MỘT KHẢO SÁT VỀ HỌC LIÊN KẾT CÁ NHÂN HÓA

Hồ Đắc Hưng [(1)]
(1) Trường Đại học Thủ Dầu Một
Ngày nhận bài: 10/11/2025; Chấp nhận đăng: 30/12/2025
Email tác giả: hunghd@tdmu.edu.vn

Tóm tắt

Học liên kết đã nổi lên như một mô hình đầy hứa hẹn cho học máy phân tán, bảo vệ quyền riêng tư dữ liệu đồng thời cho phép huấn luyện mô hình cộng tác. Tuy nhiên, học liên kết tiêu chuẩn giả định rằng tất cả các máy khách đều có chung các mục tiêu nhiệm vụ, điều này thường không thực tế trong các ứng dụng thực tế khi máy khách thể hiện sự phân phối dữ liệu không đồng nhất và các mục tiêu huấn luyện khác nhau. Học liên kết cá nhân hóa giải quyết hạn chế cơ bản này bằng cách cho phép máy khách huấn luyện các mô hình được cá nhân hóa phù hợp với các yêu cầu cụ thể của chúng đồng thời tận dụng lợi ích của sự cộng tác phân tán. Khảo sát này cung cấp tổng quan toàn diện về học liên kết cá nhân hóa, bao gồm: (1) các khái niệm và động lực cơ bản; (2) phân loại các phương pháp tiếp cận học liên kết cá nhân hóa; (3) các thách thức chính; và (4) các hướng nghiên cứu mở. Chúng tôi cũng thảo luận về sự đánh đổi giữa cá nhân hóa và khái quát hóa, phân tích các giải pháp hiện có và xác định các thách thức trong tương lai trong lĩnh vực đang phát triển nhanh chóng này.

Từ khóa: *Cá nhân hóa, học liên kết, học máy*

Abstract

A COMPREHENSIVE SURVEY ON PERSONALIZED FEDERATED LEARNING

Federated learning (FL) has emerged as a promising paradigm for distributed machine learning that preserves data privacy while enabling collaborative model training. However, standard FL assumes all clients share identical task objectives, which often proves unrealistic in practical applications where clients exhibit heterogeneous data distributions and varying learning goals. Personalized federated learning (PFL) addresses this fundamental limitation by enabling clients to learn personalized models tailored to their specific requirements while leveraging the benefits of distributed collaboration. This survey provides a comprehensive overview of personalized federated learning, covering: (1) fundamental concepts and motivations; (2) classification of PFL approaches; (3) key challenges; and (4) open research directions. We also discuss the trade-offs between personalization and generalization, analyze existing solutions, and identify future challenges in this rapidly evolving field.

1. Giới thiệu

Học liên kết đã cách mạng hóa học máy phân tán bằng cách cho phép các tổ chức cùng nhau đào tạo các mô hình học máy mà không cần chia sẻ dữ liệu thô, do đó bảo vệ quyền riêng tư và giảm thiểu chi phí giao tiếp so với học tập tập trung (McMahan và nnk., 2017). Tuy nhiên, giả định cơ bản làm nền tảng cho các khuôn khổ học liên kết thông thường - rằng tất cả các máy khách tham gia đều tối ưu hóa hướng tới một mục tiêu toàn cầu duy nhất hiếm khi phù hợp với các tình huống thực tế.

Trong các ứng dụng thực tế, máy khách thường thể hiện tính không đồng nhất đáng kể trên nhiều chiều. Tính không đồng nhất dữ liệu phát sinh từ dữ liệu không độc lập và phân phối giống hệt nhau trên các máy khách, trong đó mỗi máy khách sở hữu các phân phối dữ liệu duy nhất phản ánh các đặc điểm cục bộ (Kairouz và nnk., 2021). Tính không đồng nhất hệ thống xuất hiện từ các tài nguyên tính toán khác nhau và kết nối mạng giữa các thiết bị. Tính không đồng nhất tác vụ biểu hiện khi máy khách theo đuổi các mục tiêu huấn luyện khác nhau thay vì một mục tiêu thống nhất. Xem xét một mạng lưới chăm sóc sức khỏe nơi các bệnh viện hướng đến việc cải thiện các mô hình chẩn đoán dành riêng cho bệnh nhân, hoặc một hệ thống dự đoán bàn phím di động nơi người dùng yêu cầu hoàn thành văn bản được cá nhân hóa phản ánh các mẫu ngôn ngữ riêng lẻ. Trong những trường hợp như vậy, việc áp đặt một mô hình toàn cục duy nhất trên các máy khách không đồng nhất thường mang lại hiệu suất không tối ưu, vì mô hình toàn cục đại diện cho một sự thỏa hiệp có thể không phục vụ tốt cho bất kỳ máy khách nào.

