Apprentissage fédéré

Vers du Deep Learning plus respectueux de la vie privée ?

UNIVERSITÉ DE LYON

ÉCOLE CENTRALELYON

Plan de l'oral

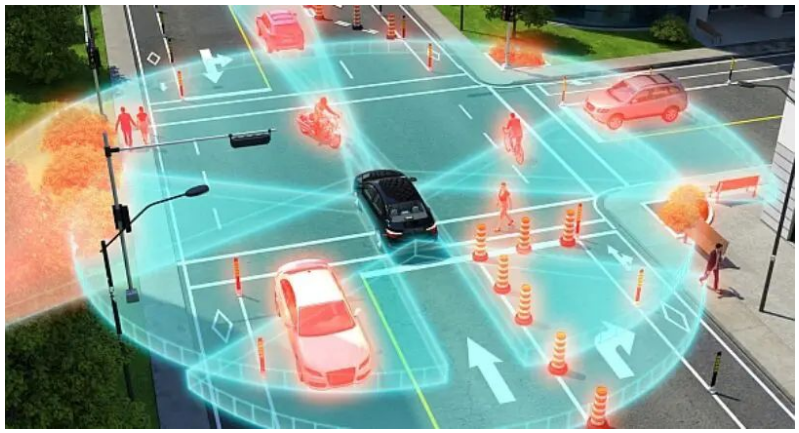
1. Données décentralisées, que faire ?
2. Introduction à l'apprentissage fédéré
3. Etude de cas : Google GBoard
4. Vraiment respectueux de la vie privée ?
5. Pistes d'améliorations du secteur

1.
Données décentralisées, que faire ?

I. Données décentralisées, que faire ?

Pourquoi des données décentralisées ?

→ Omniprésence d'appareils connectés

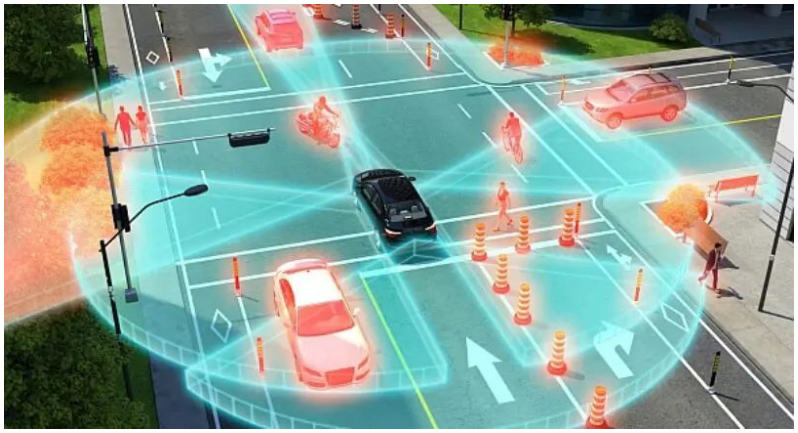


ÉCOLE CENTRALELYON

I. Données décentralisées, que faire ?

Pourquoi des données décentralisées ?

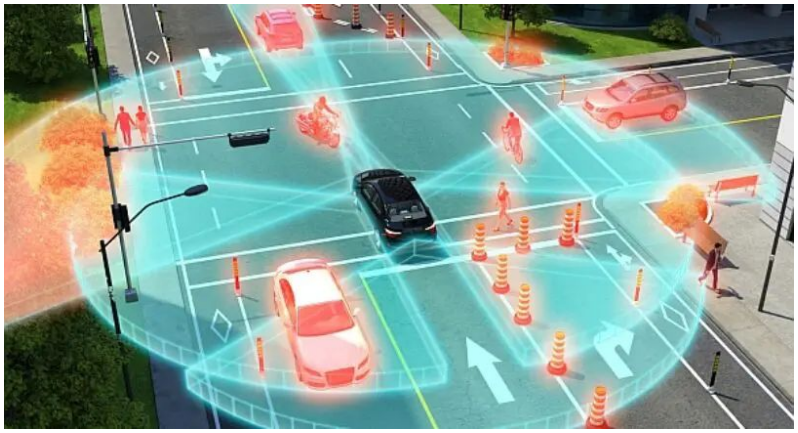
- ➔ Omniprésence d'appareils connectés
- ➔ Beaucoup de données générées (1h de véhicule connecté ~ 25go)
- ➔ Données éparpillées chez les clients finaux
- ➔ Sensible par nature



I. Données décentralisées, que faire ?

Quelles sont ces données décentralisées ?

- ➔ Texte des SMS, photos de la galerie, localisation d'un téléphone
- ➔ Données d'utilisation d'applications, enregistrements de la voix "dis Siri"
- ➔ Données LIDAR ou caméra
- ➔ Données médicales



I. Données décentralisées, que faire ?

Quelles sont ces données décentralisées ?

➔ Texte des SMS, photos de la galerie, localisation d'un téléphone

➔ Données d'utilisation d'applications, enregistrements de la voix "dis Siri"

➔ Données LIDAR ou caméra

➔ Données médicales

<u>Caractéristiques de ces données décentralisées :</u>

- **Données précieuses d'un point de vue marketing : il FAUT les exploiter**

I. Données décentralisées, que faire ?

Quelles sont ces données décentralisées ?

➔ Texte des SMS, photos de la galerie, localisation d'un téléphone

➔ Données d'utilisation d'applications, enregistrements de la voix "dis Siri"

➔ Données LIDAR ou caméra

➔ Données médicales

<u>Caractéristiques de ces données décentralisées :</u>

- **Données précieuses d'un point de vue marketing : il FAUT les exploiter**
- **MAIS problème : il est très intrusif de les extraire de leur endroit de stockage !**

I. Données décentralisées, que faire ?

Quelles sont ces données décentralisées ?

