Decentralized Collaborative AI with Federated Learning in Trustworthy Environment [S62427]

Emily Sakata, NVIDIA

Chester Chen, NVIDIA

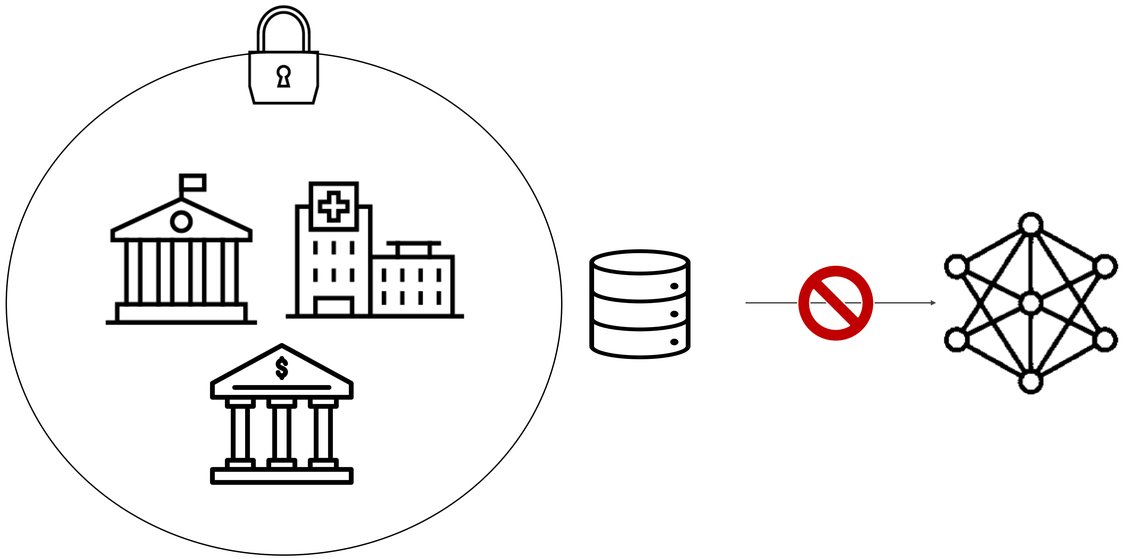
Isaac Yang, NVIDIA

March 18, 2024

Agenda

- Introduction to NVIDIA Federated Learning
- NVIDIA FLARE security and data privacy feature
- NVIDIA FLARE + NVIDIA Hopper CC
- Demo

Data Privacy and Security can be a Barrier to Delivering Value from AI



Sensitive | Private | Confidential

Evolving Landscape of Global Data Protection & Privacy Laws

- HIPAA - Health Insurance Portability and Accountability Act
- PCI DSS - Payment Card Industry Data Security Standard
- GLBA – Gramm-Leach-Bliley Act
- GDPR - General Data Protection Regulation
- CCPA - California Consumer Privacy Act
- *And More….*

82%
Data Breaches were Cloud-Based[1]

$4.45M
Global Average Total Cost of a Data Breach[1]

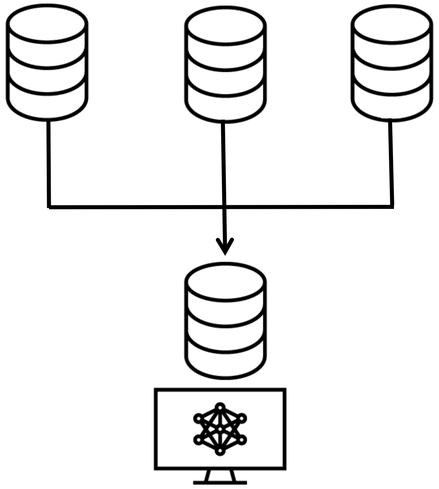
$10.93M
Average Cost of Breach in Healthcare[1]

