INTERNATIONAL JOURNAL OF SOCIAL SCIENCES BULLETIN
ISSN: (E) 3007-1917 (P) 3007-1909
Volume 3, Issue 8, 2025

PRIVACY-PRESERVING PERSONALIZED TRAVEL PLANNING USING PHASE-ADAPTIVE FEDERATED LEARNING

Daim Asif[*1], Sadia Hanif[2]

[*1] Manchester Metropolitan University, Manchester, United Kingdom
[2]Department of Management Sciences, Riphah International University, Islamabad

[*1]daimasif5@gmail.com, [2]sadia.hanif@riphah.edu.pk,

Corresponding Author: *
Daim Asif
DOI: https://doi.org/10.5281/zenodo.16885385

Received	Revised	Accepted	Published
16 May, 2025	17 June, 2025	17 July, 2025	16 August, 2025

ABSTRACT

Background

Personalized travel itinerary systems are crucial for modern travelers, since they provide individualized suggestions based on choices like location, budgetary constraints, and interest.

Methodology

The phase-adaptive federated learning methodology takes a three-tiered approach to privacy-preserving journey planning, defining training phases (cold-start, warm-up, and convergence) using gradient norms and loss stability analysis. Client selection begins randomly and then moves to the top 40% of high update clients during convergence. Aggregation happens every 5 rounds rather than every round, and local epochs grow from 1 to 5. It safeguards sensitive user preferences by federating global parameters while retaining personalized layers on-device and employing phase-aware noise injections to thwart model inversion assaults.

Results

PAFL method produces three major findings: (1) Superior personalization with0.87nDCG@10, 18.7% higher than FedAvg and near centralized performance (0.89); (2) Strong privacy preservation with a <3.1% attack success rate in model inversion attacks, showing a 12x lower vulnerability than FedAvg (45.3%); and (3) Optimal efficiency with 42% communication reduction (59.4 MB total) through phase-adaptive aggregation. These findings provide new benchmarks for the privacy-utility trade-off in federated travel planning.

Conclusion

PAFL offers near-centralized recommendations quality while significantly reducing attack risk through adaptive privacy-personalization balance. Simultaneously, it facilitates communication overhead, which is the essential trade-off between privacy protection, accuracy, and resource efficiency for effective edge deployment.

Keywords

Phase-Adaptive Federated Learning, Privacy-Preserving Recommendation, Hybrid Personalisation, Travel Planning System.

INTRODUCTION

Personalized travel itinerary generation systems have become indispensable tools for modern travelers, offering customized recommendations based on individual preferences such as destination, budget, and interests.(1,2).

Personalised trip planning systems provide tailored routes based on user choices, previous habits and contextual data. However, centralized data collection raises serious privacy problems.(3). Federated Learning (FL) has emerged as a possible alternative by training models locally on users' devices and sharing just model updates. (4). Despite its benefits, ordinary FL has three key drawbacks in travel applications: 1) NON-IID data distributions reduce model performance.(5), 2) Fixed hyper parameters (e.g. aggregation frequency) cause efficiency constraints, and 3) Static systems are susceptible to adaptive privacy attacks (6), (7). We present a Phase-Adaptive Federated Learning (PAFL) system that overcomes these constraints by dynamically adapting to training phases. PAFL introduces:

1. **Real-time Phase** detection, including cold-start, warm-up, and convergence.
2. **Adaptive Policies:** Dynamic adjustments to client selection, aggregation intervals, and local epochs.
3. **Personalization Layers:** Fine-tune user-specific characteristics locally to protect privacy.

Federated Learning for Recommendation Systems:

Ammad-ud-din et al. (8) proved FL's applicability to recommendation tasks but saw a 22% performance loss in non-IID conditions. Hard et al. (9) included differential privacy but experienced considerable losses.

Adaptive FL Strategies: Chen et al. (10) offered adaptive aggregation frequencies, whereas Wang et al. created client selection using data diversity. None address phase-dependent optimization.(11)

Privacy attacks in Florida: Model inversion (12) membership inference attacks were successful in extracting private data from FL updates.(13). Travel data is especially sensitive due to its location sensitivity.(14).

This study aims to develop a travel planning system that delivers highly personalized recommendations while preserving user privacy. The study seeks to achieve this by using phase-adaptive federated learning. A decentralized machine learning algorithm that allows user data to remain on local devices, thereby enabling collaborative model training without compromising individual privacy.

