enabler (FATE)**

## CATÉGORISATION

Le FL est caractérisé par trois grands groupes qui surviennent régulièrement, ceux ci sont le FL Horizontal, le FL vertical et le Federated Transfer Learning. Les données stockées sont placées dans différents noeuds, celles ci sont sous forme de matrice de caractéristiques. Les données sont composées de multiples instances, la partie horizontale est représentée comme un client, celle verticale se caractérise par les caractéristiques du client. Pour finir, on peut séparer le FL suivant le mode de partition des données.

### 3.0.1 Horizontal FL

Pour celui du FL Horizontal, des chevauchements peuvent apparaitrent entre les caractéristiques des données qui sont réparties sur différents noeuds, malgré le fait que les données ne sont pas semblables sur l'espace d'échantillonnage. Les données du point de vue de l'échantillonnage sont différentes dans les scénarios des appareils connecté à Internet et les appareils intelligents. Mais ils sont particulièrement similaire dans un espace de fonctionnalité. Les mises à jours, comme nous l'avons vu précédement dans le point du FL, celle si est faite de façon horizontal. En effet, la dimension d'entité est la même pour chaque données. Dans les applications médicales, une forte hausse de travail est nécessaire pour collecté un grand nombre de données. Car il est difficile voir inconcevable pour chaque hôpital de créer une banque de données à partager. Via un réseau fédéral pour les hôpitaux construit par le FL permet d'améliorer le modèle(voir Fig 3.1).

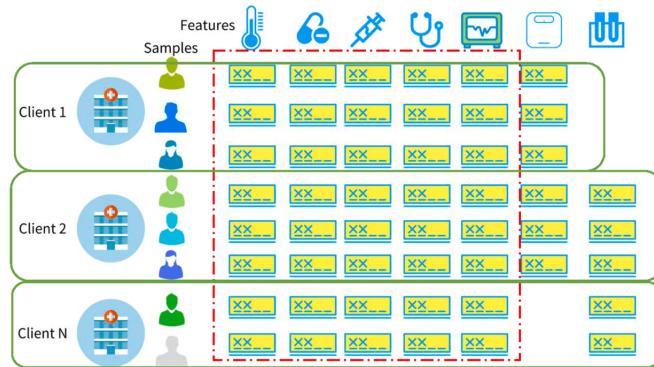


FIGURE 3.1: Horizontal FL

### 3.0.2 Vertical FL

Lorsque les données sont partitionnées, le FL vertical est plus approprié, chaque parties contient des données homogènes. Ce qui implique que les chevauchement se font en partie sur l'ID de l'échantillon alors qu'elle est différente dans l'espace fonctionnel. Prenons le cas d'un établissement médical, ils souhaitent identifier des maladies telles que le diabète. Il peut être analysé suivant certaines dimensions comme l'âge, le poids et les antécédents médicaux le type de diabète qu'un patient peut avoir. Avec le FL, certaines applications possèdent des données comme le nombre de pas ou la composition des plats qu'un personne a. Ces données peuvent être utilisées pour faciliter cette reconnaissance. La figure 3.2 illustre très bien le FL vertical.

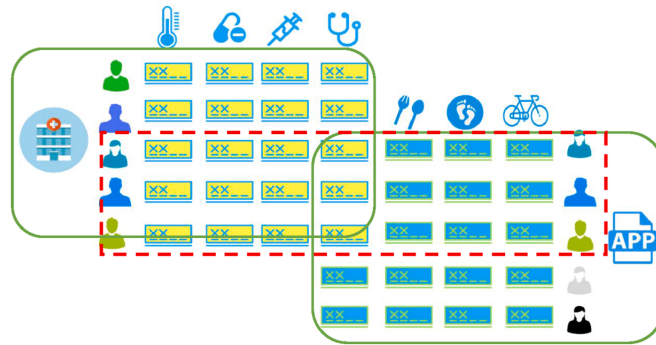


FIGURE 3.2: Vertical FL

### 3.0.3 Federated Transfer Learning (FTL)

En comparaison des deux scénarios vu précédemment, dans la plupart des situations, sur les espaces d'échantillonnage et d'espace d'entité les données n'y sont pas partagées. Ce qui implique un manque d'étiquette et une mauvaise qualité des données. Le principe du FTL est transférer les données d'un domaine vers un autre afin de réaliser de meilleurs résultats d'apprentissage. Ainsi, le FTL permet d'avoir une application étendue pour ce qui est de parties communes avec des intersections étroites. Pour un système de réseaux de neurones qui possèdent une technologie de cryptage homomorphe peut empêcher des fuites de confidentialités mais aussi garder une très bonne précision.

Dans le cadre d'une application avec le modèle FedHealth rassemble un packet de données qui appartiennent à des organisations différentes via FL et permet d'avoir un service personnalisé pour des soins de santé. Sur la Fig 3.3, des informations sur le diagnostic et le traitement de certaines maladies peuvent être partagées avec un autre hôpital dans le but de faciliter des diagnostics. Les problèmes qui surviennent à l'heure actuelle dans le milieu de l'industrialisation sont les îlots de données et la protection de la vie privée mais avec le FTL, celui ci permet d'avoir un service de sécurité fiable pour la protection des données et la confidentialité des utilisateurs tout en cassant les barreaux des îlots de données.

