Harmoniser Innovation et Confidentialité : Le Futur de l'Enseignement Grâce a l'Apprentissage Fédéré

Chahrazed Labba
Université de Lorraine, Loria, CNRS
Nancy, France
chahrazed.labba@loria.fr

Anne Boyer
Université de Lorraine, Loria, CNRS Nancy,
France
anne.boyer@loria.fr

Résumé — L'intelligence artificielle (IA) gagne de plus en plus de terrain dans le secteur de l'éducation, se révélant être un outil bénéfique capable de transformer les techniques d'enseignement traditionnelles et d'offrir aux apprenants des expériences d'apprentissage individualisées. La personnalisation de l'éducation, bien qu'essentielle pour répondre aux besoins spécifiques des apprenants, soulève des défis importants, notamment en ce qui concerne la gestion et le maintien de la confidentialité des données personnelles des apprenants. Face à ces dilemmes, l'apprentissage fédéré apparait comme une approche intéressante, permettant d'exploiter les données pour améliorer les expériences d'apprentissage tout en conservant les informations sensibles là où elles ont été générées. Cet article explore l'adoption de l'apprentissage fédéré dans l'éducation, en soulignant sa promesse d'un enseignement personnalise sécurisé, tout en abordant les défis liés à la mise en œuvre pratique et éthique dans le secteur de l'éducation.

Mots-clés — Terms—Apprentissage Machine, Confidentialité, Education

I. INTRODUCTION

Dans une ère ou la technologie influence de plus en plus l'éducation, l'introduction de méthodes d'apprentissage basées sur les données de l'apprenant devient essentielle. Les données, qui constituent la base de cette personnalisation, sont la clé de la mise en place de parcours éducatifs adaptés aux besoins de chaque apprenant. En effet, les plateformes éducatives numériques collectent une grande quantité de données, notamment des informations personnelles, des historiques d'apprentissage et des résultats scolaires, qui, si elles sont mal gérées ou exposées, peuvent compromettre la vie privée des apprenants et être potentiellement utilisées à des fins malveillantes. Alors que l'on cherche à développer des méthodes d'enseignement plus efficaces et plus personnalisées, la confidentialité et la sécurité des données des apprenants présentent des préoccupations majeures. Selon [1], six préoccupations éthiques distinctes sont identifiées dans le contexte du big data et de l'apprentissage personnalise, à savoir : la confidentialité des informations, l'anonymat, la surveillance, l'autonomie, la non-discrimination et la propriété des informations.

L'alignement de l'innovation éducative, par l'utilisation de données pour un enseignement personnalisé, et de la confidentialité se présente donc comme un défi majeur à relever afin d'assurer un environnement d'apprentissage sécurisé qui respecte la vie privée. L'apprentissage fédéré apporte une réponse prometteuse à ce défi, en permettant d'entraîner des modèles d'apprentissage automatique de manière décentralisée sans partager les données brutes. Prenons l'exemple de l'application "Gboard" [2] de Google, un clavier virtuel pour téléphones portables. Google [3] utilise l'apprentissage fédéré pour améliorer la prédiction du prochain mot que l'utilisateur va taper en apprenant à partir de chaque saisie sans jamais centraliser ces données. En adaptant ce principe au domaine de l'éducation, les algorithmes peuvent apprendre à partir des données des apprenants tout en les gardant au niveau local (e.g infrastructure Edge Computing) préservant ainsi leur confidentialité et leur sécurité.

Ainsi, dans cet article, nous proposons d'explorer en détail la manière dont l'apprentissage fédéré pourrait être utilisé dans le secteur de l'éducation, en tenant compte à la fois des avantages et des défis associés à sa mise en œuvre. En outre, nous présentons une étude de cas utilisant des données du Centre national d'enseignement à distance (Cned) qui prouve l'efficacité de l'apprentissage fédéré par rapport à l'apprentissage centralisé. Le reste de cet article est organisé comme suit : La section II décrit le principe de l'apprentissage fédéré et ses applications. La section III présente les avantages et les défis liés à l'utilisation de l'apprentissage fédéré dans le secteur de l'éducation. En outre, elle présente une étude de cas pour démontrer l'utilisation de l'apprentissage fédéré dans le contexte du Cned. La section IV conclut cet article et présente les perspectives futures.

