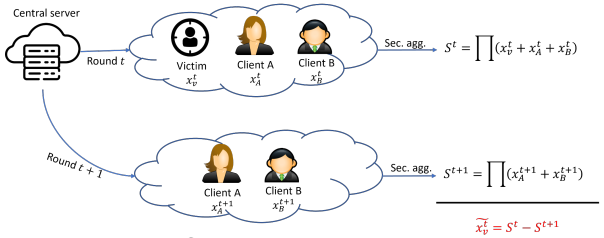
Collaborative Research: SaTC: EAGER: Trustworthy and Privacy-preserving Federated Learning

Challenge:

Privacy risks in Federated Learning (FL) with *semi-malicious/malicious server.*

Backdoor threats injected by *malicious users*



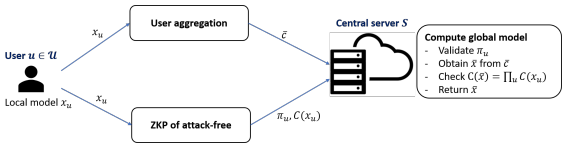
Inference attack
(even with secure aggregation)

Scientific Impact:

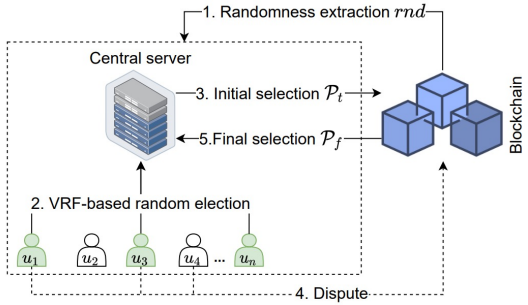
- New FL architecture with trust-free server
- Mechanisms for security check OR AND privacy protection

Solution:

- Privacy-preserving back door inspection with SNARK
- Lightweight blockchain-based FL architecture for accountable, verifiable, and inference-resistant learning



Privacy-protection backdoor inspection



Secure client selection/update protocol
(Exposing malicious/semi-malicious server)

Broader Impact and Broader Participation:

- FL as a services (FLaas) by removing the trust requirement in the server
- Offering FL services for less tech-savvy communities, e.g., SBE communities
- Integration into courses and experiential learning for undergraduate, high-school students

Award numbers: NSF CNS 2140477, 2140411

PI: My Thai, Univ. of Florida (mythai@cise.ufl.edu)
PI: Thang Dinh, Virginia Commonwealth Univ. (tndinh@vcu.edu)