Personalized Federated Learning:

The next major boost in ML Performance

Vaikkunth Mugunthan, Ph.D.
CEO and Cofounder of DynamoFL

DynamoFL

About Me

- Ph.D. in privacy-preserving distributed machine learning at MIT

- Founder and CEO of DynamoFL (YC W22)
  - Personalized and Privacy-Preserving ML
  - Backed by Samsung Next, Nexus, YCombinator, GFC, Liquid2, etc.

DynamoFL

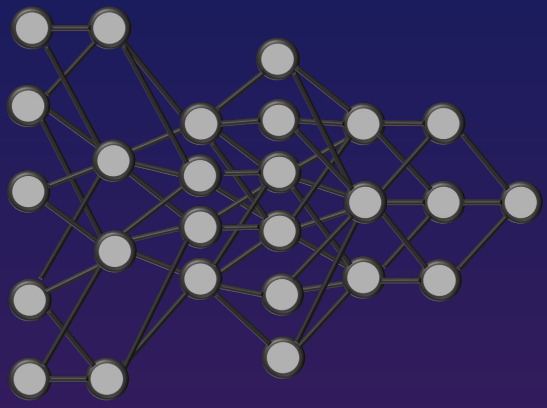
DynamoFL

How can you train a model that captures diverse real-world data?

How can you train a model that captures diverse real-world data?

Today's Solution:

One-size-fits-all Model

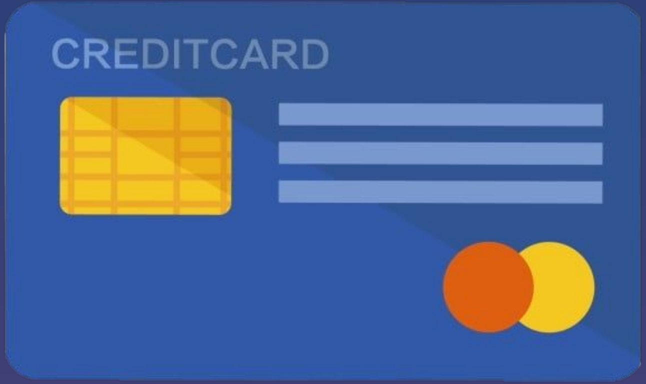


Challenge 1: Can't Access Diverse Privacy-Critical Data

DynamoFL

Privacy-Critical Data

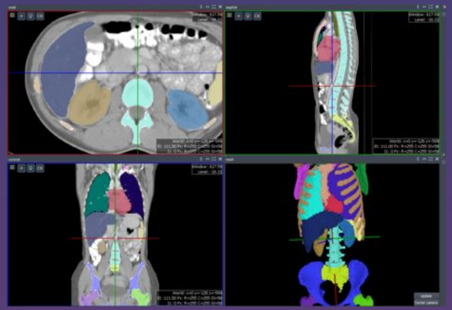
Transactional Data



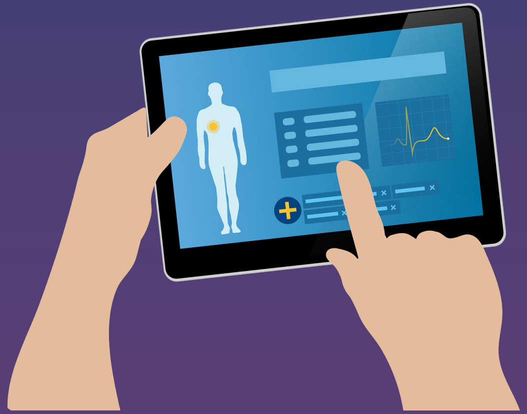
Clinical Trials / Life Sciences Data

Risk Prediction

Medical Imaging Data



EHR/EMR/PHI



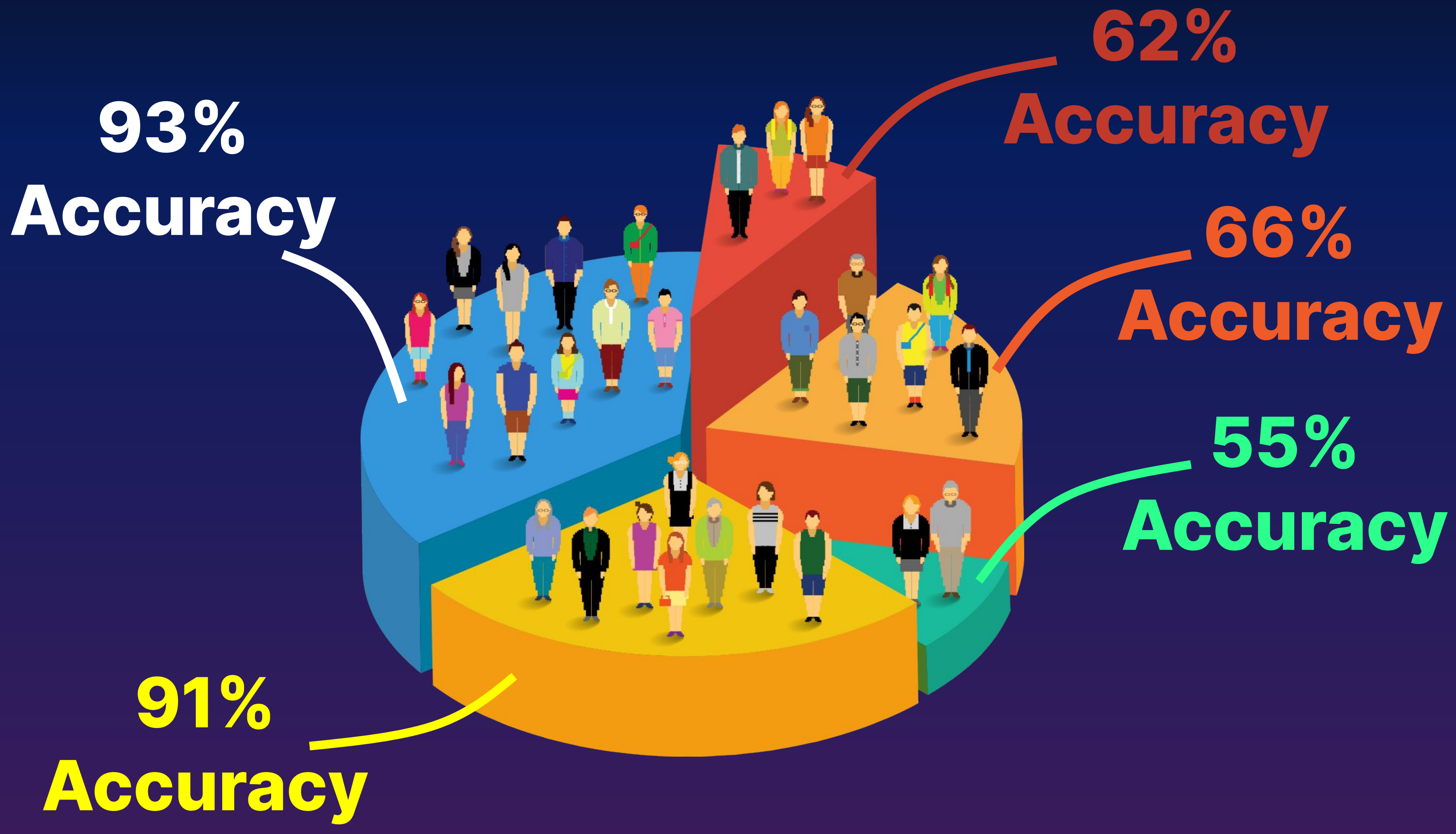
Regulations

GDPR

HIPAA

CCPA

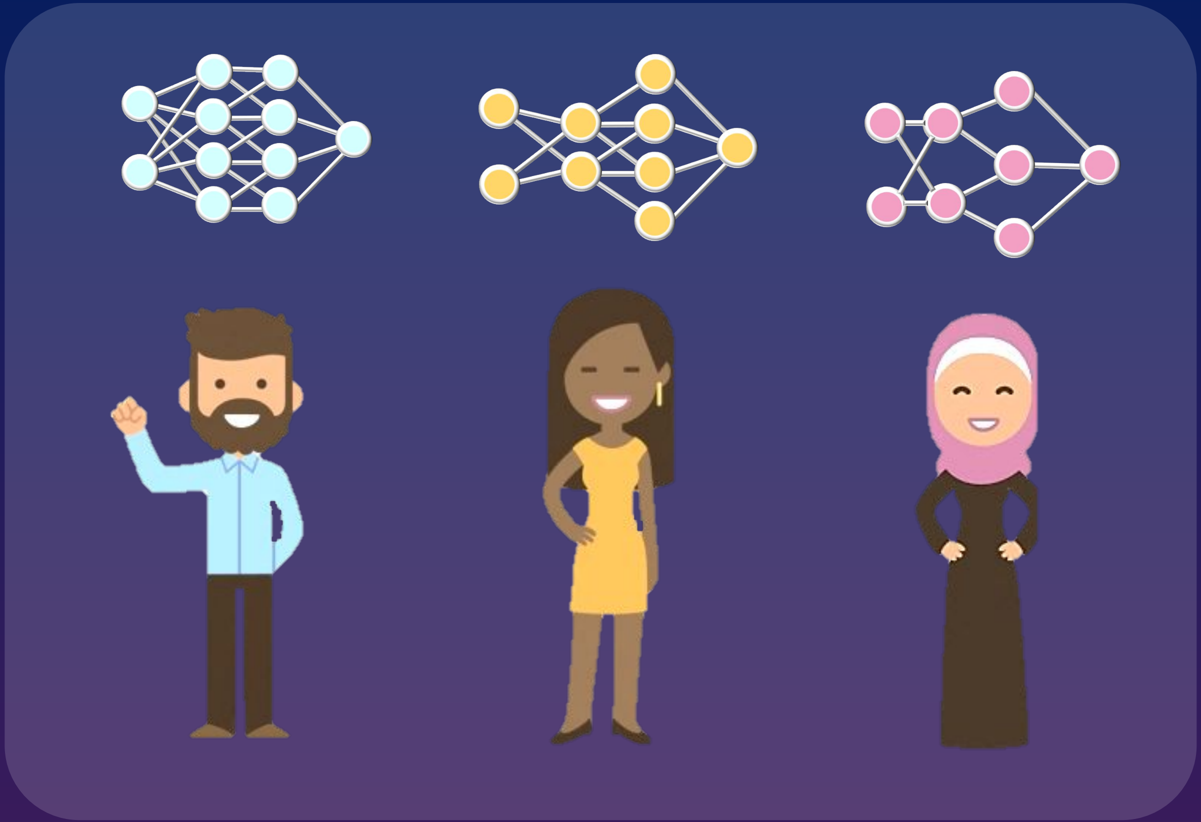
Challenge 2: Poor Performance across Diverse Cohorts



One-size-fits-all model struggles across under-represented cohorts

DynamoFL

How can you train a model that captures diverse real-world data?



