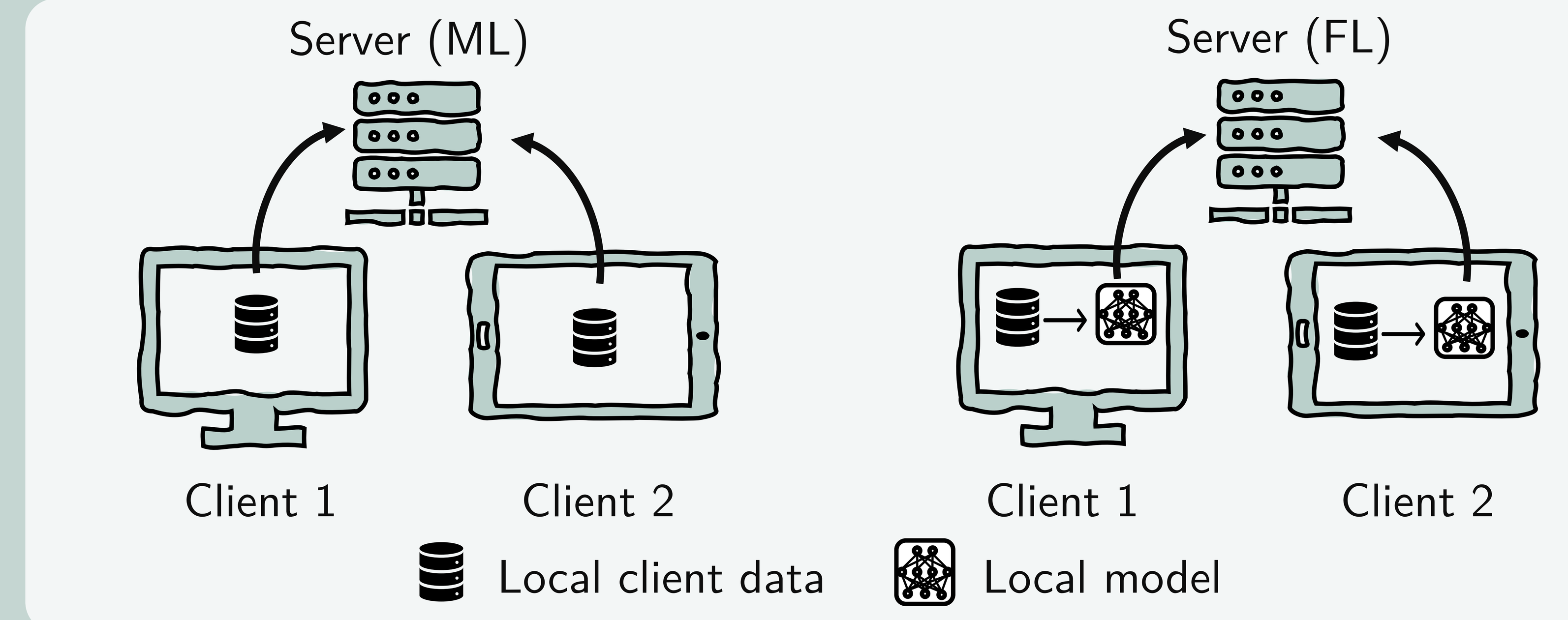
Federated Machine Learning
System Design and Practical Architecture

Chandra Gummaluru, Erick Mejia Uzeda, Maggie Ding, Cynthia Liao

Supervisor: Ashish Khisti
Administrator: Phil Anderson

Traditional Machine Learning (ML)

Requires collecting a large quantity of potentially private data in a central location

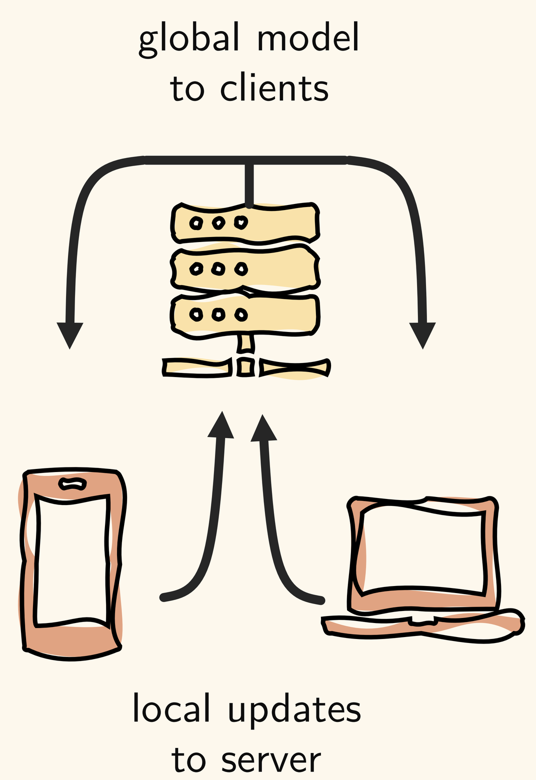


Federated Learning (FL)

