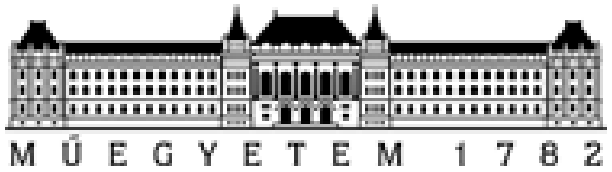
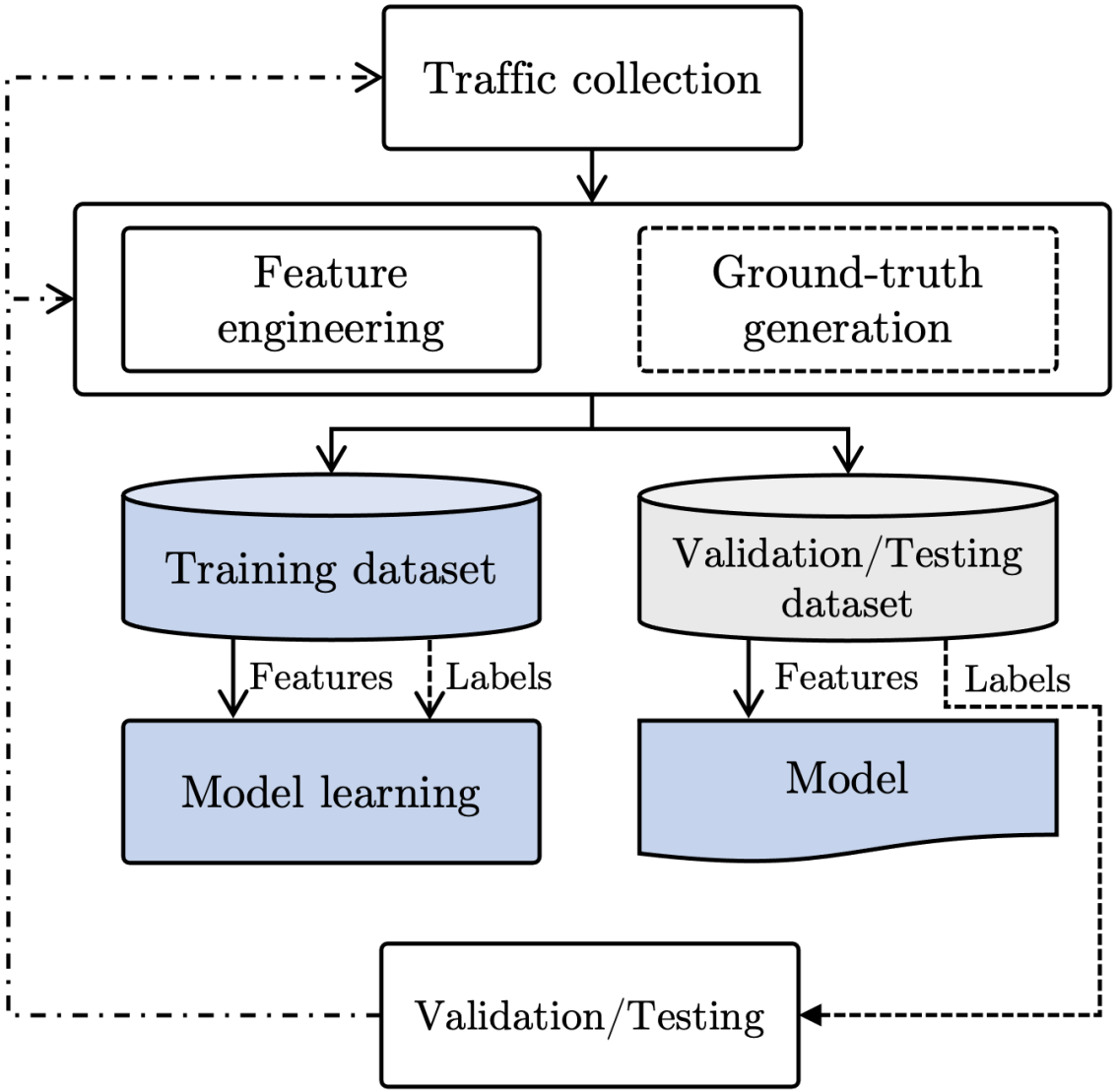


Privacy-Preserving Federated Learning: A New Horizon for Advanced Network Analytics

Dr. Adrián Pekár



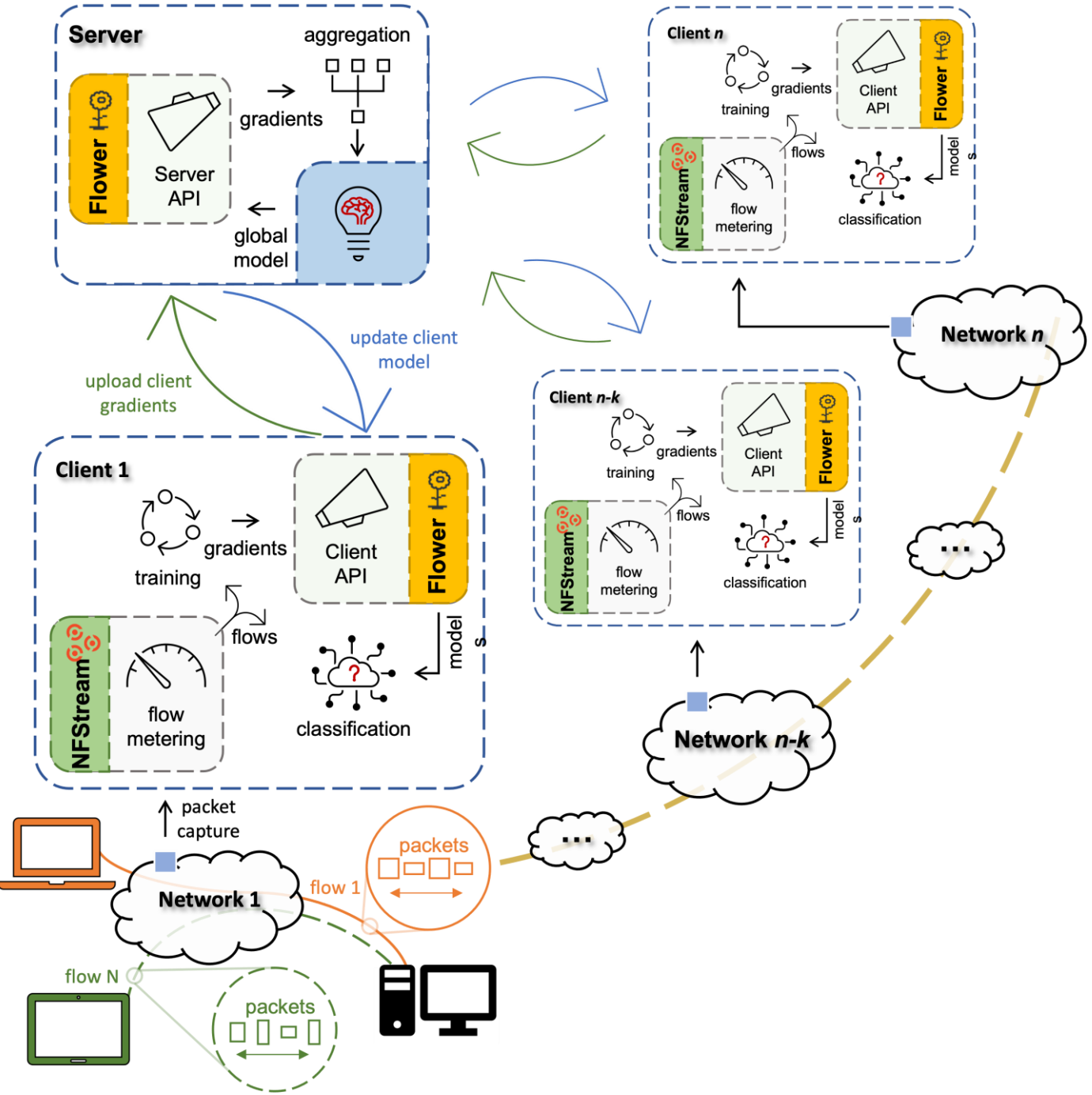
IP Flow Analysis Using Machine Learning

Smooth data sharing, although highly desired, is not always practicable.