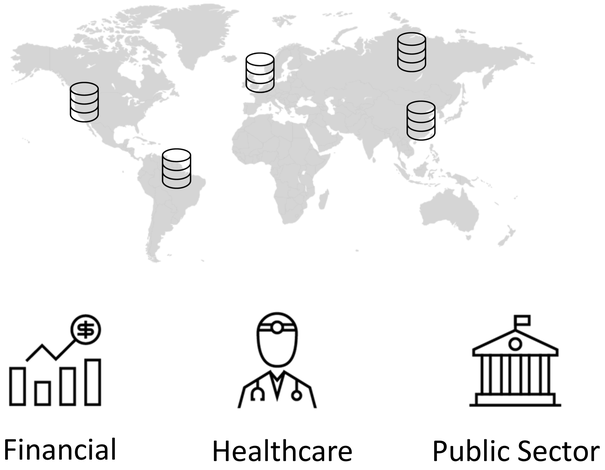
$5.90M
Average Cost of Breach in Finance[1]

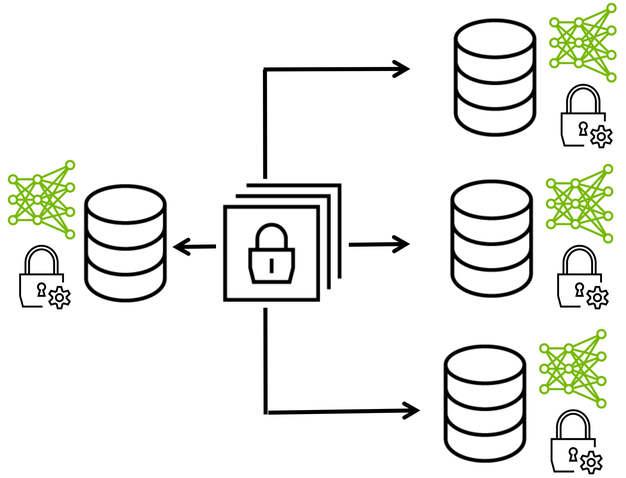
[1]*Cost of a Data Breach 2023 Report, IBM : https://www.ibm.com/reports/data-breach*

Federated Computing – Removing Data Silos

Avoid Data Copy | Regulatory Compliance | Prevent Private Data Leak







No Data Copy

Centrally aggregating the data is not possible or practical

Compliance

Data sovereignty restrictions and industry regulations

Privacy Enhancing Technology

Multiple layers of security features incl. Homomorphic Encryption & Differential Privacy

NVIDIA Federated Learning (FL)