Allows for decentralized collaborative learning without explicitly sharing client data

Naïve Federated Learning

1. Sever sends global model to clients
2. Clients train model on local data
3. Clients send local updates to server
4. Server computes global update



Testing Specification

Train a digit classification model using 3 clients, where each one only has a subset of the digits

Results

Server learns about all digits with high accuracy and clients slowly do too

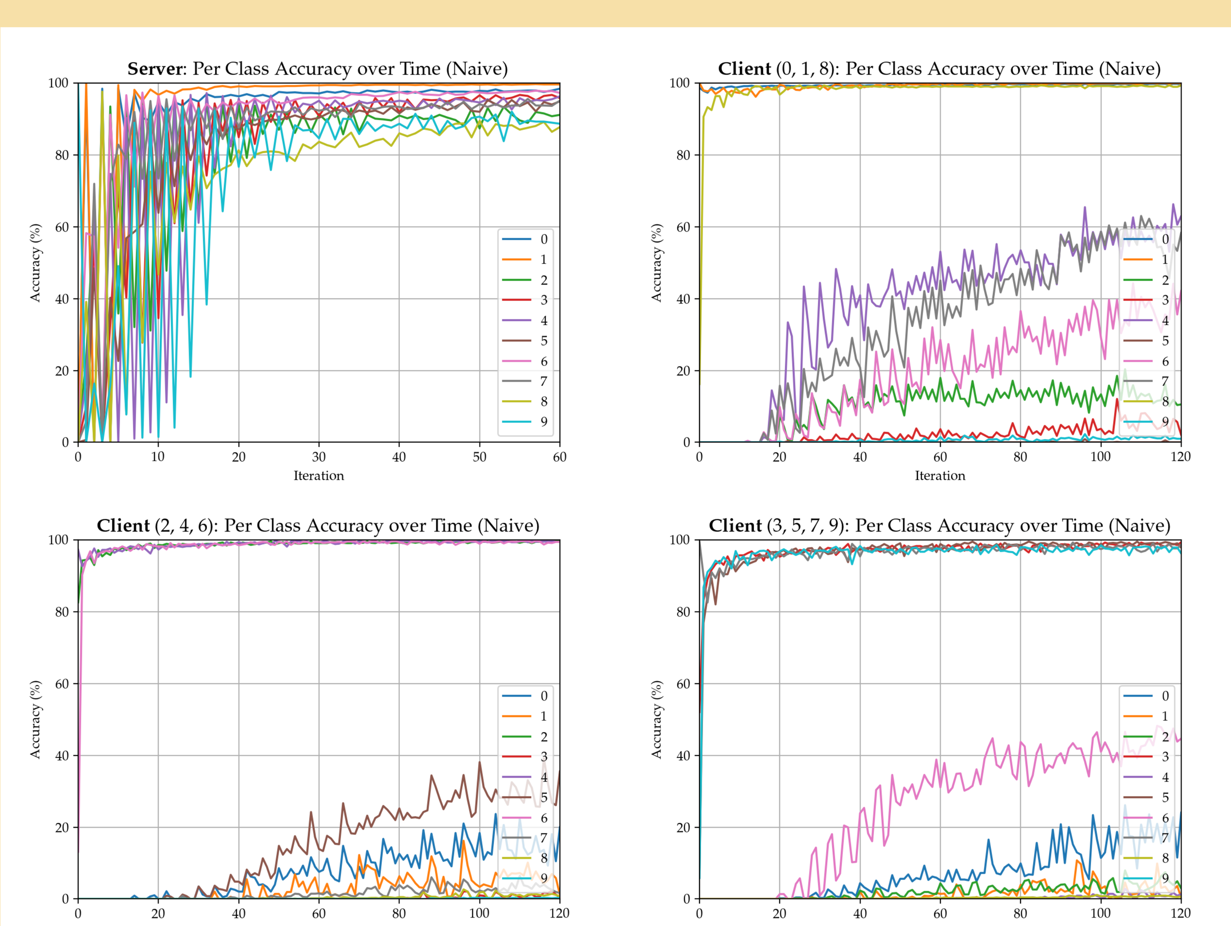


Figure 1: Server (top-left) and Clients (other) Testing Curves for Naïve FL

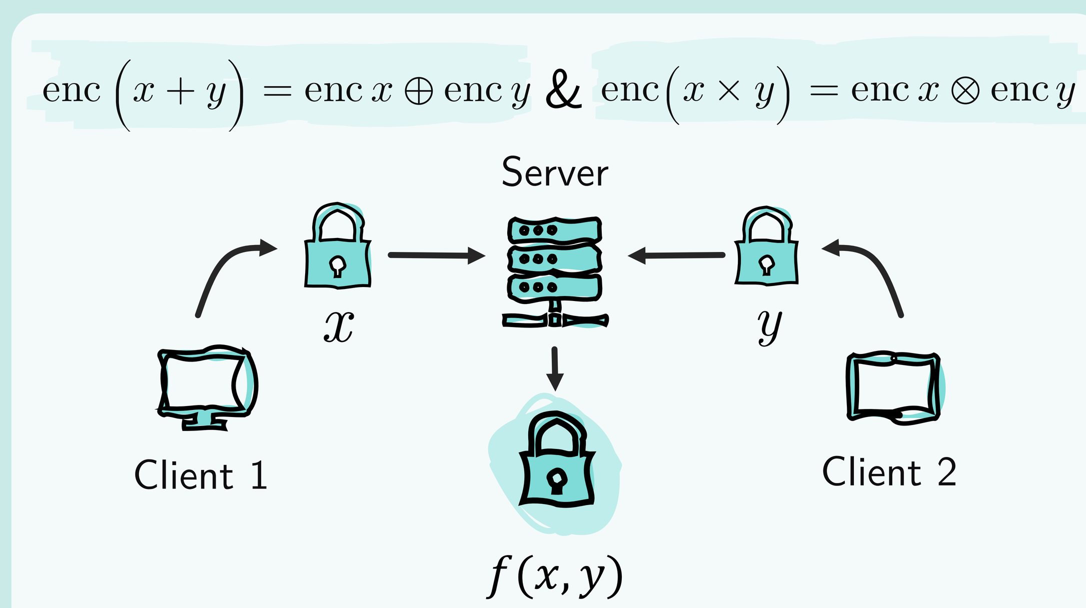
Goal: Address 3 Core Federated Learning Issues

1 Data Privacy

Keep client data private while performing arithmetic on it

Solution

Multi-party Homomorphic Encryption



Results

No impact on the model's performance despite rounding errors introduced by the scheme