II. L'APPRENTISSAGE FEDERE ET SES APPLICATIONS

L'apprentissage fédéré, comme présenté par Google [3], est une méthode d'apprentissage automatique décentralisée qui permet de former d'une manière collaborative un modèle sur des données distribuées sur plusieurs entités (appareils ou organisations). Comme le montre la Fig.1, contrairement aux approches traditionnelles, au lieu de centraliser toutes les données pour l'apprentissage, cette technique crée des modèles localement sur chaque entité et envoie seulement les mises à jour du modèle (par exemple, les poids du modèle) a un serveur central pour être agrégé.

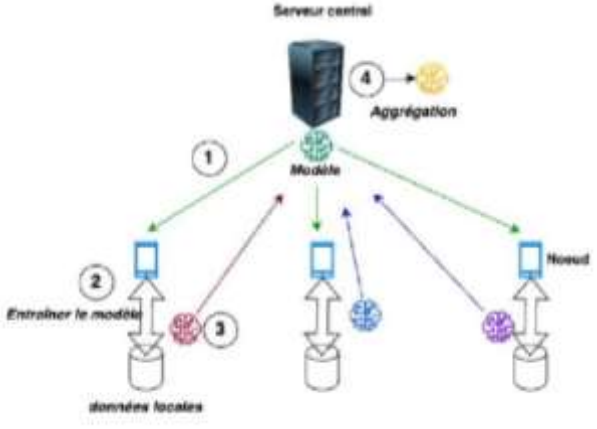


Fig. 1. Principe de l'apprentissage fédéré

Cet agrégat est ensuite envoyé vers toutes les entités locales afin de mettre à jour les modèles locaux de manière itérative jusqu' à ce que le modèle global converge. De cette manière, l'apprentissage préserve la confidentialité des données en les conservant sur l'entité locale plutôt que de les partager ou de les transférer vers un serveur central ou d'autres entités. Etant donné que seules les mises à jour du modèle, et non les données brutes, sont transmises, les informations sensibles restent sécurisées. Cette caractéristique de l'apprentissage fédéré répond à notre besoin de confidentialité des données dans le secteur de l'éducation. Une entité en apprentissage fédéré peut être un utilisateur (e.g un téléphone portable, tablette) ou une organisation (serveurs). Selon le niveau de granulation de l'application de l'apprentissage fédéré, nous distinguons deux types de travaux de recherche. D'une part, les travaux qui se concentrent sur l'apprentissage fédéré inter-organisationnelle, tels que dans [4], les auteurs présentent la manière dont l'apprentissage fédéré peut être utilise pour prédire les défaillances des chaînes de production dans différentes organisations. Dans [5], [6], des frameworks pour l'analyse des données éducatives basées sur l'apprentissage fédéré ont été proposés et peuvent être utilisés pour créer des fédérations d'analyse de données entre de nombreuses institutions. Dans [7], [8], des approches basées sur l'apprentissage fédéré ont été proposées pour traiter les questions de confidentialité et exploiter pleinement le potentiel de l'IA dans le domaine des soins de santé. D'autre part, d'autres travaux de recherche se concentrent sur l'apprentissage fédéré inter-appareils, comme dans [9], les auteurs ont utilisé l'apprentissage fédéré pour prédire le mot suivant dans un clavier virtuel pour téléphones portables. Dans [10], [11], l'apprentissage fédéré est utilisé pour fournir des recommandations personnalisées aux utilisateurs. En [12], les auteurs ont proposé une approche pour l'utilisation de l'apprentissage fédéré combiné à l'Edge computing pour l'analyse distribuée en temps réel des traces d'apprentissage des apprenants.

Bien que l'apprentissage fédéré soit fréquemment étudié dans la littérature en tant que mécanisme de préservation de la confidentialité des données, il existe une lacune notable en ce qui concerne son application et les défis à relever dans le domaine de l'éducation. Des aspects clés tels que la sélection des clients, la gestion de la qualité des données éducatives et la garantie de l'équité dans le modèle global ne sont pas suffisamment discutés ou analysés.