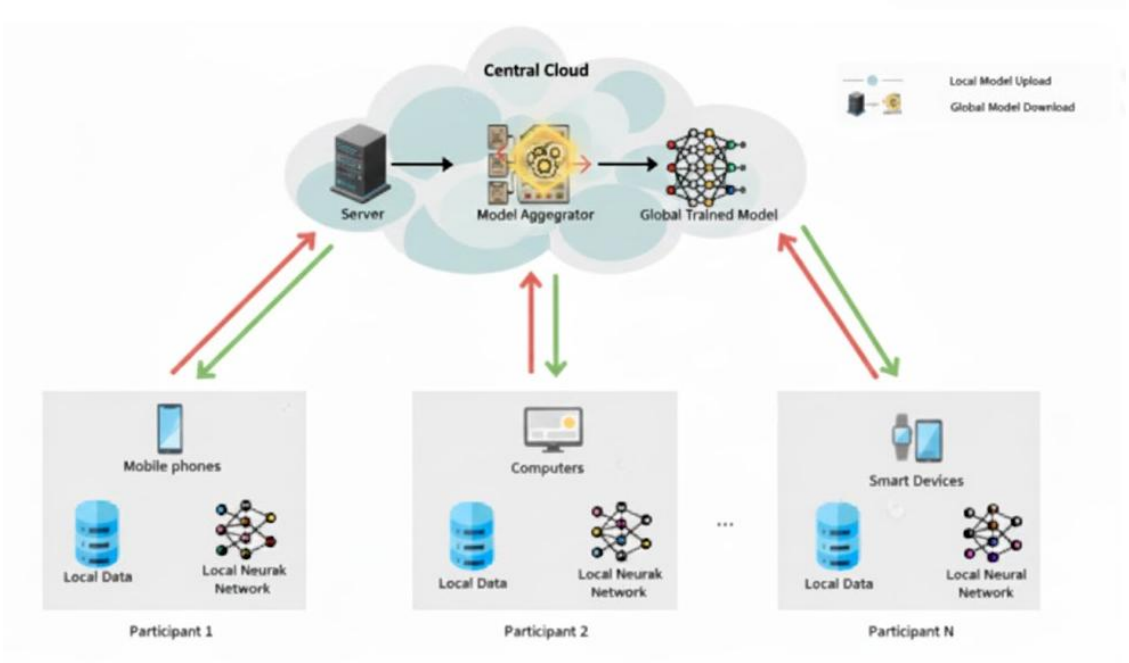
Học liên kết cá nhân hóa giải quyết những hạn chế này bằng cách cho phép mỗi máy khách phát triển các mô hình được thiết kế riêng theo yêu cầu cục bộ của chúng, đồng thời tận dụng học tập cộng tác để cải thiện chất lượng mô hình. Khảo sát này tổng hợp những tiến bộ gần đây trong học liên kết cá nhân hóa, cung cấp thông tin toàn diện về các phương pháp, thách thức và cơ hội trong tương lai.

2. Các khái niệm cơ bản

Học liên kết tiêu chuẩn hoạt động thông qua một quy trình lặp lại liên quan đến một máy chủ trung tâm và nhiều máy khách. Trong mỗi vòng, máy chủ sẽ phát mô hình toàn cục hiện tại đến các máy khách được chọn. Máy khách thực hiện các cập nhật cục bộ trên dữ liệu riêng của mình và truyền các cập nhật mô hình trở lại máy chủ. Máy chủ tổng hợp các cập nhật này bằng một cơ chế tổng hợp, thường là trung bình có trọng số, để tạo ra một mô hình toàn cục mới (McMahan và nnk., 2017). Thuật toán trung bình liên bang chuẩn (FedAvg) giảm thiểu hàm mất mát toàn cục như sau:

$$\min_{w} \frac{1}{N} \sum_{i=1}^{N} F_i(w)$$

với N biểu thị số lượng máy khách và $F_i(w) = \frac{1}{|D_i|} \sum_{z \in D_i} l(w, z)$ đại diện cho hàm mất mát cục bộ của máy khách i đối trên dữ liệu D_i của chúng.