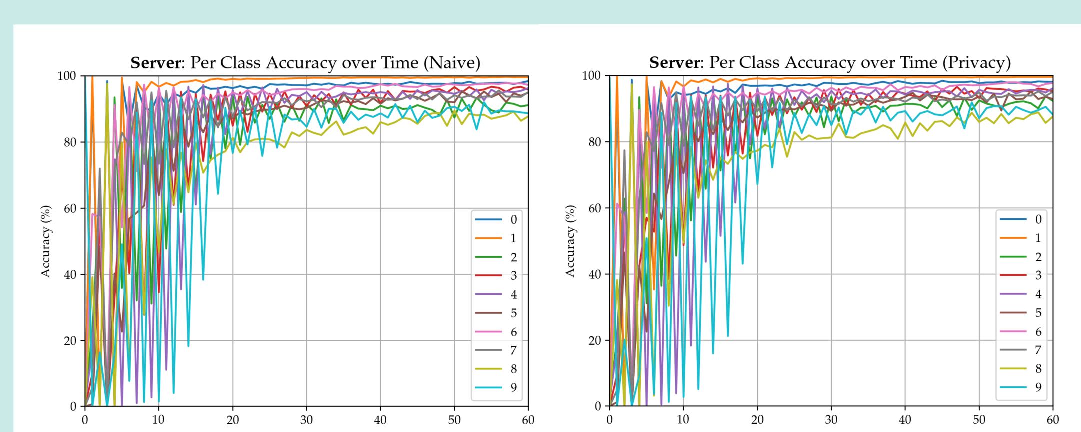


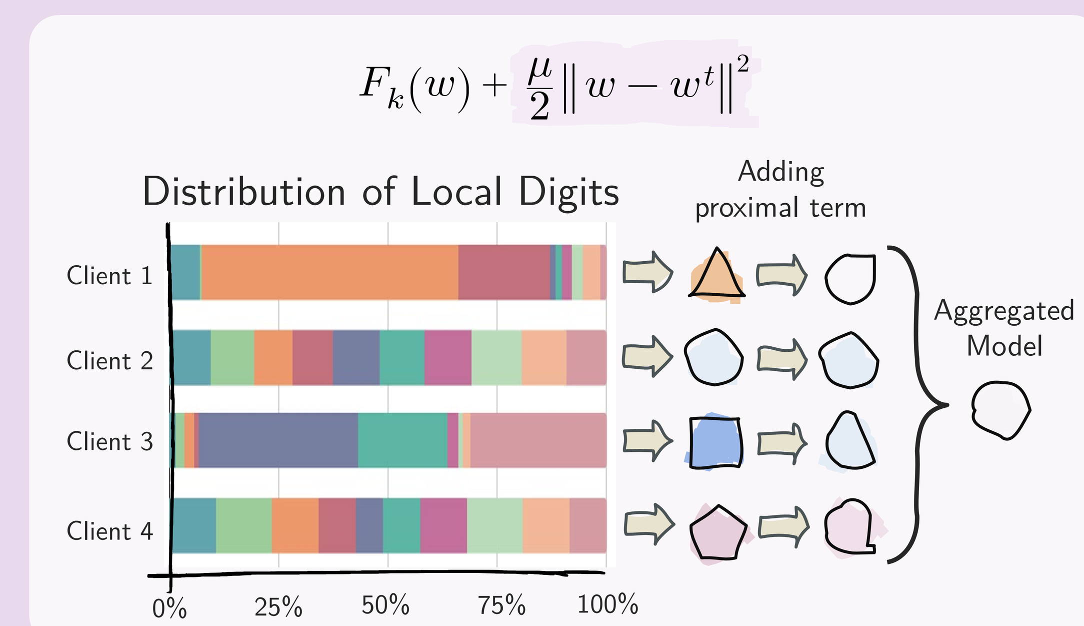
Figure 2: Naïve (left) and Multi-party Homomorphic Encryption (right) Testing Curves

2 Non-IID Data

Each client's local dataset is very different, making server-side aggregation less accurate

Solution

FedProx: add proximal term to objective



Results

Smoothed out the oscillations in the testing curves with minor degradations in accuracy