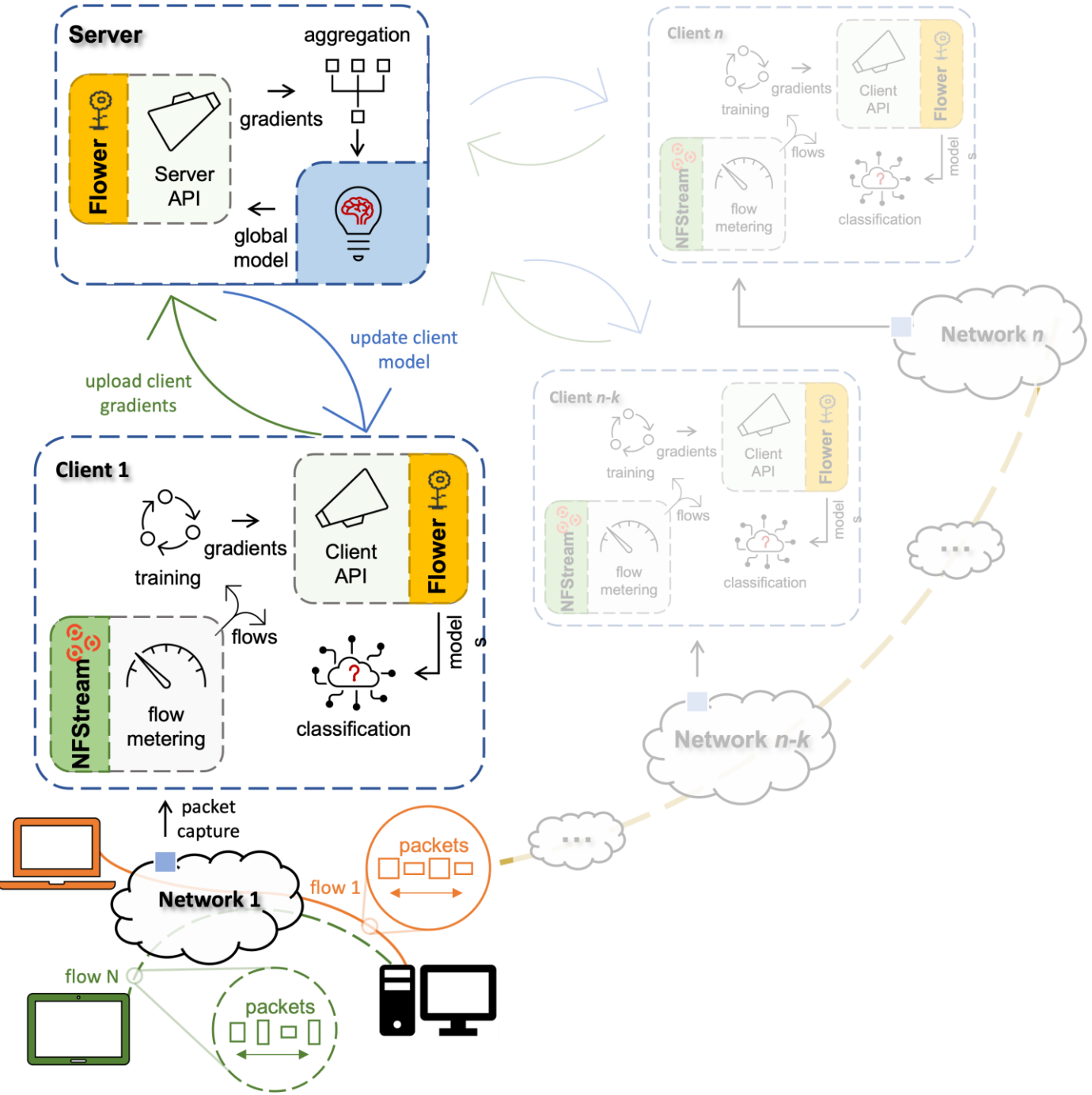
ISPs, and **Big Tech**, **Data** and **Media Companies** could contribute immensely to develop better AI models, if not hindered by privacy concerns.

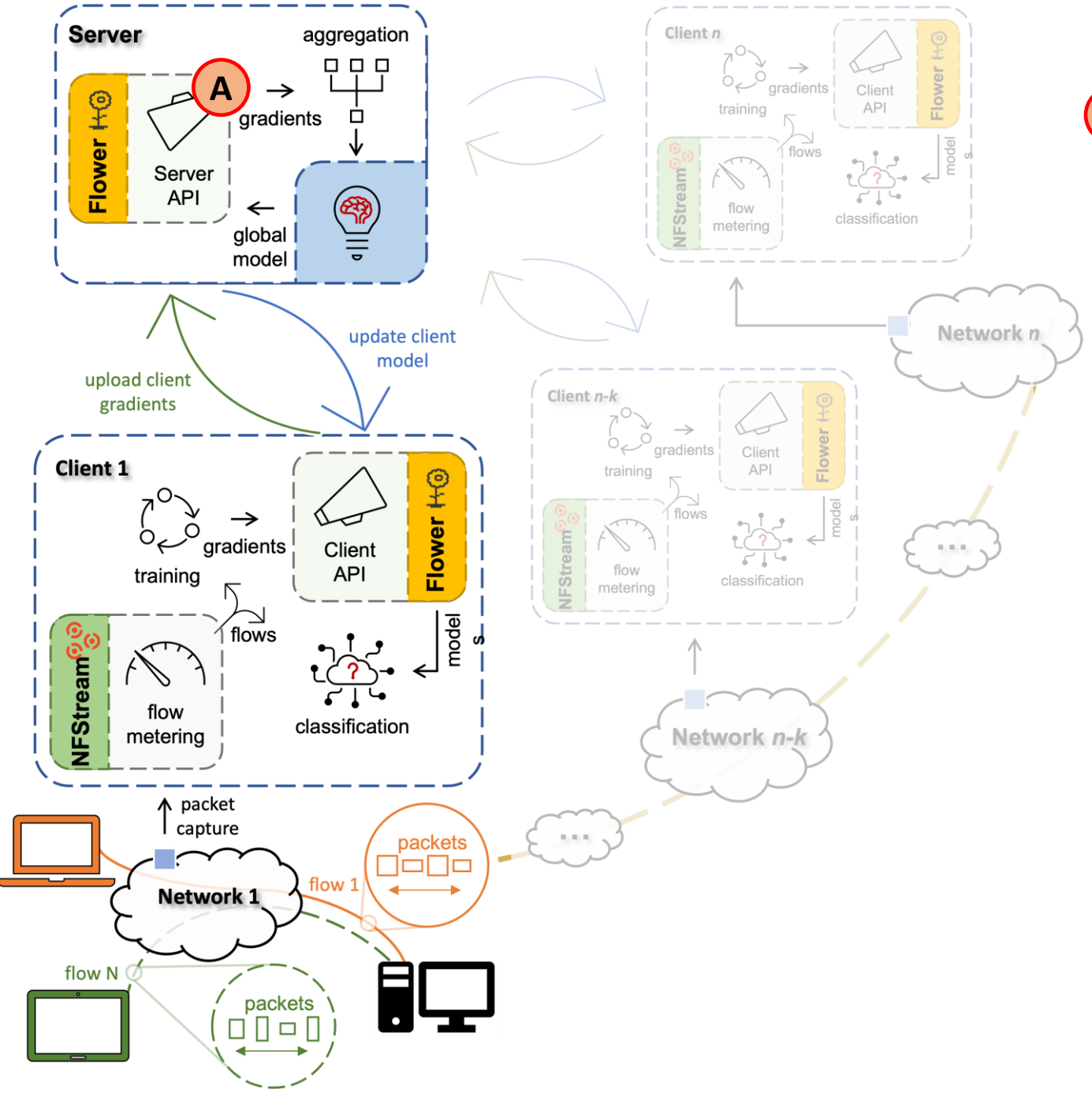
Leveraging
Federated Learning
for advanced network analytics,
all without sharing a byte of traffic data