➔ Texte des SMS, photos de la galerie, localisation d'un téléphone

➔ Données d'utilisation d'applications, enregistrements de la voix "dis Siri"

➔ Données LIDAR ou caméra

➔ Données médicales

<u>Caractéristiques de ces données décentralisées :</u>

- Données précieuses d'un point de vue marketing : il FAUT les exploiter
- MAIS problème : il est très intrusif de les extraire de leur endroit de stockage !

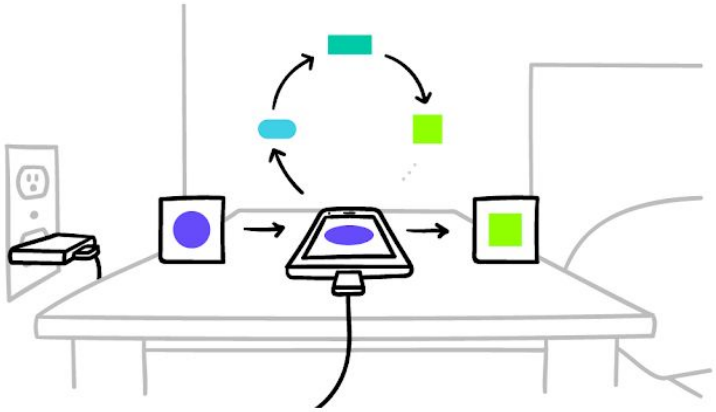
<u>Enjeu</u> : trouver une façon de traiter ces données, en respectant la vie privée des utilisateurs finaux !

UNIVERSITÉ DE LYON

ÉCOLE CENTRALELYON

I. Données décentralisées, que faire ?

Apprentissage local



Première idée : les données restent en local

Un modèle de Machine Learning est appris sur chaque appareil décentralisé avec les données locales

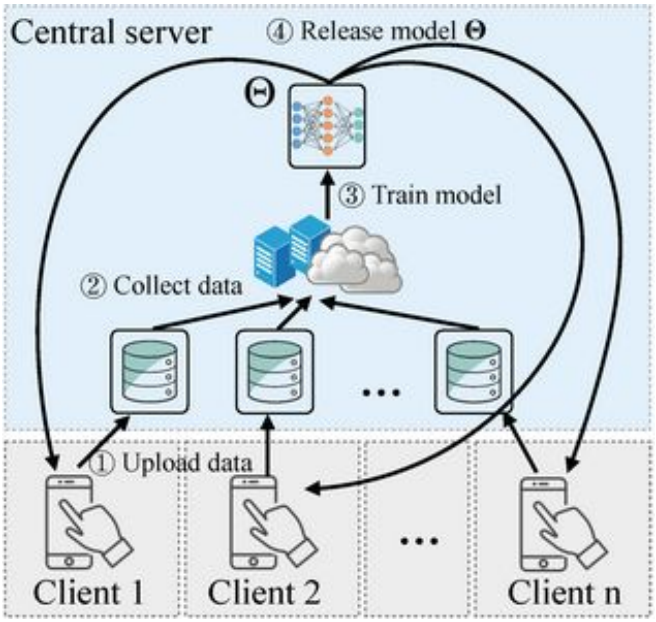
+ **Avantages** :
  - la vie privée est respectée, aucune fuite de données
  - pas de communication entre appareils décentralisés -> empreinte carbone plus faible

- **Inconvénients** :
  - pas forcément suffisamment de données en local pour du Deep Learning
  - ne tire pas parti des données des autres appareils décentralisés

I. Données décentralisées, que faire ?

Apprentissage centralisé

Seconde idée : les données sont transmises à un serveur centralisé



données transférées au serveur

modèle appris au niveau du serveur sur ces données

modèle transféré aux appareils décentralisés

\+ **Avantages** :
- beaucoup de données : apprentissage facile
- tire parti des données de tous les appareils décentralisés

\- **Inconvénients** :
- données privées transférées !!!!!
- utilisation de beaucoup de bande passante : mauvaise empreinte écologique
- forte latence

I. Données décentralisées, que faire ?

Apprentissage fédéré, le meilleur des deux mondes ?

	Local	**Centralisé**
Avantages	Faible bande passante Respect vie privée	Tire efficacement parti des données
Inconvénients	N'exploite pas les données de chaque appareil peu de données	Forte bande passante Non respect vie privée latence

Google en 2017 : Federated Learning

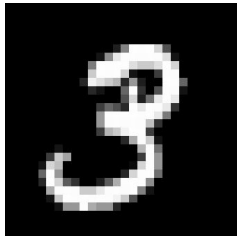
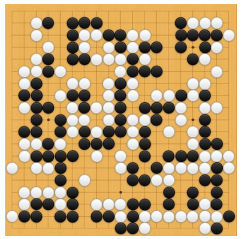
=> Contrecarre les défaillances des deux techniques précédentes

2.
Introduction à l'apprentissage fédéré

II. Introduction à l'apprentissage fédéré

Rappels de Machine Learning

Contexte : apprentissage supervisé, réseaux de neurones

Tâche	Entrée	Label
Classification d'images		3
Prédiction du prochain mot	Le réveil a été **?**	difficile
Jeu de go		prochain mouvement

But : apprendre à partir des données une fonction **f**, paramétrée par un vecteur de paramètres **W**, telle que f(entrée) ≈ label