Hình 1. *Kiến trúc mô hình học liên kết*

Nguồn: Tác giả, 2025

Không giống như học liên kết tiêu chuẩn theo đuổi một mô hình toàn cục duy nhất, học liên kết cá nhân hóa thừa nhận rõ ràng rằng máy khách có thể được hưởng lợi từ các mô hình riêng biệt. Mô hình cá nhân hóa có thể được xây dựng như một giải pháp cho nhiều bài toán tối ưu hóa liên quan:

$$\min_{w_1,\ldots,w_N} \sum_{i=1}^{N} F_i(w_i)$$

tuân theo các điều khoản chính quy hoặc ràng buộc mã hóa mối quan hệ giữa các mô hình cụ thể của máy khách. Điểm mấu chốt trong học liên kết cá nhân hóa nằm ở việc cân bằng giữa cá nhân hóa (phù hợp với dữ liệu trên máy khách) với sự hợp tác (tận dụng kiến thức toàn cục). Sự đánh đổi này là trọng tâm của tất cả các phương pháp học liên kết cá nhân hóa.

3. Phân loại các phương pháp học liên kết cá nhân hóa

3.1. Phương pháp học đa tác vụ

Các khung học đa tác vụ coi học liên kết như một bài toán đa tác vụ, trong đó mỗi máy khách đại diện cho một tác vụ riêng biệt. Quan điểm này cho phép tận dụng kiến thức về mối quan hệ tác vụ để cải thiện hiệu suất của từng tác vụ.

Federated Multi-Task Learning (FMTL) (Smith và nnk., 2017) xây dựng bối cảnh liên kết như một quá trình huấn luyện nhiều tác vụ liên quan. Máy chủ duy trì một biểu diễn chia sẻ chiều thấp mà tất cả máy khách đều có thể sử dụng, trong khi mỗi máy khách duy trì các tham số cụ thể cho từng nhiệm vụ.

Cách tiếp cận này tận dụng kết nối giữa các tác vụ của máy khách trong khi vẫn duy trì tính cá nhân hóa thông qua các tham số riêng lẻ. Tuy nhiên, nó đòi hỏi phải xác

định rõ ràng các mối quan hệ tác vụ và giả định một cấu trúc cụ thể cho mối quan hệ này.

3.2. Phương pháp học dựa tối ưu hóa cận

Các khung học dựa trên tối ưu hóa cận (meta-learning) huấn luyện các mô hình thích ứng nhanh với các nhiệm vụ mới với dữ liệu tối thiểu. Khung này đặc biệt phù hợp với học liên kết cá nhân hóa, nơi mà việc thích ứng nhanh chóng với các mục tiêu của máy khách cục bộ là điều mong muốn.

Per-FedAvg (Zhan và nnk., 2023) áp dụng các nguyên tắc học tập dựa trên siêu dữ liệu không phụ thuộc mô hình vào các thiết lập liên kết. Mỗi máy khách thực hiện thêm một bước phản hồi trong quá trình huấn luyện cục bộ để mô phỏng khả năng thích ứng nhanh. Điều này cho phép máy khách nhanh chóng cá nhân hóa mô hình toàn cục thành dữ liệu cục bộ thông qua một bước cập nhật duy nhất tại thời điểm suy luận.

Ditto (Li và nnk., 2021) mở rộng tính cá nhân hóa bằng cách cho phép máy khách duy trì cả mô hình cục bộ và mô hình toàn cục được kết nối thông qua có chế điểm phạt không giống nhau. Cách tiếp cận này tách biệt quá trình đào tạo cục bộ khỏi việc cập nhật mô hình toàn cục, cung cấp khả năng kiểm soát rõ ràng đối với sự đánh đổi giữa cá nhân hóa và khái quát hóa.

Hướng tiếp cận này cung cấp khả năng thích ứng nhanh đã được chứng minh; mức độ cá nhân hóa linh hoạt; tương thích với nhiều kiến trúc mô hình khác nhau. Tuy nhiên, chi phí tính toán tăng lên do khối lượng tính toán bổ sung, có thể yêu cầu sự điều chỉnh dựa trên kinh nghiệm và điều kiện hội tụ lý thuyết tương đối phức tạp.