Our Solution:

Personalized Federated Learning

DynamoFL

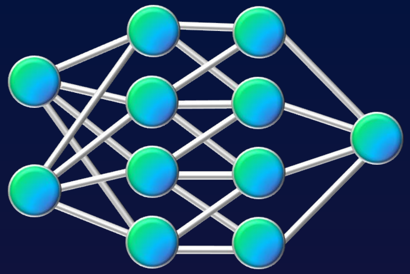
Our Solution: Personalized Federated Learning

User Privacy

Never collect sensitive user data

Robust against privacy attacks
(Model Inversion, Membership inference, *etc.*)

Boost Performance



Boosted Top-1 Accuracy by **+14.2%** for CV Task
(work accepted for ECCV '22)

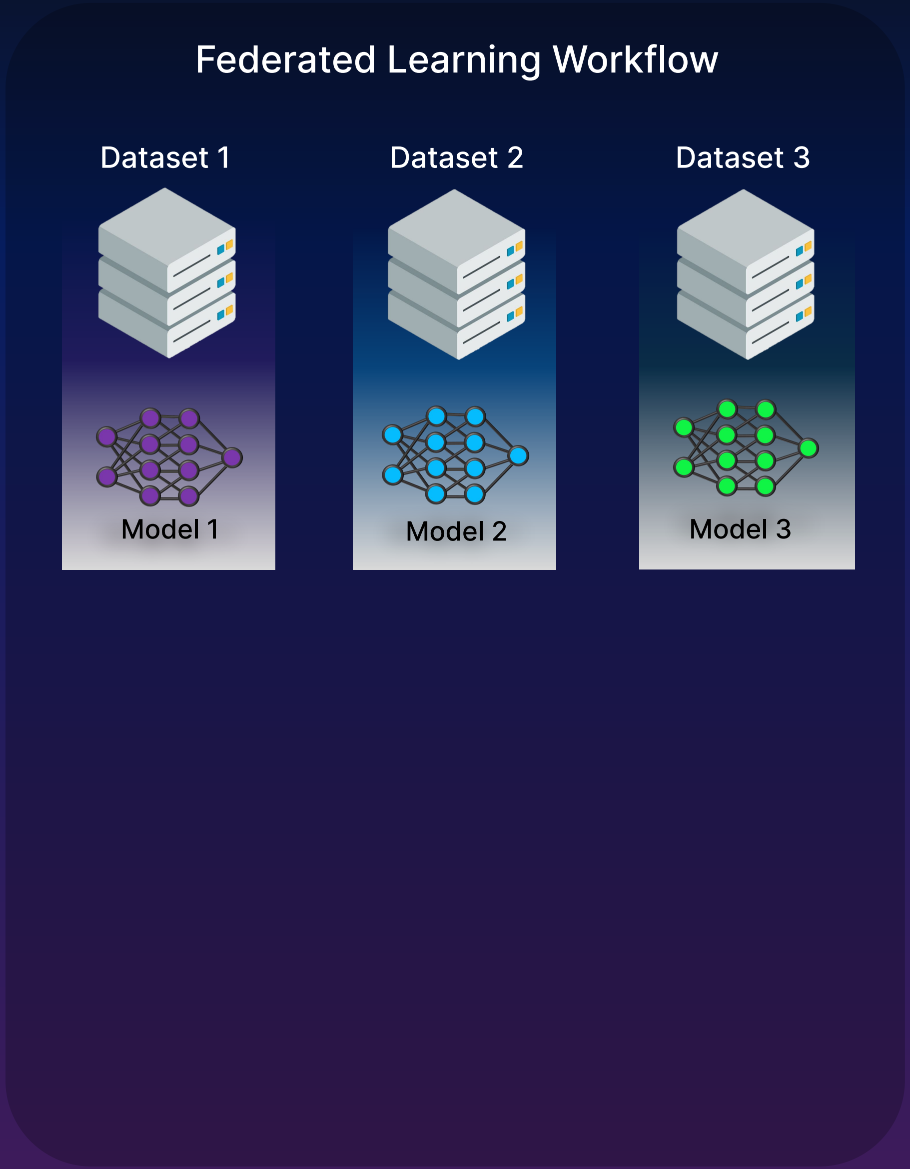
Reduced time-series prediction error by 28% for asset-forecasting case study