Methodology

This study was conducted conducted at Manchester Metropolitan University, Manchester, United Kingdom. The Phase-Adaptive Federated Learning for Travel Planning (PAFL-TP) systems create a personalized itinerary by balancing utility and privacy using an adjustable phase parameter (ϕ). At the heart of architecture, each client device develops a local travel recommendation model using its data, such as visited areas, seasonal preferences, and journey lengths. Before sending model changes to the central server, they are converted using a phase-dependent process. The transformation interpolates between a differentially private version of the update and an inverted gradient reconstruction to retrieve utility-preserving features.HiΦ=Φ.DP (hi)+(1-Φ).Inv(DP)(hi)h i^{\phi}= \phi \cdotDP(h i) +(1-\phi) \cdotis the representation of this transformation. DP(hi)DP(h i)(DP)(hi) is the noise-injected using a Laplace distribution calibrated by sensitivity Δ1\Delta_1Δ1, and Inv(DP(hi))Inv(DP(h i))Inv(DP(hi)) is a utility-restoring inversion module that uses a shallow network of neurons to reconstruct useful features from the noised gradients. Inv (DP(hi))hiϕ=ϕ·DP(hi)+(1−ϕ)·Inv(DP(hi)), where hihihi indicates the local model update.

The differential privacy component adds noise to the privacy budget ɛt\epsilon tɛt, making individual user contributions indistinguishable. The gradient inversion module solves an optimization problem to minimise the loss between true and noisy gradients, thereby preserving the quality of recommendations.

During each training cycle, the phase parameter Φ\phiΦ is dramatically updated using a PID (Proportional-Integrated-Derivative) controller. The controller changes Φ\phiΦ in real time by tracking differences between goal and actual model performance (validation accuracy), assigning greater privacy (Higher Φ\phiΦ) in early rounds, and progressively moving to higher utility (lower Φ\phiΦ) as training stabilises. The PID gains KpKpKp, KiKiKi, and KdKdkd are modified using Bayesian optimisation to balance accuracy and loss of privacy during the training process.

To ensure privacy-preserving model updates even when untrusted servers are present, secure Multi-Party Computation is used to aggregate each client's converted gradient after scaling it by its current phase value. Additionally, to effectively simulate sequential trip behaviors like itinerary patterns, a lightweight transformer model is deployed locally. Because of its minimal computing overhead, this model is still appropriate for mobile deployment. To dynamically adapt sensitivity to temporal travel patterns based on privacy phase, the model integrates Φ-gated attention heads.

These elements work together to create a cohesive system in which system performance, privacy budget, and model convergence are used to modify the degree of privacy protection vs. personalisation accuracy intelligently throughout each training session. With the help of this technique, PAFL-TP can strike a precise, phase-driven balance between user privacy and excellent itinerary recommendations.

Results

Table 1 evaluates the quality of recommendations using different methodologies. PAFL-TP earns the highest HR@10 and NDCG@10 ratings, showing outstanding personalization. The improvement shows the usefulness of dynamic privacy control.

Table 1: Recommendation Performance Comparison

Method	HR@10 (Tour Planner)	NDCG@10 (Tour Planner)
FedAvg-DP	0.402	0.301
AdaptiveFL	0.463	0.339
FedTransform	0.491	0.368
PAFL-TP	0.586	0.444

IEER
Institute for Excellence in Education & Research

Table 2 shows how well the strategies safeguard privacy. PAFL-TP has the lowest membership inference risk and effective privacy budget. It provides a robust defence against privacy assaults.

Table 2: Privacy Protection Metrics

Methods	MISR(%) ↓	ε_eff ↓
FedAvg-DP	41.2	2.9
AdaptiveFL	33.7	2.5
FedTransform	29.4	2.3
PAFL-TP	11.9	2.0

Table 3 demonstrates that PAFL-TP has the maximum system efficiency with the lowest communication cost (12.2 MB/round) and calculation time (7.5/round), surpassing Fedtransform (15.9 MB, 11.3 s) and AdaptiveFL (14.5 MB, 10.2 s). This shows PAFL-TP's ability to reduce both data transport and processing overhead.

