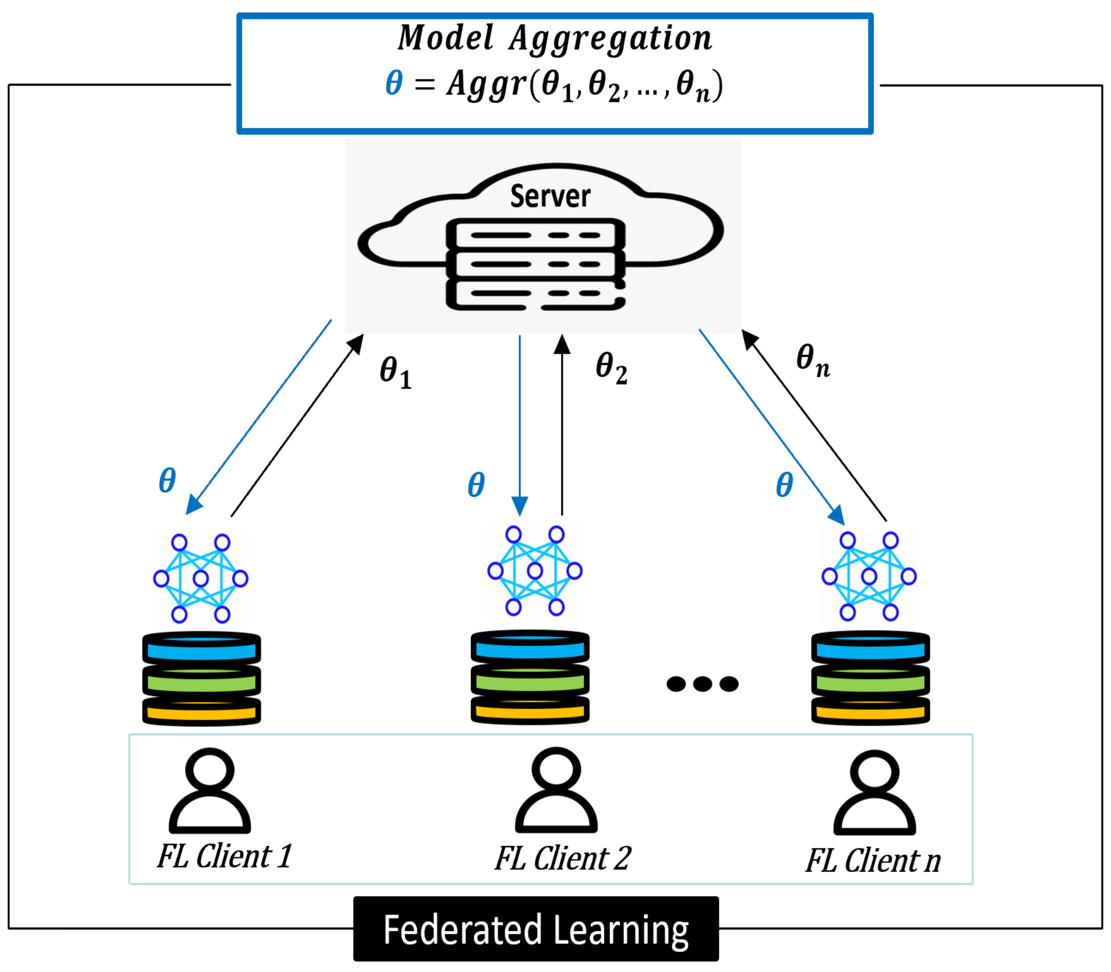
Privacy-Preserving Federated Learning

Aftab Akram, Clementine Gritti, Melek Önen

Federated Learning (FL)