3.3. Hỗn hợp các mô hình chuyên gia

Khung hỗn hợp chuyên gia phân tách mô hình thành các thành phần chuyên biệt, cho phép kích hoạt có chọn lọc dựa trên các đặc điểm đầu vào. Điều này tự nhiên phù hợp với các kịch bản học liên kết cá nhân hóa, trong đó các máy khách khác nhau được hưởng lợi từ các thành phần mô hình khác nhau.

Federated Mixture of Experts (Reisser và nnk., 2021) duy trì một kho lưu trữ các mô-đun chuyên gia trên máy chủ. Mỗi máy khách lựa chọn và tinh chỉnh một tập hợp con các chuyên gia liên quan đến nhiệm vụ của mình.

Personalized FedPAQ (Chen và nnk., 2021) kết hợp các chuyên gia với đào tạo nhận thức về lượng tử hóa, cho phép cá nhân hóa trong môi trường hạn chế về tài nguyên. Mỗi máy khách huấn luyện một lớp các mô-đun chuyên gia cục bộ trong khi chia sẻ kho lưu trữ chuyên gia toàn cục.

Hướng tiếp cận cho phép cá nhân hóa chi tiết thông qua lựa chọn chuyên gia, đáp ứng các yêu cầu đa dạng của máy khách, hỗ trợ cá nhân hóa dần dần. Tuy nhiên mô hình phức tạp hơn, yêu cầu khởi tạo và quản lý các mô-đun chuyên gia cần phải cẩn thận và có thể ảnh hưởng đến hiệu năng.

3.4. Phương pháp dựa trên cụm

Các phương pháp phân cụm phân chia máy khách thành các nhóm có mục tiêu hoặc phân phối dữ liệu tương tự, cho phép đào tạo mô hình cấp cụm cân bằng giữa tính cá nhân hóa và hiệu quả.

Clustered Federated Learning (Ghosh và nnk., 2022) nhóm máy khách vào các cụm, trong đó các thành viên theo đuổi các mục tiêu liên quan. Các mô hình cấp cụm

được đào tạo cộng tác trong mỗi cụm, cung cấp khả năng cá nhân hóa ở cấp cụm thay vì cấp cá nhân.

Hierarchical Federated Learning (Cai và nnk., 2022) xây dựng các cấu trúc cụm phân cấp, trong đó các máy khách ở cấp thấp hơn kết nối với các bộ tổng hợp trung gian, sau đó kết nối với một bộ tổng hợp toàn cục. Điều này cho phép cá nhân hóa đa cấp.

Hướng tiếp cận này giảm chi phí trao đổi thông tin so với các mô hình máy khách riêng lẻ, tận dụng tính tương đồng của máy khách, có khả năng mở rộng cho các nhóm máy khách lớn. Tuy nhiên, hướng tiếp cận này cũng tiềm ẩn lỗi phân cụm và chi phí phân cụm cao, khó lựa chọn mức độ chi tiết cụm tối ưu, yêu cầu các số liệu tương đồng có thể chưa được biết trước.

3.5. Các phương pháp tiếp cận lai và mới nổi

Những phát triển gần đây kết hợp nhiều chiến lược học liên kết cá nhân hóa để nâng cao hiệu suất.

Federated Learning with Matched Averaging (Cai và nnk., 2020) xác định các máy khách có cấu trúc tương tự thông qua việc so khớp biểu diễn và tính trung bình các mô hình của chúng một cách có chọn lọc, đạt được sự cá nhân hóa chi tiết mà không cần phân cụm rõ ràng.

Personalized Federated Learning with Theoretical Guarantees (Fallah và nnk., 2020) kết hợp tổng hợp mô hình thích ứng với phân tích hội tụ lý thuyết, cung cấp các đảm bảo mạnh mẽ cho các môi trường không đồng nhất.

Contrastive Learning-Based Personalized Federated Learning (Zhou và nnk., 2024) tận dụng các mục tiêu học tương phản mô hình để tăng cường cá nhân hóa trong các thiết lập liên kết, đặc biệt là đối với các tình huống đa phương thức. Cách tiếp cận này học các biểu diễn được cá nhân hóa bằng cách tối đa hóa sự đồng thuận giữa các chế độ xem hoặc phương thức khác nhau của cùng một dữ liệu người dùng trong khi giảm thiểu sự đồng thuận giữa các người dùng khác nhau.

