NT FILE chapter1.tex

Introduction cha:introduction

Chapters/Figures/Covers/

12.5cm 0pt

In recent years, the exponential growth of data generated through distributed devices and platforms has driven the development of collaborative learning methods such as Federated Learning (FL). Federated learning allows a network of participants to train a machine learning model without centralizing data, addressing critical issues related to data privacy and security. However, FL still faces inherent limitations, particularly in its dependence on a central aggregator and the computational resources required on individual devices to train complex models. Furthermore, reliance on centralized platforms raises significant privacy concerns as they can introduce vulnerabilities or potential access points to sensitive data. Alternatively, Split Learning (SL) has emerged as a promising approach within distributed learning paradigms, allowing computational load to be shared among participants, which can help alleviate resource constraints and increase data privacy by increasing sensitive data that remains on the source device.

The objective is to design, implement and evaluate a fully self-managed and decentralized platform capable of leveraging SL techniques, allowing participants to independently configure and reconfigure as needed, even in the presence of dynamic network conditions.

This decentralized platform seeks to minimize human intervention and ensure robustness by allowing participants to help each other in the training process, thus addressing privacy concerns that arise from centralized architectures.

This research will first address the current state of the art in decentralized learning systems and evaluate existing methods, followed by the design of a decentralized SL architecture. Through this approach, we aim to improve the efficiency and privacy of federated systems, ultimately contributing to a more robust infrastructure for distributed learning.

Objective sub:time$_i s_m oney$

The objective of this thesis is to develop a fully decentralized federated learning platform that integrates key principles of Split Learning (SL) to enhance privacy, efficiency, and robustness. By moving away from reliance on a central aggregator, this research aims to build a secure and autonomous framework where participants can collaborate without compromising data privacy.

To achieve this, the study will focus on the following key areas:

enumerate

[novathesis!Citation]Decentralized Federated Learning: Design a federated learning system that operates in a decentralized manner, reducing reliance on central servers and enabling greater autonomy for participants.

Privacy:

Implement privacy-preserving mechanisms that ensure sensitive data remains secure on the source devices, minimizing data exposure risks within the learning process.

Split Learning:

Incorporate split learning techniques to distribute computational loads, allowing resource-constrained devices to participate effectively in the model training without overextending their capabilities.

Delegation Protocols:

Develop delegation protocols that allow to assign an idle node with enough processing capabilities available as a helper to train a model.

Helper Membership Management:

Establish mechanisms for helper membership management, enabling participants to support one another in the training process and foster a robust, collaborative learning environment.