Slash Data Costs

~10,000× lower data transfer costs compared to mass data upload

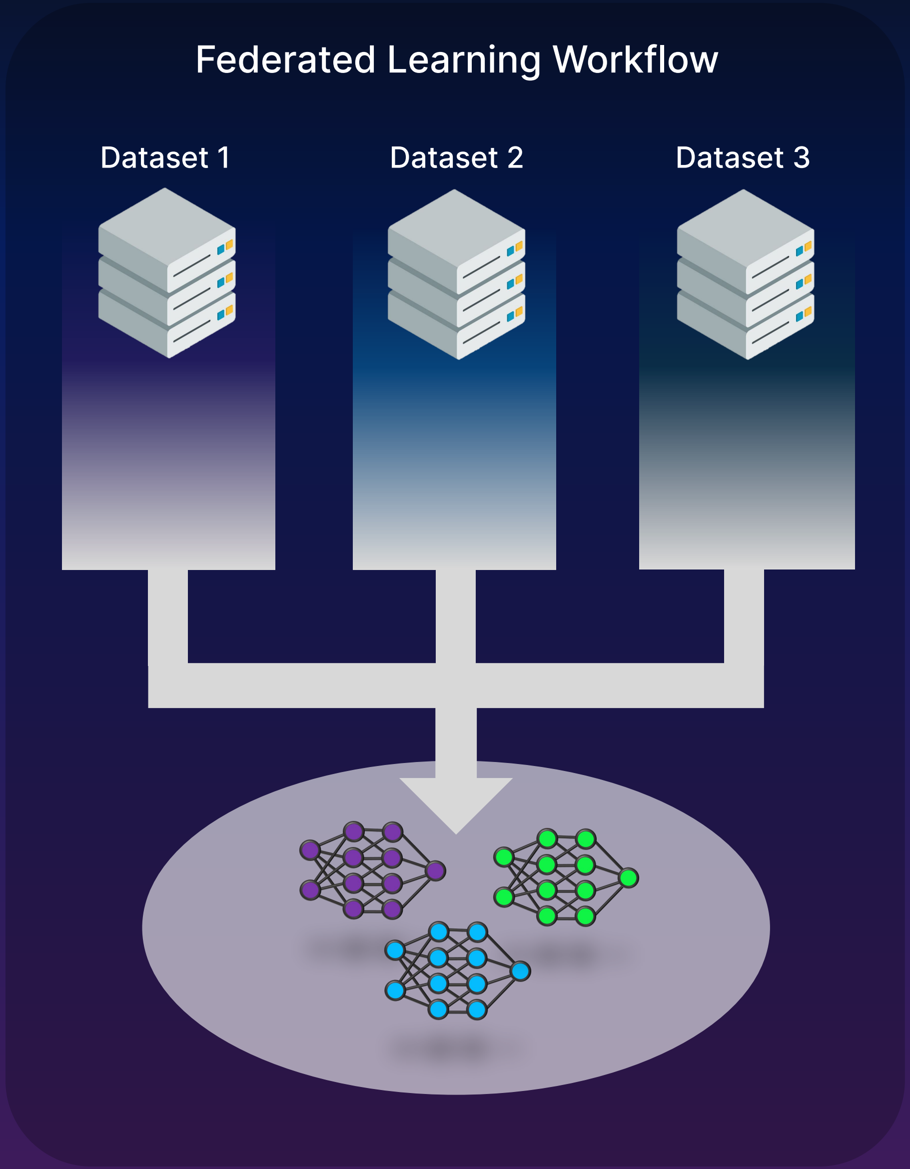
Never Collect Sensitive User Data

DynamoFL



1 Models independently trained on local datasets

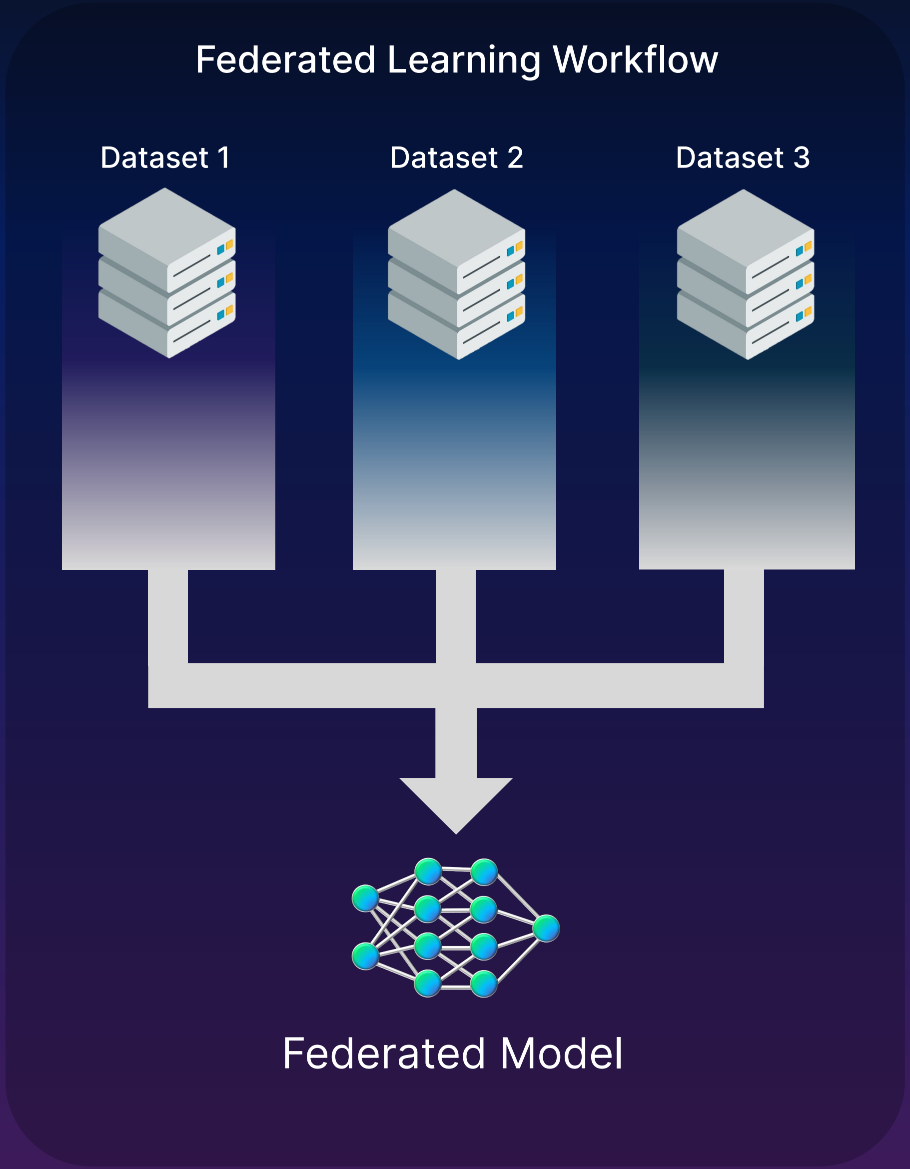
Never Collect Sensitive User Data



1. Models independently trained on local datasets

2. Models pushed to central federation server

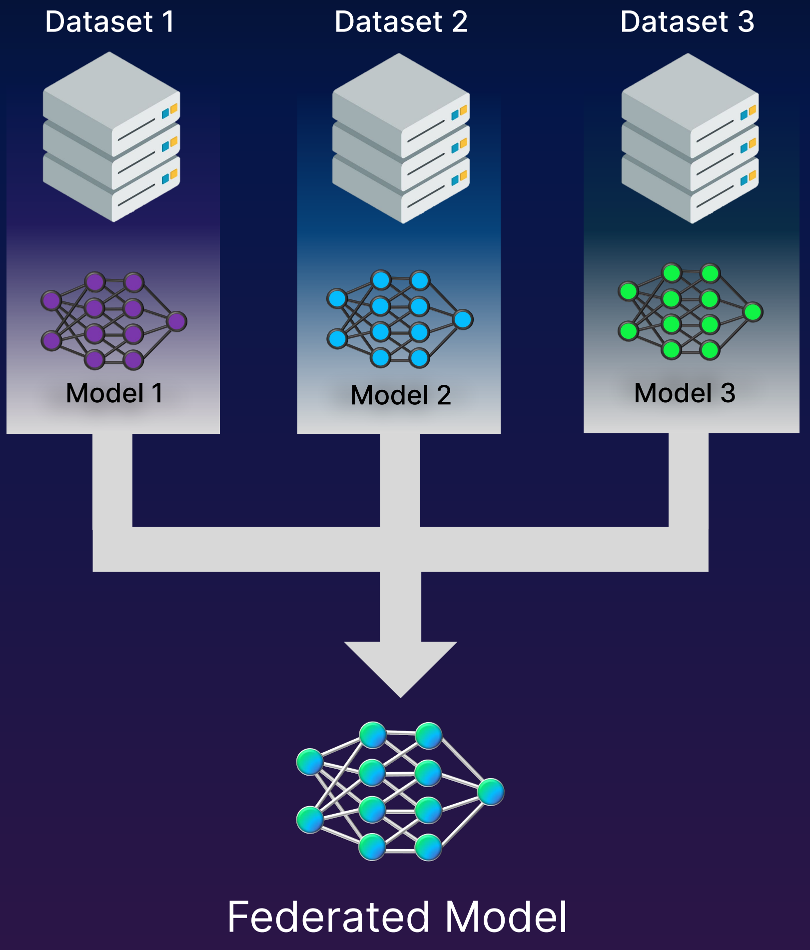
Never Collect Sensitive User Data



1. Models independently trained on local datasets
2. Models pushed to central federation server
3. Models combined on central federation server

Never Collect Sensitive User Data

Federated Learning Workflow

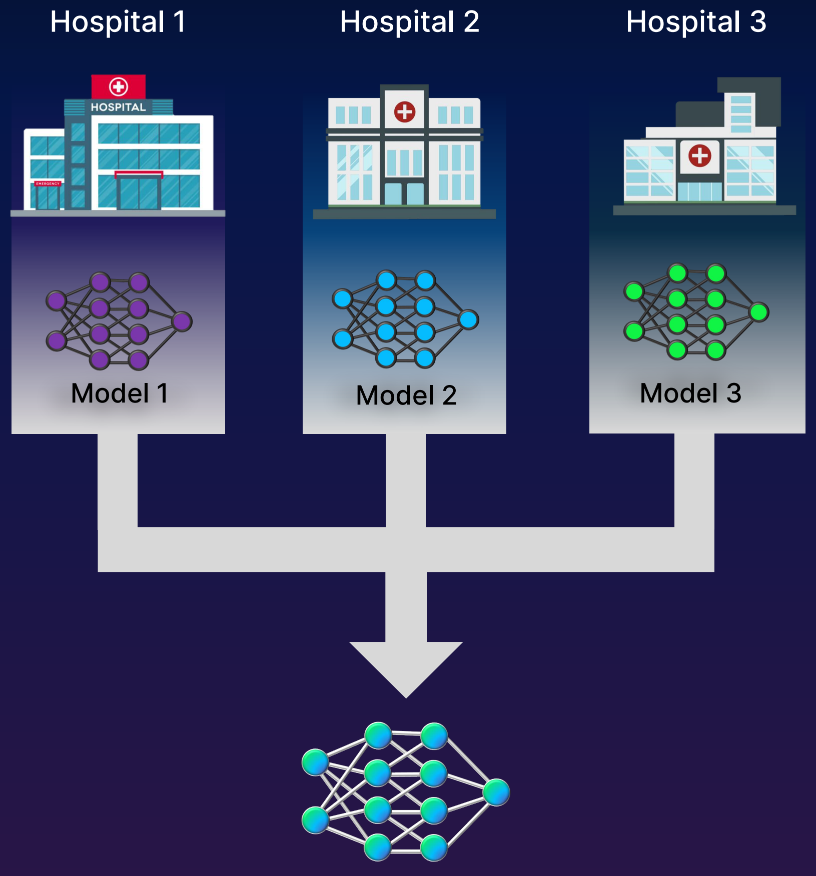


Private data never leaves its original source!

DynamoFL

Never Collect Sensitive **Medical** Data

Federated Learning Workflow

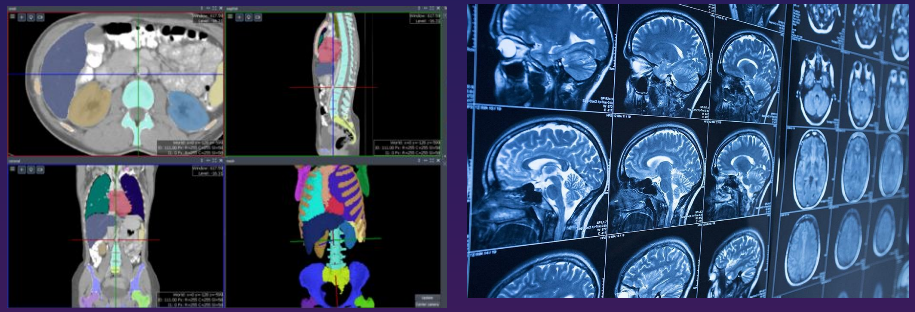


Federated Model

Clinical Trials / Life Sciences Data

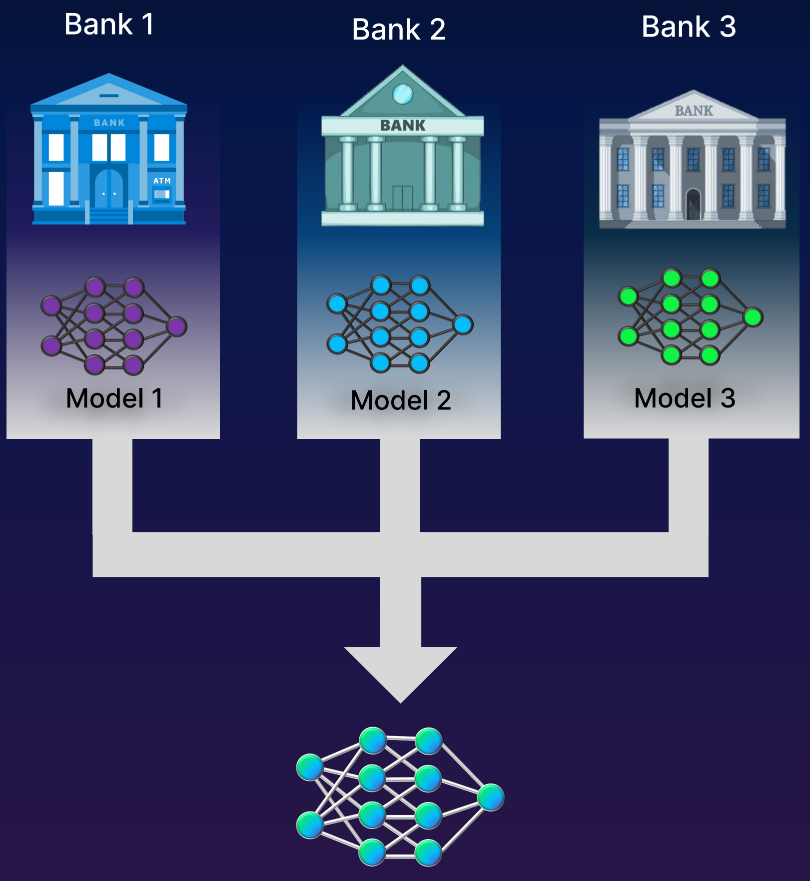
EHR/EMR/PHI

Medical Imaging Data



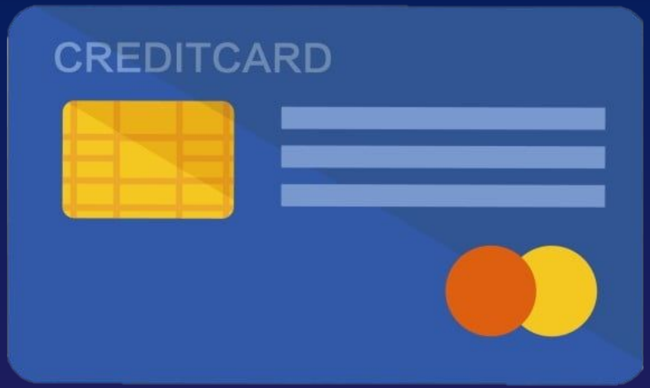
Never Collect Sensitive **Financial** Data

