Contribution ID: **34** Type: **Long Talk**

Comparative Study of Federated Learning Frameworks NVFlare and Flower for Detecting Thermal Anomalies in Urban Environments

Thursday, 3 October 2024 11:40 (20 minutes)

With the expansion of applications and services based on machine learning (ML), the obligation to ensure data privacy and security has become increasingly important in recent times. Federated Learning (FL) is a privacy-preserving machine learning paradigm introduced to address concerns related to data sharing in centralized model training. In this approach, multiple parties collaborate to jointly train a model without disclosing their individual data.

There are various aggregation algorithms for aggregating the local model updates in Federated Learning, e.g. FedAVG, FedProx, Scafflod, and Ditto to overcome the challenges posed by the fact that data can be unbalanced, non-independent, or non Identically Distributed (non-IID) in FL environments. There exist as well various workflows like Scatter and Gather, Cyclic Learning and Swarm Learning for communication strategies. In addition, various security enhancements including Differential Privacy (DP), Homomorphic Encryption (HE), and secure model aggregation have been developed to address privacy concerns. Key considerations when setting up an FL process involve selecting the best framework that meets the specific requirements of the task in terms of the best aggregation algorithm, workflow, and security enhancements.

To help researchers make informed decisions, within the AI4EOSC project, we provide a comprehensive evaluation and comparison of the two most widely used frameworks for federated learning NVFlare and Flower, which have also recently announced a collaboration between the two.

To compare the frameworks in terms of the features they offer, we develop a deep learning solution for the Detection of thermal anomalies use case of AI4EOSC. We use this real-world case study to demonstrate the practical impact and performance of various FL aggregation algorithms, workflows, and security enhancements, and their implementation in each FL framework.

We highlight the different features and capabilities that these frameworks bring to FL settings to provide a better understanding of their respective strengths and applications. The Flower server was seamlessly integrated into the AI4EOSC dashboard, which simplified our experimentation process. All experiments are monitored and tracked using the MLflow instance provided by the AI4EOSC project. Our evaluation included analyses of the convergence speed of various aggregation methods offered by these frameworks, global model accuracy, communication overhead in various workflows, and privacy-preserving functionalities of both frameworks such as HE and DP. Furthermore, we explore the novel collaboration between these two frameworks to explore synergies and potential improvements in federated learning methods for thermal bridge detection.

Topic

Needs and solutions in scientific computing: Artificial Intelligence

Primary authors: Mr DUDA, Leonhard (Karlsruhe Institute of Technology - KIT, Computer Science, Karlsruhe, Baden-Württemberg, Germany); Dr ALIBABAEI, Khadijeh (Karlsruhe Institute of Technology - KIT, SCC, Eggenstein-Leopoldshafen, Baden-Württemberg, Germany); Ms VOLLMER, Elena (Karlsruhe Institute of Technology - KIT, IIP, Karlsruhe, Baden-Württemberg, Germany); Mr KLUG, Leon (Karlsruhe Institute of Technology - KIT, IIP, Karlsruhe, Baden-Württemberg, Germany); Dr BENZ, Mishal (Karlsruhe Institute of Technology - KIT, SCC, Eggenstein-Leopoldshafen, Baden-Württemberg, Germany); Dr KOZLOV, Valentin (Karlsruhe Institute of Technology); Dr VOLK, Rebekka (Karlsruhe Institute of Technology - KIT, IIP, Karlsruhe, Baden-Württemberg, Germany); Dr GÖTZ, Markus (Karlsruhe Institute of Technology - KIT, SCC, Eggenstein-Leopoldshafen, Baden-Württemberg, Germany); Prof. SCHULTMANN, Frank (Karlsruhe Institute of Technology - KIT, IIP, Karlsruhe, Baden-Württemberg, Germany); Prof. STREIT, Achim (Karlsruhe Institute of Technology - KIT, SCC, Eggenstein-Leopoldshafen, Baden-Württemberg, Germany)

Presenter: Dr ALIBABAEI, Khadijeh (Karlsruhe Institute of Technology - KIT, SCC, Eggenstein-Leopoldshafen,

Baden-Württemberg, Germany)

Session Classification: Processing Research Data with Artificial Intelligence and Machine Learning