Operational Principles



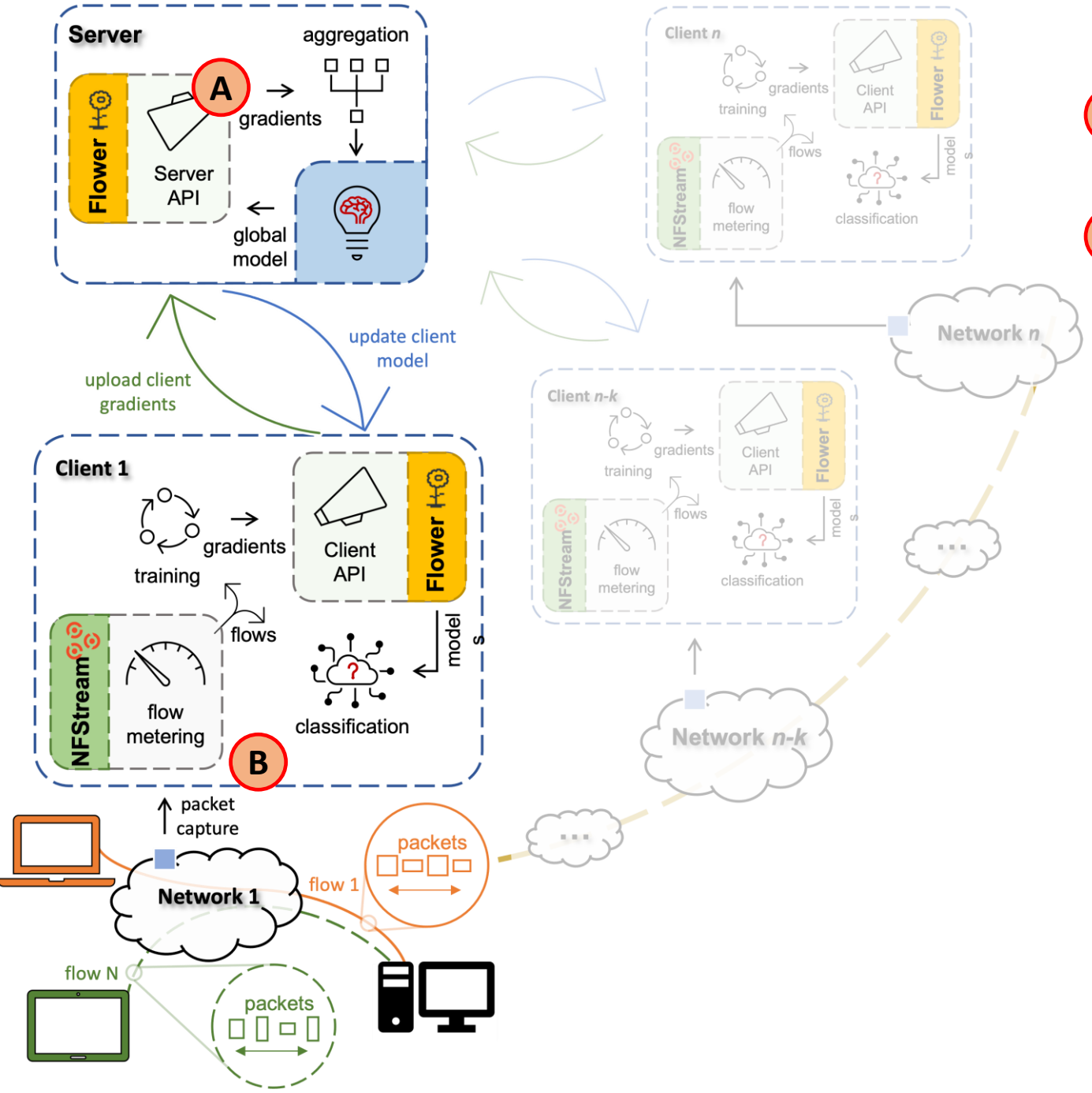
Operational Principles





Operational Principles

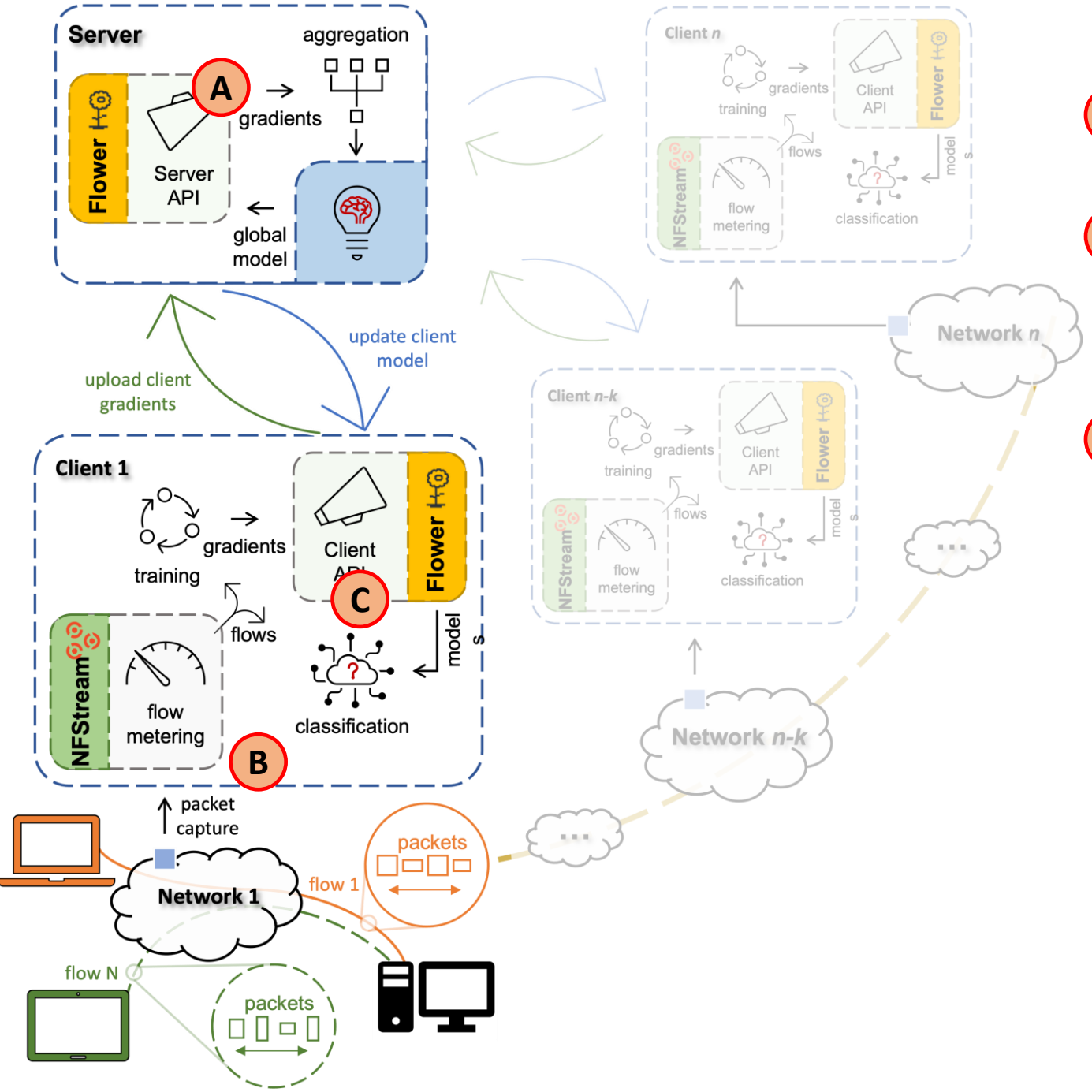
A **Server Operation:** We run a secure server orchestrating the federated network, your cornerstone for collaborative learning.



Operational Principles

A **Server Operation:** We run a secure server orchestrating the federated network, your cornerstone for collaborative learning.

B **Client Application:** We supply an all-in-one client-side application. From packet capture to flow record organization and preprocessing for local ML model training, it's got you covered.

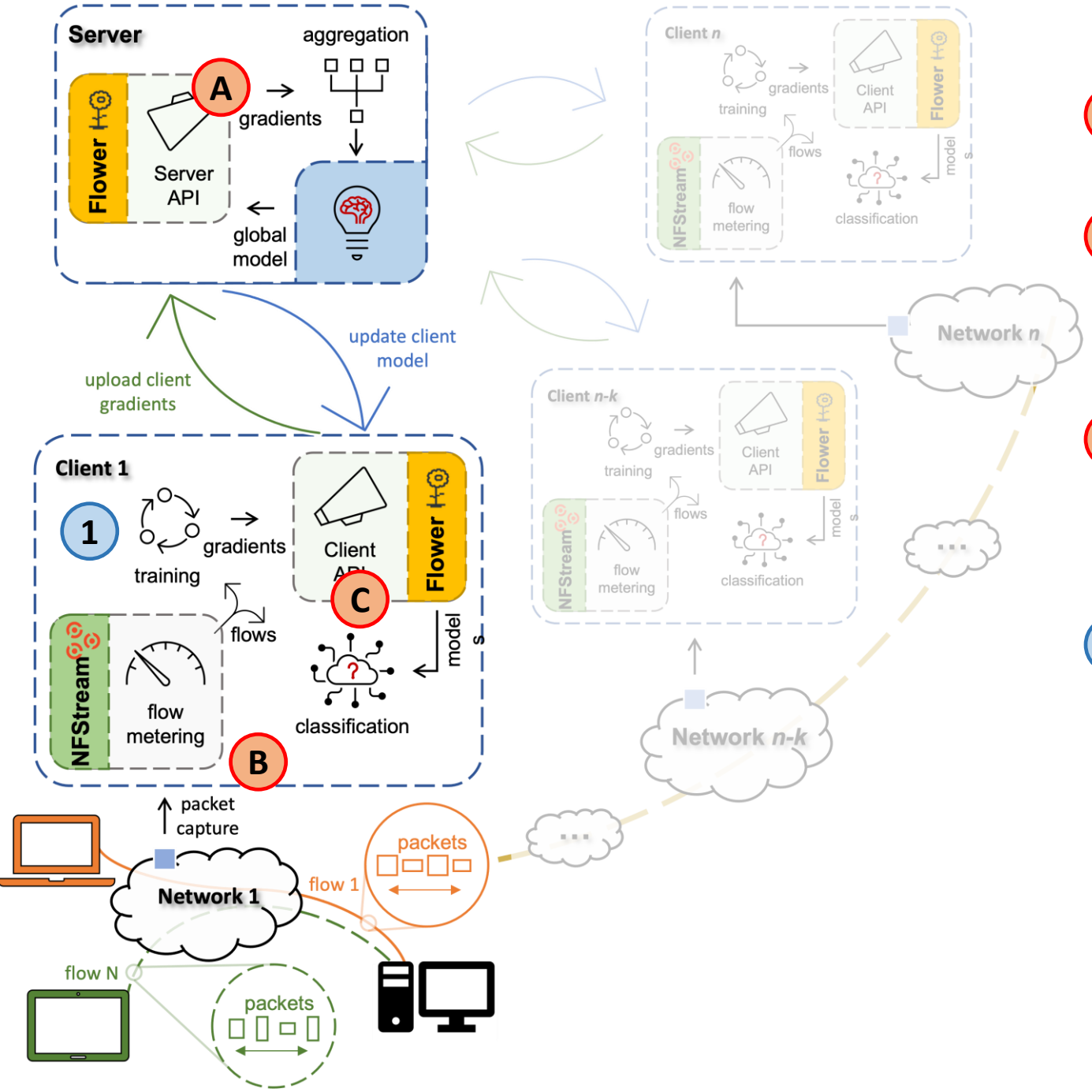


Operational Principles

A **Server Operation:** We run a secure server orchestrating the federated network, your cornerstone for collaborative learning.

B **Client Application:** We supply an all-in-one client-side application. From packet capture to flow record organization and preprocessing for local ML model training, it's got you covered.

C Plus, clients can also operate in a ”benefit-only" mode, leveraging the latest global model to categorize flows without participating in collaborative learning.