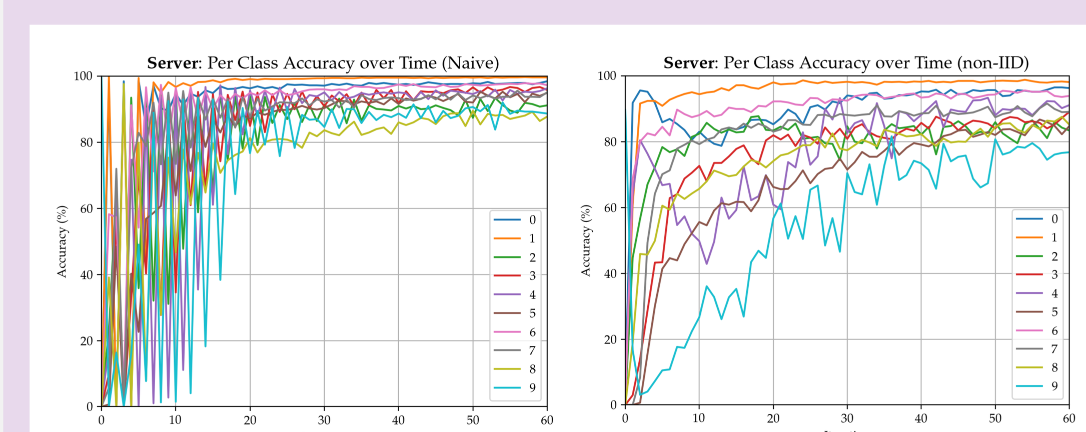


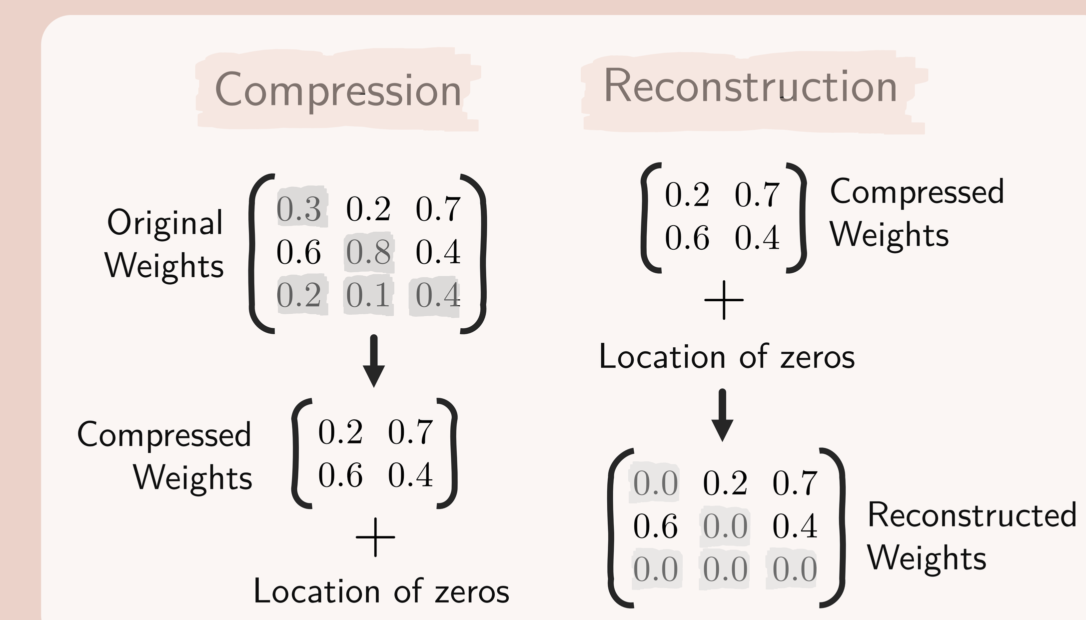
Figure 3: Naïve (left) and FedProx (right) Testing Curves

