Les articles

karim houidi

December 2023

1 Introduction

2 Problématiques

L'apprentissage fédéré est une approche de plus en plus utilisée dans le domaine de l'apprentissage machine, permettant de former des modèles sur des données distribuées sans avoir à les centraliser. Cependant, l'application de cette méthode à des modèles mathématiques comportant des équations et des algorithmes soulève plusieurs problématiques spécifiques.

1. Gestion des équations distribuées : Lorsque les équations d'un modèle mathématique sont distribuées sur différents appareils ou serveurs, la coordination de la résolution des équations devient complexe. Il est nécessaire de mettre en place des mécanismes de synchronisation et de communication efficaces pour assurer la convergence vers une solution globale.

2. Sécurité et confidentialité des données : Les données utilisées pour entraîner le modèle sont souvent sensibles et confidentielles. Il est crucial de garantir la sécurité et la confidentialité de ces données tout au long du processus d'apprentissage, en mettant en place des protocoles de chiffrement et d'authentification robustes.

3. Hétérogénéité des données et des appareils: Les données détenues par différentes entités peuvent être hétérogènes en termes de distribution, de format et de qualité. De plus, les appareils sur lesquels ces données résident peuvent varier en termes de puissance de calcul, de connectivité et de ressources disponibles. Gérer cette hétérogénéité de manière efficace pour garantir des performances optimales du modèle.

4. Communication et coordination: L'apprentissage fédéré nécessite une communication étroite et une coordination entre les différentes entités participantes. La mise en œuvre d'algorithmes de coordination efficaces tout en minimisant la quantité de données échangées constitue un défi complexe. De plus, la gestion des éventuelles défaillances ou interruptions de communication nécessite une attention particulière pour assurer la robustesse du processus d'apprentissage.

5. Biais et équité : Lorsque les données sont réparties entre plusieurs entités, il est essentiel de s'assurer que le processus d'apprentissage ne renforce pas les biais existants ou n'introduise pas de nouvelles inégalités. La conception d'algorithmes d'apprentissage fédéré qui prennent en compte ces considérations est un défi important pour garantir l'équité et la représentativité des modèles résultants.

References

[1] A. Nilsson, S. Smith, G. Ulm, E. Gustavsson, and M. Jirstrand, "A performance evaluation of federated learning algorithms," in *Proceedings of the Second Workshop on Distributed Infrastructures for Deep Learning*. ACM, pp. 1–8. [Online]. Available: https://dl.acm.org/doi/10.1145/3286490.3286559

[2] L. Li, Fan, and Yuxi, "A review of applications in federated learning," vol. 149, p. 106854, publisher: Pergamon. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0360835220305532

[3] X. Ma, J. Zhu, Z. Lin, S. Chen, and Y. Qin, "A state-of-the-art survey on solving non-IID data in federated learning," vol. 135, pp. 244–258. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0167739X22001686

[4] W. Shiqiang, T. Tiffany, S. Theodoros, K. L. Kin, M. Christian, H. Ting, and C. Kevin, "Adaptive federated learning in resource constrained edge computing systems."

[5] S. Reddi, Z. Charles, M. Zaheer, Z. Garrett, K. Rush, J. Konečný, S. Kumar, and H. B. McMahan, "Adaptive federated optimization." [Online]. Available: http://arxiv.org/abs/2003.00295

[6] P. Kairouz, H. B. McMahan, B. Avent, A. Bellet, M. Bennis, A. N. Bhagoji, K. Bonawitz, Z. Charles, G. Cormode, R. Cummings, R. G. L. D'Oliveira, H. Eichner, S. E. Rouayheb, D. Evans, J. Gardner, Z. Garrett, A. Gascón, B. Ghazi, P. B. Gibbons, M. Gruteser, Z. Harchaoui, C. He, L. He, Z. Huo, B. Hutchinson, J. Hsu, M. Jaggi, T. Javidi, G. Joshi, M. Khodak, J. Konečný, A. Korolova, F. Koushanfar, S. Koyejo, T. Lepoint, Y. Liu, P. Mittal, M. Mohri, R. Nock, A. Özgür, R. Pagh, M. Raykova, H. Qi, D. Ramage, R. Raskar, D. Song, W. Song, S. U. Stich, Z. Sun, A. T. Suresh, F. Tramèr, P. Vepakomma, J. Wang, L. Xiong, Z. Xu, Q. Yang, F. X. Yu, H. Yu, and S. Zhao, "Advances and open problems in federated learning." [Online]. Available: http://arxiv.org/abs/1912.04977