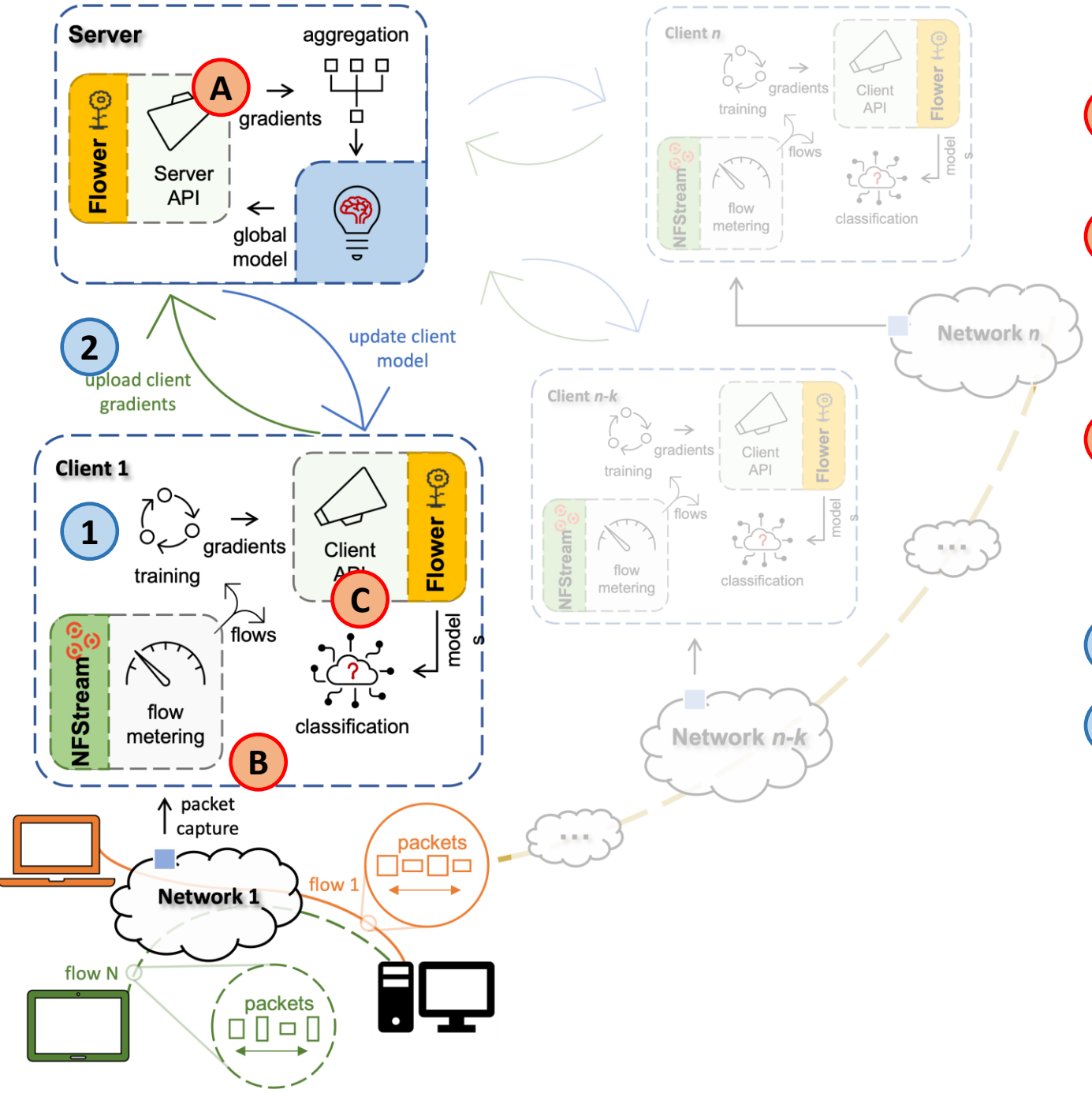
Operational Principles

A **Server Operation:** We run a secure server orchestrating the federated network, your cornerstone for collaborative learning.

B **Client Application:** We supply an all-in-one client-side application. From packet capture to flow record organization and preprocessing for local ML model training, it's got you covered.

C Plus, clients can also operate in a ”benefit-only" mode, leveraging the latest global model to categorize flows without participating in collaborative learning.

1 **Local Training:** Participants independently compute training gradients using their local data.



Operational Principles

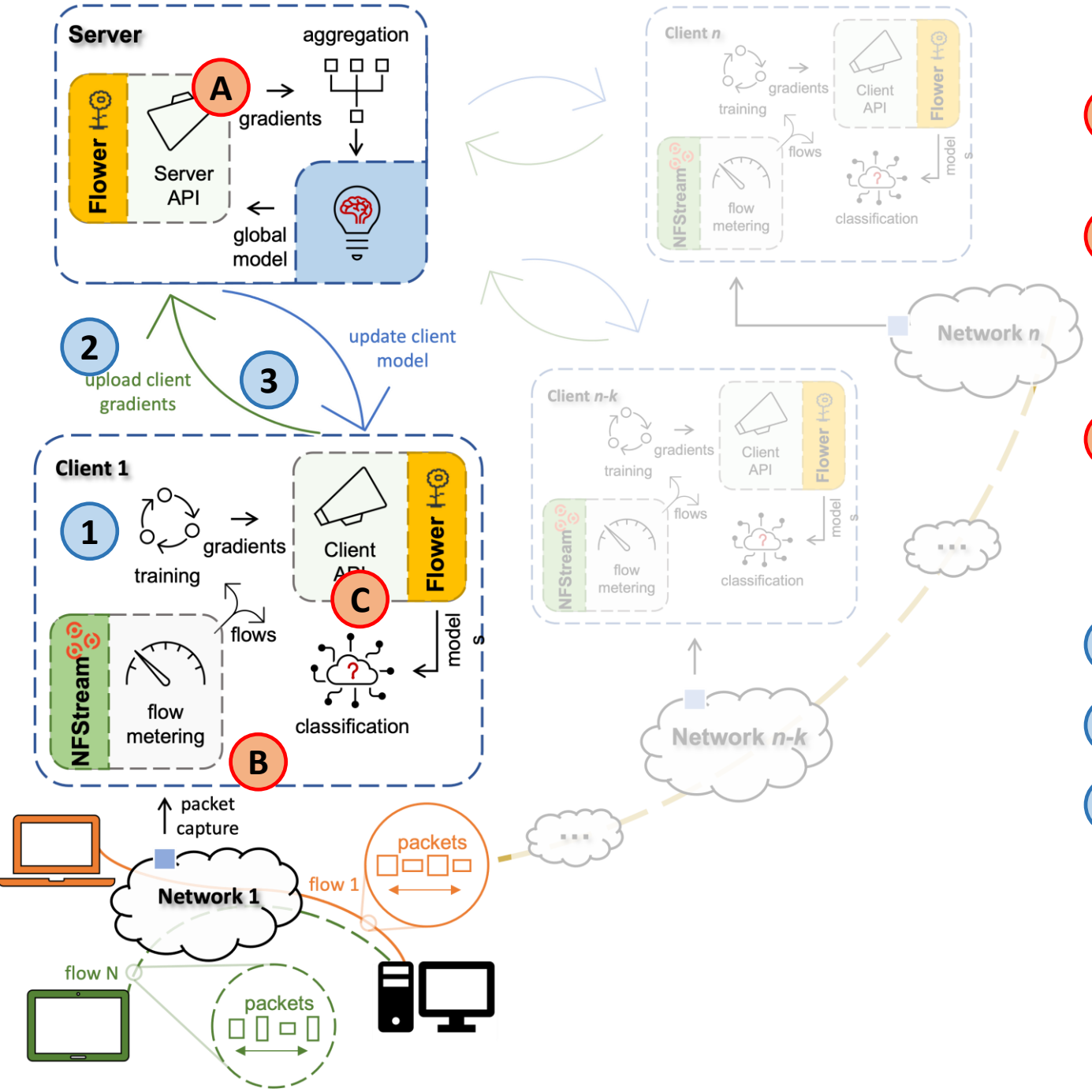
A **Server Operation:** We run a secure server orchestrating the federated network, your cornerstone for collaborative learning.

B **Client Application:** We supply an all-in-one client-side application. From packet capture to flow record organization and preprocessing for local ML model training, it's got you covered.

C Plus, clients can also operate in a ”benefit-only" mode, leveraging the latest global model to categorize flows without participating in collaborative learning.

1 **Local Training:** Participants independently compute training gradients using their local data.

2 **Global Model Update:** Our server collects these gradients periodically, using them to update the global model.



Operational Principles

A **Server Operation:** We run a secure server orchestrating the federated network, your cornerstone for collaborative learning.

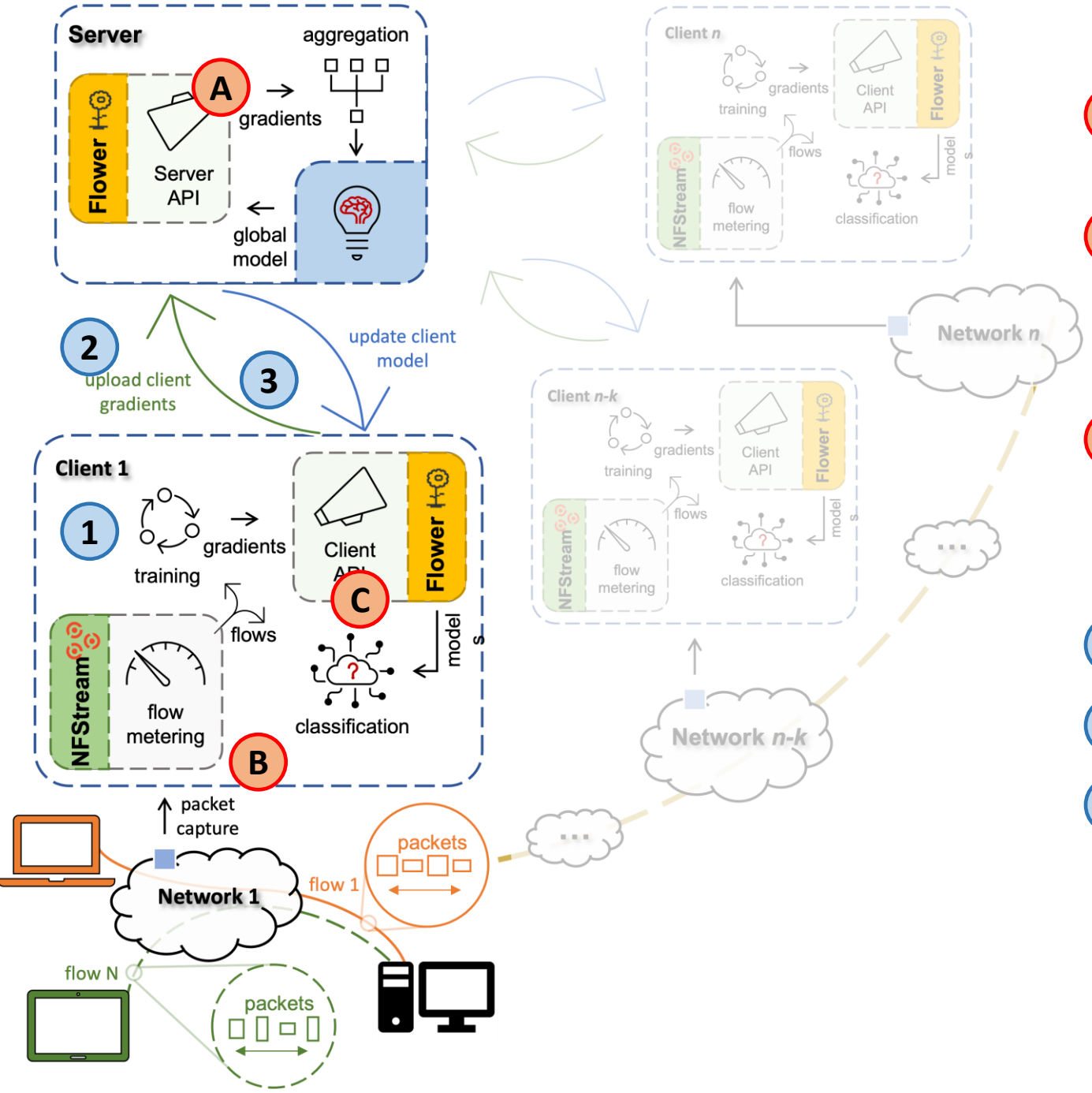
B **Client Application:** We supply an all-in-one client-side application. From packet capture to flow record organization and preprocessing for local ML model training, it's got you covered.

