Federated Learning with secure Multiparty Computation

Student - Palash Jain
Faculty Advisor - Prof. Minseok Kwon
Motivation

- Protect sensitive information of individual/organization while building models using federated learning.
- Combine machine learning models in a distributed environment.
- Use differential differential privacy to secure models from revealing information.
Federated Learning

- Traditional machine learning approaches require centralizing data on one machine/datacenter.
- With Federated Learning, mobile devices can collaboratively work to learn a prediction model.
- Keeps all the data local to the device.
- Mobile devices fetch the latest model, improve it, and upload the changes to the model.
- Advantages - More updated model, less latency and less power consumption.

*Figure reference - [https://ai.googleblog.com/2017/04/federated-learning-collaborative.html](https://ai.googleblog.com/2017/04/federated-learning-collaborative.html)*
Secure Multiparty Computation

- Computes functions between parties by keeping their inputs private with each other.
- Simple example, find average salary within a group without revealing salaries of any person.
- Uses additive secret sharing.
- Alice - $50k, Bob - $60k, Cathy - $70k
  - Alice: (-10, 30, 30), Bob: (70, -20, 10), Cathy: (40, 60, -30)
  - Adding all the number will give 180k. Average = 180/3 = $60k
Differential Privacy

- Prevent adversary to learn any sensitive information from revealed data.
- Differentially private algorithms are resilient to attacks using auxiliary information.
- Introduces random noise in data, which restricts the adversary from learning anything sensitive.
- Uses laplace mechanism to add noise.
Proposed Work

- Introduce a layer of privacy in federated learning.
- Federated learning allows devices to build a common machine learning model without sharing data.
- Single central server is being used to collect data.
- Collect data using multiple servers in a distributed environment by introducing differential privacy.
- Use Secure Multiparty Computation as the underlying infrastructure.
Milestones

Phase 1 - Planning

Phase 2 - Implementation

Phase 3 - Evaluation, documentation and describing future work.
Thank You!