[7] K. Hyesung, P. Jihong, B. Mehdi, and K. Seong-Lyun, "Blockchained on-device federated learning."

[8] J. Mills, J. Hu, and G. Min, "Communication-efficient federated learning for wireless edge intelligence in IoT," vol. 7, no. 7, pp. 5986–5994. [Online]. Available: https://ieeexplore.ieee.org/document/8917724/

Titre	Année	Auteurs	Résumer	Avantages	Inconvénients
A Performance Evaluation of Federated Learning Algorithms [1]	ACM Reference, 2018	Adrian Nilsson,Simon Smith, Gregor Ulm, Emil Gustavsson, and Mats Jirstrand	**Problématique**:l'analyse de données dans un contexte de grande quantité de données générées par des appareils mobiles tels que les téléphones portables ou les véhicules connectés. Le transfert de ces données vers un serveur centralisé peut être problématique en raison de la limitation de la bande passante et des préoccupations liées à la confidentialité des données. Pour résoudre ce problème, l'article propose l'utilisation de l'apprentissage fédéré, où les appareils locaux effectuent des tâches d'apprentissage et ne communiquent qu'un modèle mis à jour à un serveur de coordination. L'article évalue ensuite trois algorithmes d'apprentissage fédéré et les compare à une approche centralisée pour déterminer leur efficacité dans la résolution de ce problème	Avantages de l'apprentissage fédéré par rapport aux approches centralisées traditionnelles : 1. Réduction de la quantité de données transférées : Avec l'apprentissage fédéré, seuls les modèles mis à jour sont transférés entre les appareils clients et le serveur central, ce qui réduit considérablement la quantité de données transférées par rapport aux approches centralisées traditionnelles. 2. Protection de la vie privée : L'apprentissage fédéré permet de protéger la vie privée des utilisateurs en ne transférant que des modèles mis à jour plutôt que des données brutes. Les modèles sont également temporairement stockés et immédiatement supprimés après leur utilisation, ce qui limite la quantité de données stockées. 3. Évolutivité : L'apprentissage fédéré permet de traiter des ensembles de données massifs en distribuant la charge de travail sur plusieurs appareils clients, ce qui permet de traiter des ensembles de données plus volumineux que les approches centralisées traditionnelles. 4. Flexibilité : L'apprentissage fédéré permet de travailler avec des ensembles de données non équilibrés et non identiquement distribués, ce qui est souvent le cas dans les environnements distribués. 5. Réduction des coûts : L'apprentissage fédéré peut réduire les coûts de stockage et de traitement des données en évitant la nécessité de stocker des données brutes sur un serveur centralisé et en distribuant la charge de travail sur plusieurs appareils clients	L'article ne mentionne pas d'inconvénients spécifiques de l'apprentissage fédéré, mais il souligne certains des défis et des limitations associés à cette approche : 1. Hétérogénéité des données : Les données collectées par les appareils clients peuvent être hétérogènes en termes de qualité, de format et de distribution, ce qui peut rendre difficile la création d'un modèle global cohérent. 2. Communication limitée : Les appareils clients peuvent avoir des limitations de communication, telles que des connexions réseau lentes ou intermittentes, ce qui peut affecter la qualité et la vitesse de l'apprentissage fédéré. 3. Sécurité : L'apprentissage fédéré peut être vulnérable à des attaques de sécurité, telles que des attaques par injection de données malveillantes ou des attaques par déni de service. 4. Complexité : L'apprentissage fédéré peut être plus complexe que les approches centralisées traditionnelles, car il nécessite la coordination de nombreux appareils clients et la gestion de modèles mis à jour. 5. Besoin de ressources : L'apprentissage fédéré peut nécessiter des ressources importantes, telles que des capacités de stockage et de traitement, pour gérer les modèles mis à jour et les données distribuées