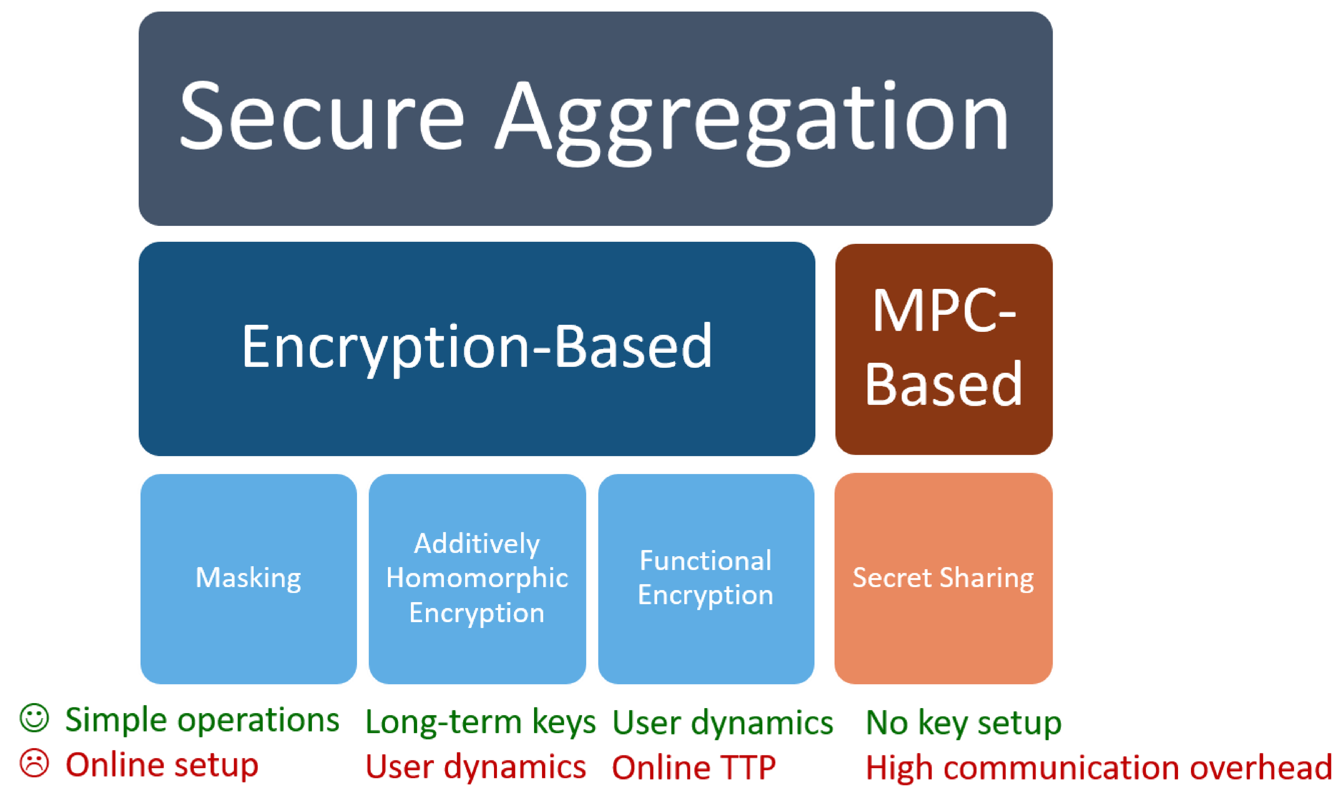
Overview



Privacy & Security Requirements

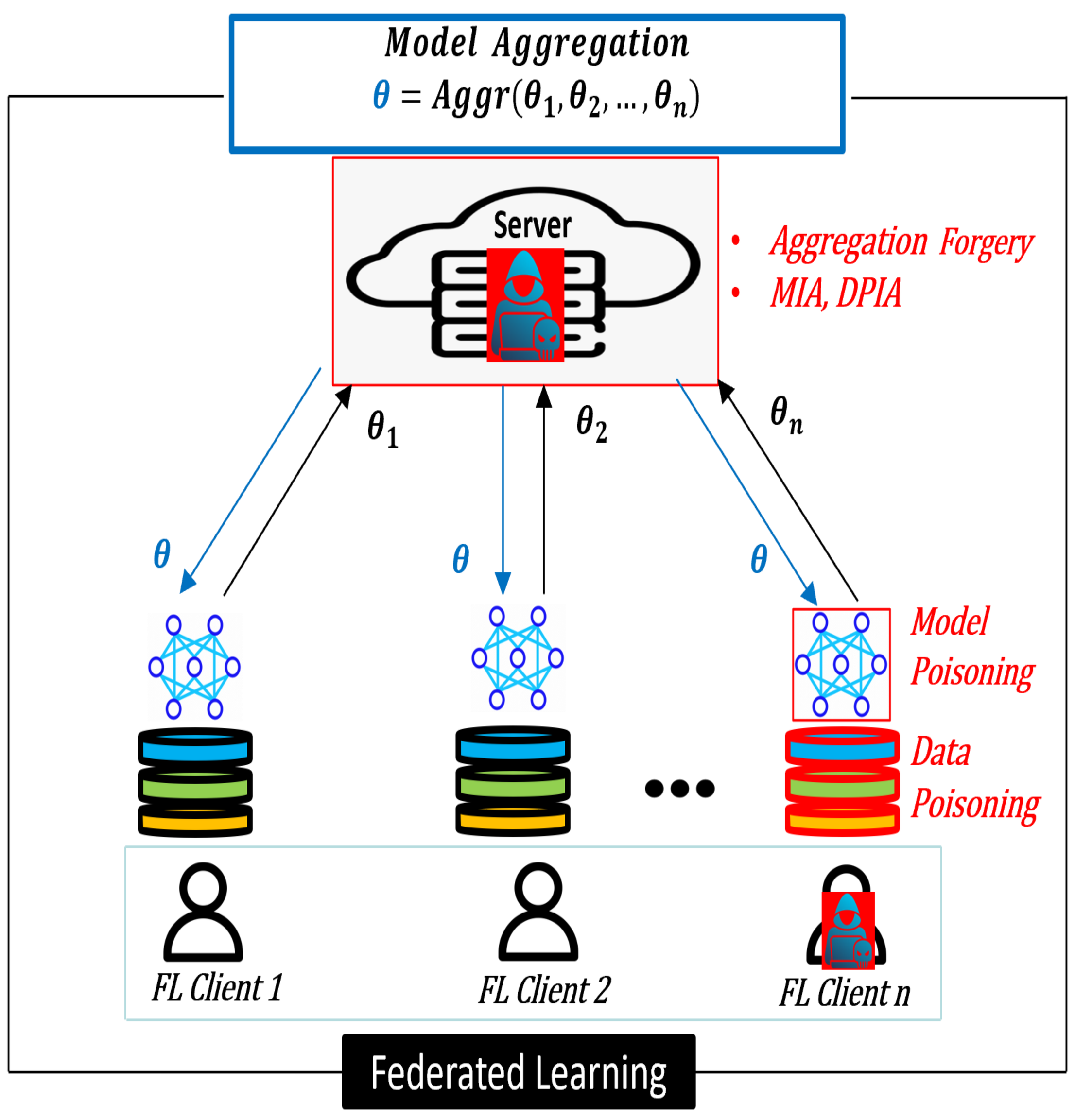
- **Local model privacy**
  - Threats:
    - Membership Inference attack (MIA)
    - Data property inference attack (DPIA)
- **Aggregate integrity**
  - Threats:
    - Global model degradation
    - Aggregate forgery
- **Robustness**
  - Threats:
    - Data poisoning
    - Model poisoning
- **Non-IID settings**
  - Threats
    - Inaccurate model
    - Client dropouts