Federated Learning Workflow



Federated Model

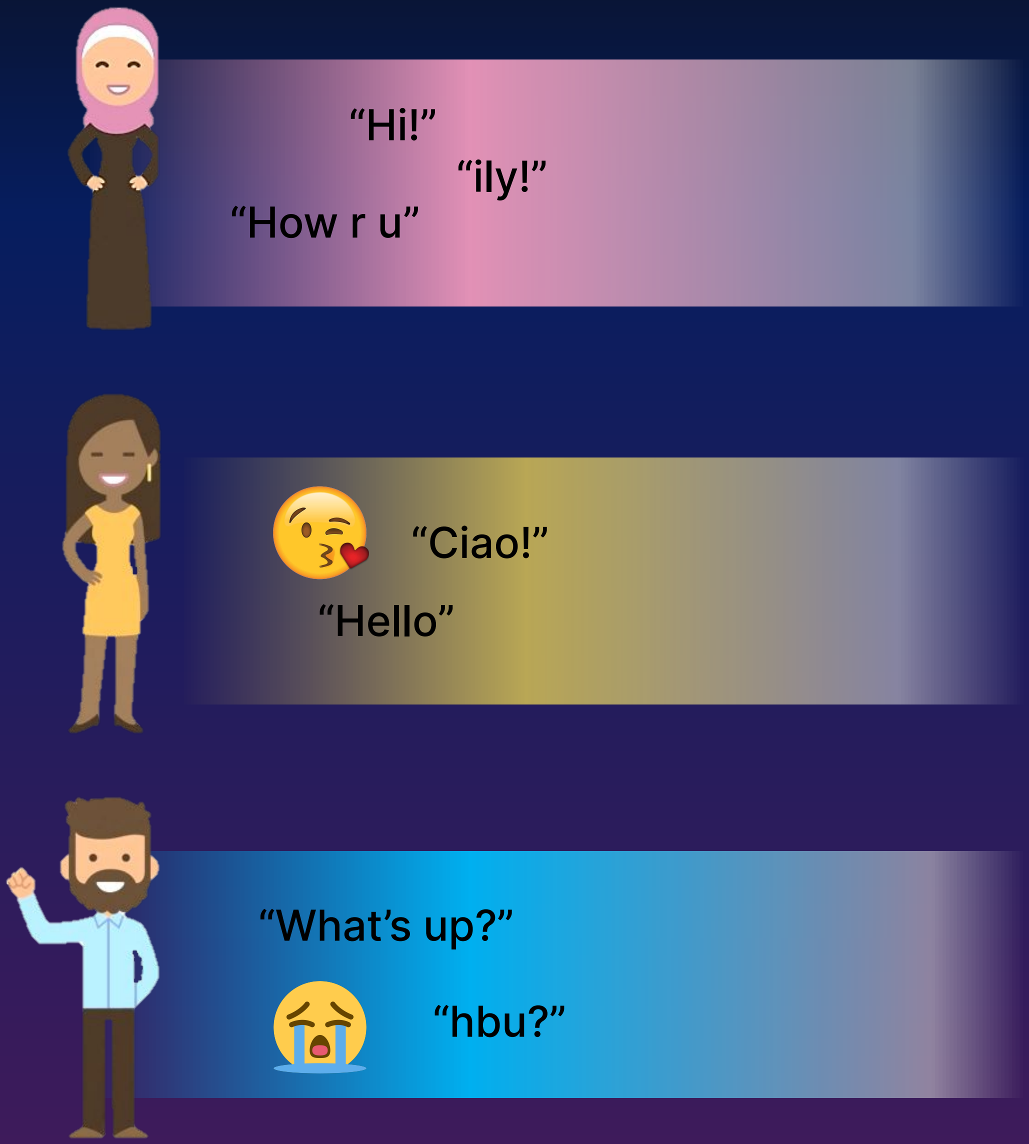
Fraud Detection Models



Risk Prediction

Financial Services & Product Recommendations

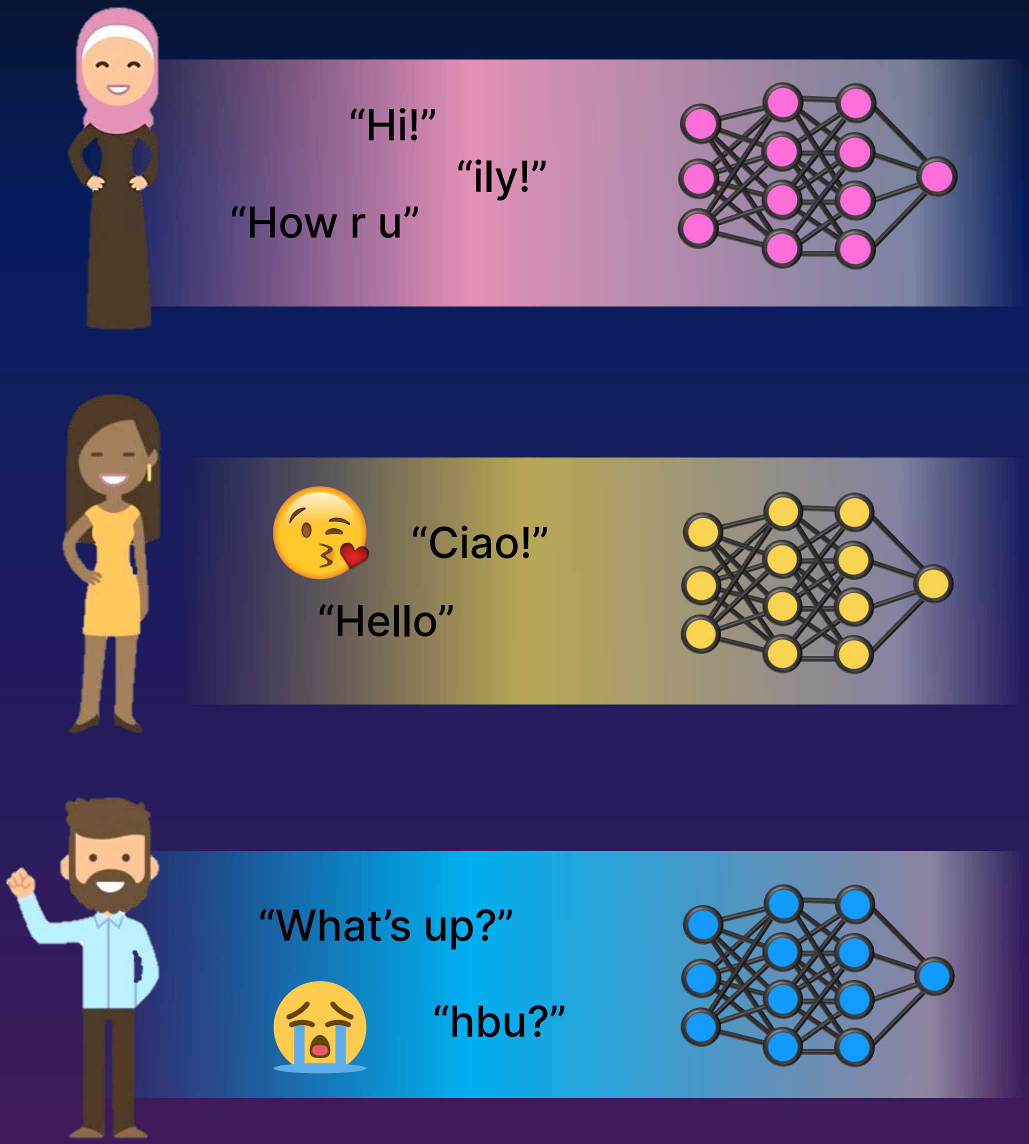
Our Solution: Personalized Federated Learning



Users have diverse texting patterns

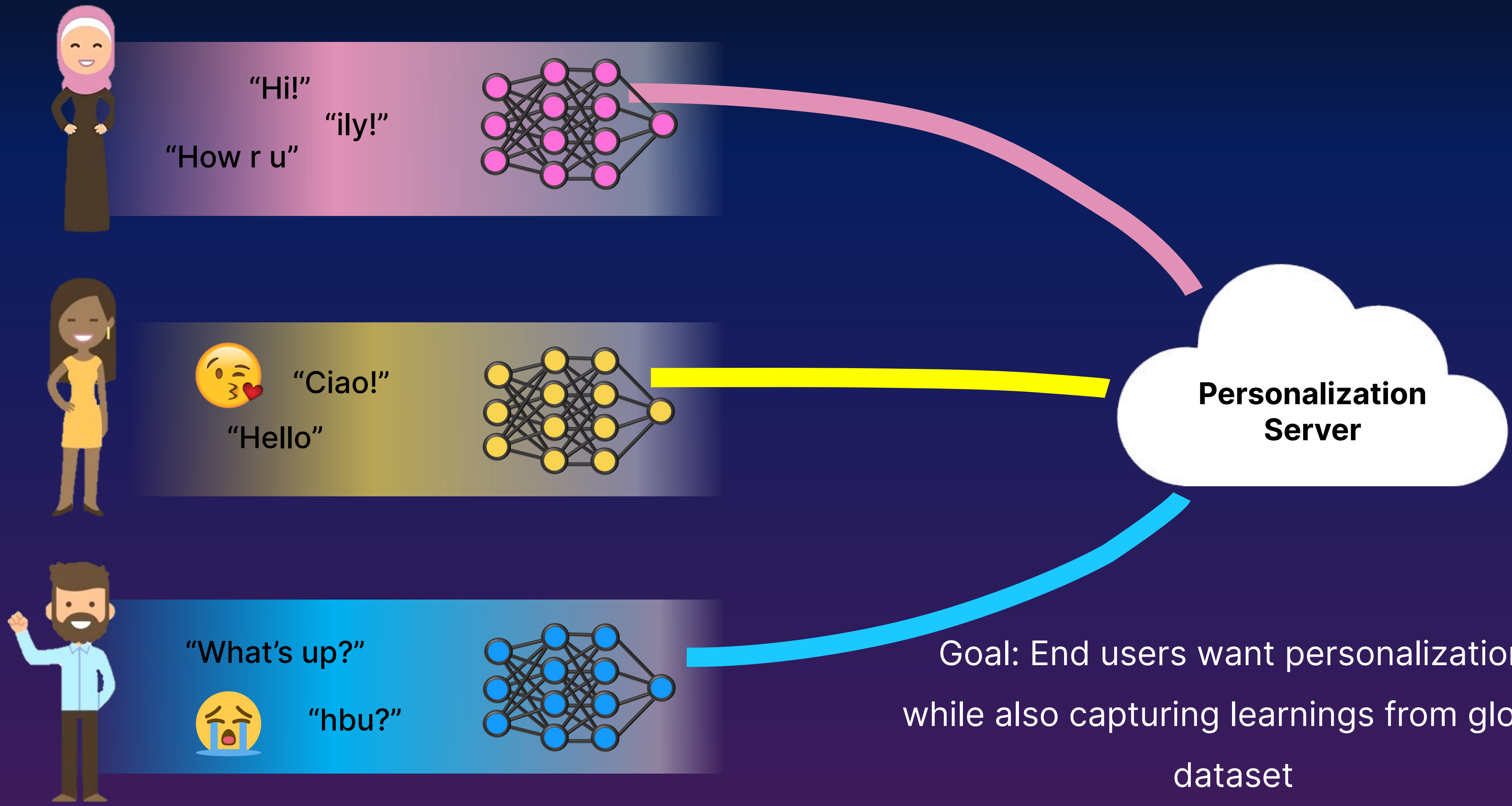
DynamoFL

Our Solution: Personalized Federated Learning



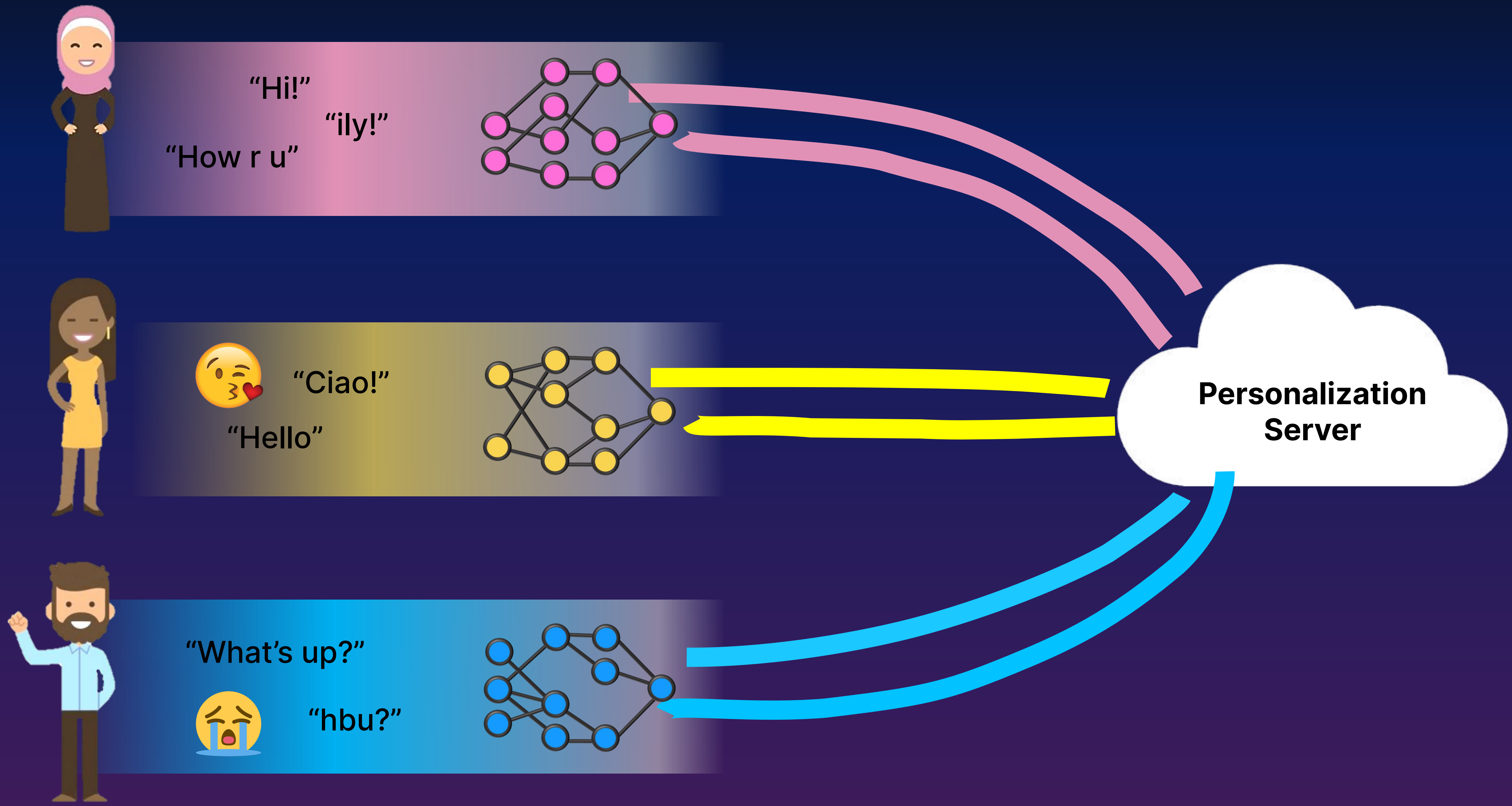
Train Next-Word-Prediction Models on User Text Data