Titre	Années	Autres	Résumer	Avantages	Inconvenantes
A review of applications in federated learning [2]	ORCA, 2021	Li Li, Yuxi Fan, Mike Tse, Kuo-Yi Lin	**Problématique**:aborde plusieurs problématiques liées à l'apprentissage fédéré, notamment : 1. La communication : L'apprentissage fédéré implique la communication entre les appareils clients et le serveur central, ce qui peut entraîner des problèmes de latence, de bande passante et de sécurité. 2. La préservation de la confidentialité : Les données des clients sont souvent sensibles et doivent être protégées contre les fuites d'informations. Les méthodes de préservation de la confidentialité doivent être mises en place pour garantir que les données des clients ne sont pas compromises. 3. La qualité des modèles : Les modèles d'apprentissage fédérés peuvent être affectés par la qualité des données des clients, qui peuvent être non représentatives ou biaisées. Des méthodes doivent être mises en place pour garantir que les modèles sont de haute qualité et représentatifs de l'ensemble des données. 4. La gestion des appareils clients : Les appareils clients peuvent être hétérogènes et avoir des capacités de calcul et de stockage différentes. La gestion de ces appareils peut être complexe et nécessite des méthodes efficaces pour garantir que les appareils sont utilisés de manière optimale.	Les avantages sont des solutions proposées pour chaque problématiques: 1. la communication: des stratégies visant à améliorer l'efficacité de la communication entre les appareils clients et le serveur central sont discutées, telles que l'optimisation de la quantité de données échangées et l'utilisation de protocoles de communication efficaces 2. la préservation de la confidentialité: l'article aborde des méthodes de préservation de la confidentialité des données des clients, telles que la cryptographie et la confidentialité différentielle, pour garantir que les données des clients ne sont pas compromises lors du processus d'apprentissage fédéré 3. la qualité des modèles: des approches visant à atténuer les biais potentiels dans les données des clients sont discutées, ainsi que des méthodes pour agréger les modèles locaux de manière à garantir la qualité du modèle global 4. la gestion des appareils clients: des stratégies d'allocation de ressources et de tolérance aux pannes sont abordées pour garantir que les appareils clients sont utilisés de manière efficace et robuste dans le cadre de l'apprentissage fédéré	L'apprentissage fédéré peut entraîner des coûts de communication élevés en raison de la nécessité de transférer des données entre les appareils clients et le serveur central, ce qui peut être un inconvénient dans des environnements avec des ressources limitées. De plus, la gestion de la confidentialité des données des clients peut être complexe et nécessiter des efforts supplémentaires pour garantir que les données ne sont pas compromises lors du processus d'apprentissage fédéré. En outre, la qualité des modèles peut être affectée par la nature hétérogène des données des clients, ce qui peut nécessiter des techniques avancées pour atténuer les biais potentiels et garantir la qualité du modèle global.

