Swarm Learning - A Fully Decentralised Approach To Machine Learning

Josh Pattman

University Of Southampton

March 2023

The Problems

Privacy

- Data stored in multiple locations
- Cannot share the data between locations for privacy reasons
- *Medical records*

Performance

- Machine learning needs lots of processing power
- A supercomputer is not available to many
- However they may have access to many lower power devices (nodes)
- *Company with many unused computers during the night*

Federated Learning - The Current Solution

- A single model is stored on the server
- Each node has its own dataset
  - This is not shared with other nodes or the server
- The model can be shared between the server and clients
- **Goal:** Perform machine learning without sharing the model

Federated Learning - How Does It Work?

- Many variations of federated learning
  - One of the originals is *Federated Averaging (FedAvg)*
  - Many other algorithms are based off this
- FedAvg has repeated Training Steps. Each Step:
  - Server sends model to a set of nodes
  - Nodes perform training on the model
  - Nodes send their models back to server
  - New model is the average (mean) of all nodes models

Federated Learning - Issues

- Vulnerable to central server going down
- Requires that every node has direct access to the server

What is Swarm Learning?

Swarm Learning

- Each node has a model
  - Every model approximates the *global model*
- Each node has it's own dataset
  - This dataset cannot be shared with any other nodes
- The goal is to train the *global model* using all available data
- Additionally, there should be no central server or node acting as a central server