C Plus, clients can also operate in a ”benefit-only" mode, leveraging the latest global model to categorize flows without participating in collaborative learning.

1 **Local Training:** Participants independently compute training gradients using their local data.

2 **Global Model Update:** Our server collects these gradients periodically, using them to update the global model.

3 **Local Model Update:** Participants then update their local models using the improved global model.



Operational Principles

A **Server Operation:** We run a secure server orchestrating the federated network, your cornerstone for collaborative learning.

B **Client Application:** We supply an all-in-one client-side application. From packet capture to flow record organization and preprocessing for local ML model training, it's got you covered.

C Plus, clients can also operate in a ”benefit-only" mode, leveraging the latest global model to categorize flows without participating in collaborative learning.

1 **Local Training:** Participants independently compute training gradients using their local data.

2 **Global Model Update:** Our server collects these gradients periodically, using them to update the global model.

3 **Local Model Update:** Participants then update their local models using the improved global model.

Learning & Privacy: By repeating these steps, we achieve a continuous learning cycle that keeps data local and privacy intact.

Proof of Concept Validation

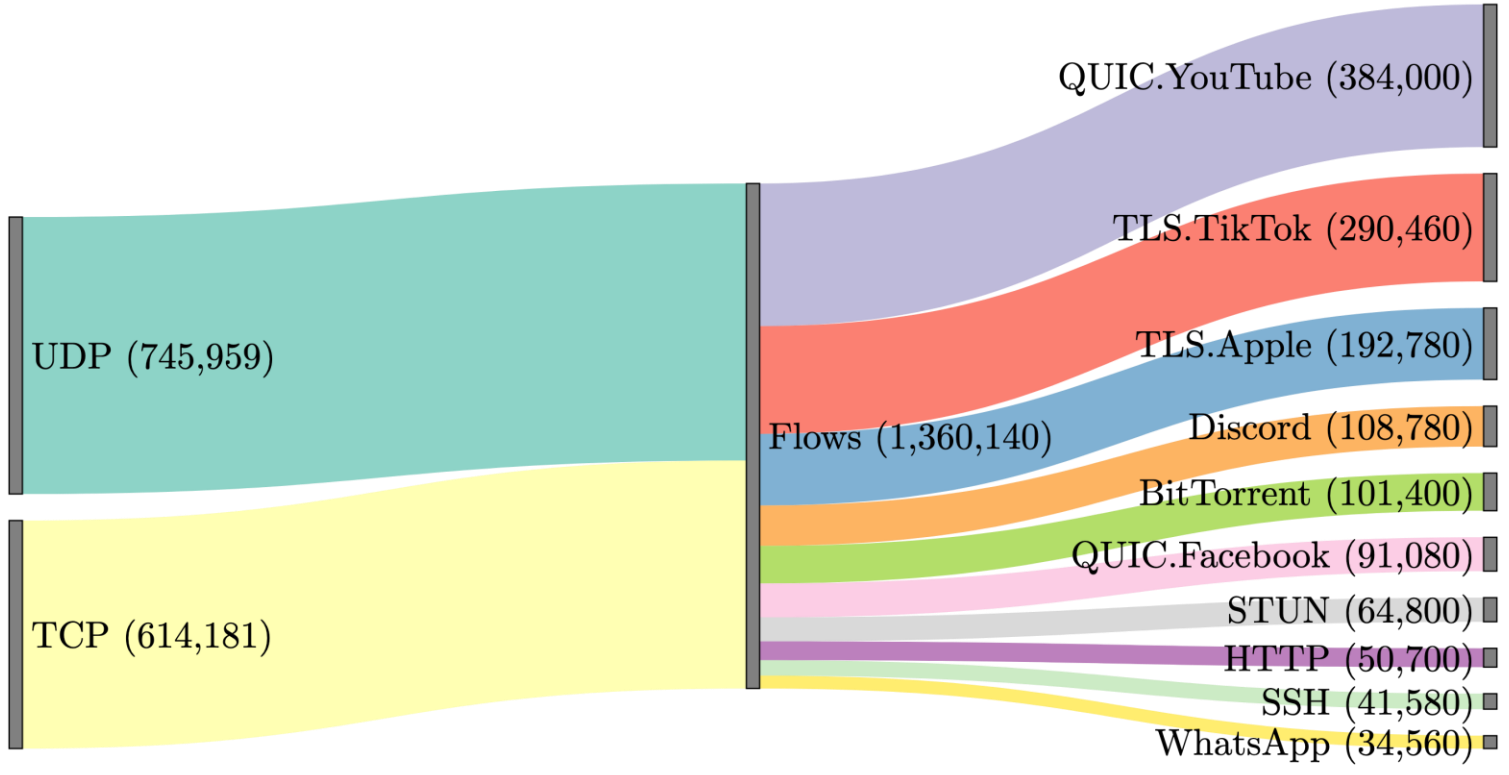
- L7 classification

- University network traffic

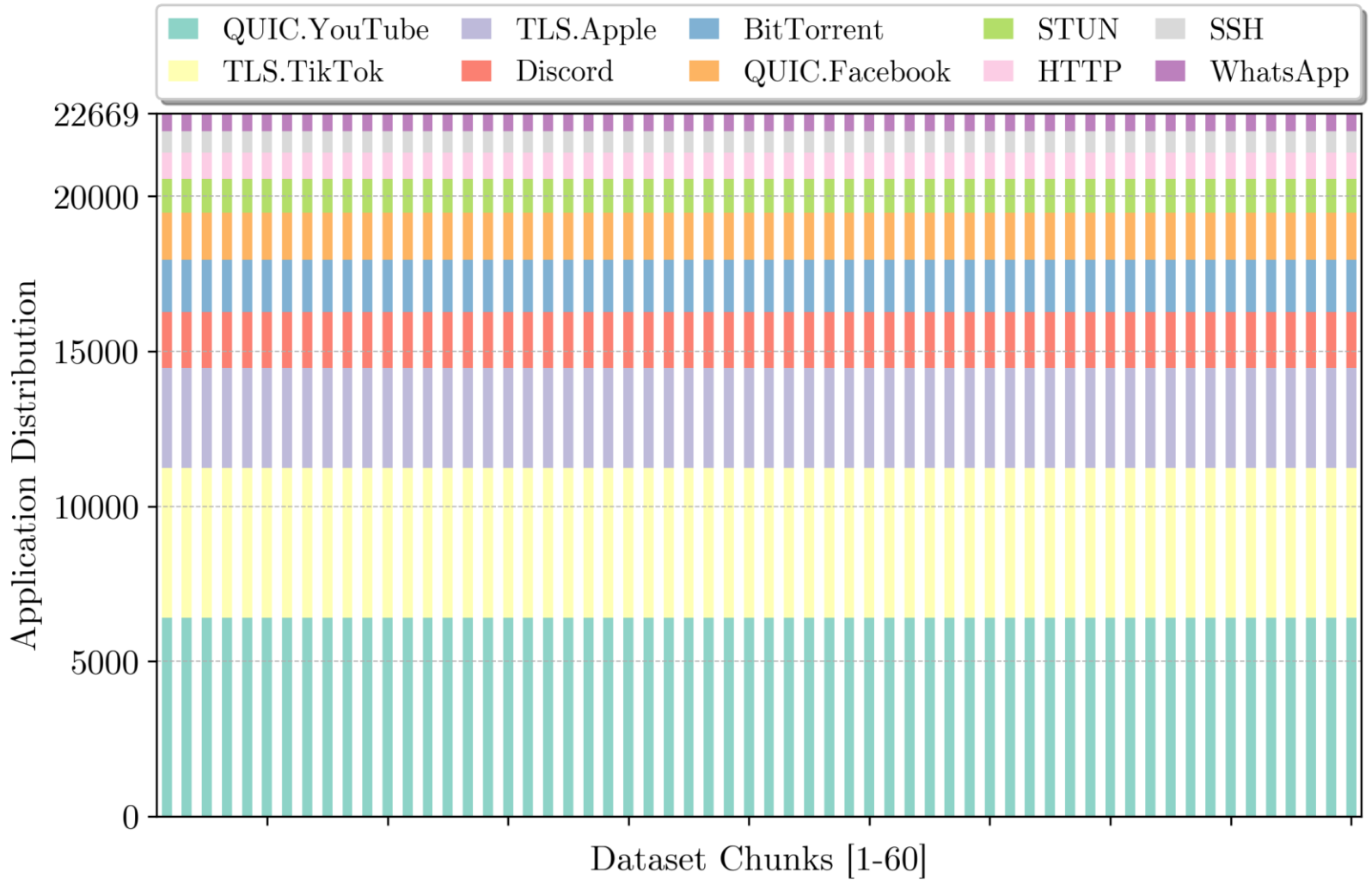
- 1 server
- 5 participants

- FNN: 18 (Input), 22 (ReLU), 18 (ReLU), 10 (Softmax/Output)