Titre	Année	Autres	Résumé	Avantages	Inconvénients
A state-of-the-art survey on solving non-IID data in Federated Learning [3]	ScienceDirect, 2022	Xiaodong Ma, Jia Zhu, Zhihao Lin, Shanxuan Chen, Yangjie Qi	Cet article présente une étude approfondie sur la résolution des données non-IID (indépendantes et identiquement distribuées) dans l'apprentissage fédéré. Il analyse les problèmes de données non-IID et les défis statistiques qu'ils posent pour l'apprentissage fédéré. L'article classe les méthodes existantes pour résoudre ce problème et met en évidence l'importance de résoudre les problèmes de données non-IID pour améliorer les performances et la participation active des utilisateurs dans le processus d'apprentissage fédéré. *Les données* ***non-IID****(indépendantes et identiquement distribuées) sont des données qui ne suivent pas la même distribution statistique ou qui ne sont pas générées de manière indépendante les unes des autres. Cela signifie que les données sur différents appareils ou dans différents ensembles ne sont pas uniformément réparties ou ne présentent pas les mêmes caractéristiques, ce qui peut poser des défis pour l'apprentissage fédéré en raison de la variabilité des données entre les appareils participants.*	Les méthodes couramment utilisées pour résoudre les problèmes de données non-IID dans l'apprentissage fédéré comprennent : • Le partage de données entre les appareils participants pour réduire les différences de poids entre les appareils. • L'amélioration des données pour équilibrer les échantillons non-IID en ajoutant des étiquettes cibles manquantes à l'aide d'un algorithme spécifique. • La sélection de données pour améliorer la représentation des données partagées entre les appareils.	L'article discute des défis liés aux coûts de communication dans l'apprentissage fédéré, en particulier en raison de la complexité croissante des modèles de réseaux neuronaux et des données non-IID. Il met en évidence la nécessité de réduire les coûts de communication et mentionne des sujets de recherche potentiels tels que la compression de la communication et l'élagage du modèle pour améliorer l'efficacité de la communication dans l'apprentissage fédéré.

Titre	Année	Autres	Résumer	Avantages
Adaptive Federated Learning in Resource Constrained Edge Computing Systems [4]	IEEE, 2019	Shiqiang Wang, Tiffany Tuor, Theodoros Salonidis, Kin K. Leung, Christian Makaya, Ting He, Kevin Chan	Cet article traite de l'apprentissage fédéré adaptatif dans les systèmes de calcul en périphérie des ressources. Il examine comment les modèles d'apprentissage automatique peuvent être formés à partir de données distribuées sur plusieurs nœuds de périphérie sans envoyer les données brutes à un endroit centralisé. Les auteurs proposent un algorithme de contrôle qui détermine le meilleur compromis entre la mise à jour locale et l'agrégation des paramètres globaux pour minimiser la fonction de perte dans une limite de ressources donnée. Les performances de l'algorithme proposé sont évaluées à l'aide d'expériences approfondies avec de vrais ensembles de données. La problématique abordée dans l'article semble se concentrer sur la minimisation de la fonction de perte globale tout en optimisant l'utilisation des ressources disponibles pour l'apprentissage fédéré.	Les défis associés à l'apprentissage fédéré dans les systèmes de calcul en périphérie des ressources incluent la distribution non-i.i.d. des données entre les nœuds en périphérie, la contrainte de ressources en termes de calcul et de communication, ainsi que l'adaptation dynamique de la fréquence des mises à jour et des agrégations pour minimiser la perte d'apprentissage sous un budget de ressources fixe. L'algorithme proposé par les auteurs parvient à minimiser la fonction de perte tout en respectant les contraintes de ressources en adaptant dynamiquement la fréquence des mises à jour locales et des agrégations globales. Ceci est réalisé en déterminant les valeurs optimales de T et pour minimiser la fonction de perte globale sous une contrainte de ressources donnée.Les applications potentielles de l'apprentissage fédéré dans les systèmes de calcul en périphérie des ressources comprennent la possibilité d'analyser de grandes quantités de données pour la détection, la classification et la prédiction d'événements futurs, tout en respectant les contraintes de bande passante, de stockage et de confidentialité associées aux systèmes en périphérie. l'algorithme proposé pour l'adaptation dynamique de la fréquence des mises à jour locales et des agrégations globales dans le processus d'apprentissage fédéré est conçu pour optimiser l'apprentissage avec un budget de ressources donné pour les systèmes MEC.