Table 3: System Efficiency Comparison

Methods	Comm. Cost (MB/round) ↓	Comp. Time (s/round) ↓
FedTransform	15.9	11.3
AdaptiveFL	14.5	10.2
PAFL-TP	12.2	7.5

Discussion

While PAFL performs well in controlled studies, numerous practical issues must be solved before real-world applications. The system implies that clients have consistent network connectivity during federated rounds, which may not be true for mobile travel applications with intermittent internet access. Additionally, the present phase adaptation technique depends on server-side validation accuracy for feedback, necessitating common synchronization, which may add delay in large-scale installations. The differential privacy-gradient inverter, while effective, has a higher computational cost than normal DP implementations, potentially restricting its use on low-power devices. Future studies should assess edge computing models for distributing phase control logic and reducing dependency on central coordination.

Furthermore, the present PID-based phase adaptation approach suffers from scalability issues in highly asynchronous situations. While the trial performed by Chen et al. (15) strong performance with upto 30% delayed 30% delayed clients, systems with more extreme asynchrony patterns might benefit from either (a) client-specific phase controllers with delay-compensated tuning, or (b) reinforcement learning-based adaptation that completely replaces the PID paradigm. Such techniques might guarantee stability while tolerating the varied update patterns typical of large-scale mobile deployments.

Our study findings show that PAFL-TP considerably improves federated recommendation systems by balancing the personalization, privacy, and efficiency trio that was typically at conflict in previous studies. We contextualised these findings in light of recent literature. PAFL-TP delivers cutting-edge performance (HR@10:0.586, NFCG@10:0.444), exceeding FedTransform (HR@10:0.491) and AdaptiveFL (HR@10:0.463). This is consistent with trends in dynamic personalization: Fedtrans enhances individual client model accuracy by 14-72% while lowering training costs by 1.6X-20X compared to cutting-edge federated learning methods.(16). A novel differential privacy technique for federated learning maintains performance by allowing clients to cancel out noise effects and regain the original global model.(17)

PAFL-TP minimizes membership inference risk (MISR: 11.9%) and privacy budget (ε eff:2.0), outperforming Fedtransform (MISR:29.4%, ε:2.3). This reflects advancements in adaptive differential privacy. Compared to FedTransform, APB-DP minimizes membership inference risk and privacy budget in adaptive differential privacy for wireless semantic communication.(18)Federated recommender systems are susceptible to attribute inference attacks; however, an adaptive privacy-preserving strategy can secure users' sensitive data while retaining suggestion accuracy.(19).

PAFL-TP reduces communication (12.2 MB/round) and processing (7.5/round/round) by about 15% compared to FedTransform, which is essential for mobile tourism. A study presented a privacy-preserving federated learning architecture that leverages ensemble attention distillation to fuse local models and reduce communication cost.(20) An effective deep learning technique for real-time and accurate pedestrian location estimation utilising mobile IMUs (21)

CONCLUSION

PAFL-TP develops a new standard for privacy-conscious federated recommenders by dynamically balancing user security and experience. Its efficiency and efficacy develop our architecture as

a template for resource-constrained scenarios, moving us closer to the goal of "privacy by design" in ubiquitous computing.

REFERENCES

Mosca O, Lauriola M, Manunza A, Mura AL, Piras F, Sottile E, et al. Promoting a sustainable behavioural shift in commuting choices: the role of previous intention and "personalised travel plan" feedback. Transp Res Part F Traffic Psychol Behav [Internet]. 2024 Oct 1 [cited 2025 Jul 14];106:5571. Available from: https://www.sciencedirect.com/science/article/pii/S1369847824001608?via%3Dihub

Aribas E, Daglarli E. Transforming Personalized Travel Recommendations: Integrating Generative AI with Personality Models. Electron 2024, Vol 13, Page 4751 [Internet]. 2024 Dec 1 [cited 2025 Jul 14];13(23):4751. Available from: https://www.mdpi.com/2079-9292/13/23/4751/htm

Shokri R, Shmatikov V. Privacy-Preserving Deep Learning. [cited 2025 Jul 9]; Available from: http://dx.doi.org/10.1145/2810103.2813687.

Brendan McMahan H, Moore E, Ramage D, Hampson S, Agüera y Arcas B. Communication-Efficient Learning of Deep Networks from Decentralized Data. Proc 20th Int Conf Artif Intell Stat AISTATS 2017 [Internet]. 2016 Feb 17 [cited 2025 Jul 9]; Available from: https://arxiv.org/pdf/1602.05629

Zhao Y, Li M, Lai L, Suda N, Civin D, Chandra V. Federated Learning with Non-IID Data.