Applications Across Industries

Conversation

Healthcare

Financial

Autonomous Driving

Instrument

Monitoring

AI Model

NVIDIA FLARE

Privacy Preserving Algorithms

Federated Workflows

Runtime Environment

Global Model

FL

FL

FL

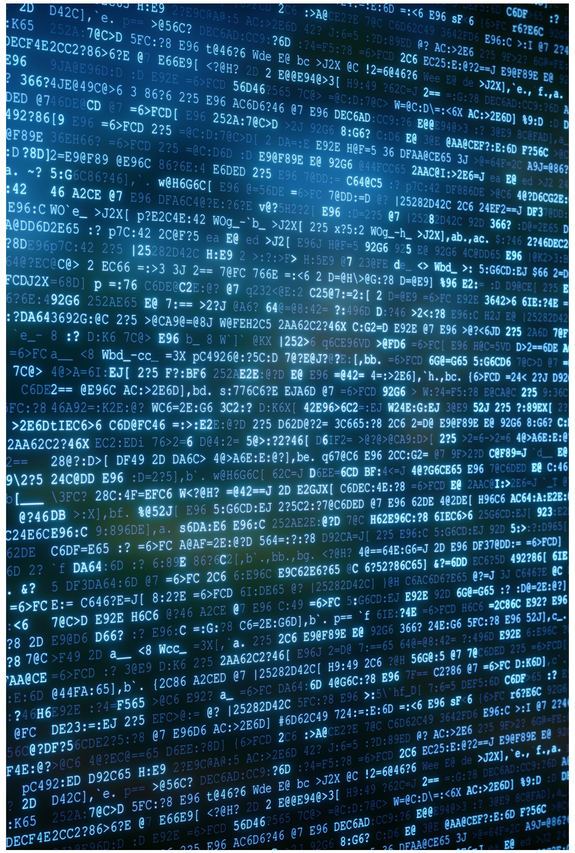
Global Sites

NVIDIA FLARE Security and Data Privacy

Defense in Depth approach to protecting data privacy and model IP

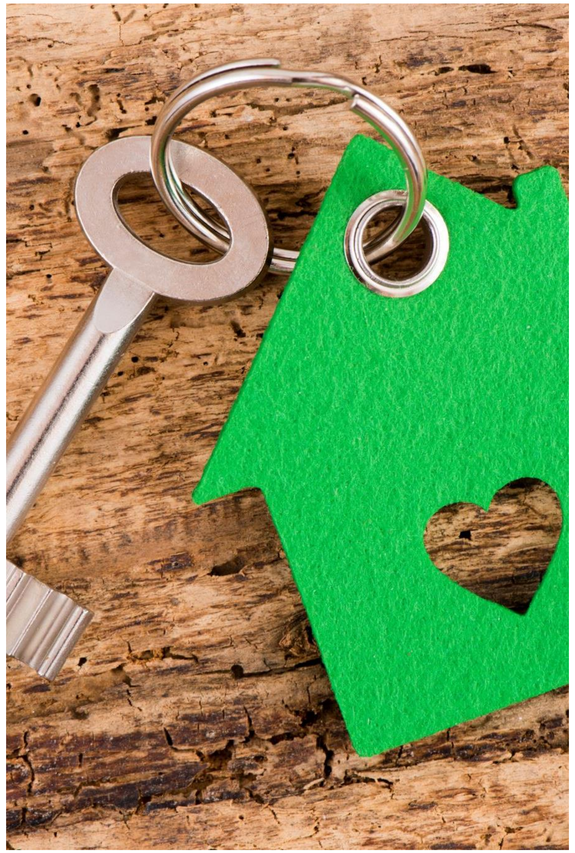
User Identity Verification

Certificate and derived token authentication