Titre	Années	Autres	Résumer	Avantages	Inconvenantes
ADAPTIVE FEDERATED OPTIMIZATION [5]	ICLR, 2021	Sashank J. Reddi, Zachary Charles,Manzil Zaheer, Zachary Garrett, Keith Rush, Jakub Kone ˇ cný,Sanjiv Kumar, H. B	Dans cet article, les auteurs proposent des optimiseurs adaptatifs pour l'apprentissage fédéré, une méthode de machine learning distribuée dans laquelle de nombreux clients coordonnent avec un serveur central pour apprendre un modèle sans partager leurs données d'entraînement. Les optimiseurs adaptatifs sont conçus pour améliorer la convergence et les performances de l'apprentissage fédéré. Les résultats montrent l'interaction entre l'hétérogénéité des données des clients et l'efficacité de la communication. Dans l'apprentissage fédéré,les**problèmes** de convergence incluent le décalage des modèles locaux par rapport au modèle global optimal et le manque d'adaptabilité des méthodes d'optimisation standard comme FEDAVG, qui peut être inadapté pour des distributions de bruit de gradient stochastique à queue lourde.	Les optimiseurs adaptatifs (FEDADAM, FEDADAGRAD et FEDYOGI) peuvent améliorer les performances de l'apprentissage fédéré en offrant une adaptabilité aux distributions de bruit de gradient stochastique à queue lourde. Cela permet d'atténuer les problèmes de convergence et d'améliorer l'efficacité de l'optimisation dans des environnements hétérogènes.L'hétérogénéité des données des clients a des implications sur l'apprentissage fédéré, car elle peut entraîner des problèmes de convergence et d'efficacité de la communication. Les optimiseurs adaptatifs sont conçus pour atténuer ces effets en offrant une adaptabilité aux distributions de bruit de gradient stochastique à queue lourde, ce qui améliore la convergence et les performances dans des environnements hétérogènes	Les inconvénients des optimiseurs adaptatifs dans le contexte de l'apprentissage fédéré peuvent inclure une complexité accrue par rapport aux méthodes d'optimisation standard, des besoins en calcul plus élevés et une sensibilité à certains paramètres(le taux d'apprentissage , le taux d'apprentissage du client l, et pour les méthodes adaptatives, le paramètre d'adaptativité). Ces aspects doivent être pris en compte lors de l'application de ces optimiseurs dans des scénarios d'apprentissage fédéré.

Titre	Années	Autres	Résumer	Avantages
Advances and Open Problems in Federated Learning [6]	arXiv, 2021	Peter Kairouz,H.Brendan McMahan,Brendan Avent,Aurélien Bellet,Mehdi Bennis,Arjun Nitin Bhagoji,Kallista Bonawitz,Zachary Charles,Graham Cormode,Rachel Cummings6 Rafael G.L.D'Oliveira,Hubert Eichner,Salim El Rouayheb,David Evans,Josh Gardner,Zachary Garrett,Adrià Gascon,Badih Ghazi,Phillip B. Gibbons,Marco Gruteser,Zaid Harchaoui,Chaoyang He,Lie He,Zhouyuan Huo,Ben Hutchinson,Justin Hsu,Martin Jaggi,Tara Javidi,Gauri Joshi,Mikhail Khodak,Jakub Konecny,Aleksandra Korolova, Farinaz Koushanfar,Sanmi Koyejo,Tancrède Lepoint,Yang Liu,Prateek Mittal,Mehryar Mohri,Richard Nock,Ayfer Ozgur,Rasmus Pagh,Hang Qi,Daniel Ramage,Ramesh Raskar,Mariana Raykova,Dawn Song,Weikang Song,Sebastian U. Stich,Ziteng Sun, Ananda Theertha Suresh,Florian Tramèr,Praneeth Vepakomma,Jianyu Wang,Li Xiong,Zheng Xu,Qiang Yang,Felix X. Yu,Han Yu,Sen Zhao	Le Federated Learning (FL) est un cadre d'apprentissage automatique dans lequel de nombreux clients collaborent pour former un modèle sous l'orchestration d'un serveur central, tout en conservant les données d'entraînement décentralisées. Cet article discute des avancées récentes et présente une collection étendue de problèmes ouverts et de défis liés au FL.	Le Federated Learning (FL) présente des avantages potentiels tels que la préservation de la confidentialité des données, la réduction des risques de violation de la vie privée et l'amélioration de la diversité des données d'entraînement. Cependant, il comporte également des risques liés à la sécurité et à l'équité, notamment en ce qui concerne les biais introduits par l'échantillonnage des clients et la sensibilité des attributs.Les principaux problèmes et défis à résoudre dans le domaine du Federated Learning incluent la gestion de la sécurité et de la confidentialité des données, la coordination efficace entre les clients pour l'entraînement du modèle, la gestion des biais introduits par l'échantillonnage des clients, et l'assurance de l'équité dans le processus d'apprentissage. De plus, l'efficacité des algorithmes sous contraintes système et la modélisation de la protection des données sont des défis importants à relever.Les principaux problèmes et défis à résoudre dans le domaine du Federated Learning incluent : • Garantir la confidentialité des données des clients tout en permettant au serveur d'agréger les rapports des clients • Concevoir des méthodes de divulgation privée efficaces, notamment en utilisant des notions de confidentialité différentielle • Gérer les faiblesses des méthodes existantes, telles que le besoin d'un serveur central de confiance et les limitations des méthodes de divulgation privée prometteuses.