4. Thách thức và hướng nghiên cứu mở

Trên các tập dữ liệu không đồng nhất phổ biến như CIFAR-10/100 hoặc các bộ dữ liệu chăm sóc sức khỏe, các phương pháp học liên kết tiên tiến như Per-FedAvg, pFedME, hoặc các biến thể của FL-MAML thường đạt được mức cải thiện độ chính xác từ 5% đến 15% so với FedAvg cơ bản trên các máy khách cục bộ. Trong các kịch bản cực kỳ không đồng nhất, mức tăng có thể vượt quá 20% vì FedAvg có thể thất bại trong việc hội tụ. Các phương pháp học liên kết cá nhân hóa như FedPer hoặc Ditto thường yêu cầu số lượng vòng giao tiếp máy chủ/máy khách ít hơn 2-5 lần để đạt được mức độ chính xác tương đương so với FedAvg. Điều này đặc biệt quan trọng trong môi trường băng thông thấp. Khi đối mặt với sự không đồng nhất về số lượng dữ liệu, các phương pháp học liên kết cá nhân hóa đã giảm thiểu độ lệch chuẩn của độ chính xác giữa các máy lên đến 50%, đảm bảo một giải pháp công bằng và ổn định hơn cho tất cả các bên tham gia (Li và nnk., 2020).

Môi trường liên kết thường có băng thông hạn chế và chi phí giao tiếp cao (Chen và nnk, 2021). Mặc dù học liên kết tiêu chuẩn giảm thiểu việc giao tiếp so với các

phương pháp tập trung, nhưng việc học liên kết cá nhân hóa tập trung vào các mô hình riêng lẻ có khả năng làm tăng thêm gánh nặng giao tiếp. Việc áp dụng các cơ chế nén có thể giảm thiểu chi phí giao tiếp nhưng sẽ có thể làm mất đi một số thông tin cụ thể cần cho cá nhân hóa. Tùy theo từng ngữ cảnh cụ thể có thể áp dụng các kỹ thuật nén phù hợp băng thông, độ trễ và độ chính xác yêu cầu.

Phân tích lý thuyết về hội tụ học liên kết cá nhân hóa trong điều kiện dữ liệu không đồng nhất vẫn chưa hoàn thiện. Tối ưu hóa không lồi với mất mát không đồng nhất, tần suất cập nhật cục bộ khác nhau và các thành phần cá nhân hóa làm phức tạp việc phân tích hội tụ. Hầu hết các kết quả lý thuyết đều đòi hỏi những giả định có thể không đúng trong các tình huống thực tế rất không đồng nhất. Việc mô tả chặt chẽ hơn mối quan hệ giữa mức độ không đồng nhất, mức độ cá nhân hóa và tỷ lệ hội tụ vẫn là một vấn đề chưa có lời giải.

Việc cá nhân hóa quá mức có nguy cơ quá khớp với dữ liệu cục bộ hạn chế và làm mất đi lợi ích tổng quát từ việc cộng tác. Cá nhân hóa không đủ sẽ không nắm bắt được các yêu cầu cụ thể của máy khách. Việc tìm ra sự cân bằng tối ưu phụ thuộc vào vấn đề và khó có thể xác định trước. Mức độ cá nhân hóa tối ưu thay đổi đáng kể tùy theo máy khách và nhiệm vụ. Việc phát triển các phương pháp có nguyên tắc để tự động xác định mức độ cá nhân hóa vẫn là một hướng nghiên cứu quan trọng. Các phương pháp hiện tại thường yêu cầu điều chỉnh thủ công hoặc tìm kiếm lưới tốn kém về mặt tính toán.

Việc cá nhân hóa gây ra thêm rủi ro về quyền riêng tư. Các mô hình dành riêng cho máy khách có thể dễ bị tấn công suy luận hơn, và việc chia sẻ các bản cập nhật mô hình được cá nhân hóa có thể làm rò rỉ thông tin riêng của máy. Khi các mô hình cá nhân hóa ngày càng trở nên cụ thể hơn với từng máy khách, chúng có thể tự nhiên mã hóa nhiều thông tin nhận dạng hơn. Việc định lượng rò rỉ quyền riêng tư cụ thể cho các mô hình cá nhân hóa và phát triển các cơ chế bảo vệ quyền riêng tư phù hợp là một lĩnh vực nghiên cứu quan trọng.