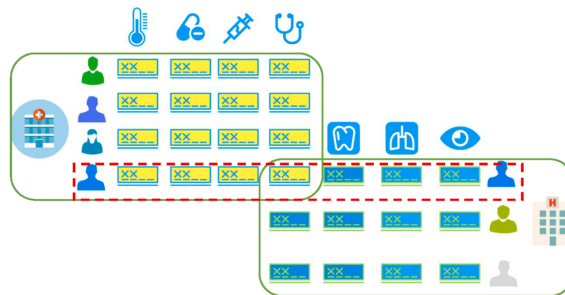


FIGURE 3.3: FTL

## EXEMPLES D'UTILISATIONS

Dans notre société, le FL peut être un atout majeur pour plusieurs secteurs comme la finance, les soins de santé et l'éducation. Plusieurs applications qui peuvent faciliter les employeurs dans leur travail de tous les jours ou encore aider à la reconnaissance de certaines maladies et bien entendu aider nos têtes blondes pour améliorer et faciliter leur apprentissage pour qu'ils deviennent les hommes et les femmes de demain. Beaucoup de possibilités et pour se faire, un aperçu des ses applications dans lesquels il est possible d'utiliser le FL.

Les deux problèmes qui surgissent sont la protection de la vie privée et la sécurité des données

### 4.0.1 La Finance

Le secteur de la finance est très important avec des réglementations gouvernementales pour la protection des investisseurs contre la fraude et la mauvaise gestion, conserver la confidentialité et la sécurité des données des utilisateurs. Dans le but de réduire les coûts et la charge de travail, des sociétés bancaires et financières exploitent les technologies modernes comme l'IA, les services de cloud et la technologie sur les téléphone mobile pour assurer un service financier de qualité tout en respectant les réglementations gouvernementales. Un cas bien particulier est le financement intelligent à la consommation, son objectif vise à prendre parti des techniques de ML afin de proposer des services financiers propre à chacun. Les données utilisées dans un crédit à la consommation sont fait d'informations sur les consommateurs comme le pouvoir d'achat, la préférence d'achat et aussi les caractéristiques du produit. Ces données peuvent être utilisée par diversses entreprises ou sociétés. Ainsi dans la figure 4.1, les informations de qualifications et le pou-

voir d'achat peuvent être déduit de son épargne bancaire et de sa préférence d'achat sur des produits ou services. On fait face dans notre exemple à deux problèmes. Le premier est la protection de la vie privée des consommateurs et la sécurité des données barrière entre les banques, les réseaux sociaux, les sites d'e-commerce. Le deuxième, ce sont le stockages des données par trois sections hétérogènes, ce qui empêche le ML classique de fonctionner sur ces données hétérogènes. C'est pour cette raison que le FL résout ces problèmes. Le FL peut scinder les données en trois parties sans exposer les données. On peut aussi utiliser l'apprentissage par transfert pour examiner les données hétérogènes.

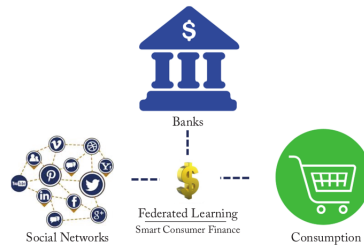


FIGURE 4.1: FL dans une petite entreprise financière

## 4.0.2 La santé

Dans le domaine médical l'intervention de l'IA peut aider à réduire les coûts et les erreurs humaines dans les hôpitaux. En effet, un programme développé pour la diologie et la radiologie permet d'aider à poser un diagnostic sur des maladies cardiaques et identifier des cellules du cancer dans les premiers stades. Avec ces applications encourageantes de l'IA, beaucoup de fournisseurs de soins de santé tirent parti de l'IA pour augmenter l'efficacité et améliorer les soins pour les patients. Cependant, l'utilisation de cette technologie n'en est qu'à ses débuts car il est déjà arrivé des erreurs suites à un mauvais diagnostic. Le plus gros problème dans ce domaine est la quantité d'informations suffisantes pour diagnostiquer précisément des symptômes sur un patient. Par exemple pour diagnostiquer un rhume, il faut plusieurs caractéristiques provenant de différentes sources, ainsi que les symptômes de la maladie.

C'est pour cette raison, que les institutions médicales doivent partagé leur données en respectant les règles de la protection de la vie privée. Par après, on peut former un grand ensemble de données qui fonctionne bien mieux que des données provenant d'un seul établissement. Si on fusionne le FL et l'apprentissage par transfert, cela promet une bonne solution pour

réaliser cet objectif. L'apprentissage fédéré permet de former un modèle partager sans exposition et échange de données propre à un patient. Ensuite, les techniques d'apprentissage par transfert aide à élargir l'échantillonnage et améliore les performances de partages des données. Pour terminer, l'apprentissage par transfert joue un rôle considérable pour le développement des systèmes médicaux. Si plusieurs institutions médicales établissent une bonne base de données grâce à l'apprentissage fédéré, l'avenir de l'IA dans le domaine de la santé peut avoir un net avantage sur les maladies.