3 Communication Efficiency

Reduce the data transfer size to increase communication efficiency

Solution

Federated Dropout: zero out some terms



Results

Communication cost is reduced by 1% with minimal impact on overall performance

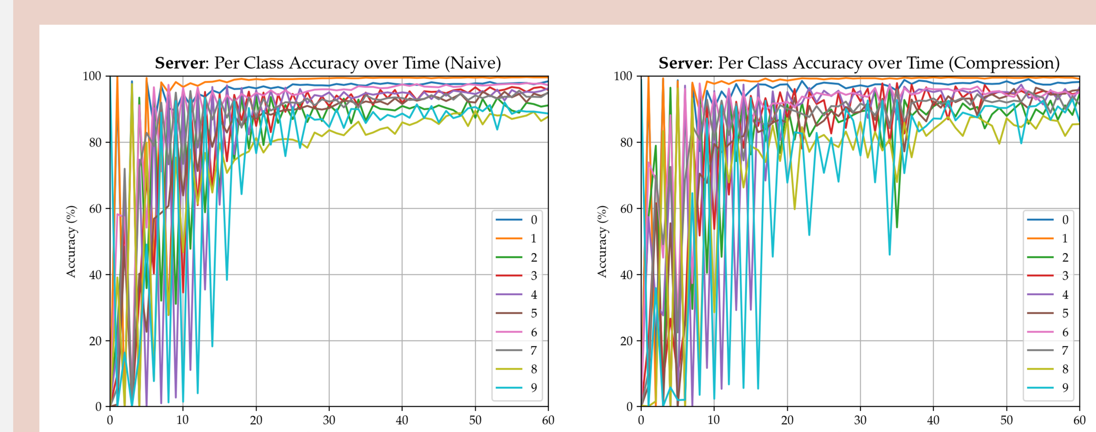
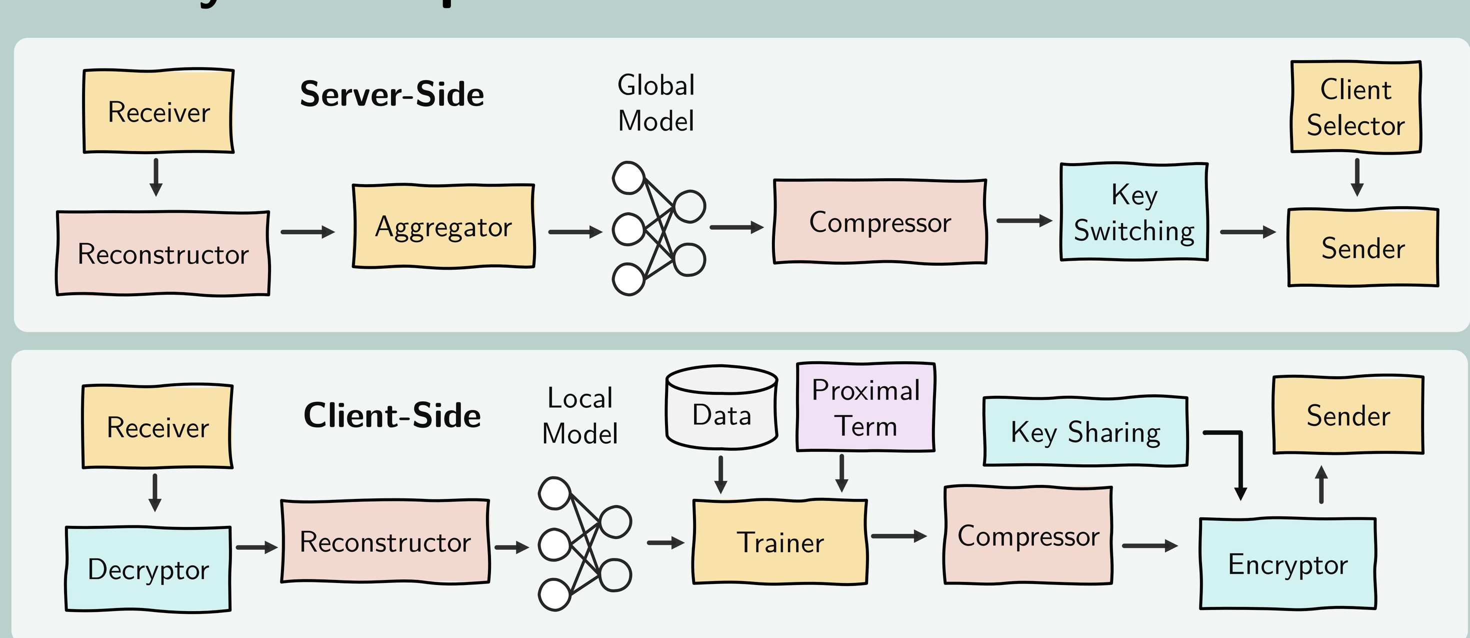


Figure 4: Naïve (left) and Federated Dropout (right) Testing Curves

Full System Pipeline



Overall Results

Slower but more stable convergence

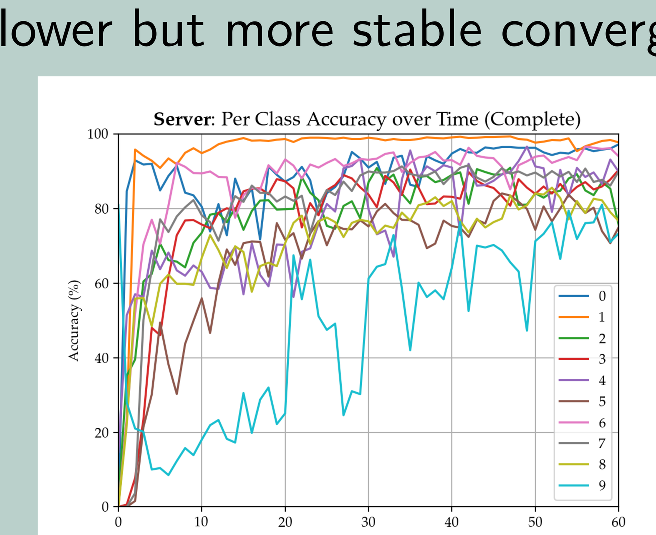


Figure 5: Testing Curves for the Overall System

Conclusion

Demonstrated the feasibility of creating a Federated Learning system that addresses the practical issues of privacy, non-IID data, and communication efficiency.

Future Work

- Benchmarking
- Unsupervised Learning
- Addressing Fairness

UNIVERSITY OF TORONTO