Research Statement – Ehsan Tanghatari

Summary

My research focuses on communication-efficient, privacy-preserving, and robust federated learning (FL) for heterogeneous edge networks. During my doctoral studies at the University of Tehran, I developed frameworks that distribute deep learning over IoT devices using transfer learning and knowledge distillation, enabling practical training under stringent computational and bandwidth constraints (Neurocomputing 2022, 2023). As a postdoctoral researcher in the DML Lab under Prof. Hamid R. Rabiee (Sharif University of Technology), I am advancing two complementary threads: (i) protection of deep neural network parameters in FL through encryption-aware training and aggregation; and (ii) soft client clustering and curriculum mechanisms to address non-iid and dynamically drifting client data. At IPM, I intend to consolidate these directions into a principled and deployable FL stack that integrates theory, algorithms, and edge-centric applications.

Background and Contributions

- Federated/distillation for constrained edges: I proposed training schemes that replace full model exchange with transfer- and distillation-based updates, substantially reducing communication and device-side computation while maintaining accuracy under heterogeneous data distributions.

- Privacy of model parameters: My current work designs encryption-informed protocols—combining secure aggregation with lightweight, homomorphism-friendly transformations—to preserve the confidentiality of model weights and updates with limited accuracy and latency overhead.

- Heterogeneity-aware client organization: I am developing soft clustering of clients based on representation and gradient similarity, with mixture-of-experts and multi-head global models to improve personalization, convergence, and fairness under label and feature shift.

- Systems perspective: Prior experience as a Computer Vision/AI engineer informs co-design across algorithms, communication, and device constraints to ensure practical deployability.

Research Plan at IPM

1) Confidential Federated Learning: Encryption and Secure Aggregation for DNN Parameters

Objective: Provide confidentiality guarantees for model parameters and updates in FL with rigorous security analysis and controlled utility loss.

Approach:

- Hybrid cryptographic pipeline integrating secure aggregation, selective layer encryption, quantization/sketching compatible with homomorphic operations, and masked updates.

- Theoretical analysis of privacy leakage from encrypted or masked gradients/logits; utility bounds under quantization, noise, and partial homomorphism; characterization of attack surfaces (inversion, reconstruction) and defenses.

Outcomes: Protocols with formal guarantees, reference implementations, and evaluations on vision/NLP benchmarks reflecting realistic edge constraints.

2) Soft Clustering and Personalization for Heterogeneous Clients

Objective: Improve accuracy, stability, and fairness under non-iid and drifting data via adaptive, soft client grouping and curriculum-based training.

Approach:

- Representation-level clustering using embedding and gradient statistics; soft memberships realized through mixture-of-experts or multi-head global models.

- Adaptive scheduling and routing by uncertainty, drift, and resource profiles; integration of meta-learning for rapid personalization with convergence analysis.

Outcomes: Algorithms with theoretical and empirical validation; benchmarks demonstrating consistent gains across heterogeneity regimes; modular components for existing FL frameworks.

Fit with IPM

This research agenda aligns closely with IPM's expertise in ML, optimization, and security; I look forward to collaborating with Professor Rabiee and Professor Knonsari and contributing to IPM seminars and student mentorship while advancing confidential and heterogeneous federated learning for edge applications.

Near-Term Milestones (first 12 months)

- Submission of a confidential-FL protocol enabling encrypted per-layer updates with formal security and utility guarantees.

- Release of a soft-clustering FL library with non-iid benchmarks and analyses of personalization and fairness.

Selected References

- E. Tanghatari, M. Kamal, A. Afzali-Kusha, M. Pedram, "Federated learning by employing knowledge distillation on edge devices with limited hardware resources," Neurocomputing, 2023.

- E. Tanghatari, M. Kamal, A. Afzali-Kusha, M. Pedram, "Distributing DNN training over IoT edge devices based on transfer learning," Neurocomputing, 2022.