Secure Aggregation for Model privacy



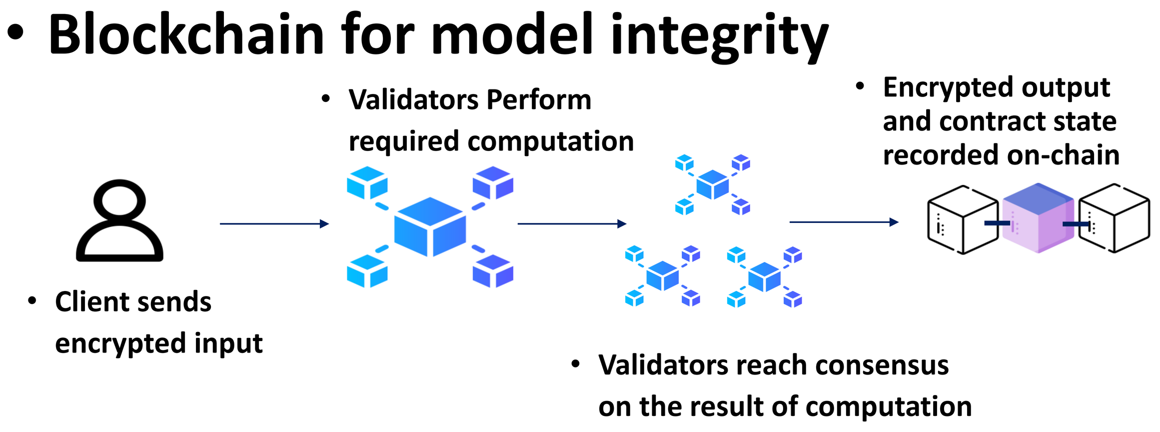
Robust Blockchain-based Federated learning [ICISSP'25]