III. L'APPRENTISSAGE FEDERE AU SERVICE DE L'EDUCATION

L'apprentissage fédéré a le potentiel de transformer les systèmes éducatifs en rendant l'apprentissage plus personnalise, plus efficace et plus accessible. Cependant, son utilisation soulève un certain nombre de défis. Les questions d'éthique et de confidentialité restent au premier plan des préoccupations. Cette section résume les avantages et les défis potentiels de l'utilisation de l'apprentissage fédéré dans le secteur de l'éducation (Section III-A, Section III-B). Elle présente en outre une étude de cas sur l'utilisation de l'apprentissage fédéré pour prédire l'échec des étudiants le plus tôt possible compare à une approche centralisée (Section III-C).

A. Avantage de l'approche decentralisée

L'apprentissage fédéré fait partie d'une approche de protection des données. Il s'agit d'un moyen prometteur d'utiliser des données sensibles tout en les préservant au niveau local, ce qui permet la mise en œuvre de modèles d'apprentissage automatique sans nécessiter de stockage centralise des données. Dans le contexte éducatif, où les données personnelles des étudiants peuvent être particulièrement sensibles, cette approche réduit le risque de fuite de données et leur utilisation inappropriée, tout en tirant parti des informations distribuées pour améliorer les méthodes et parcours pédagogiques. En effet, lorsque l'apprentissage fédéré est mis en œuvre de manière appropriée et dans le respect de l'égalité, son utilisation offre un potentiel important de personnalisation des parcours éducatifs, permettant un accès plus équitable aux ressources et aux opportunités éducatives pour les étudiants issus de milieux et d'environnements différents. Ainsi, en utilisant les connaissances générées par l'apprentissage fédéré, les établissements peuvent améliorer et optimiser les ressources et les stratégies d'enseignement, rendant l'éducation plus accessible à divers apprenants. Les contenus pédagogiques et les méthodes d'enseignement peuvent être adaptes pour répondre aux besoins de chaque étudiant, indépendamment de sa situation géographique ou de son statut socio-économique.

B. Défis de l'approche decentralisée

Bien que l'apprentissage fédéré semble être une solution prometteuse, pour des secteurs tels que l'éducation où la confidentialité des données est essentielle, il pose un certain nombre de défis qu'il convient de relever. En effet, la gestion des données dans un contexte décentralisé tel que celui de l'apprentissage fédéré pose des défis à la fois pratiques et techniques. La synchronisation des modèles, la qualité des données et la gestion des erreurs ou des anomalies sont autant de problématiques qui doivent être abordées pour garantir la robustesse et la fiabilité des modèles d'apprentissage fédéré.´ En outre, l'explicabilité des modèles d'apprentissage automatique, en particulier dans le contexte de l'apprentissage fédéré, est une question cruciale car elle détermine la capacité des utilisateurs et des parties prenantes à comprendre, à faire confiance et, en fin de compte, à adopter les modèles et les prédictions générées par ces systèmes. En effet, le processus d'apprentissage est réalisé de manière distribuée où les données restent au niveau local. Cette décentralisation, tout en offrant des avantages en termes de confidentialité des données, rend également le processus d'explication des prédictions du modèle plus compliqué, puisque la connaissance globale est construite sans accès direct aux données locales. Un autre défi consiste à sélectionner soigneusement les clients qui participeront à la phase d'entraînement, afin d'éviter les modèles biais es´ et sous-optimaux. Une bonne stratégie de sélection équilibrant la représentation des données et la gestion de la variabilité des données est nécessaire. La sélection des clients soulève également la question de la qualité et de l'homogénéité des données, afin d'éviter la transmission de problèmes tels que le bruit ou les biais au modèle fédéré global. La résolution de ce problème est cruciale, d'autant plus que nous n'avons pas accès aux données des clients pour juger de leur qualité

