# ResilientFl Panel Discussion
# “FL security: Old wine in new bottle, or NWNB?”

Shiva Kasiviswanthan, Amazon

# About Me

Interests:

Theoretical Aspects of ML, especially

- (Distributed) Optimization
- Differential Privacy
- Algorithm Design

# Question 1: Topics in resilient FL where we are working and we are making progress?

1. Modeling to Emerging Scenarios: Lots of research on relaxing assumptions
    - device (client) reliability
    - reducing communication
    - data distribution
    - data/device availability
    - device statefulness
    - # of devices supported
    - …..

# Question 1: Topics in resilient FL where we are working and we are making progress?

1. Modeling to Emerging Scenarios: Lots of research on relaxing assumptions
   - device (client) reliability
   - reducing communication
   - data distribution
   - data/device availability
   - device statefulness
   - # of devices supported
   - …..

Led to

1. Practical deployment at scale
2. Easy to use tools and framework

# Question 1: Topics in resilient FL where we are working and we are making progress?

2. Theoretical Understanding:
   - Convergence results
   - Rigorous privacy/security guarantees

# Question 2: Topics in resilient FL where we have learned important lessons from existing literature ?

1. Distributed optimization: Most of FL convergence analysis relies of existing results in distributed learning (techniques such as local SGD)
2. Differential privacy: Commonly used in FL for achieving privacy
3. Cryptographic Techniques: Secure MPC, Verifiability techniques such as ZK proofs
4. …

# Question 3: Topics in resilient FL which we should be working on but are not ?

Current DP privacy:

- Central DP (requires trusted server)
- Local (hard to achieve, strong lower bounds)
- Shuffle model (trusted intermediary)

Privacy trust models: assumption on clients/server?

# Question 3: Topics in resilient FL which we should be working on but are not ?

Verifiability: enables parties to prove that they have executed their parts of a computation faithfully

- Current techniques such as based on ZKP can still not be deployed at large scale

How can we simplify this with federated learning's unique computational model?

- realistic assumptions on adversary
- can we assume that only a small fraction of clients can be corrupted