Privacy, Integrity and Byzantine Attacks

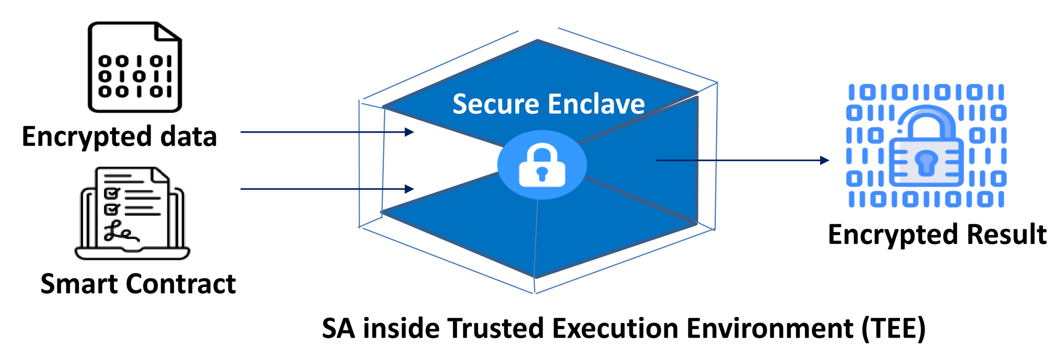


Building Blocks

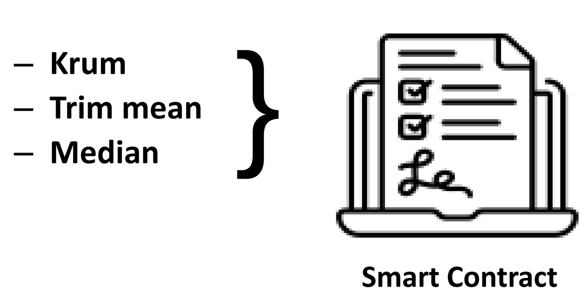
