Federated Learning with Secure Multiparty Computation

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

- Protect sensitive information of individual/organization while building models using federated learning.
- Make federated learning more scalable.
- Use differential differential privacy to secure models from revealing sensitive information.
- Combine machine learning models in a distributed environment using Secure Multiparty Computation.
**Goals Planned**

- **Read papers/books**
  - How to Share a Secret - Adi Shamir
  - A Pragmatic Introduction to Secure Multi-Party Computation
  - Programming Differential Privacy

- **Topics**
  - Shamir Secret Sharing
  - Additive Secret Sharing
  - Differential Privacy
  - Federated Learning
  - Multiparty Secure Computation

- **Tools**
  - Setup MPyC
Goals achieved

- **Read papers/books**
  - How to Share a Secret - Adi Shamir
  - A Pragmatic Introduction to Secure Multi-Party Computation
  - Programming Differential Privacy

- **Topics**
  - Shamir Secret Sharing
  - Additive Secret Sharing
  - Differential Privacy
  - Federated Learning
  - Multiparty Secure Computation

- **Tools**
  - Setup MPyC
Additional Topics Covered

- Read papers
  - Combining Differential Privacy and Secure Multiparty Computation
  - Secure Multi-party Differential Privacy

- Topics
  - Laplace Mechanism
  - Gaussian Mechanism
Plan for Milestone 2

- Task 1 - Understand and play around the code for Lightweight MPC Framework for Python.
- Task 2 - Start with the implementation of layer of Differential Privacy.
Thank You!