5. Kết luận

Học liên kết cá nhân hóa giải quyết những hạn chế cơ bản của học liên kết tiêu chuẩn bằng cách cho phép máy khách học các mô hình được điều chỉnh theo yêu cầu cụ thể của chúng, đồng thời tận dụng lợi ích của huấn luyện cộng tác. Qua khảo sát, có thể khẳng định học liên kết cá nhân hoá không chỉ là một giải pháp kỹ thuật cho bài toán dữ liệu không đồng nhất, mà còn là một bước tiến quan trọng hướng tới tính công bằng và hiệu quả thực tế trong học máy phân tán.

Trong một số lĩnh vực yêu cầu tính riêng tư của dữ liệu như y tế, việc áp dụng cách tiếp cận này để triển khai các mô hình sẽ đáp ứng được tiêu chí riêng tư. Trong tương lai, khi sự giao thoa giữa trí tuệ nhân tạo trên điện toán biên và internet vạn vật ngày càng sâu sắc, học liên kết cá nhân hoá sẽ đóng vai trò then chốt trong việc xây dựng các hệ thống trí tuệ nhân tạo bền vững và lấy người dùng làm trung tâm. Khảo sát này đã cung cấp cái nhìn tổng quan toàn diện về các phương pháp học liên kết, những thách thức và hướng nghiên cứu.

TÀI LIỆU THAM KHẢO

[1] Cai, Y., Xi, W., Shen, Y., Peng, Y., Song, S., & Zhao, J. (2022). High-efficient hierarchical federated learning on non-IID data with progressive collaboration. *Future Generation Computer Systems*, *137*, 111-128.

[2] Chen, M., Shlezinger, N., Poor, H. V., Eldar, Y. C., & Cui, S. (2021). Communication-efficient federated learning. *Proceedings of the National Academy of Sciences*, *118*(17), e2024789118.

[3] Fallah, A., Mokhtari, A., & Ozdaglar, A. (2020). Personalized federated learning with theoretical guarantees: A model-agnostic meta-learning approach. *Advances in neural information processing systems*, *33*, 3557-3568.

[4] Ghosh, A., Chung, J., Yin, D., & Ramchandran, K. (2022). An efficient framework for clustered federated learning. *IEEE Transactions on Information Theory*, *68*(12), 8076-8091.

[5] Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., ... & Zhao, S. (2021). Advances and open problems in federated learning. *Foundations and trends® in machine learning*, *14*(1–2), 1-210.

[6] Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020). Federated learning: Challenges, methods, and future directions. *IEEE signal processing magazine*, *37*(3), 50-60.

[7] Li, T., Hu, S., Beirami, A., & Smith, V. (2021, July). Ditto: Fair and robust federated learning through personalization. In *International conference on machine learning* (pp. 6357-6368). PMLR.

[8] McMahan, B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017, April). Communication-efficient learning of deep networks from decentralized data. In *Artificial intelligence and statistics* (pp. 1273-1282). PMLR.

[9] Reisser, M., Louizos, C., Gavves, E., & Welling, M. (2021). Federated mixture of experts. *arXiv preprint arXiv:2107.06724*.

[10] Smith, V., Chiang, C. K., Sanjabi, M., & Talwalkar, A. S. (2017). Federated multi-task learning. *Advances in neural information processing systems*, *30*.

[11] Wang, H., Yurochkin, M., Sun, Y., Papailiopoulos, D., & Khazaeni, Y. (2020). Federated learning with matched averaging. *arXiv preprint arXiv:2002.06440*.

[12] Zhan, Z., & Zhang, X. (2023, July). Computation-effective personalized federated learning: A meta learning approach. In *2023 IEEE 43rd International Conference on Distributed Computing Systems (ICDCS)* (pp. 957-958). IEEE.

[13] Zhou, X., Yang, Q., Zheng, X., Liang, W., Wang, K. I. K., Ma, J., ... & Jin, Q. (2024). Personalized federated learning with model-contrastive learning for multi-modal user modeling in human-centric metaverse. *IEEE Journal on Selected Areas in Communications*, *42*(4), 817-831.