II. Introduction à l'apprentissage fédéré

Rappels de Machine Learning

Contexte : apprentissage supervisé, réseaux de neurones

But : apprendre à partir des données une fonction **f**, paramétrée par un vecteur de paramètres **W**, telle que f(entrée) ≈ label

Ici, la fonction **f** est un réseau de neurones

=> entre 10 et 500M paramètres, voire +

Vocabulaire :

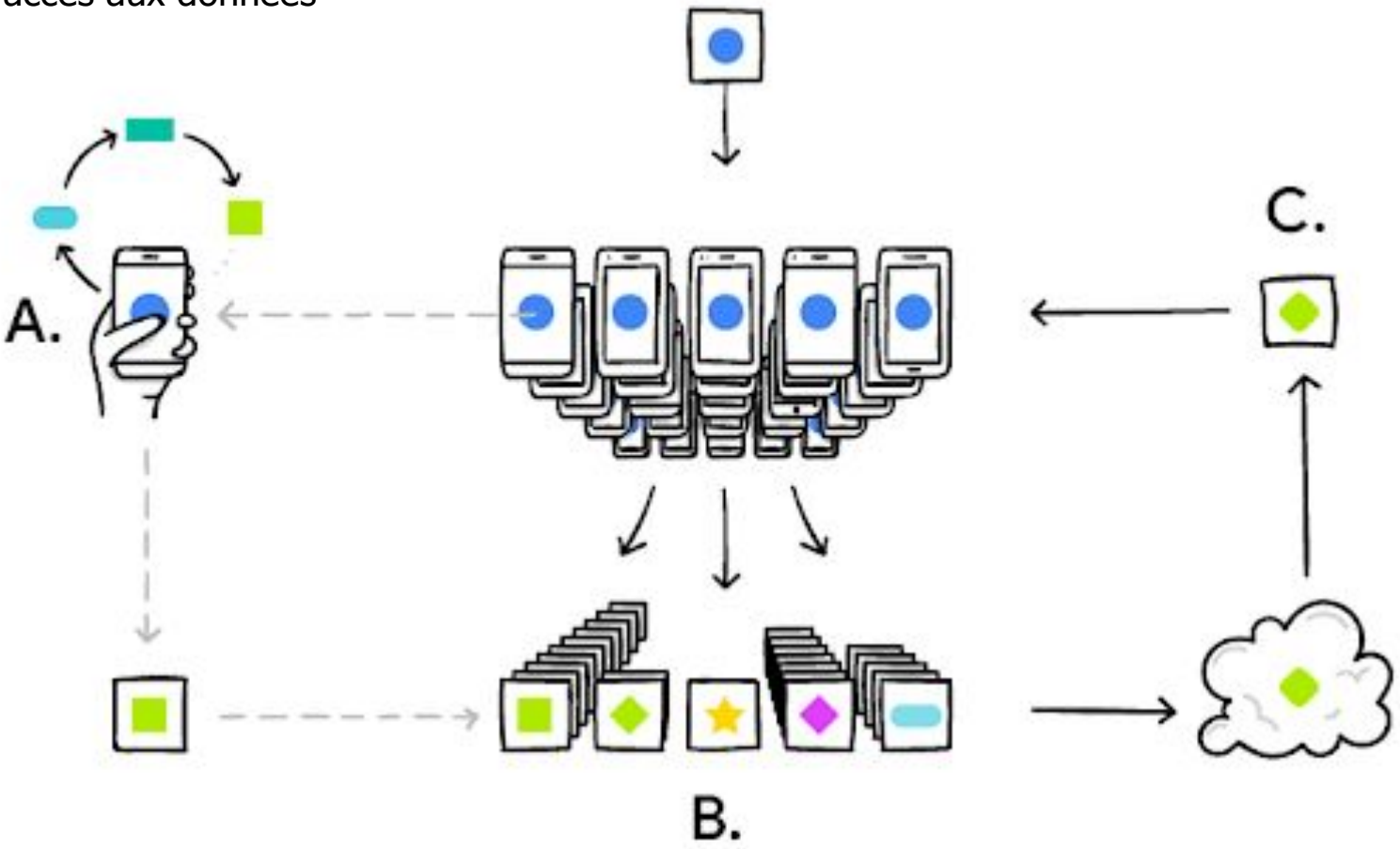
client = appareil avec donnée décentralisée

serveur

II. Introduction à l'apprentissage fédéré

Apprentissage fédéré

Apprendre au niveau du serveur, un modèle à partir des données des clients, sans avoir accès aux données



https://ai.googleblog.com/2017/04/federated-learning-collaborative.html

II. Introduction à l'apprentissage fédéré

Apprentissage fédéré

Algorithm 1 `FederatedAveraging` targeting updates from K clients per round.

Server executes:

initialize w_0

for each round $t = 1, 2, \dots$ **do**

Select $1.3K$ eligible clients to compute updates

Wait for updates from K clients (indexed $1, \dots, K$)

$(\Delta^k, n^k) = \text{ClientUpdate}(w)$ from client $k \in [K]$.

