Towards Robust Federated Learning using Knowledge Distillation Techniques

Arindam Jain
School of Computing & Augmented Intelligence
Arizona State University
ajain243@asu.edu

Kiran Sthanusubramonian
School of Computing & Augmented Intelligence
Arizona State University
ksthanus@asu.edu

I. Introduction

With the onset of improved privacy standards, edge computing capabilities, and large-scale machine learning requirements, Federated Learning has emerged as a privacy-preserving training paradigm for localized devices without data-sharing and aggregation requirements. With privacy-preserving benefits, users of these localized devices (e.g., mobile phones) also benefit from lower latencies in terms of required responses. Potential Federated Learning applications include improved mobile computing [1], healthcare [2], and autonomous vehicles.

In this project, we explore the use of Knowledge Distillation to create highly accurate and robust Federated Learning paradigms. Knowledge Distillation is conceptualized as a model compression technique in which large models with complex architectures are used to train a single smaller model that can run on devices with lesser computational capabilities while still achieving comparable performance levels. The most common Knowledge Distillation architecture is the Teacher-Student architecture (Fig.1).

The rest of this proposal is arranged as follows: Section II will detail the findings of the Literature Survey (including potential shortcomings), Section III will highlight the Problem Statement, Section IV will discuss the Methodology (including execution plan, datasets to be used, and the metrics to evaluate & validate the methodology), Section V will summarize the objectives and learning outcomes from this project.

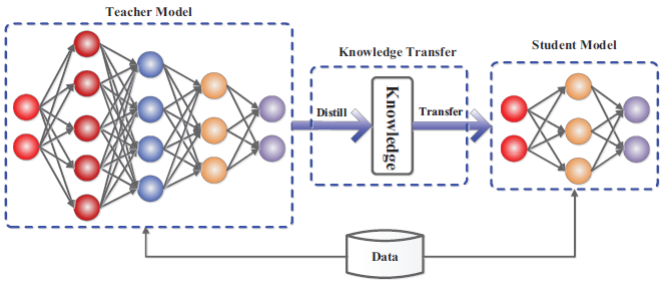

Fig. 1. Teacher-Student Architecture for Knowledge Distillation [3]

II. Literature Survey

A. Knowledge Distillation-based Solutions for Federated Learning

B. Improving Fairness and Robustness of Federated Learning Architectures

III. Problem Statement

IV. Methodology

A. Execution Plan

B. Datasets

C. Evaluation Metrics

V. Objectives & Learning Outcomes

TABLE I
Table Type Styles

Table Head	Table Column Head		
	Table column subhead	*Subhead*	*Subhead*
copy	More table copy[a]		

[a]Sample of a Table footnote.

References

[1] W. Y. B. Lim et al., "Federated Learning in Mobile Edge Networks: A Comprehensive Survey," in IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 2031-2063, thirdquarter 2020.
[2] Xu, J., Glicksberg, B.S., Su, C. et al. Federated Learning for Healthcare Informatics. J Healthc Inform Res 5, 1–19 (2021).
[3] Gou, J., Yu, B., Maybank, S.J. et al. Knowledge Distillation: A Survey. Int J Comput Vis 129, 1789–1819 (2021).
[4] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.
[5] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].
[6] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.