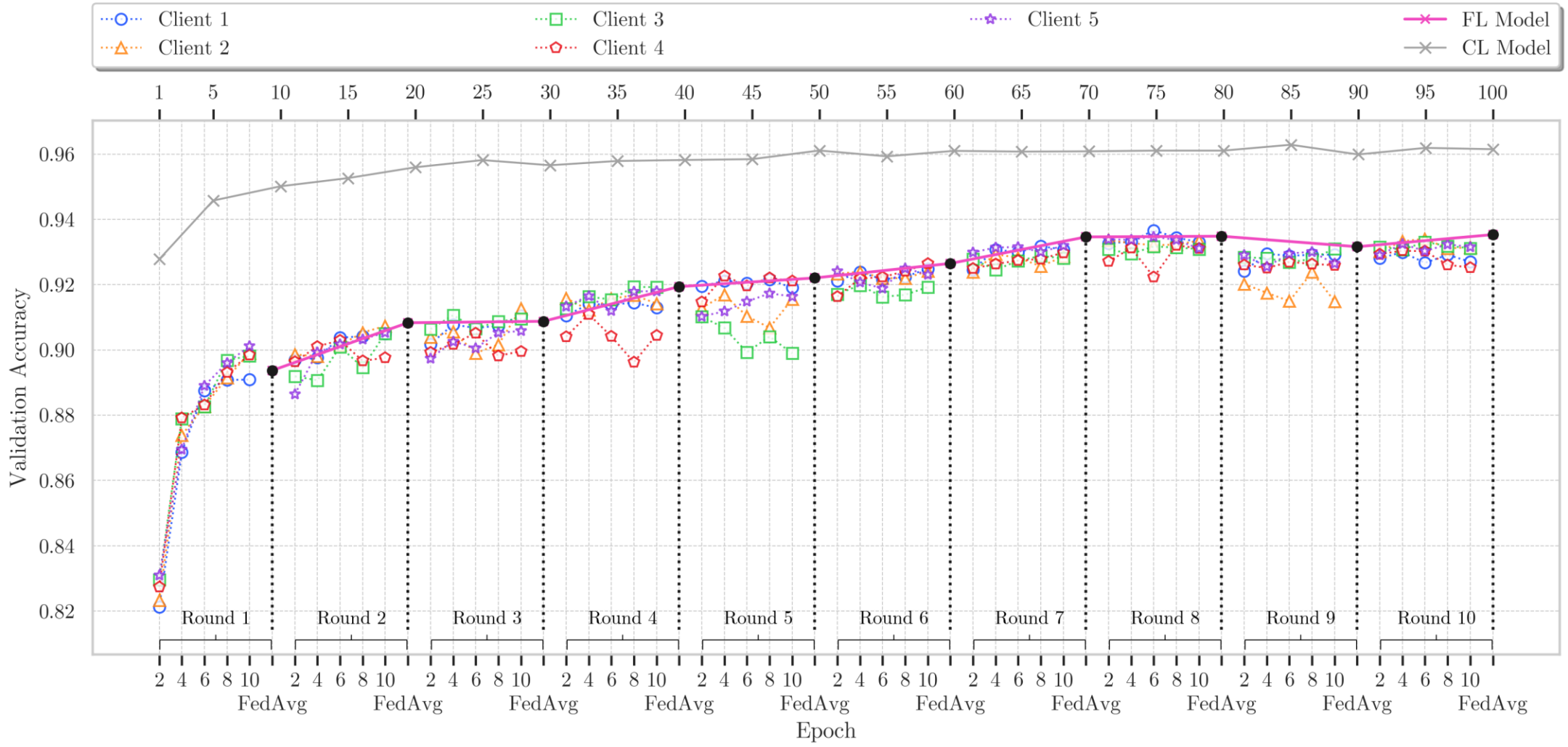
- CL vs FL IID vs FL non-IID



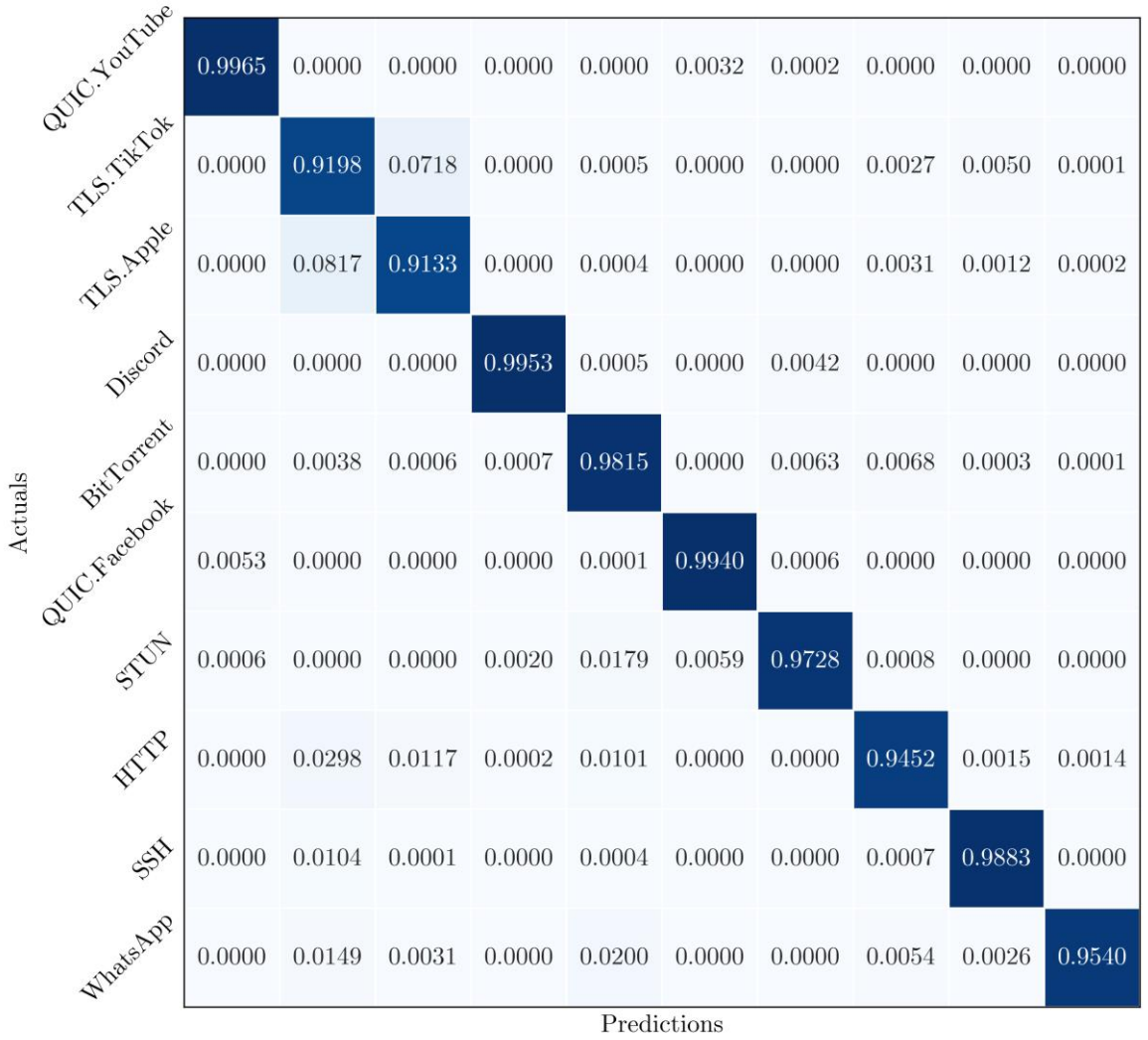
FL IID Scenario



FL IID Scenario



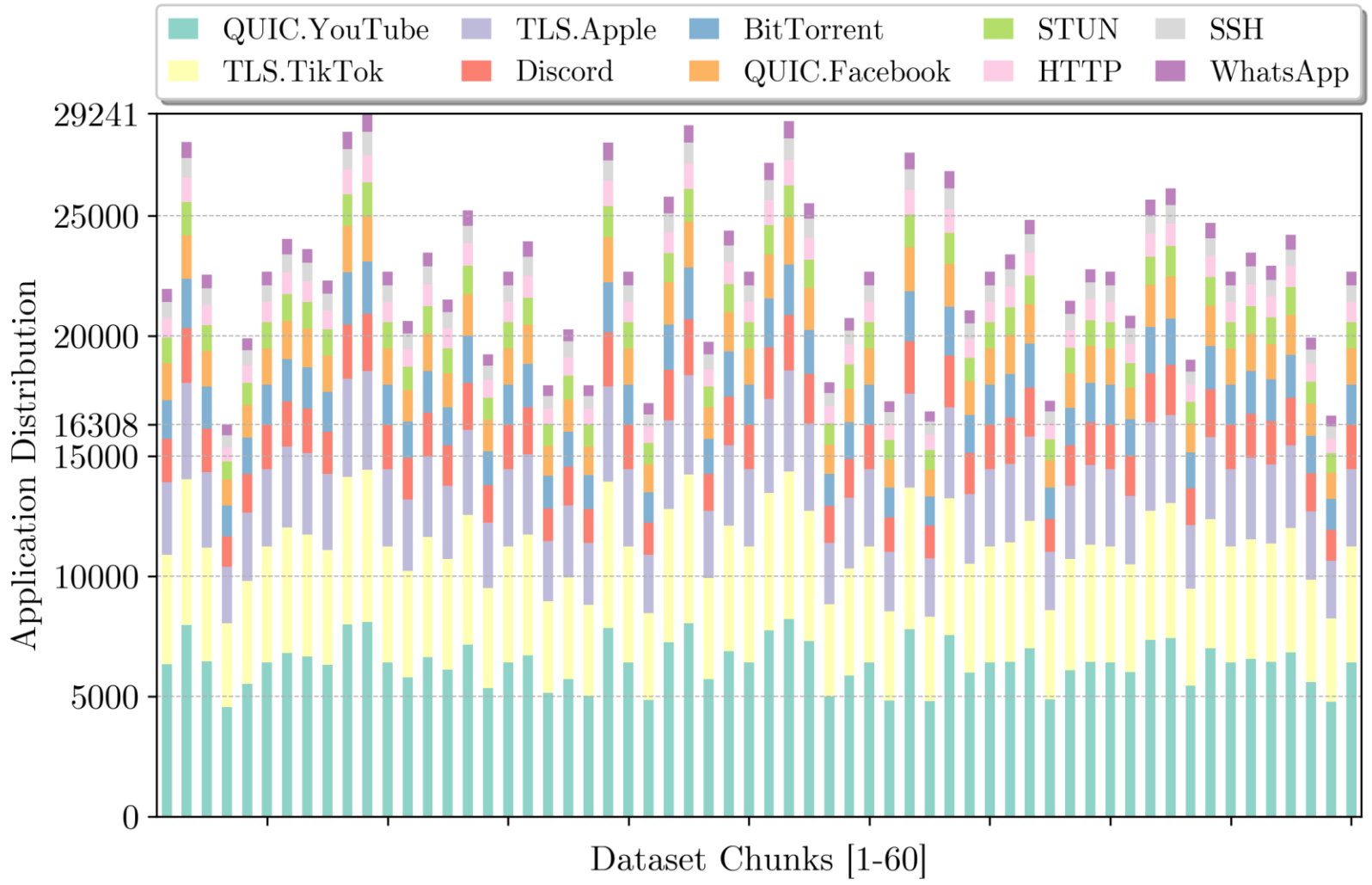
FL IID Scenario



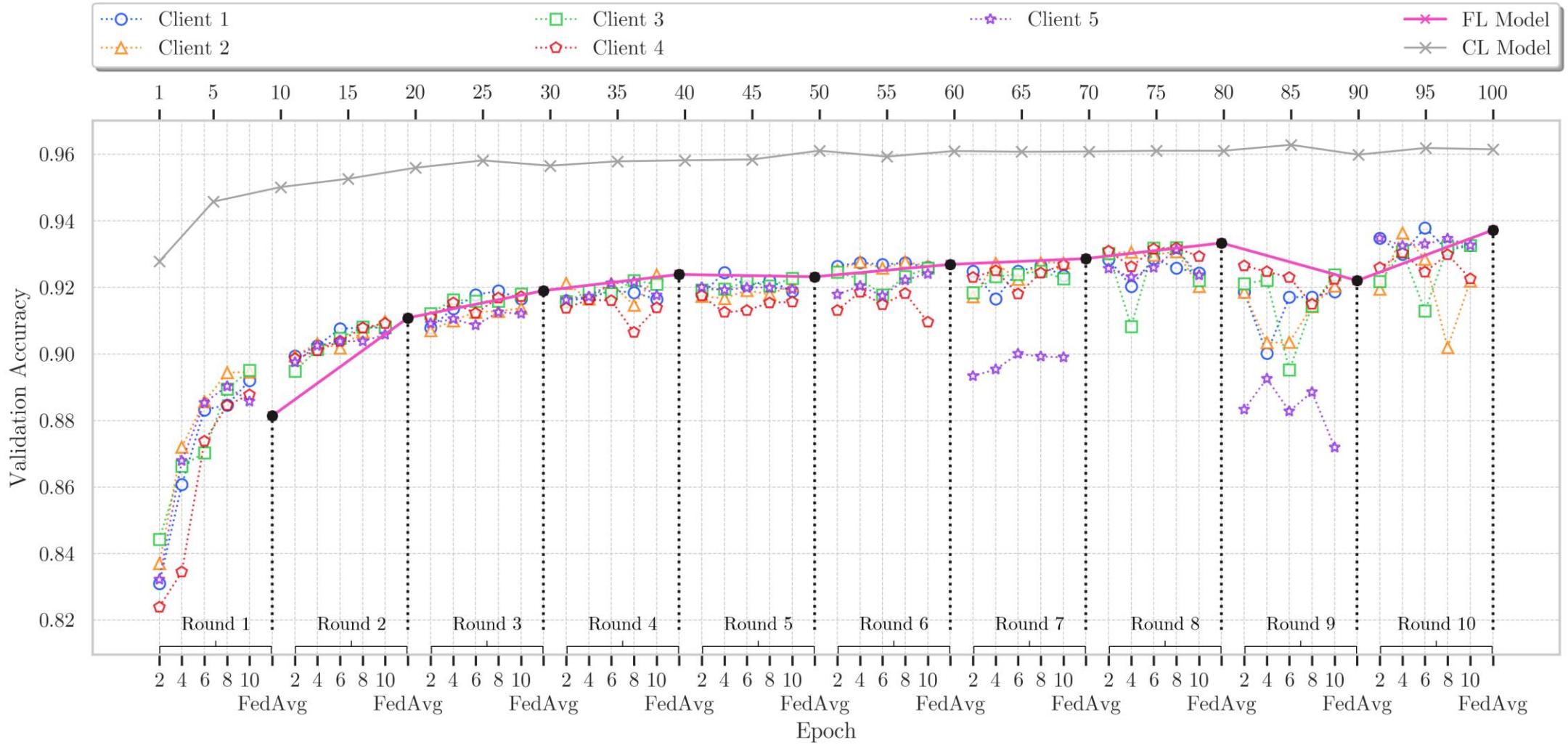