$\bar{w}_t = \sum_k \Delta^k$ *// Sum of weighted updates*

$\bar{n}_t = \sum_k n^k$ *// Sum of weights*

$\Delta_t = \Delta_t^k / \bar{n}_t$ *// Average update*

$w_{t+1} \leftarrow w_t + \Delta_t$

ClientUpdate(w)**:**

$\mathcal{B} \leftarrow$ (local data divided into minibatches)

$n \leftarrow |\mathcal{B}|$ *// Update weight*

$w_{\text{init}} \leftarrow w$

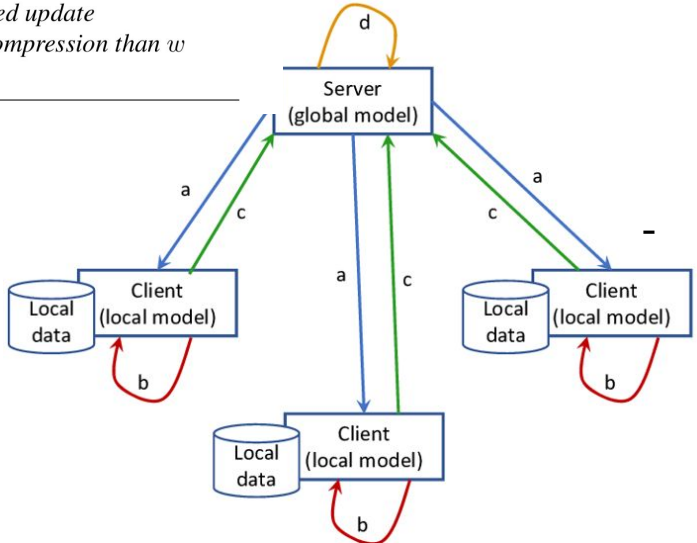
for batch $b \in \mathcal{B}$ **do**

$w \leftarrow w - \eta \nabla \ell(w; b)$

$\Delta \leftarrow n \cdot (w - w_{\text{init}})$ *// Weighted update*

// Note Δ is more amenable to compression than w

return (Δ, n) to server



Paramètres :

- Nombre de rounds R
- Nombre d'epochs de mise à jour locale E
- Taille des batchs B
- Fraction de clients sélectionnés à chaque round C

\+ **Avantages** :

- tire parti des données de tous les appareils décentralisés
- respecte la vie privée
- bande passante faible => impact CO^2 réduit

\- **Inconvénients** :

- À venir

II. Introduction à l'apprentissage fédéré

Acteurs majeurs de l'apprentissage fédéré

- Google : GBoard, fonction "Hey Google", († FLoC)
- Apple : "Dis Siri", QuickType, "trouvé dans l'application"
- Facebook, Amazon, Microsoft
- Samsung, Huawei
- IBM
- Nvidia
- Owkin (biotech franco-américaine avec données hospitalières)

II. Introduction à l'apprentissage fédéré
Usages actuels de l'apprentissage fédéré

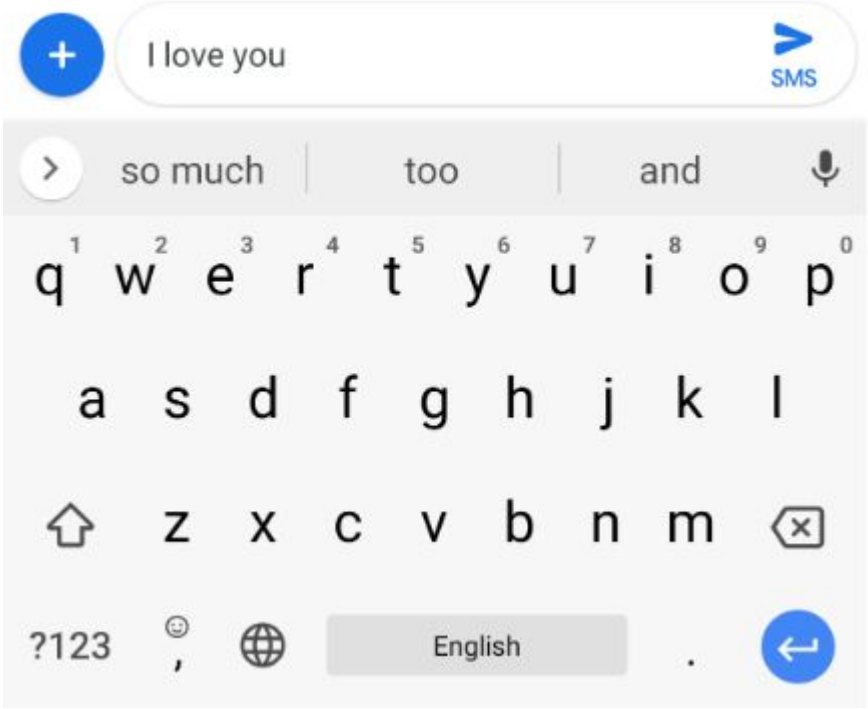
- Amélioration de fonctions internes du téléphone
- Véhicules intelligents et connectés
- Données d'institutions (en particulier hospitalières, bancaires ou d'assurance)