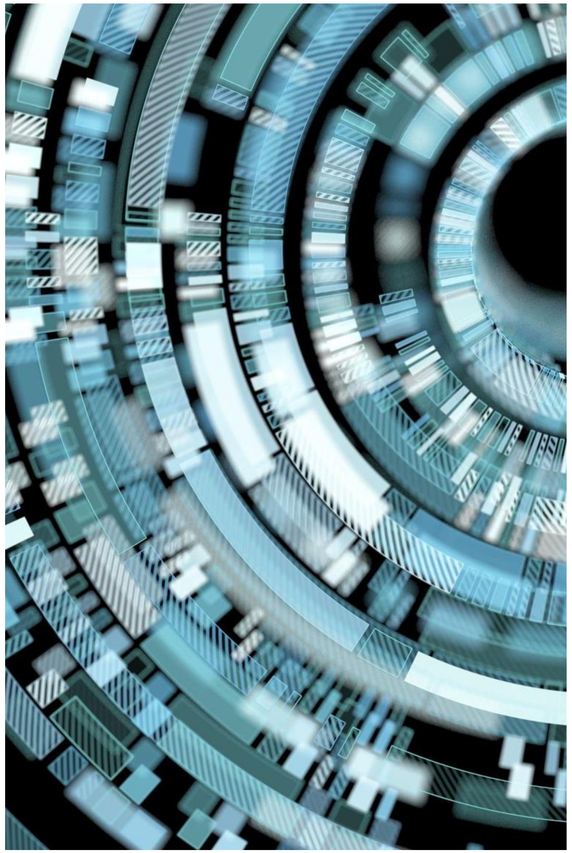
Data Encryption in Transit

Server-Client communication encrypted



User Defined Security Policy

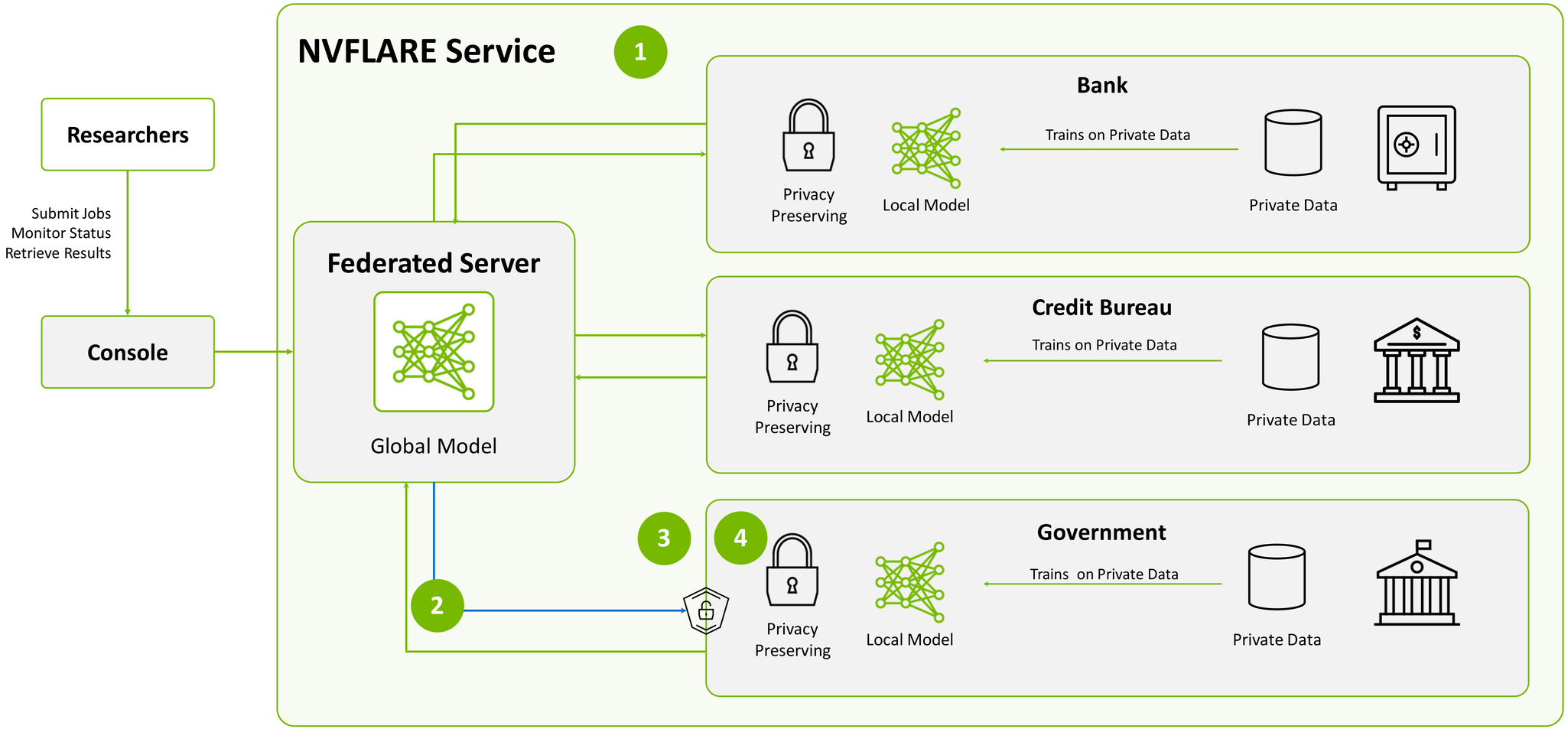
Site-Specific authentication & job authorization



Privacy Preserving Algorithm

Differential Privacy & Homomorphic Encryption

NVIDIA FLARE Deployment Architecture

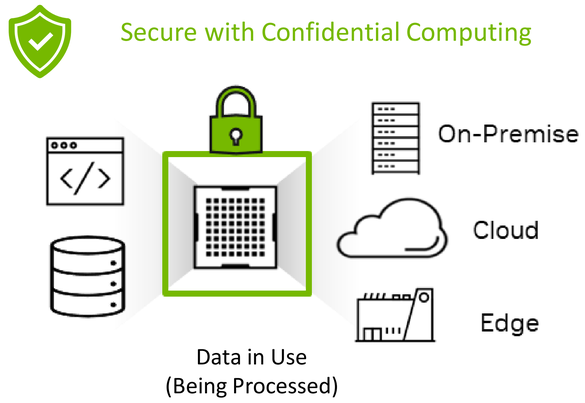


1. User Identity Verification
2. Data Encryption in Transit
3. User Defined Security Policy
4. Privacy Preserving Algorithm