CL

FL IID

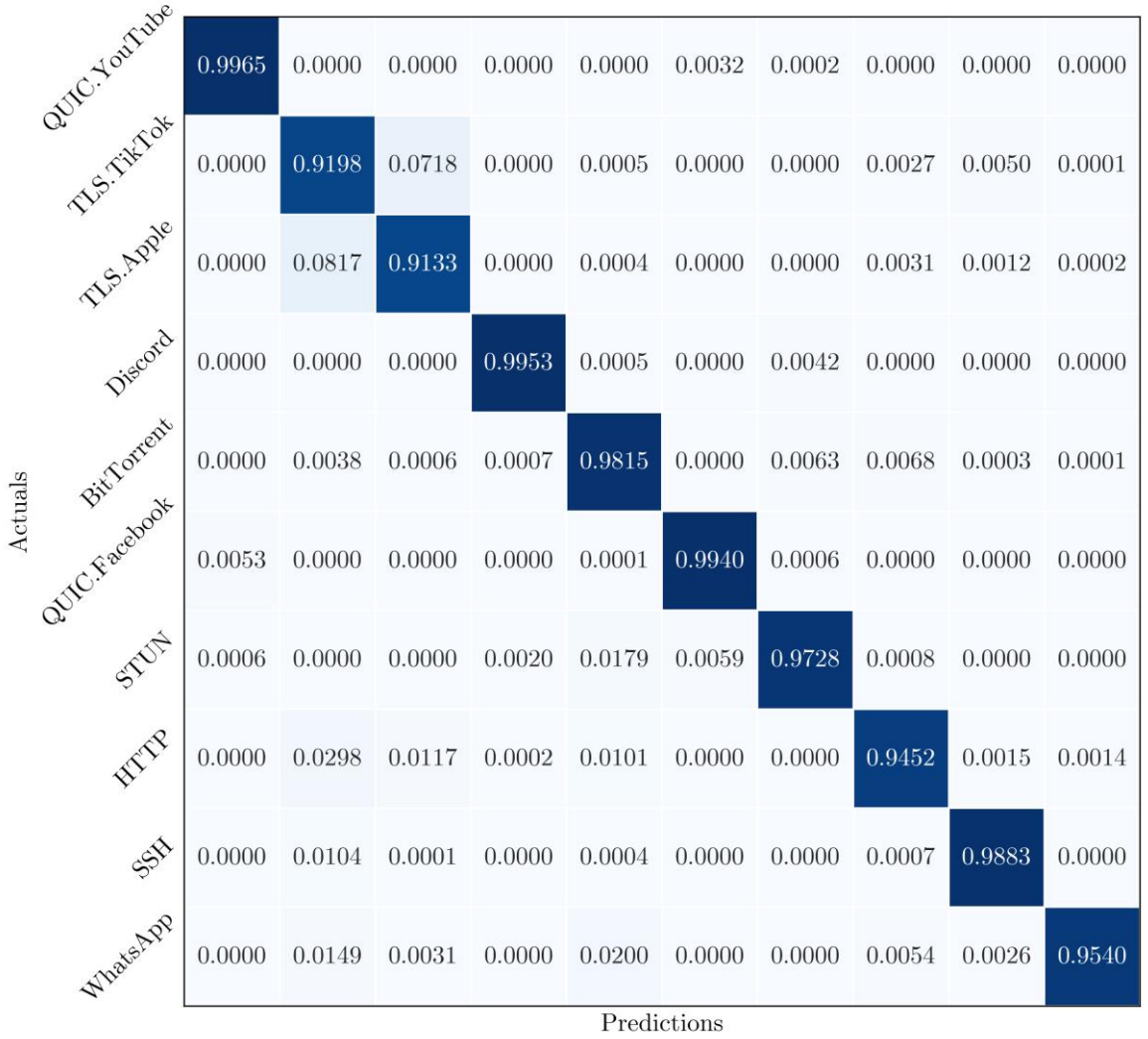
FL non-IID Scenario A



FL non-IID Scenario A



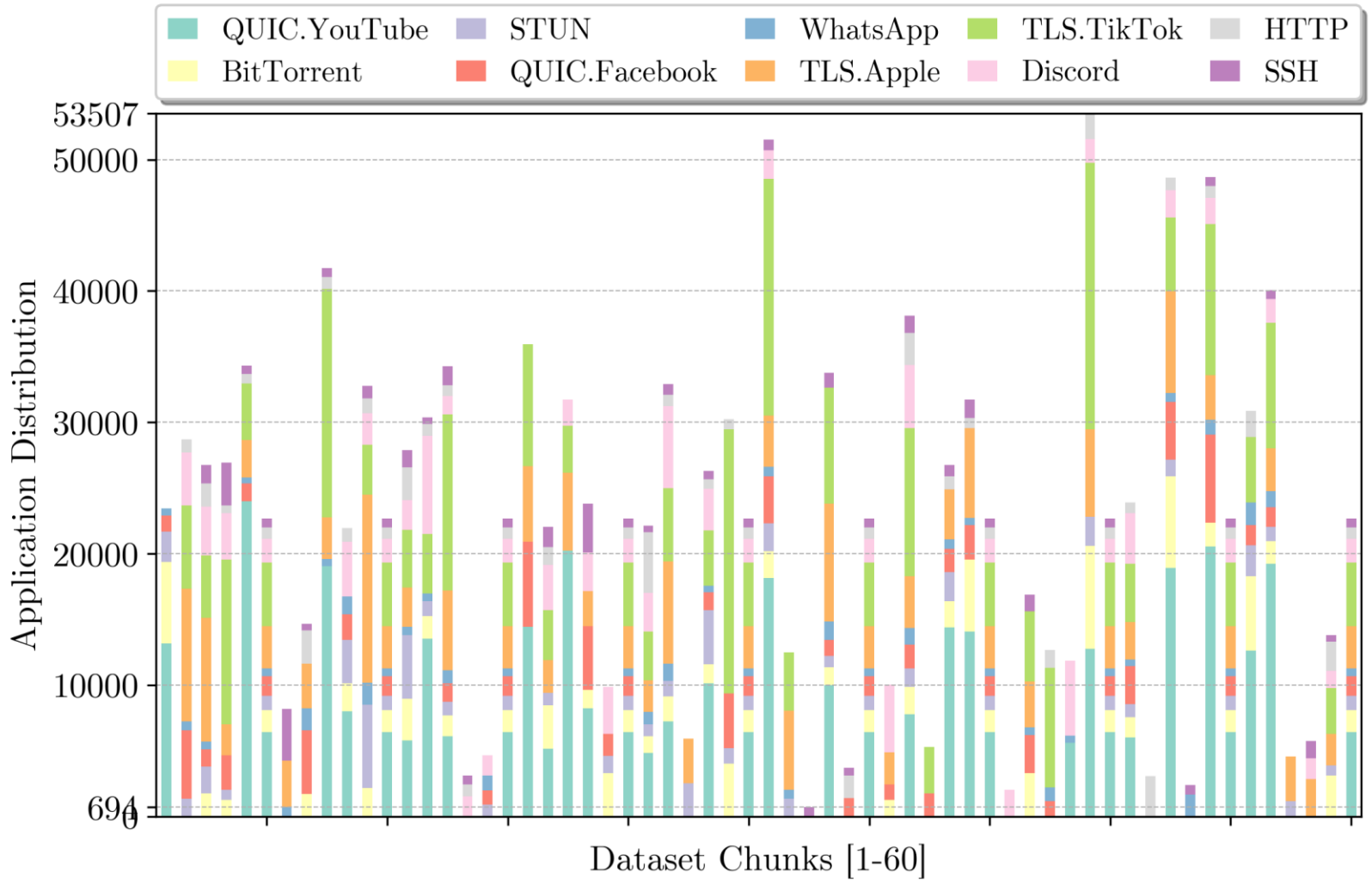
FL non-IID Scenario A



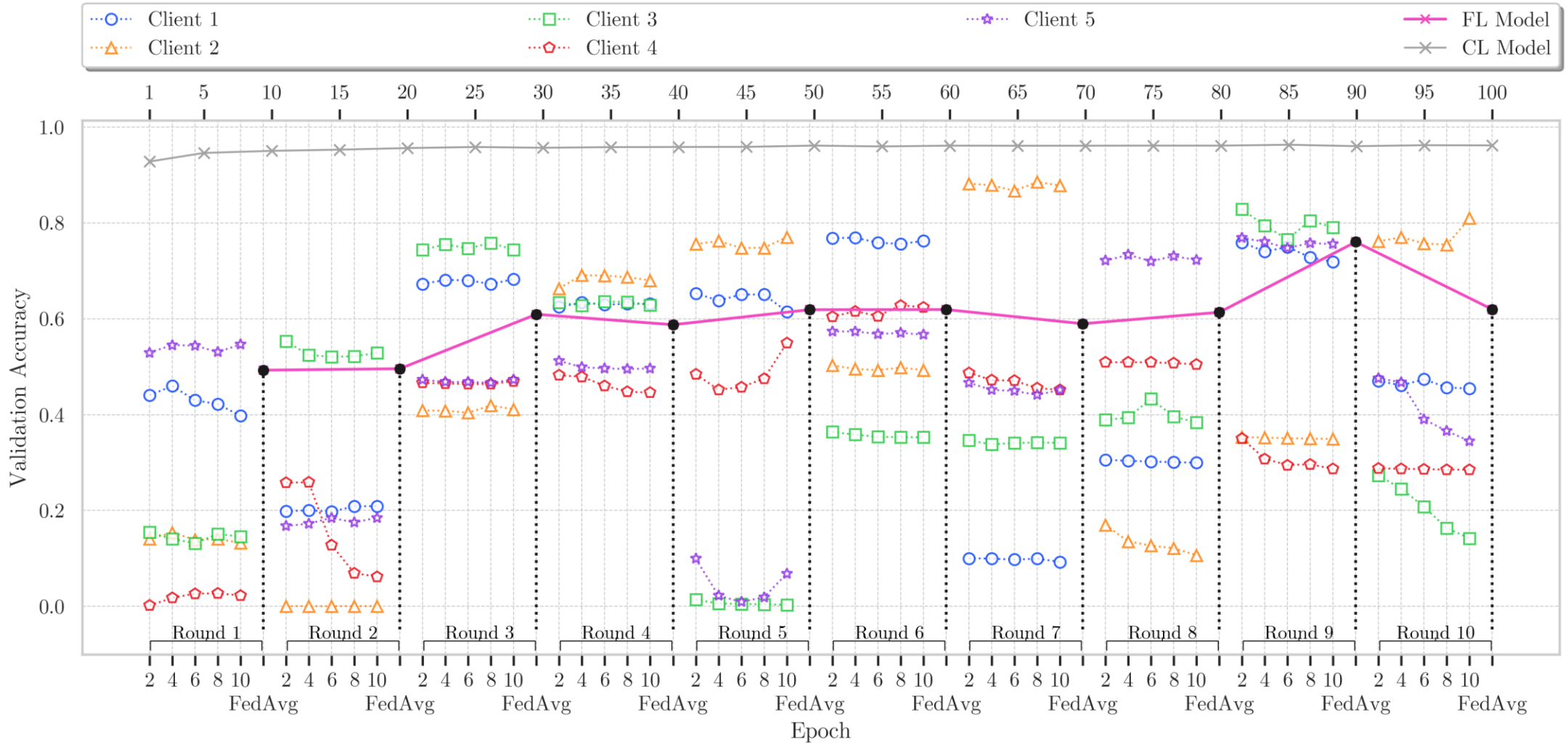
CL

FL non-IID A