3.
Etude de cas : Google GBoard

III. Etude de cas : Google GBoard

Contexte

- 2 Mds appareils Android dans le monde

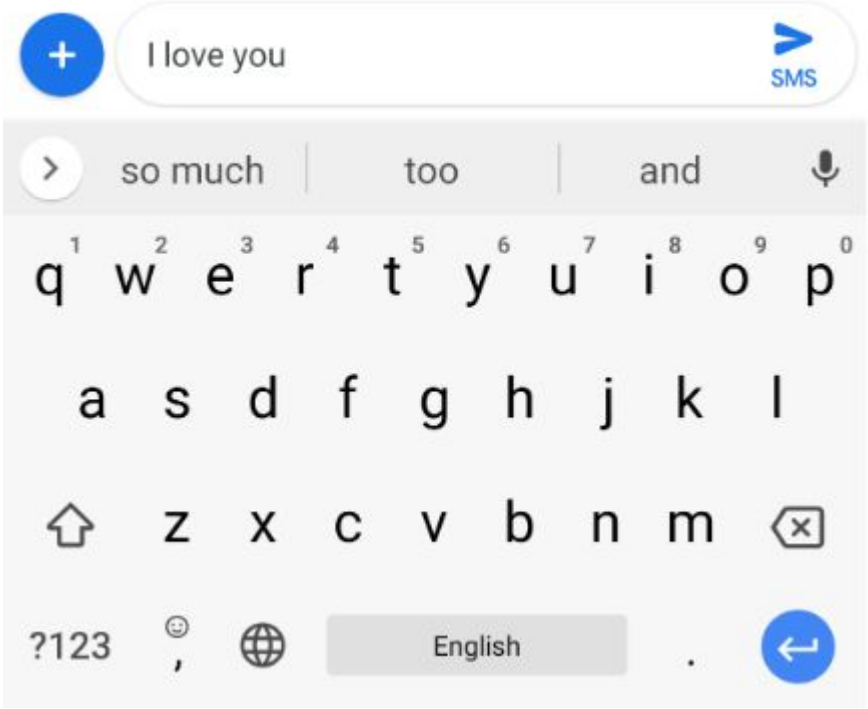


III. Etude de cas : Google GBoard

Contexte

- 2 Mds appareils Android dans le monde

- données naturellement labellisées : chaque phrase écrite peut être utilisée pour l'entraînement du modèle



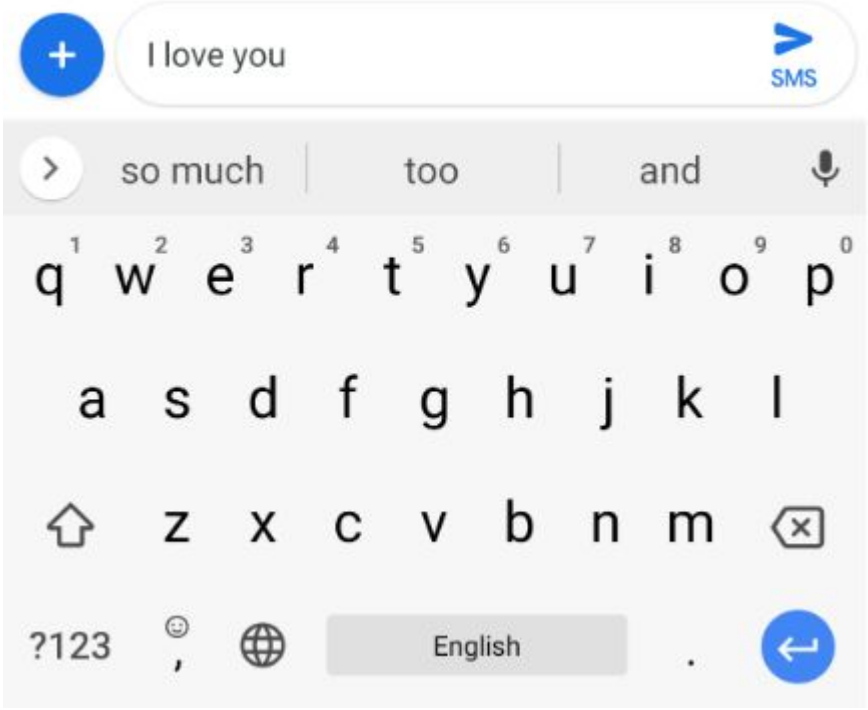
III. Etude de cas : Google GBoard

Contexte

- 2 Mds appareils Android dans le monde

- données naturellement labellisées : chaque phrase écrite peut être utilisée pour l'entraînement du modèle

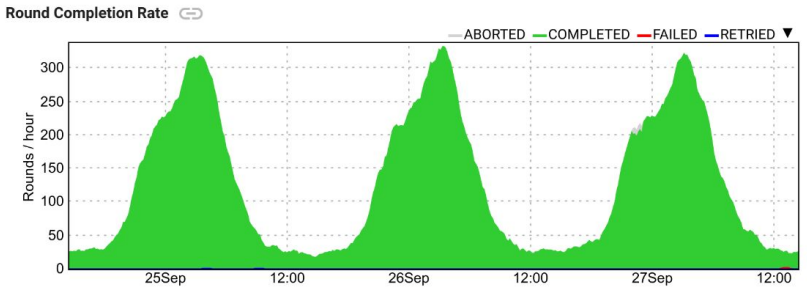
- Appareils peu fiables : les appareils qui contribuent à l'entraînement peuvent se déconnecter à tout moment