Our Solution: Personalized Federated Learning

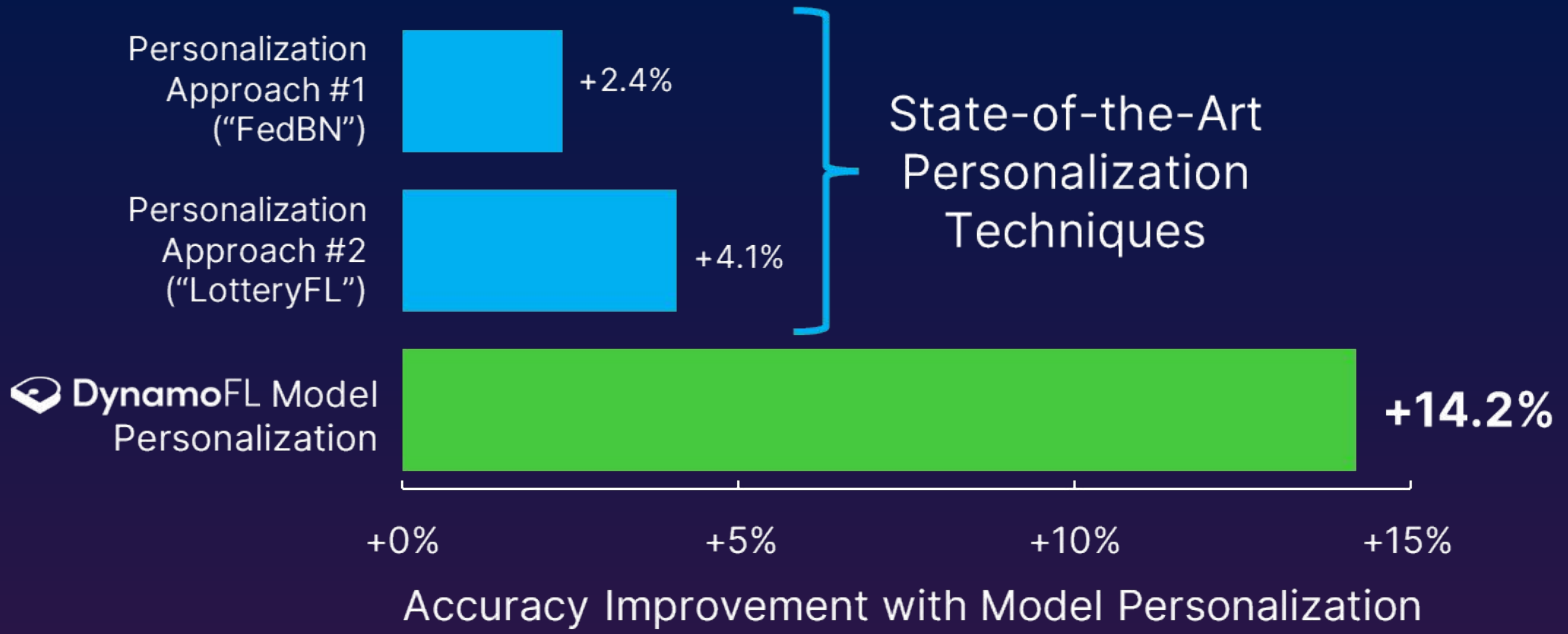


Goal: End users want personalization while also capturing learnings from global dataset

Our Solution: Personalized Federated Learning

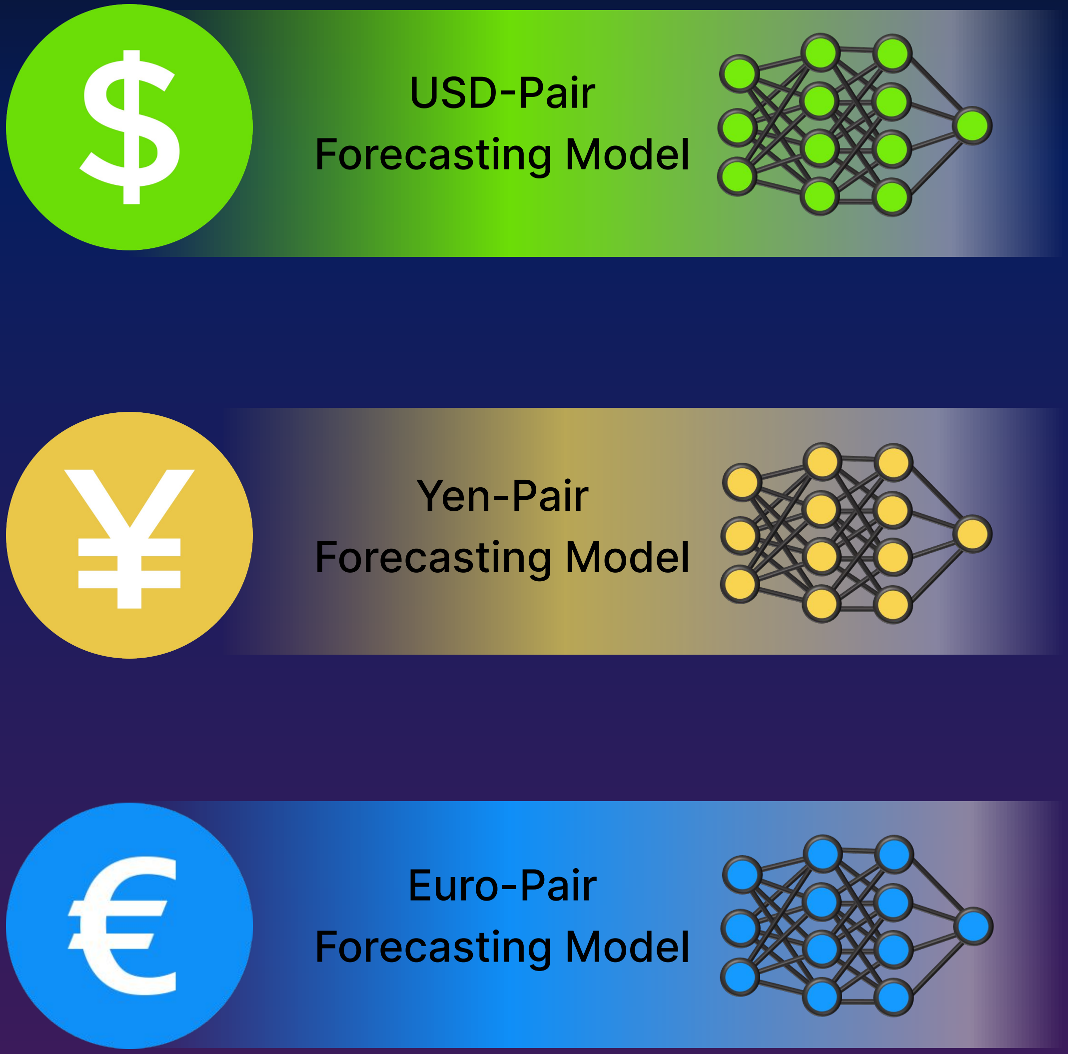


Boost Performance with Personalized Federated Learning



Results to be Presented at European Conference for Computer Vision (ECCV) 2022

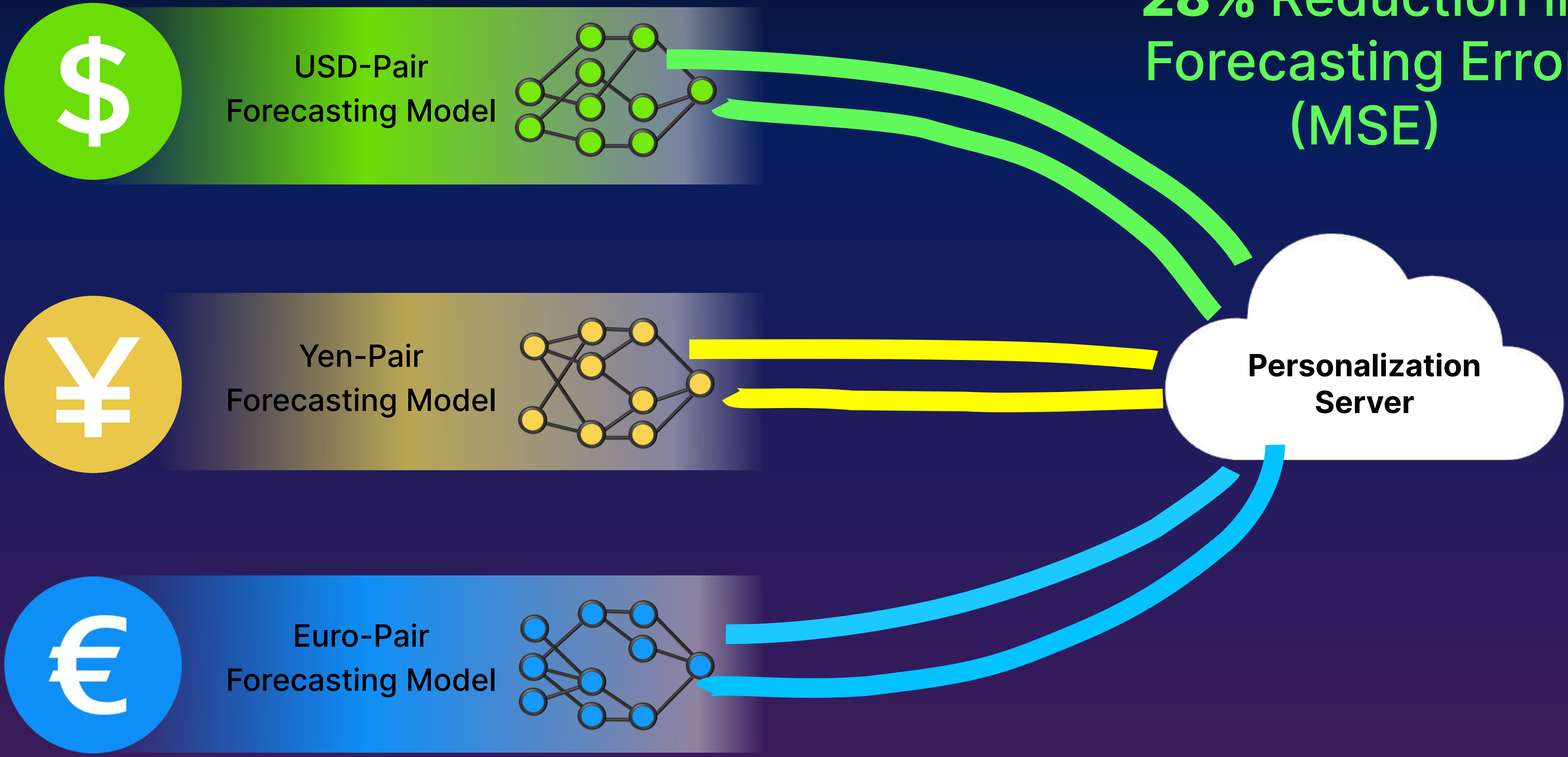
Performance Case Study: Quantitative Finance