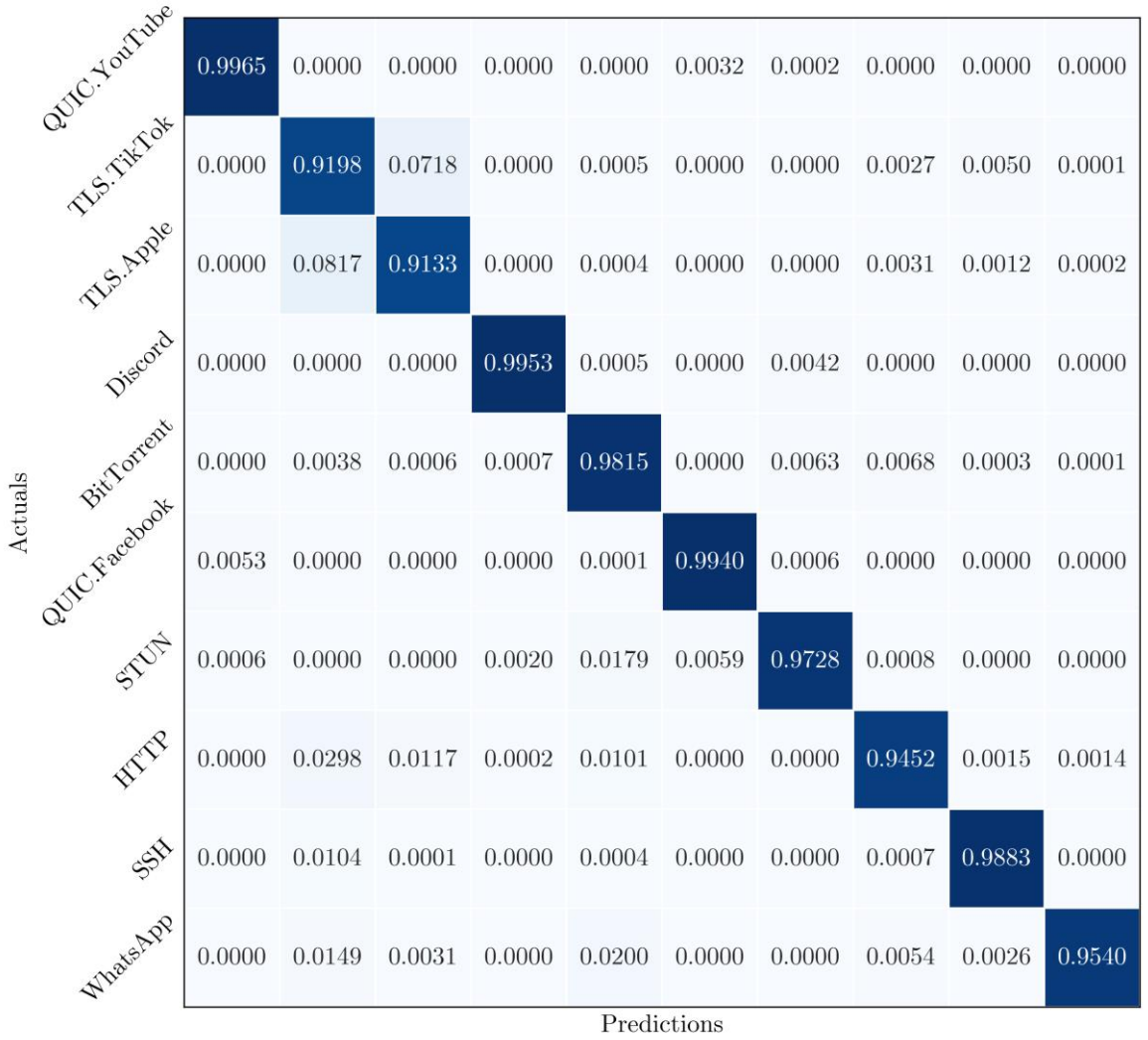
FL non-IID Scenario B



FL non-IID Scenario B



FL non-IID Scenario B



CL

FL non-IID B

Prospects

CYBERSECURITY
THREAT DETECTION

PREDICTIVE
MAINTENANCE

INDUSTRY
NETWORK

LIVE TRAFFIC
ANALYTICS

Thank you

apekar@hit.bme.hu