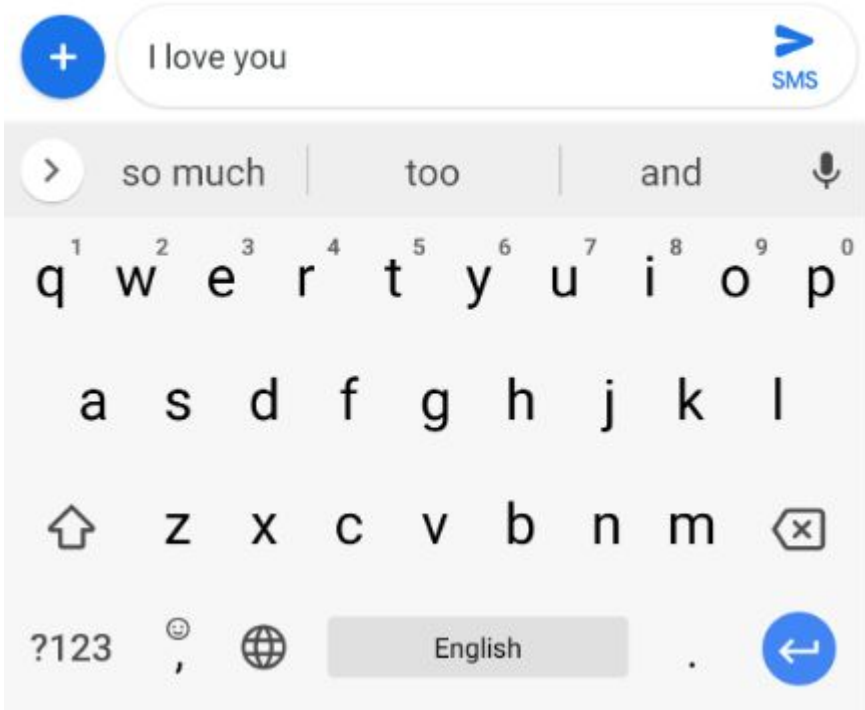


III. Etude de cas : Google GBoard

Contexte

- 2 Mds appareils Android dans le monde
- données naturellement labellisées : chaque phrase écrite peut être utilisée pour l'entraînement du modèle
- Appareils peu fiables : les appareils qui contribuent à l'entraînement peuvent se déconnecter à tout moment
- LSTM : 1.4M params
  3000 rounds
  100 clients par round
  80 clients minimum

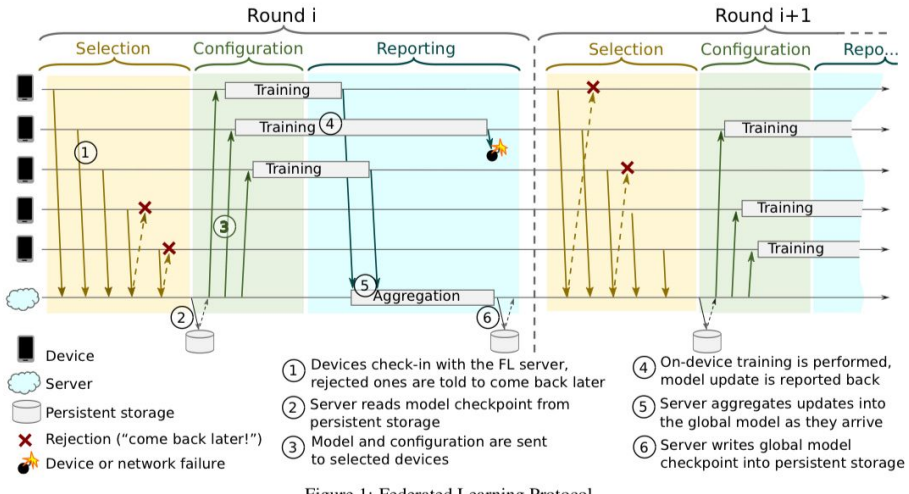


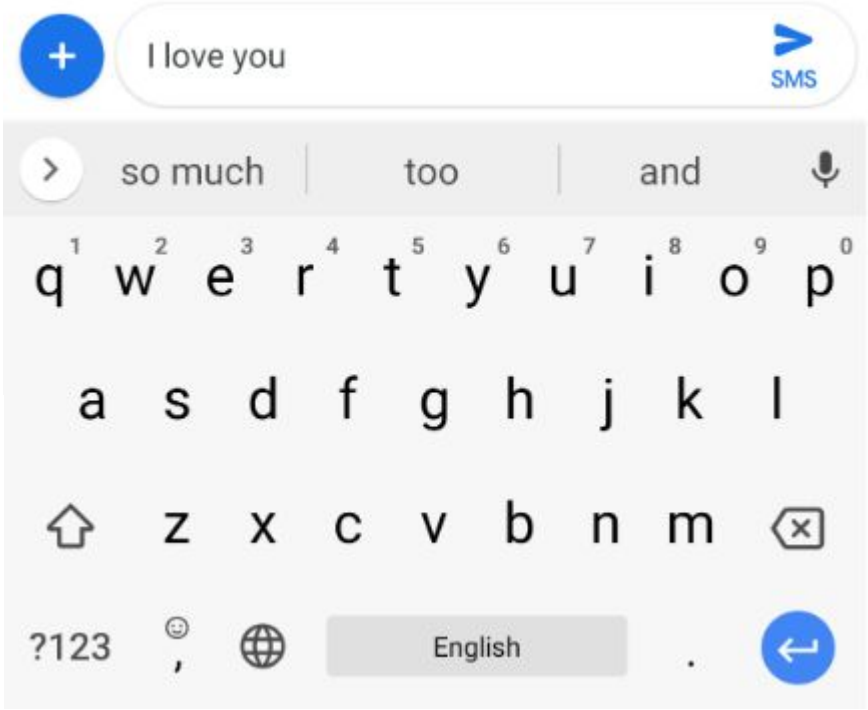


III. Etude de cas : Google GBoard

Sélection des clients

- Entraînement local : téléphone branché + connecté au WiFi
- 6 à 10% des clients se déconnectent
- Le modèle est d'abord évalué, puis entraîné sur les données locales
- Mêmes performances que le modèle centralisé