- **Blockchain for model integrity**



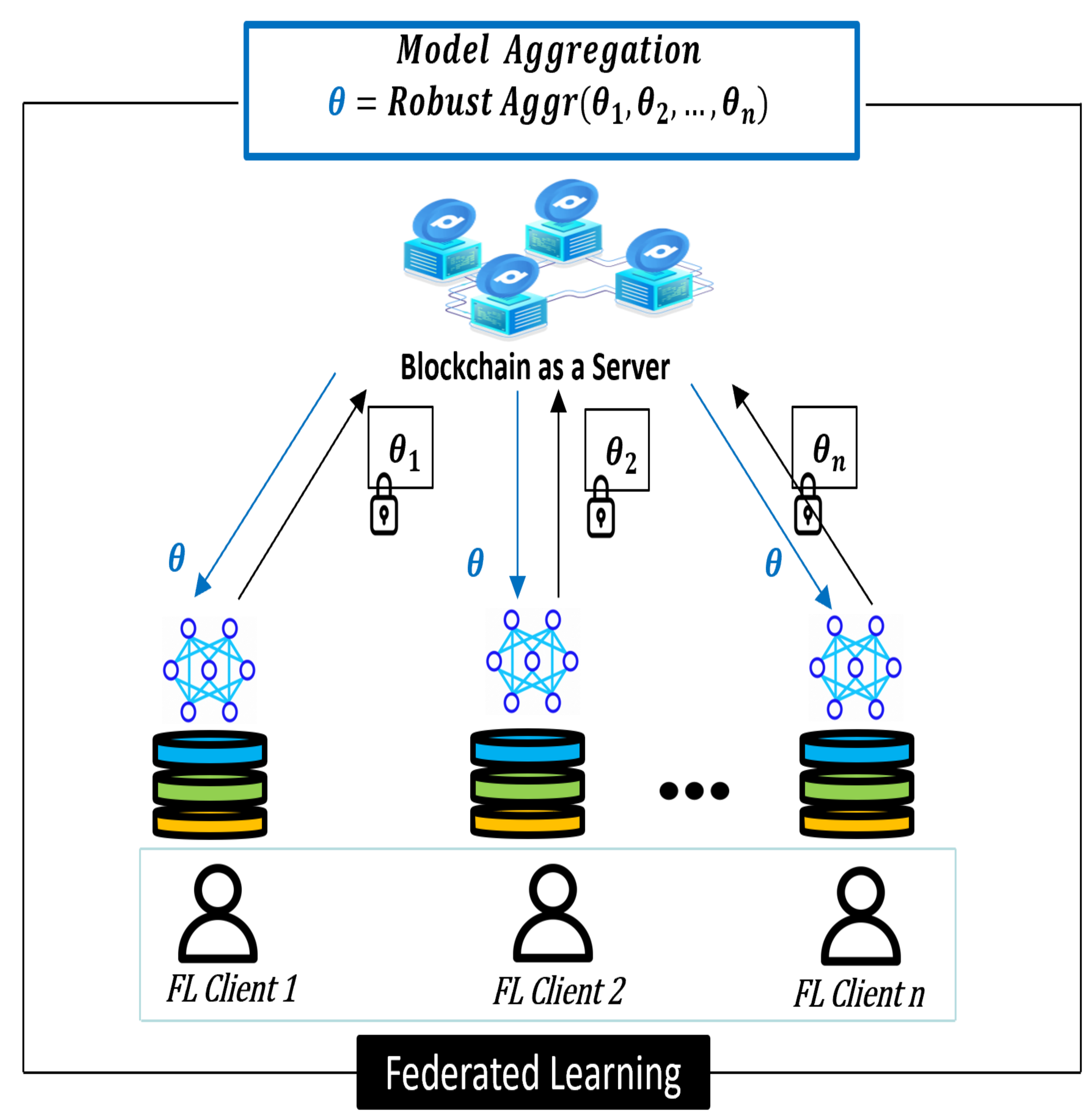
- **TEE for SA**



- **Byzantine-Robust Aggregation**

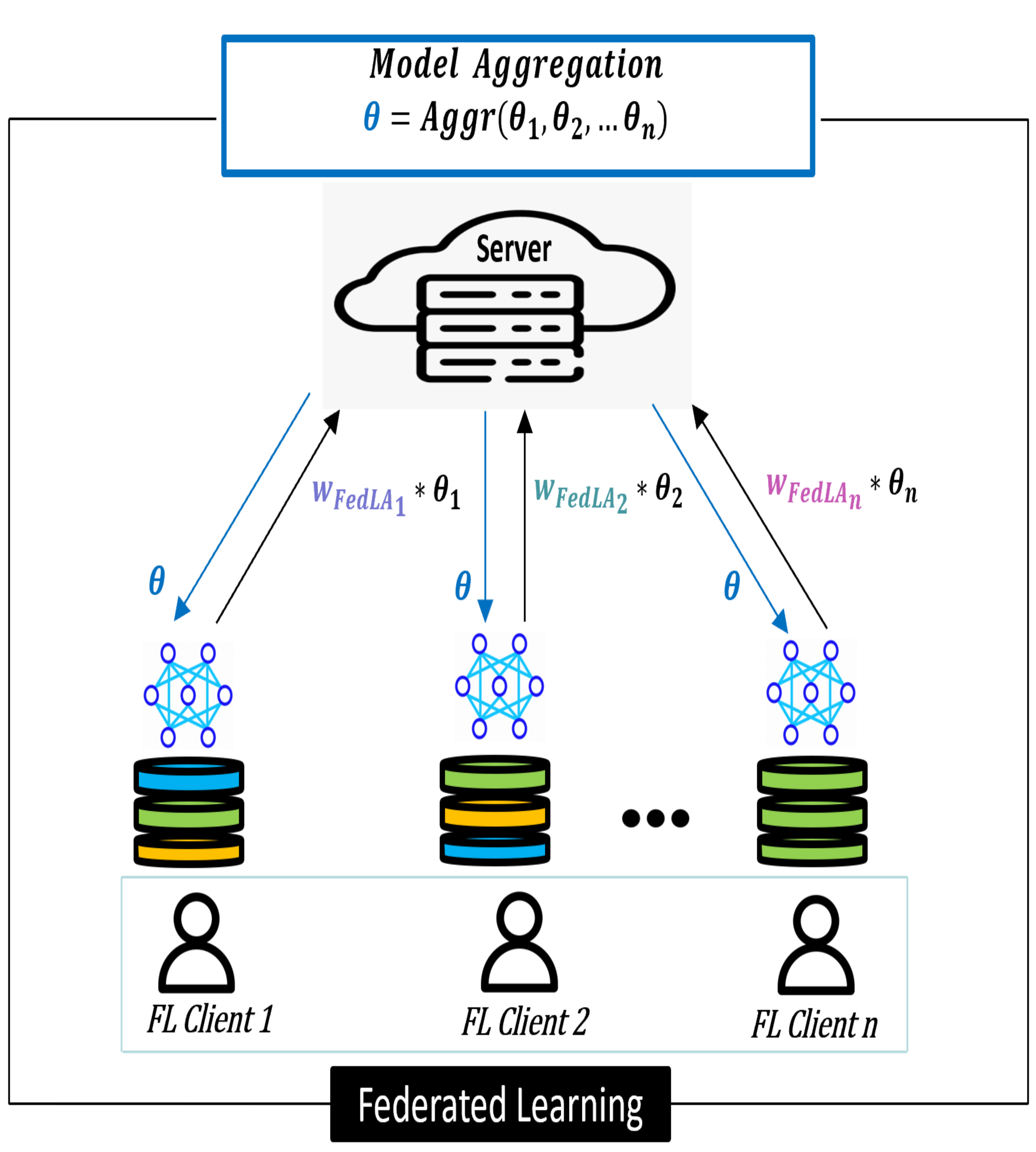