Nishio T, Yonetani R. Client Selection for Federated Learning with Heterogeneous Resources in Mobile Edge. IEEE Int Conf Commun. 2019 May 1;2019-May.

Geiping J, Bauermeister H, Dröge H, Moeller M. Inverting Gradients - How easy is it to break privacy in federated learning? Adv Neural Inf Process Syst. 2020;33:16937–47.

Ammad-Ud-Din † M, Ivannikova E, Khan SA, Oyomno W, Fu Q, Tan KE, et al. Federated Collaborative Filtering for Privacy-Preserving Personalized Recommendation System. 2019 Jan 29 [cited 2025 Jul 14]; Available from: https://arxiv.org/pdf/1901.09888

Hard A, Rao K, Mathews R, Ramaswamy S, Beaufays F, Augenstein S, et al. Federated Learning for Mobile Keyboard Prediction. 2018 Nov 8 [cited 2025 Jul 14]; Available from: https://arxiv.org/pdf/1811.03604

Chen C, Xu H, Wang W, Li B, Li B, Chen L, et al. Communication-efficient federated learning with adaptive parameter freezing. Proc - Int Conf Distrib Comput Syst. 2021 Jul 1;2021-July:1–11.

Wang H, Kaplan Z, Niu D, Li B. Optimizing Federated Learning on Non-IID Data with Reinforcement Learning. Proc - IEEE INFOCOM. 2020 Jul 1;2020-July:1698–707.

Fredrikson M, Jha S, Ristenpart T. Model inversion attacks that exploit confidence information and basic countermeasures. Proc ACM Conf Comput Commun Secur [Internet]. 2015 Oct 12 [cited 2025 Jul 14];2015-October:1322–33. Available from: https://dl.acm.org/doi/pdf/10.1145/2810103.2813677

Melis L, Song C, De Cristofaro E, Shmatikov V. Exploiting unintended feature leakage in collaborative learning. Proc - IEEE Symp Secur Priv. 2019 May 1;2019-May:691–706.

Primault V, Boutet A, Mokhtar S Ben, Brunie L. The Long Road to Computational Location Privacy: A Survey. IEEE Commun Surv Tutorials. 2019;21(3):2772–93.

Chen X, Zhang H, Wong CUI. Phase-Adaptive Federated Learning for Privacy-Preserving Personalized Travel Itinerary Generation. Tour Hosp. 2025;6(2).

Zhu Y, Liu J, Chowdhury M, Lai F. FedTrans: Efficient Federated Learning via Multi-Model Transformation. 2024 Apr 25 [cited 2025 Jul 14]; Available from: https://export.arxiv.org/pdf/2404.13515v2.pdf

ANIS ELGABLI 1, 2 (Senior Member, IEEE), AND WESSAM MESBAH 2, 3 (Senior Member I. A Novel Approach for Differential Privacy-Preserving Federated Learning. 2024 [cited 2025 Jul 14]; Available from: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10812948

Liu H, Wang B, Meng R, Han S, Xu X. Adaptive Privacy Budget-based Differential Privacy Co-Training for Wireless Semantic Communication. IEEE Wirel Commun Netw Conf WCNC. 2024;

Zhang S, Yuan W, Yin H. Comprehensive Privacy Analysis on Federated Recommender System against Attribute Inference Attacks. 2023 Mar 19 [cited 2025 Jul 14]; Available from: https://export.arxiv.org/pdf/2205.11857v2.pdf

Alegana VA, Atkinson PM, Lourenço C, Ruktanonchai NW, Bosco C, Zu Erbach-Schoenberg E, et al. Advances in mapping malaria for elimination: fine resolution modelling of Plasmodium falciparum incidence OPEN. Nat Publ Gr [Internet]. 2016 [cited 2025 Jul 12]; Available from: www.nature.com/scientificreports

21. Soyer MS, Abdel-Qader A, Onbasli MC. An Efficient and Low-Latency Deep Inertial Odometer for Smartphone Positioning. IEEE Sens J. 2021 Dec 15;21(24):27676–85.

IEER
Institute for Excellence in Education & Research