III. Etude de cas : Google GBoard
Contexte

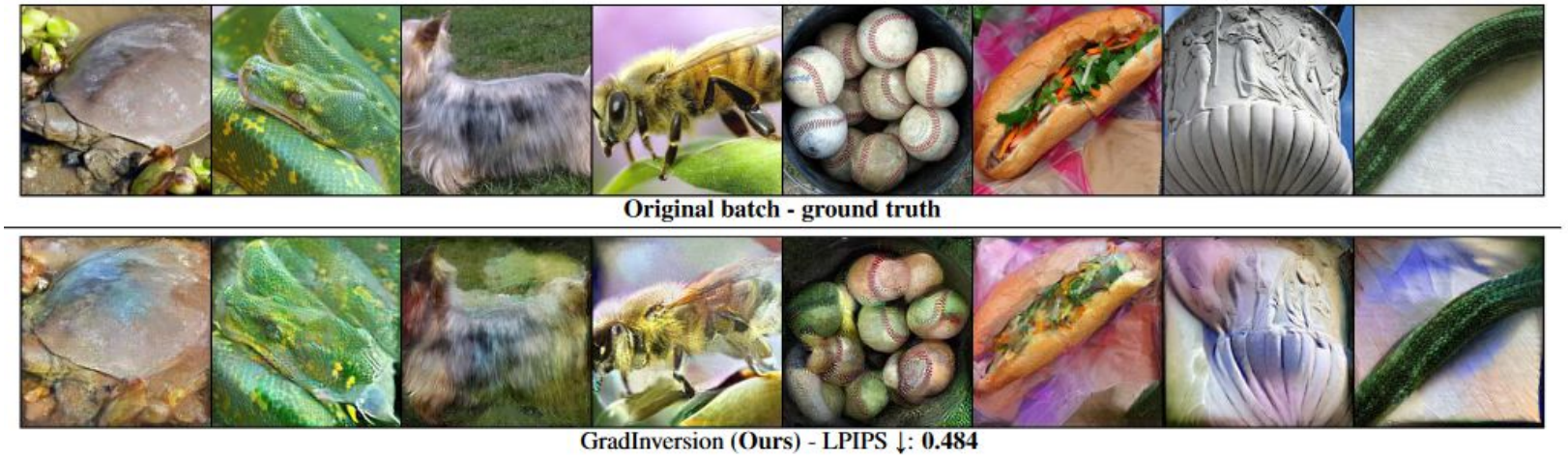
Poids : 145M de scalaires
Valeurs faibles -> mises à 0
Quantization des valeurs des paramètres
approximation de rang faible des poids
Codage de Huffman

Compression d'un facteur 50-100

(Federated Learning : Strategies for Improving Communication Efficiency)

4.
Vraiment respectueux de la vie privée ?

IV. Vraiment respectueux de la vie privée?
Inversion des gradients



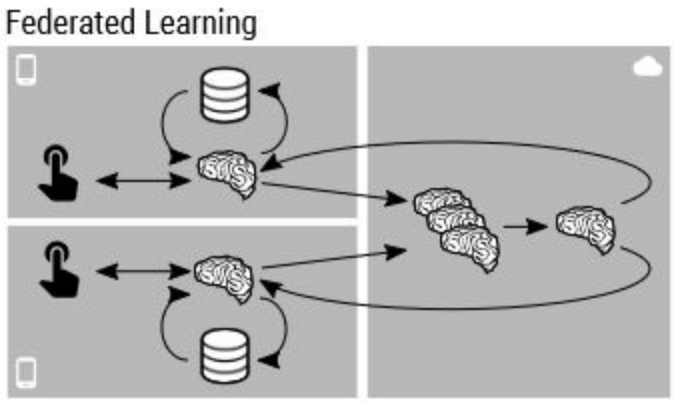
A partir des mises à jour faites par les clients, il est possible de reconstruire les données d'entraînement !

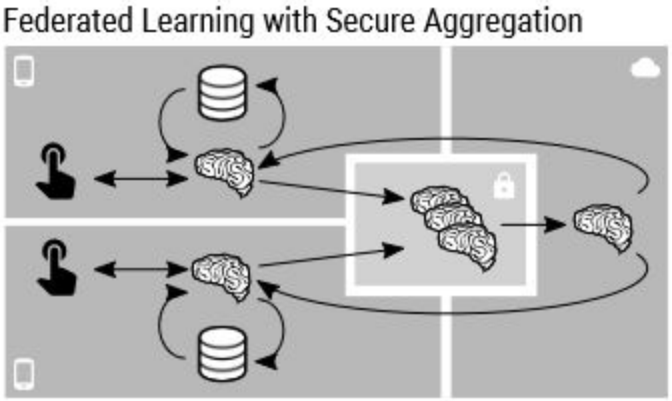
=> Nécessité de cryptographie pour protéger cette information

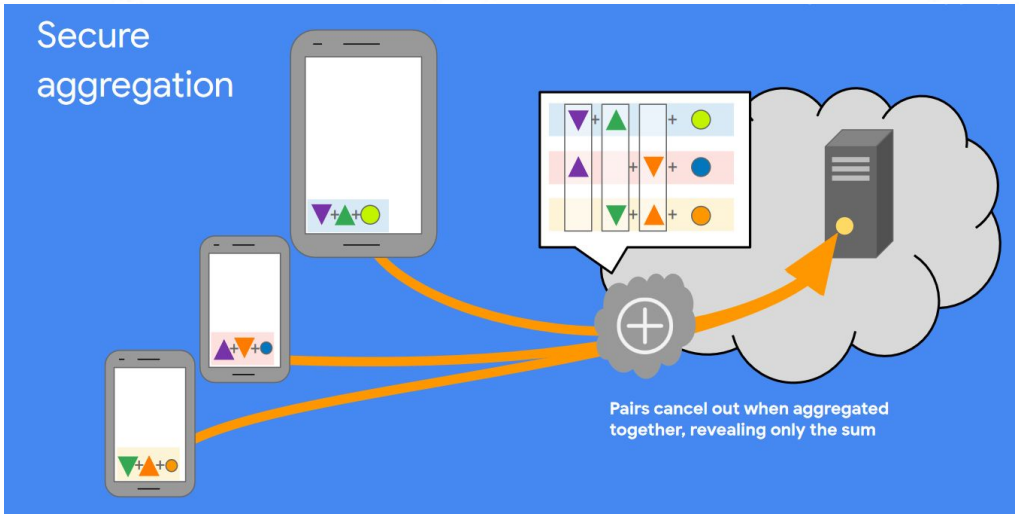
(Federated Learning : Strategies for Improving Communication Efficiency)