Our solution

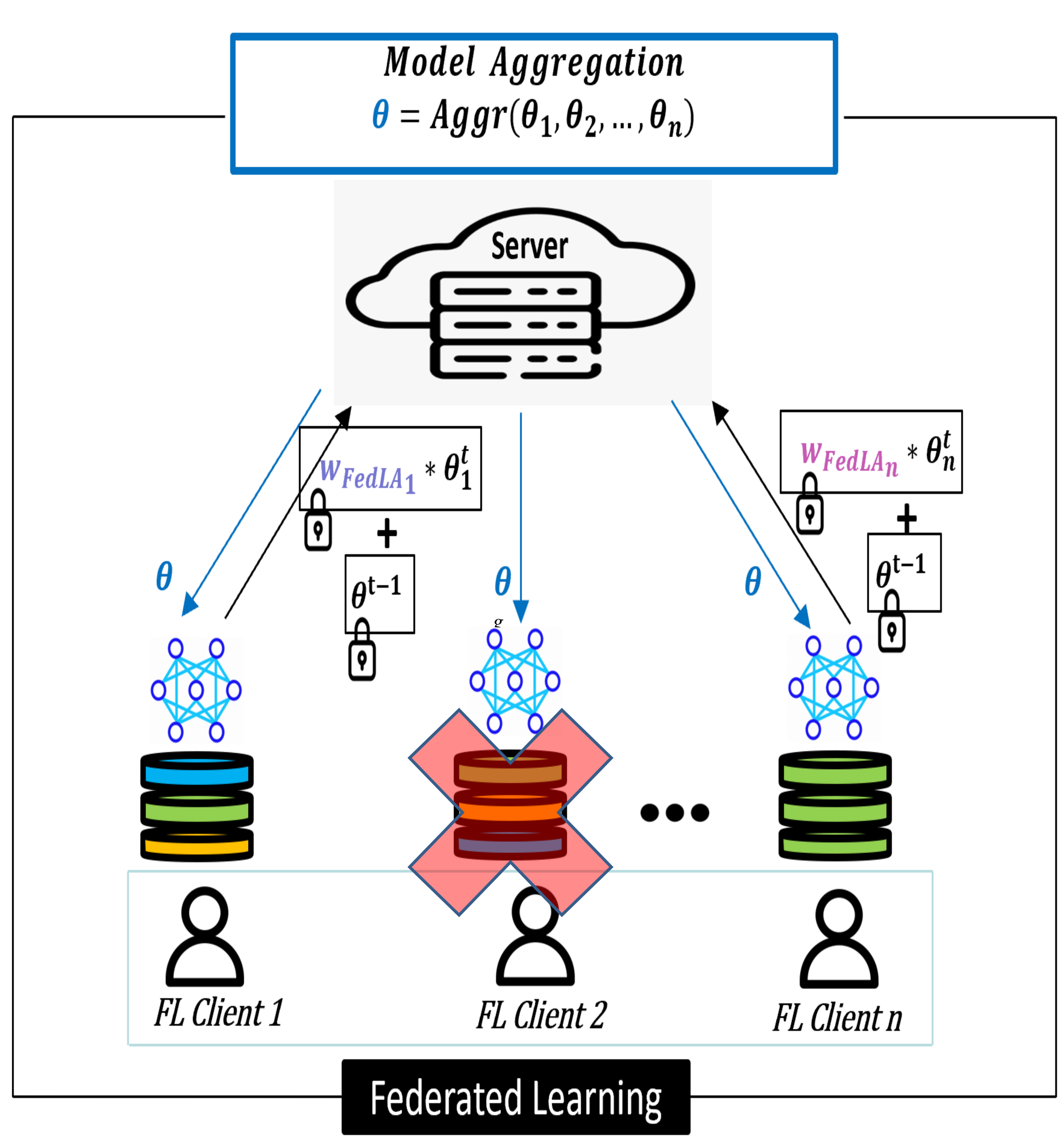


SAAFL: Secure Aggregation for Label-Aware Federated Learning [under submission]