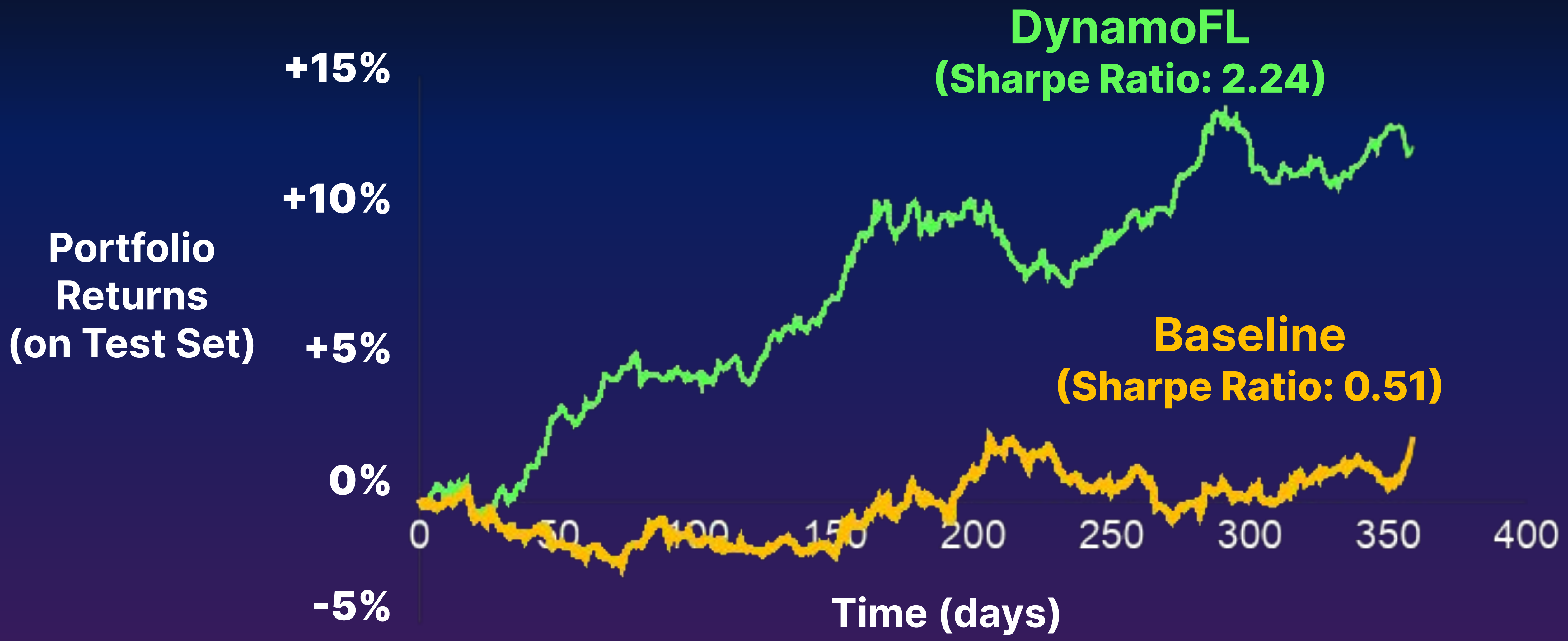
Train ForEx Models Locally on Currency Data

Performance Case Study: Quantitative Finance

28% Reduction in Forecasting Error (MSE)

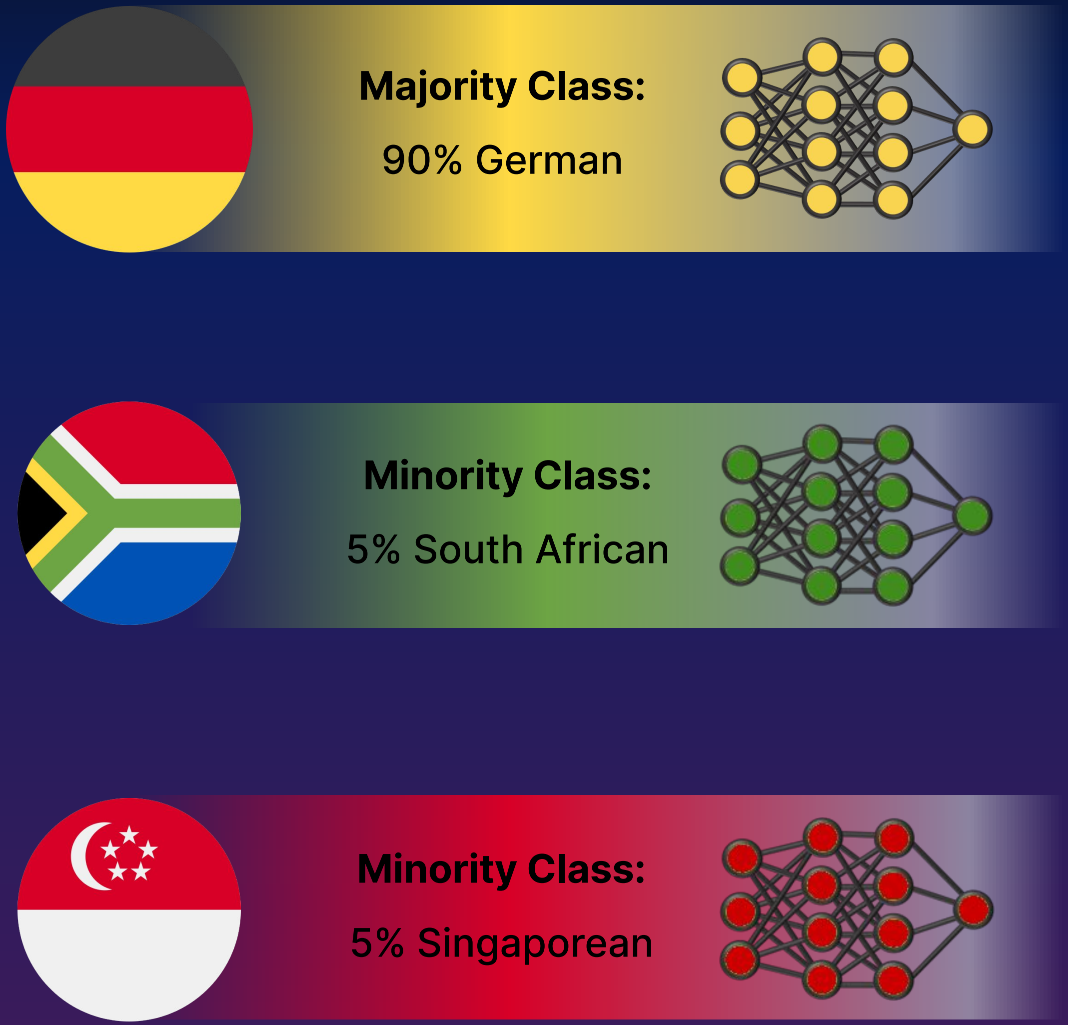


Performance Case Study: Quantitative Finance



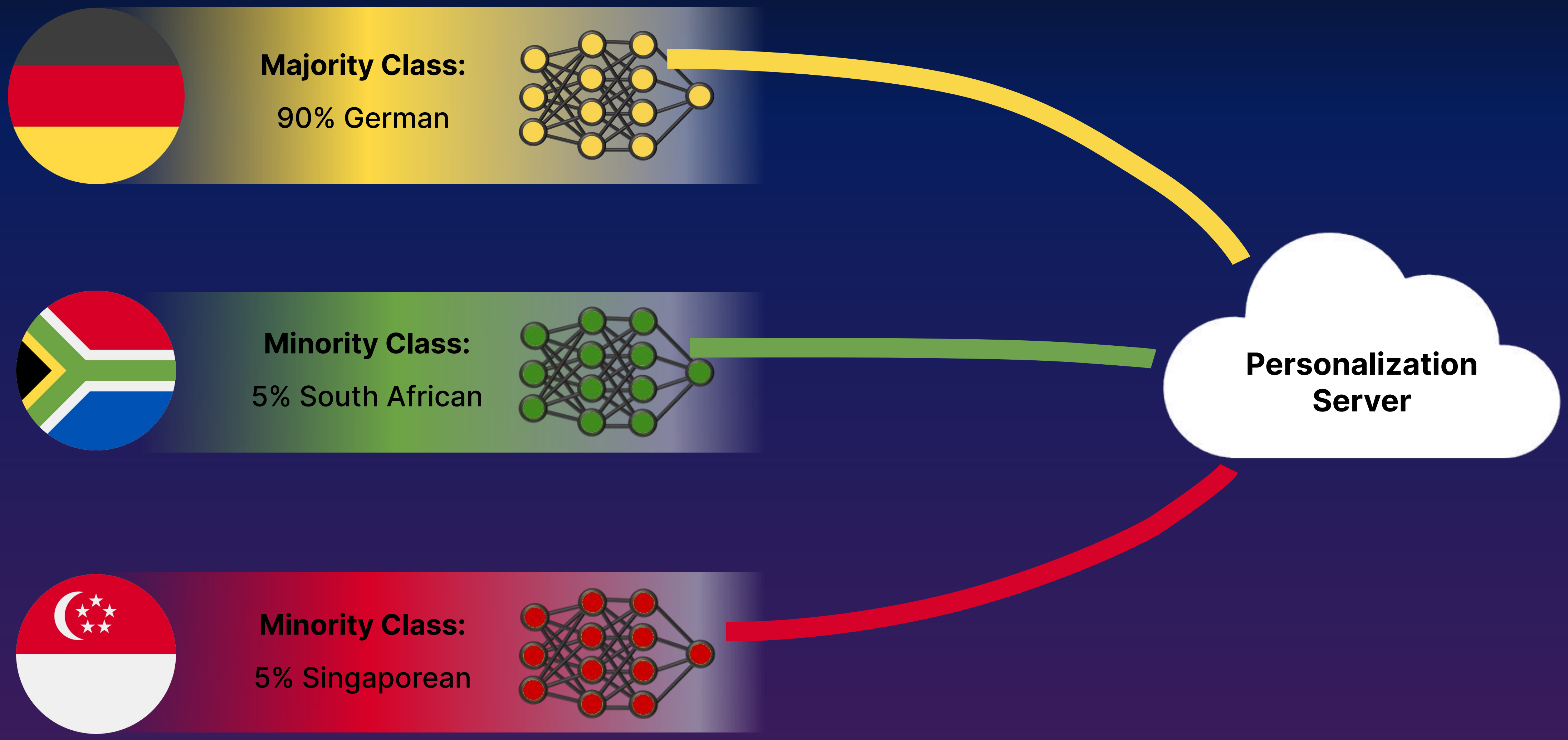
Portfolio created by trading 9 ETFs daily. Both DynamoFL and Baseline methods use the same autoformer model architecture for forecasting prices. Baseline uses models trained independently on ETFs. DynamoFL Method uses FL to personalize Baseline models.