## BIBLIOGRAPHIE

- [1] Leslie Lamport, *LaTeX : A Document Preparation System*. Addison Wesley, Massachusetts, 2nd Edition, 1994.
- [2] Li Li, Fan de Yuxi, Mike Tse, Kuo-Yi Lin, *LaTeX : A review of applications in federated learning*. Computers and Industrial Engineering, Volume 149, November 2020, 106854
- [3] Qiang Yang, Yang Liu, Yong Cheng, Yan Kang, Tianjian Chen, Han Yu *LaTeX : Federated Learning, Synthesis Lectures on Artificial Intelligence and Machine Learning*. Ronald J. Brachlan, Francesca Rossi and Peter Stone, Morgan and Claypool publishers, Series Editors December 2019
- [4] Pour la partie sur le Machine Learning  
<https://www.lebigdata.fr/machine-learning-et-big-data>

---

ANNEXE

**A**

---

ANNEXE

---

# TOWARDS FEDERATED LEARNING AT SCALE: SYSTEM DESIGN

---

Keith Bonawitz<sup>1</sup> Hubert Eichner<sup>1</sup> Wolfgang Grieskamp<sup>1</sup> Dmitry Huba<sup>1</sup> Alex Ingerman<sup>1</sup> Vladimir Ivanov<sup>1</sup>  
 Chloé Kiddon<sup>1</sup> Jakub Konečný<sup>1</sup> Stefano Mazzocchi<sup>1</sup> H. Brendan McMahan<sup>1</sup> Timon Van Overveldt<sup>1</sup>  
 David Petrou<sup>1</sup> Daniel Ramage<sup>1</sup> Jason Roselander<sup>1</sup>

## ABSTRACT

Federated Learning is a distributed machine learning approach which enables model training on a large corpus of decentralized data. We have built a scalable production system for Federated Learning in the domain of mobile devices, based on TensorFlow. In this paper, we describe the resulting high-level design, sketch some of the challenges and their solutions, and touch upon the open problems and future directions.

## 1 INTRODUCTION

Federated Learning (FL) (McMahan et al., 2017) is a distributed machine learning approach which enables training on a large corpus of decentralized data residing on devices like mobile phones. FL is one instance of the more general approach of “bringing the code to the data, instead of the data to the code” and addresses the fundamental problems of privacy, ownership, and locality of data. The general description of FL has been given by McMahan & Ramage (2017), and its theory has been explored in Konečný et al. (2016a); McMahan et al. (2017; 2018).

A basic design decision for a Federated Learning infrastructure is whether to focus on asynchronous or synchronous training algorithms. While much successful work on deep learning has used asynchronous training, e.g., Dean et al. (2012), recently there has been a consistent trend towards synchronous large batch training, even in the data center (Goyal et al., 2017; Smith et al., 2018). The Federated Averaging algorithm of McMahan et al. (2017) takes a similar approach. Further, several approaches to enhancing privacy guarantees for FL, including differential privacy (McMahan et al., 2018) and Secure Aggregation (Bonawitz et al., 2017), essentially require some notion of synchronization on a fixed set of devices, so that the server side of the learning algorithm only consumes a simple aggregate of the updates from many users. For all these reasons, we chose to focus on support for synchronous rounds, while mitigating potential synchronization overhead via several techniques we describe subsequently. Our system is thus amenable to running large-batch SGD-style algorithms as well as Feder-

ated Averaging, the primary algorithm we run in production; pseudo-code is given in Appendix B for completeness.

In this paper, we report on a system design for such algorithms in the domain of mobile phones (Android). This work is still in an early stage, and we do not have all problems solved, nor are we able to give a comprehensive discussion of all required components. Rather, we attempt to sketch the major components of the system, describe the challenges, and identify the open issues, in the hope that this will be useful to spark further systems research.

Our system enables one to train a deep neural network, using TensorFlow (Abadi et al., 2016), on data stored on the phone which will never leave the device. The weights are combined in the cloud with Federated Averaging, constructing a global model which is pushed back to phones for inference. An implementation of Secure Aggregation (Bonawitz et al., 2017) ensures that on a global level individual updates from phones are uninspectable. The system has been applied in large scale applications, for instance in the realm of a phone keyboard.

Our work addresses numerous practical issues: device availability that correlates with the local data distribution in complex ways (e.g., time zone dependency); unreliable device connectivity and interrupted execution; orchestration of lock-step execution across devices with varying availability; and limited device storage and compute resources. These issues are addressed at the communication protocol, device, and server levels. We have reached a state of maturity sufficient to deploy the system in production and solve applied learning problems over tens of millions of real-world devices; we anticipate uses where the number of devices reaches billions.

---

<sup>1</sup>Google Inc., Mountain View, CA, USA. Correspondence to: Wolfgang Grieskamp <wgg@google.com>, Vladimir Ivanov <vlivan@google.com>, Brendan McMahan <mcma-han@google.com>.