Titre	Années	Autres	Résumer	Avantages
Blockchained On-Device Federated Learning [7]	IEEE, 2019	Hyesung Kim, Jihong Park, Mehdi Bennis,Seong-Lyun Kim	Cet article propose une architecture d'apprentissage fédéré basée sur la technologie de la blockchain, appelée BlockFL, qui permet les mises à jour des modèles locaux d'apprentissage à échanger et à vérifier. Cela permet l'apprentissage sur les appareils sans données d'entraînement centralisées en utilisant un mécanisme de consensus dans la blockchain. L'article présente également un modèle de latence de bout en bout de BlockFL et caractérise le taux de génération de bloc optimal en tenant compte des retards de communication, de calcul et de consensus.La technologie de la blockchain est utilisée dans l'architecture BlockFL pour faciliter l'apprentissage fédéré sur les appareils en permettant l'échange et la vérification des mises à jour des modèles d'apprentissage locaux. Cela est réalisé grâce à un mécanisme de consensus dans la blockchain, qui permet l'apprentissage machine sur les appareils sans données d'entraînement centralisées ni coordination. Le réseau blockchain permet l'échange des mises à jour des modèles locaux des appareils tout en vérifiant et en fournissant leurs récompenses correspondantes, favorisant ainsi la fédération de plus d'appareils avec un plus grand nombre d'échantillons d'entraînement. De plus, l'utilisation de la blockchain surmonte le problème du point de défaillance unique et étend la portée de sa fédération à des appareils non fiables dans un réseau public, grâce à un processus de validation des résultats d'entraînement locaux.	Les avantages de l'utilisation de BlockFL par rapport à l'apprentissage fédéré traditionnel sont multiples. BlockFL exploite la technologie de la blockchain pour permettre l'apprentissage fédéré sur les appareils, offrant plusieurs avantages : **Décentralisation** : BlockFL élimine le besoin d'un serveur central unique, qui constitue une vulnérabilité dans l'apprentissage fédéré traditionnel. Cette décentralisation garantit que la mise à jour du modèle global est calculée localement sur chaque appareil, le rendant robuste contre les dysfonctionnements et empêchant les surcharges computationnelles excessives des mineurs. **Sécurité et confidentialité** : En utilisant la blockchain pour échanger et vérifier les mises à jour des modèles locaux, BlockFL garantit la confidentialité des échantillons de données brutes provenant d'autres appareils. Cela renforce la sécurité et la confidentialité dans le processus d'apprentissage fédéré. **Incitation** : BlockFL offre des récompenses proportionnelles aux tailles des échantillons d'entraînement, favorisant la fédération de plus d'appareils avec un plus grand nombre d'échantillons d'entraînement. Cette incitation encourage la participation active et la contribution d'appareils avec des tailles d'échantillons de données variables. **Robustesse contre les dysfonctionnements** : En cas de dysfonctionnement d'un mineur, BlockFL est conçu pour empêcher la distorsion des mises à jour du modèle global. Le système peut restaurer les distorsions en fédérant avec d'autres appareils qui fonctionnent normalement, garantissant ainsi une robustesse contre les dysfonctionnements. **Optimisation de la latence** : BlockFL aborde le problème de latence en formulat un modèle de latence de bout en bout et en optimisant le taux de génération de blocs pour minimiser la latence. Cette optimisation garantit l'achèvement efficace et en temps opportun du processus d'apprentissage fédéré.En résumé, BlockFL offre une sécurité, une confidentialité, une décentralisation, une incitation, une robustesse contre les dysfonctionnements et une optimisation de la latence améliorées par rapport aux méthodes traditionnelles d'apprentissage fédéré.Le modèle de latence de bout en bout de BlockFL est formulé en tenant compte des retards de communication, de calcul et de consensus. La latence est déterminée par les retards de calcul, les retards de communication et les retards de génération de blocs. Le taux de génération de blocs optimal λ qui minimise la latence est dérivé en se basant sur le modèle de latence d'une seule époque. Le taux de génération de blocs est optimisé pour minimiser la latence moyenne de complétion de l'apprentissage sur le processus de Preuve-de-Travail (PoW), garantissant ainsi l'achèvement efficace et opportun du processus d'apprentissage fédéré.