C. Etude de cas

Dans cette section, nous fournissons une preuve de concept en décrivant l'application de l'apprentissage fédéré

au cadre spécifique du Cned. L'objectif est d'examiner la capacité d'un modèle fédéré à prévoir l'échec des apprenants du Cned au plus tôt possible. Cette étude est réalisée en tenant compte de l'un des défis cruciaux de l'apprentissage fédéré, à savoir la sélection des clients qui participeront à la phase d'entrainement. L'application de l'apprentissage fédéré peut être facilement transposée au contexte du Cned. En effet, les étudiants se connectent au Learning Management System et a d'autres applications via leurs terminaux (par exemple smartphone, tablette, ordinateur personnel), qui représentent les dispositifs locaux. L'infrastructure de stockage du Cned est quant à elle considérée comme le serveur central. Une question ouverte est de savoir si l'utilisation du l'apprentissage fédéré dans le contexte du Cned permet de construire un système d'alerte fiable qui prédit les performances des étudiants sur une base hebdomadaire. Dans le cadre de ce travail, notre cas d'étude est constitué des apprenants inscrits au cours de physique-chimie durant l'année scolaire 2017-2018. Au total, l'année scolaire compte 46 semaines et 671 étudiants inscrits. Pour prédire les performances des étudiants sur une base hebdomadaire, le problème est formalisé comme un problème de n-classification. La classification se compose de trois classes : risque d'échec élevé, risque d'échec moyen et succès. Pour chaque semaine w_i , un apprenant est défini par un tuple $X = (f_1, ..., f_m, y)$ ou` $f_1, ..., f_m$ sont les caractéristiques et y la classe à prédire.

Dans un premier temps, nous avons étudié l'impact de la sélection des clients sur les performances du modèle fédéré global. Deux stratégies sont évaluées : une stratégie aléatoire qui consiste à sélectionner au hasard les clients pour d'entraînement et une stratégie guidée qui fournit une sélection équilibrée en termes d'étiquettes de classe.

Les données utilisées présentent des déséquilibres en ce qui concerne l'étiquette de la classe "risque d'échec moyen".

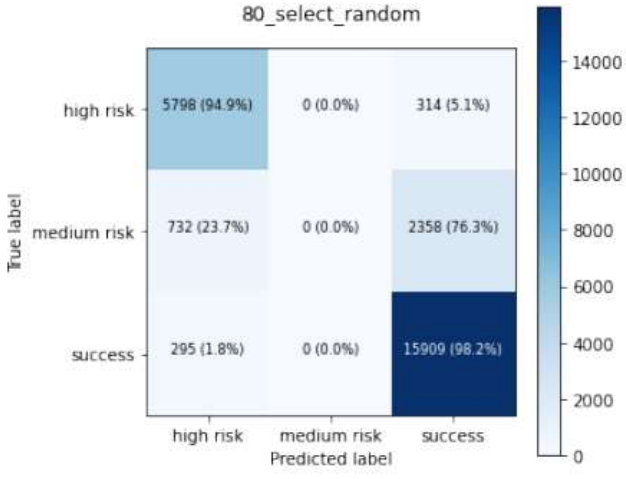


Fig. 2. Sélection Aléatoire

La première stratégie consiste à prendre au hasard un ensemble d'échantillons de clients, pour l'entraînement, sans vérifier les proportions des 3 classes prises dans celui-ci. La seconde stratégie consiste à sélectionner un ensemble de clients dont 30 % des échantillons appartiennent à la classe à haut risque d'échec, 30 % à la classe a risque moyen d'échec et le reste a la classe de succès. Le nombre d'échantillons d'entraînement est fixé à 80 pour les deux stratégies. Nous constatons qu'avec une stratégie de sélection aléatoire (Fig. 2), il y a un problème de classification des étudiants à risque moyen et que la plupart du temps, ils sont classés comme ayant réussi. Cette classification est due au fait que dans l'échantillon aléatoire, la classe a risque moyen est sous-représentée par rapport aux autres classes. Comme le montre la Fig 3, la classe a risque moyen est mieux prédite dans le cadre de la stratégie de sélection guidée.