Performance Case Study: Speech Recognition



Accented Speech Recognition with Minority Classes

Performance Case Study: Speech Recognition



Performance Case Study: Speech Recognition

	Central Model	DynamoFL
WER German	36.0%	34.7%
WER South African	52.9%	48.8%
WER Singaporean	65.0%	45.9%
WER Average	51.3%	43.2%

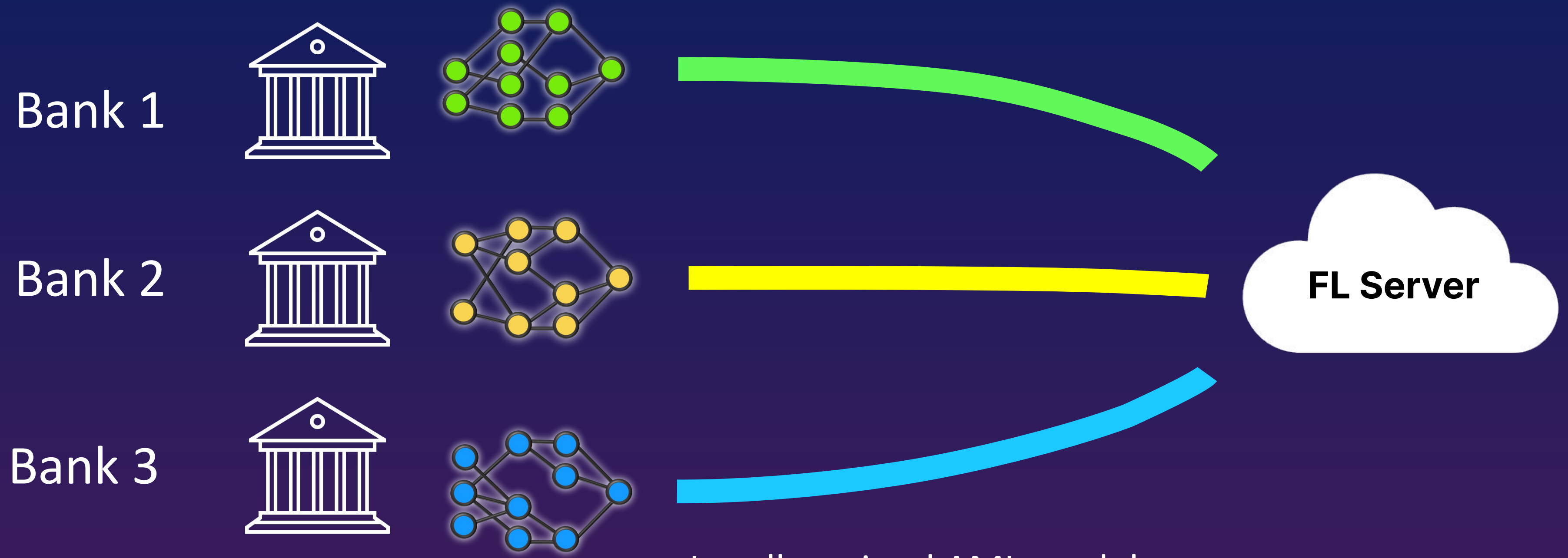
Strong performance improvement for minority classes enables fairer models

Training and evaluation performed on CommonVoice dataset. Both DynamoFL and central experiments were performed using the same pretrained Wav2Vec 2.0 model architecture

Compliance Case Study: Anti-Money Laundering (AML)

DynamoFL

Banks across different regions can collaborate to train AML model



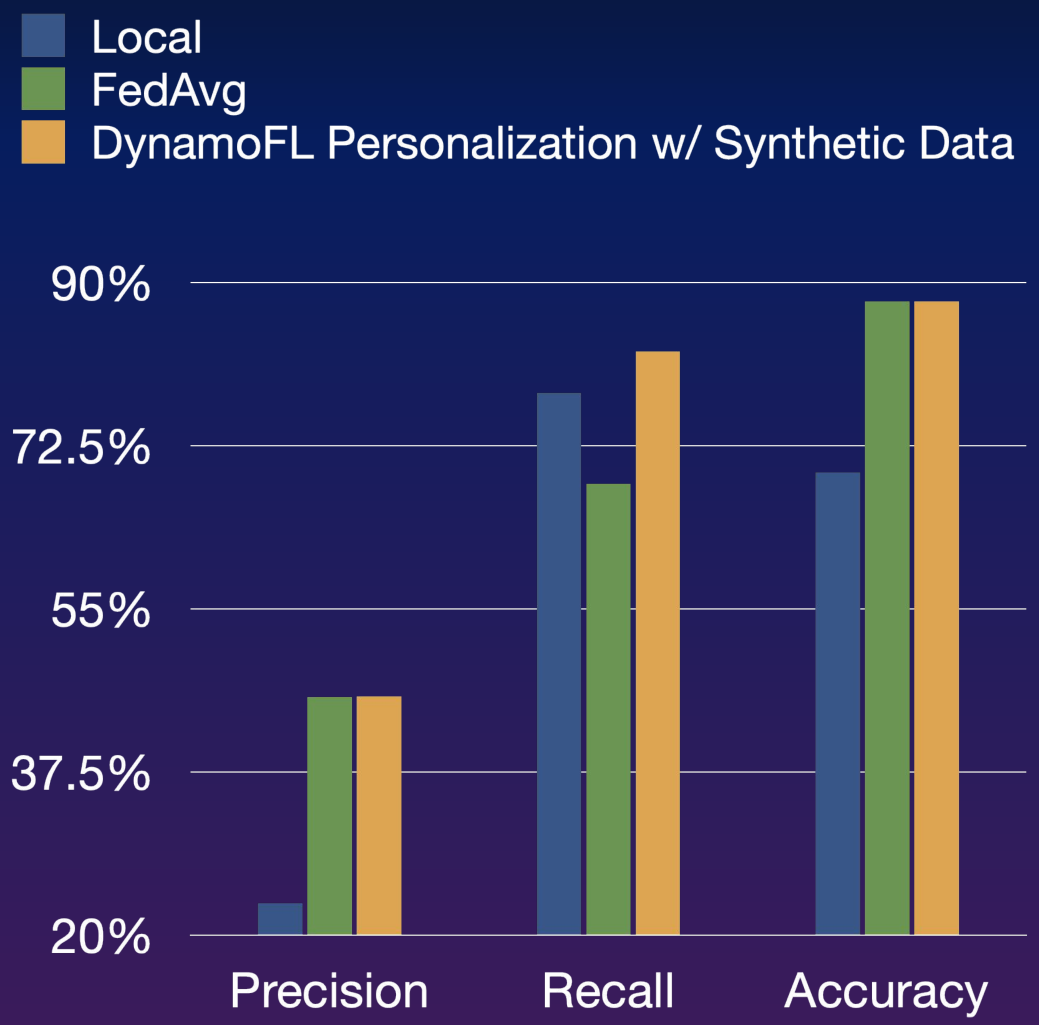
Locally trained AML models
(e.g., account anomaly detection)

Compliance Case Study: Anti-Money Laundering (AML)

DynamoFL

On a public AML dataset with accounts siloed across geographic regions (states):

- Local-only models achieves poor precision and accuracy
- FedAvg improves precision (for minority/anomaly class) at the expense of recall
- **DynamoFL model personalization boosts or matches baselines across all metrics**



Analytics Case Study: Privacy Risk Score

- Often, we'd like to get an intuition for **how private** are the trained models

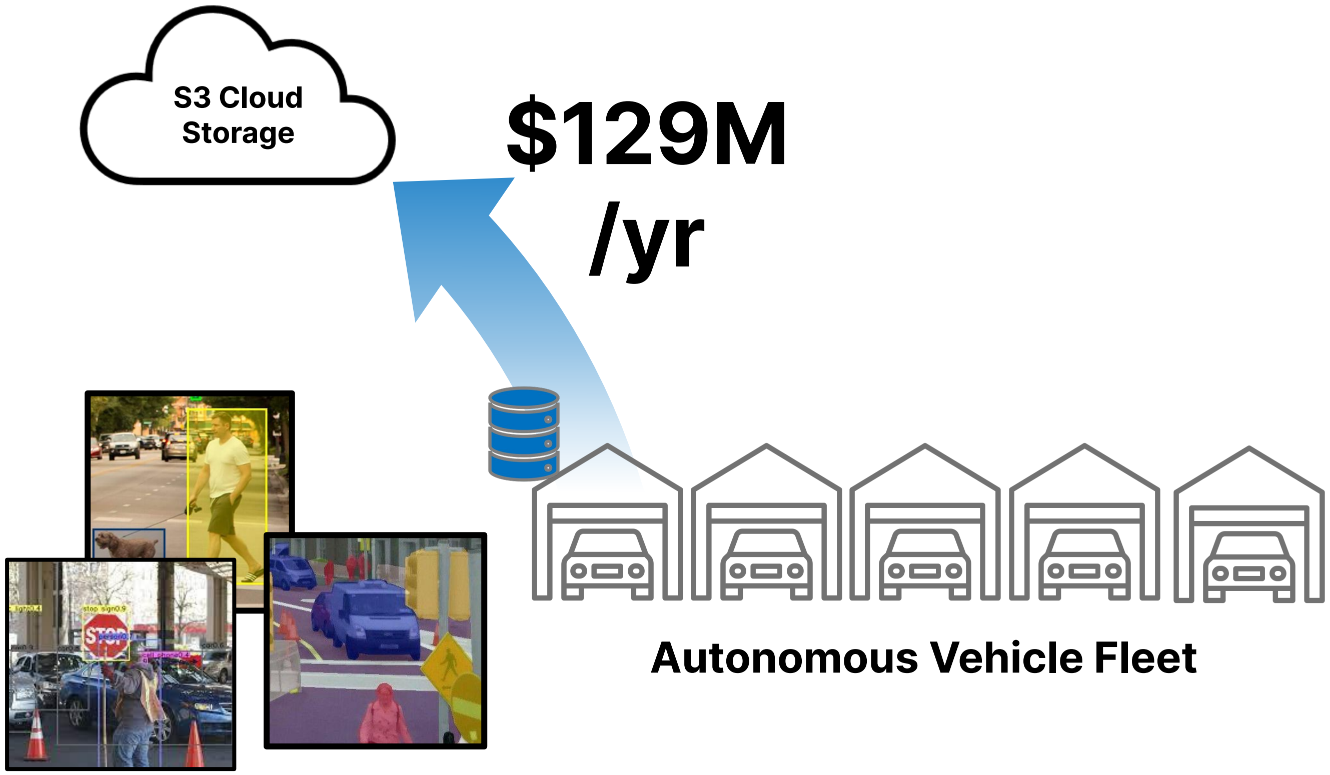
- DynamoFL systematically examines
  - potential attacks,
  - deployed defenses, and
  - a suite of empirical tests