Titre	Années	Autres	Résumer	Avantages	Inconvenantes
Communication-Efficient Federated Learning for Wireless Edge Intelligence in IoT [8]	IEEE, 2019	Jed Mills, Jia Hu, Geyong Min	Ce document présente une solution pour l'apprentissage fédéré dans les appareils IoT en utilisant des serveurs périphériques et des passerelles pour construire un modèle central sans téléverser les données vers un serveur central. Les auteurs proposent d'adapter l'algorithme FedAvg en utilisant une forme distribuée de l'optimisation Adam pour réduire les coûts de communication et améliorer la convergence avec des ensembles de données clients non-IID. L'utilisation de l'intelligence périphérique sans fil pour les appareils IoT peut avoir des implications potentielles importantes en termes de confidentialité des données et d'efficacité de l'apprentissage automatique. En termes de confidentialité des données, l'utilisation de l'intelligence périphérique sans fil peut permettre de construire des modèles d'apprentissage automatique sans avoir à téléverser les données clients vers un serveur central. Cela peut aider à protéger la confidentialité des données clients, car les données ne quittent pas les appareils clients. Cependant, il est important de noter que les modèles d'apprentissage automatique peuvent encore révéler des informations sensibles sur les données clients, il est donc important de prendre des mesures pour protéger la confidentialité des modèles eux-mêmes. En termes d'efficacité de l'apprentissage automatique, l'utilisation de l'intelligence périphérique sans fil peut permettre de construire des modèles plus rapidement et plus efficacement en utilisant les ressources de calcul et de stockage disponibles sur les appareils clients. Cela peut aider à réduire les coûts de communication et à améliorer la vitesse de convergence de l'apprentissage automatique. Cependant, il est important de noter que l'utilisation de l'intelligence périphérique sans fil peut également présenter des défis en termes de coordination et de gestion des ressources sur les appareils clients. Il est également important de prendre en compte les limites de bande passante et de consommation d'énergie des appareils clients pour garantir que l'apprentissage automatique ne perturbe pas les autres fonctions des appareils. En résumé, l'utilisation de l'intelligence périphérique sans fil pour les appareils IoT peut avoir des implications potentielles importantes en termes de confidentialité des données et d'efficacité de l'apprentissage automatique, mais il est important de prendre en compte les défis et les limites des appareils clients pour garantir une utilisation efficace et responsable de cette technologie.	Les principaux défis dans la mise en œuvre de l'apprentissage fédéré pour les appareils IoT sont les suivants : 1. Confidentialité des données : Les données collectées par les appareils IoT peuvent être sensibles et les utilisateurs peuvent ne pas vouloir les partager avec un serveur central. L'apprentissage fédéré permet de construire un modèle central sans téléverser les données vers un serveur central, mais il est important de garantir la confidentialité des données clients. 2. Hétérogénéité des appareils : Les appareils IoT ont des capacités de calcul et de communication très différentes, ce qui peut rendre difficile la coordination de l'apprentissage fédéré entre les appareils. 3. Distribution non-IID des données : Les données collectées par les appareils IoT peuvent être très différentes les unes des autres, ce qui peut rendre difficile la construction d'un modèle précis à partir de ces données. 