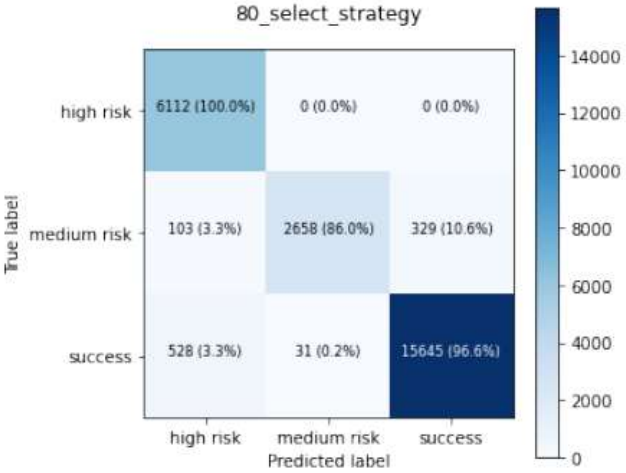
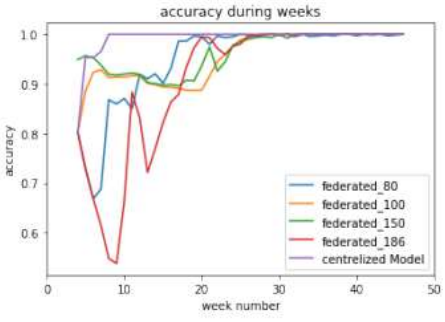


Fig. 3. Sélection Guidée

Dans un deuxième temps, nous avons comparé les résultats des prédictions utilisant une approche centralisée, ou les données sont centralisées en un seul endroit, à l'approche fédérée où nous utilisons une approche guidée pour sélectionner les participants qui contribueront à l'entraînement du modèle global (Artificial Neural Network). Une série d'expériences a été menée pour trouver les meilleurs paramètres pour notre modèle, y compris la définition de l'optimiseur, le taux d'apprentissage (TA) et le nombre de tours. Pour des raisons d'espace, les paramètres appropriés sont présentés directement dans le tableau et ne seront pas discutés. Les configurations diffèrent principalement en termes de nombre des participants sélectionnés (80, 100, 150, 186) a` utiliser pendant la phase d'entraînement.

	nb_participants	optimizeur	nb_tours	TA
Config.1	80	SGD-SGD	15	0.02-1.0
Config.2	100			
Config.3	150			
Config.4	186			

TABLE I
CONFIGURATIONS



Comme le montre la Fig. 4 et comme prévu, le modèle centralise est plus performant que les modèles fédérés en termes de précision des tests. Chaque semaine, le modèle centralise est entraîné sur toutes les données disponibles, tandis que les modèles fédérés sont entraînés sur un sous-ensemble de données. Cependant, la première chose à remarquer est que tous les modèles fédérés finissent par converger pour atteindre une précision très proche ou même égale à celle du modèle centralise. Dans notre contexte, l'objectif est de prédire le plus tôt possible quand les étudiants présentent un risque d'échec élevé ou moyen afin de prendre les mesures appropriées. Nous avons donc besoin d'un modèle fédéré pour atteindre cet objectif. Avec les trois premières configurations 80, 100 et 150 respectivement, les modèles fédérés ont une précision qui dépasse 85% à partir de la semaine 8. Ainsi, en sélectionnant le nombre approprie d'échantillons, en appliquant une bonne stratégie de sélection et en choisissant les bons paramètres pour l'entraînement, le modèle fédéré peut progressivement s'approcher des performances du modèle centralise.