  to arrive a normalized **privacy risk score** for non-technical users

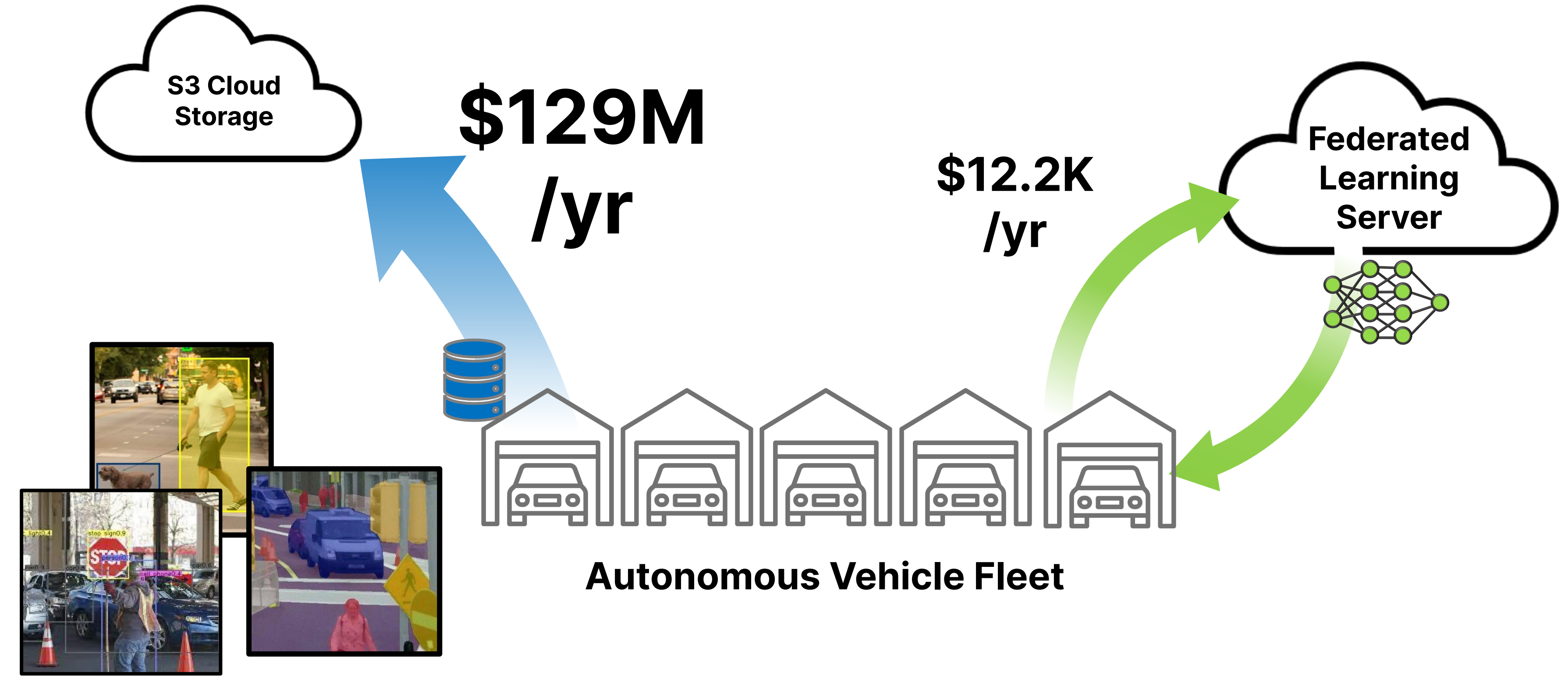
	De-identification (e.g., k-anonymity)	Robust Aggregation	SecAgg	Differential Privacy (DP)	…	Empirical Test Score
Membership Inference	Weak	Weak	Weak	Strong		…
Attribute Inference	Weak	Weak	Weak	Strong		…
Model Inversion	Weak	Weak	Weak	Strong		
Unreliable Channels	Moderate	Strong	Weak	Moderate/ Strong		…
Semi-Honest Server	Weak	Weak	Strong	Moderate/ Strong		…
Poisoning	Weak	Moderate	Weak	Moderate		…
Model Backdoors	Weak	Weak	Weak	Moderate		…
…						…

Example attacks and how they may be mitigated

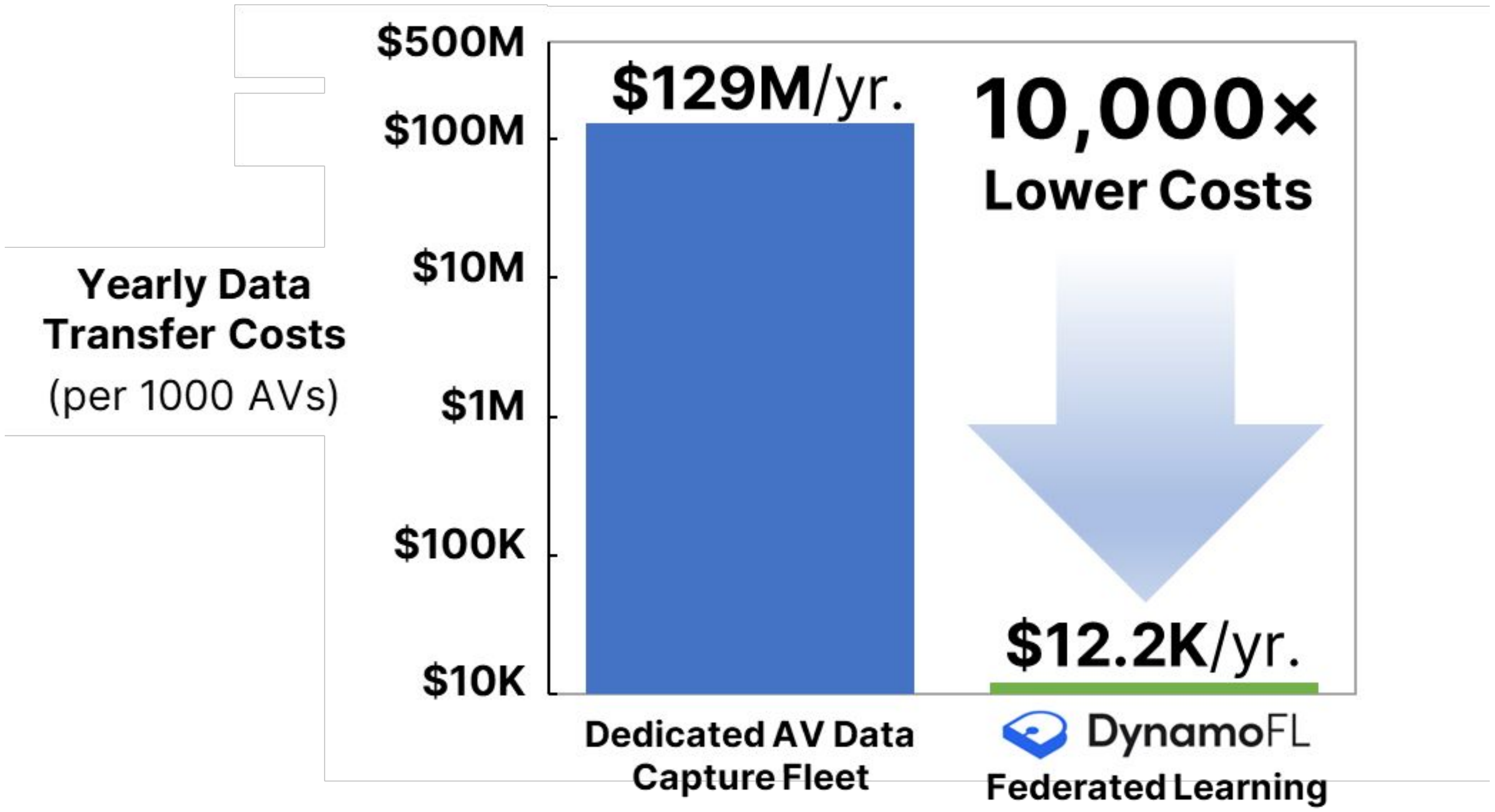
Cost Savings Case Study: Automotive



Cost Savings Case Study: Automotive

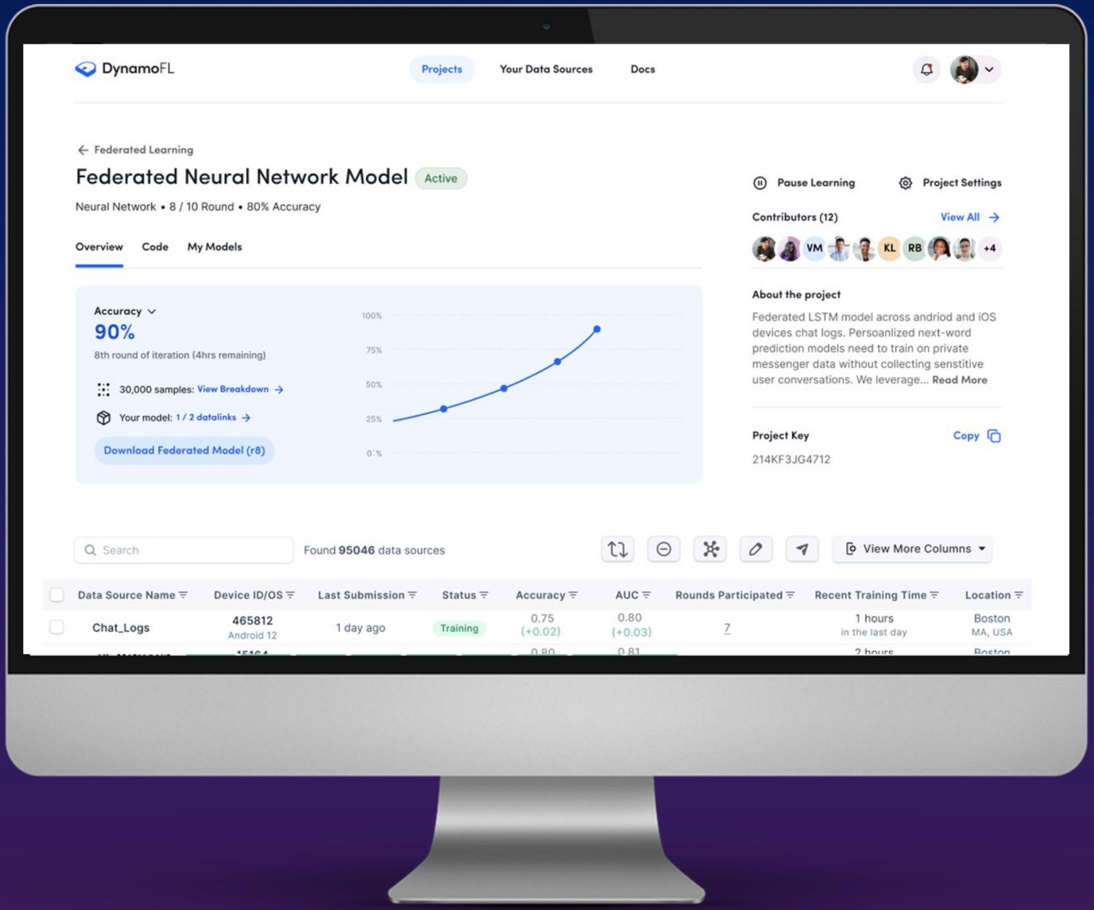


Cost Savings Case Study: Automotive



DynamoFL

The Platform for Personalized Federated Learning



- Integrated Personalized FL Technology
- End-to-end federated learning infrastructure
- Mobile and Python SDKs + Dockerized Solutions

safe secure https://

Contact

vaik@dynamofl.com

or visit https://www.dynamofl.com/

Vaikkunth Mugunthan, Ph.D.

CEO and Cofounder of DynamoFL