4. Coûts de communication : Les appareils IoT ont souvent des limites de bande passante et de consommation d'énergie, ce qui peut rendre coûteuse la communication entre les appareils et le serveur central. 5. Convergence : L'apprentissage fédéré peut nécessiter un grand nombre de rounds de communication pour atteindre une convergence satisfaisante, en particulier avec des ensembles de données clients non-IID. L'adaptation proposée de l'algorithme FedAvg, appelée Communication-Efficient FedAvg (CE-FedAvg), aborde les coûts de communication et les problèmes de convergence de la manière suivante : 1. Réduction des coûts de communication : CE-FedAvg utilise des techniques de compression pour réduire la quantité de données téléversées entre les clients et le serveur central. Les auteurs proposent deux schémas de quantification des poids et des moments d'Adam (Uniforme et Exponentielle) qui sont utilisés en conjonction avec la sparsification et l'encodage de Golomb pour la compression. 2. Réduction du nombre de rounds de communication : CE-FedAvg utilise une forme distribuée de l'optimisation Adam pour réduire le nombre de rounds de communication nécessaires pour atteindre la convergence. Cette méthode permet aux clients de faire plus de mises à jour de poids localement avant de téléverser leurs modèles compressés au serveur central, ce qui réduit le nombre total de rounds nécessaires pour atteindre la convergence. Les expériences menées par les auteurs montrent que CE-FedAvg peut converger vers une précision cible en beaucoup moins de rounds que FedAvg, tout en téléversant moins de données et en étant plus robuste à la compression agressive. En résumé, CE-FedAvg aborde les coûts de communication et les problèmes de convergence en utilisant des techniques de compression et une forme distribuée de l'optimisation Adam pour réduire la quantité de données téléversées et le nombre de rounds nécessaires pour atteindre la convergence.	L'algorithme CE-FedAvg présente plusieurs avantages en termes de réduction des coûts de communication et de convergence plus rapide par rapport à l'algorithme FedAvg. Cependant, il est important de noter qu'il peut également présenter certaines limitations ou inconvénients potentiels : • Complexité accrue : L'ajout de techniques de compression et d'optimisation distribuée, telles que l'optimisation Adam, peut augmenter la complexité de l'algorithme CE-FedAvg. Cela peut rendre sa mise en œuvre et sa gestion plus complexes par rapport à des approches plus simples. • Besoin de ressources supplémentaires : L'utilisation de techniques de compression et d'optimisation distribuée peut nécessiter des ressources supplémentaires, telles que la puissance de calcul et la mémoire, sur les appareils clients. Cela peut être un inconvénient pour les appareils IoT avec des capacités limitées. • Sensibilité aux paramètres : Comme pour tout algorithme d'optimisation, CE-FedAvg peut être sensible à certains paramètres, tels que les taux d'apprentissage et les paramètres d'optimisation. La sélection et le réglage de ces paramètres peuvent nécessiter une expertise supplémentaire. • Besoin de validation expérimentale : Bien que les expériences initiales aient montré des résultats prometteurs, il est important de valider les performances de CE-FedAvg dans une variété de scénarios et de conditions réelles pour évaluer sa robustesse et sa généralisabilité.