IV. Conclusion et perspectives futures

Le secteur de l'éducation est actuellement confronté à un certain nombre de limites, notamment les menaces pesant sur la confidentialité des données et les couts d'infrastructure considérables lies à la bande passante et aux ressources informatiques nécessaires à la gestion de grandes quantités de données. Face à ces dilemmes, l'apprentissage fédéré apparaît comme une approche intéressante, permettant de transformer les systèmes éducatifs en rendant l'apprentissage plus personnalise, plus efficace et plus accessible tout en conservant les informations sensibles la où elles ont été générées. Dans cet article, nous avons présenté la manière dont l'apprentissage fédéré pourrait être utilisé dans le secteur de l' éducation, en tenant compte à la fois des avantages et des défis associés à sa mise en œuvre. En outre, nous avons expose une étude de cas en employant des données provenant du Cned afin de démontrer l'efficacité de l'apprentissage fédéré, en mettant particulièrement l'accent sur le défi que représente la sélection des clients pour procéder à l'entraînement. L'apprentissage fédéré est prometteur, notamment en termes de protection des données. Cependant, malgré ce potentiel, il révèle plusieurs défis cruciaux tels que l'explicabilité des modèles et la gestion de la qualité des données. L'explicabilité est essentielle pour garantir la transparence et la confiance dans les systèmes basés sur l'IA, en particulier dans un secteur sensible comme l'éducation, où les décisions prises par l'IA peuvent avoir un impact direct et significatif sur le parcours des étudiants. Enfin, la qualité des données est essentielle à l'efficacité du modèle, et des problèmes à ce niveau peuvent entraver la performance et la fiabilité du système d'apprentissage fédéré. Il est donc impératif de relever ces défis afin de garantir l'utilisation éthique, transparente et fiable de l'IA dans l'éducation.

REFERENCES

[1] P. M. Regan and J. Jesse, "Ethical challenges of edtech, big data and personalized learning: Twenty-first century student sorting and tracking," Ethics and Information Technology, vol. 21, no. 3, pp. 167-179, 2019.

[2] T. Yang, G. Andrew, H. Eichner, H. Sun, W. Li, N. Kong, D. Ramage, and F. Beaufays, "Applied federated learning: Improving google keyboard query suggestions," arXiv preprint arXiv:1812.02903, 2018.

[3] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in Artificial intelligence and statistics. PMLR, 2017, pp. 12731282.

[4] N. Ge, G. Li, L. Zhang, and Y. Liu, "Failure prediction in production line based on federated learning: an empirical study," Journal of Intelligent Manufacturing, pp. 1-18, 2021.

[5] S. Guo, D. Zeng, and S. Dong, "Pedagogical data analysis via federated learning toward education 4.0," American Journal of Education and Information Technology, vol. 4, no. 2, p. 56, 2020.

[6] C. Fachola, A. Tornana, P. Bermolen, G. Capdehourat, L. Etcheverry, and M. I. Fariello, "Federated learning for data analytics in education," Data, vol. 8, no. 2, 2023. [Online]. Available: https://www.mdpi.com/2306-5729/8/2/43

[7] Q. Wu, X. Chen, Z. Zhou, and J. Zhang, "Fedhome: Cloud-edge based personalized federated learning for in-home health monitoring," IEEE Transactions on Mobile Computing, 2020.

[8] N. Rieke, J. Hancox, W. Li, F. Milletari, H. R. Roth, S. Albarqouni, S. Bakas, M. N. Galtier, B. A. Landman, K. Maier-Hein et al., "The future of digital health with federated learning," NPJ digital medicine, vol. 3, no. 1, pp. 1-7, 2020.

[9] A. Hard, C. M. Kiddon, D. Ramage, F. Beaufays, H. Eichner, K. Rao, R. Mathews, and S. Augenstein, "Federated learning for mobile keyboard prediction," 2018. [Online]. Available: https://arxiv.org/abs/1811.03604

[10] S. Zhao, R. Bharati, C. Borcea, and Y. Chen, "Privacy-aware federated learning for page recommendation," in 2020 IEEE International Conference on Big Data (Big Data), 2020, pp. 1071-1080.

[11] P. Zhou, K. Wang, L. Guo, S. Gong, and B. Zheng, "A privacy-preserving distributed contextual federated online learning framework with big data support in social recommender systems," IEEE Transactions on Knowledge and Data Engineering, vol. 33, no. 3, pp. 824-838, 2021.

[12] C. Labba, R. Ben Atitallah, and A. Boyer, "combining artificial intelligence and edge computing to reshape distance education (case study: K-12 learners)," in International Conference on Artificial Intelligence in Education. Springer, 2022, pp. 218-230

.