FL with non-IID data - FedLA

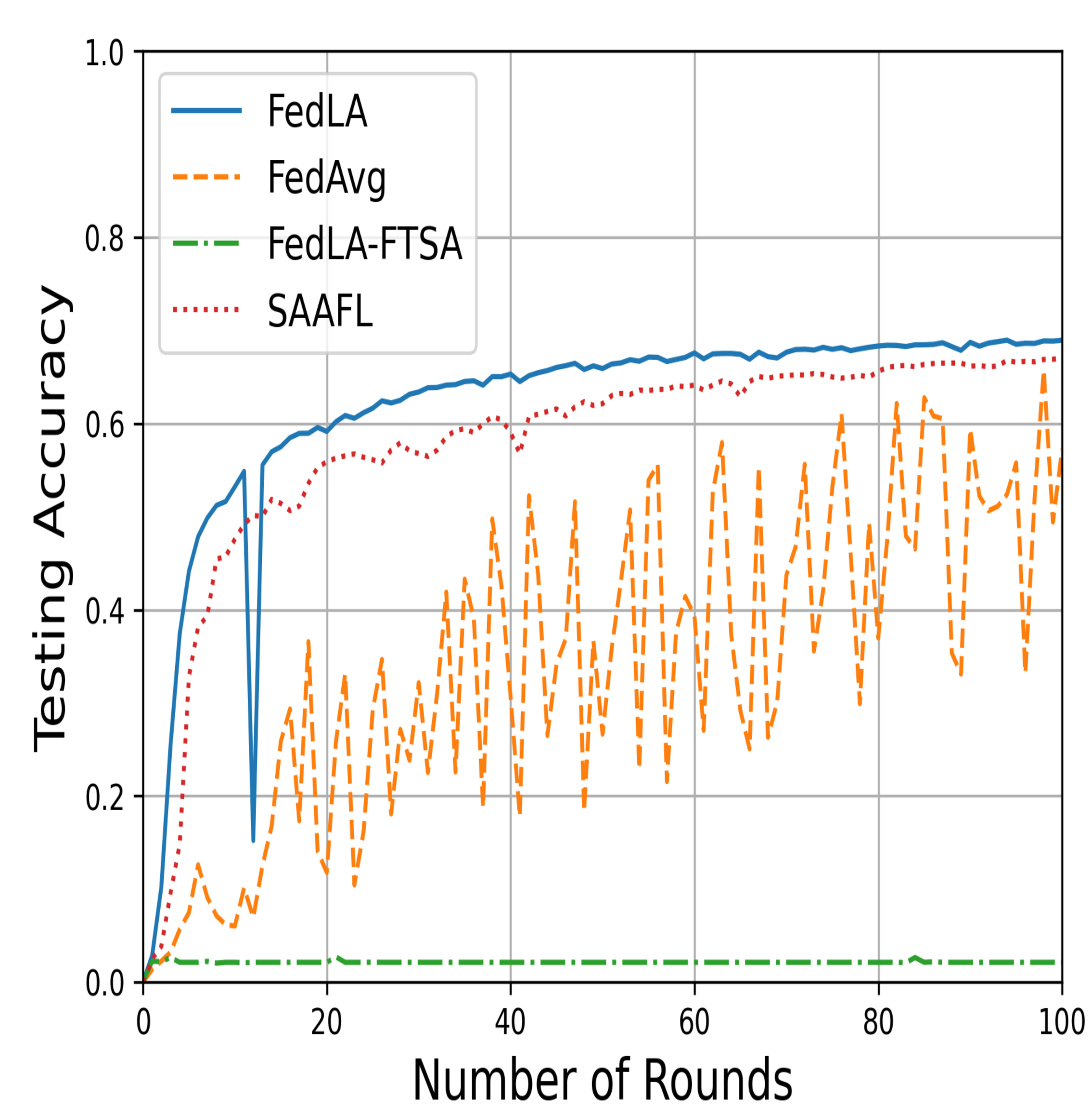


Our solution - SAAFL



- Online clients encrypt nonzero value for the dropout and non-selected clients.

Experimental results



- FedAvg is not ideal for non-IID data.
- Zero-values for dropout clients (FedLA-FTSA) fail in FedLA.
- SAAFL achieves accuracy comparable to FedLA.

EURECOM
www.eurecom.fr

These works are partially funded by TRAIN (ANR-22-FAI1-0003) and The 3IA Côte d'Azur programme (ANR-19-P3IA-0002).

Contact: {aftab.akram, melek.onen}@eurecom.fr