IV. Vraiment respectueux de la vie privée?
Secure aggregation

=> Nécessité de cryptographie pour protéger cette information







5.
Pistes d’améliorations du secteur

V. Pistes d'amélioration du secteur
Equité et données non-iid

- apprentissage fédéré = collaboration
- au niveau des utilisateurs : compétition pour avoir meilleures perfs
- Si beaucoup de clients ont des données biaisées, le modèle appris global sera biaisé

Ex : un modèle relié aux véhicules autonomes appris sur des véhicules thermiques. Fonctionne beaucoup moins bien sur véhicule électrique

=> Beaucoup de recherche sur la réduction des biais et des inégalités engendrées par l'apprentissage fédéré

(Fair ressource allocation in Federated Learning)

V. Pistes d'amélioration du secteur

Personnalisation

Parfois, modèle global appris avec les données de tous n'est pas adapté

=> combinaison apprentissage fédéré + entraînement local : modèle global ré-entraîné avec données locales

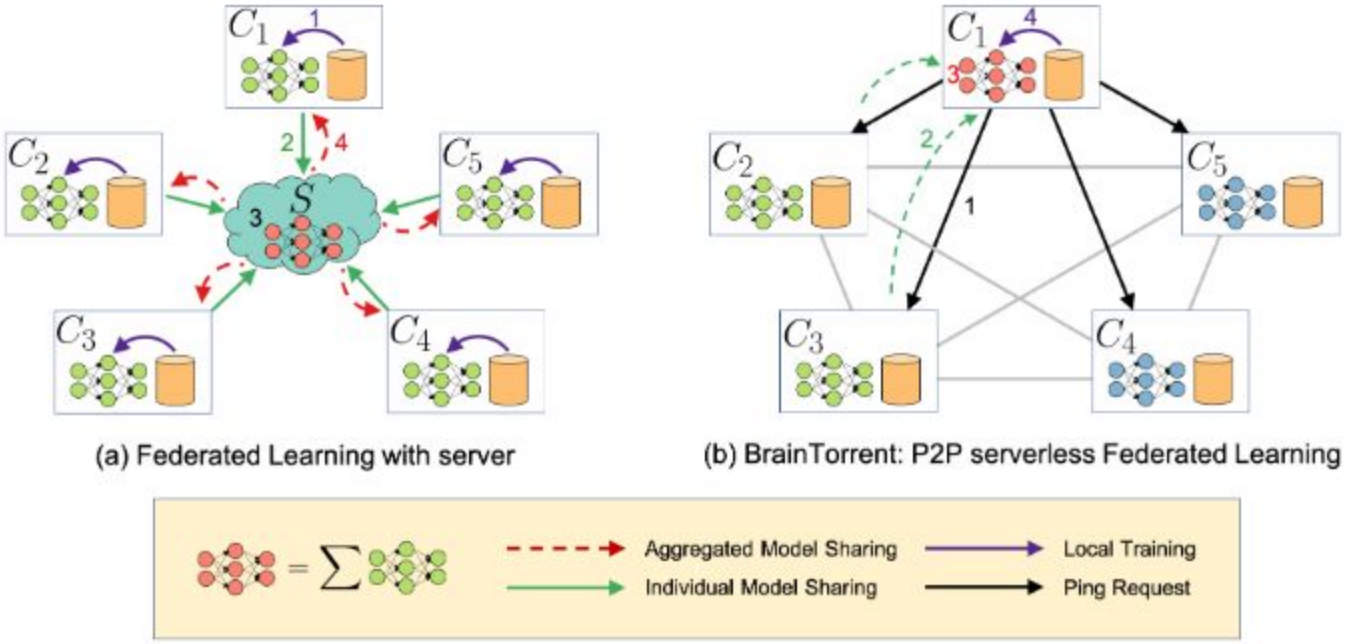
=> Cela s'appelle la personnalisation

(Personalized federated learning: A meta-learning approach)

V. Pistes d'amélioration du secteur

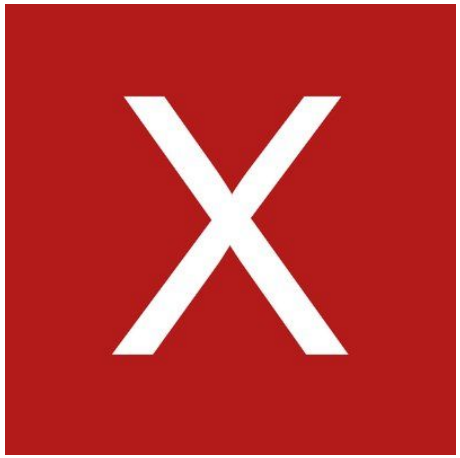
Apprentissage sans serveur

Variante de l'apprentissage fédéré sans serveur



(BrainTorrent: A Peer-to-Peer Environment for Decentralized Federated Learning)

Outils de veille utilisés



ÉCOLE
CENTRALE LYON

36, avenue Guy de Collongue 69130 Écully - France
+33 (0)4 72 18 60 00

www.ec-lyon.fr