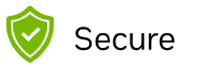
Protecting Data in Use With H100 Tensor Core GPUs

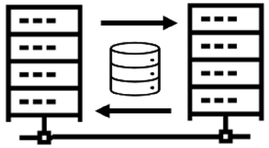
Confidential Computing

Address the Security Gap in Data Protection



Data at Rest
(In Storage)

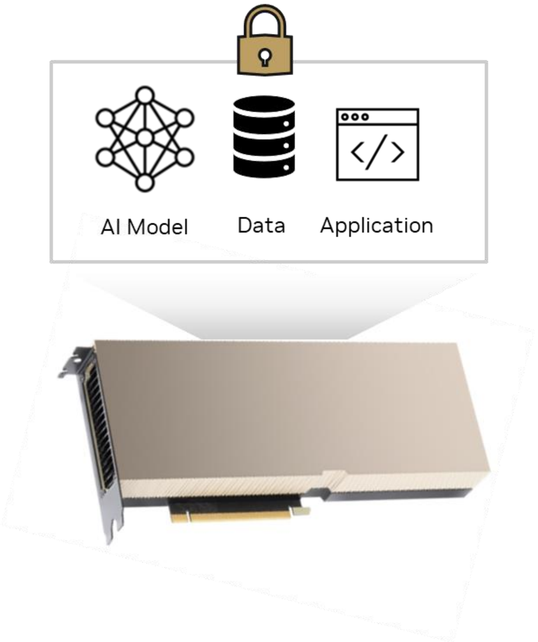




Data in Transit
(Across a Network)

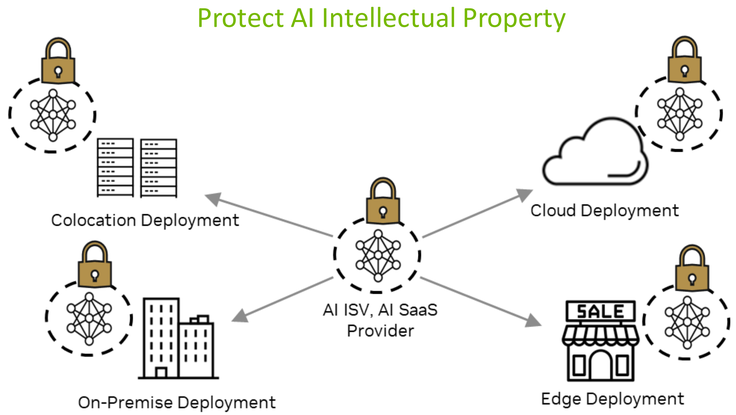
NVIDIA H100 Tensor Core GPUs

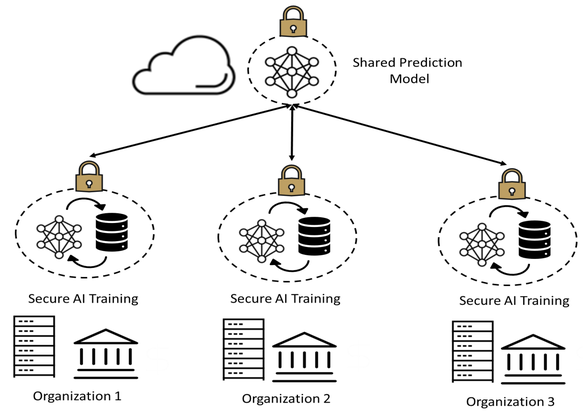
World's 1st GPU for Confidential Computing



Secure Data and AI Workloads In Use

Unlock New Business Models with Secure AI





Building Trust Across Federated Learning Model

Implicit Trust to Explicit Trust

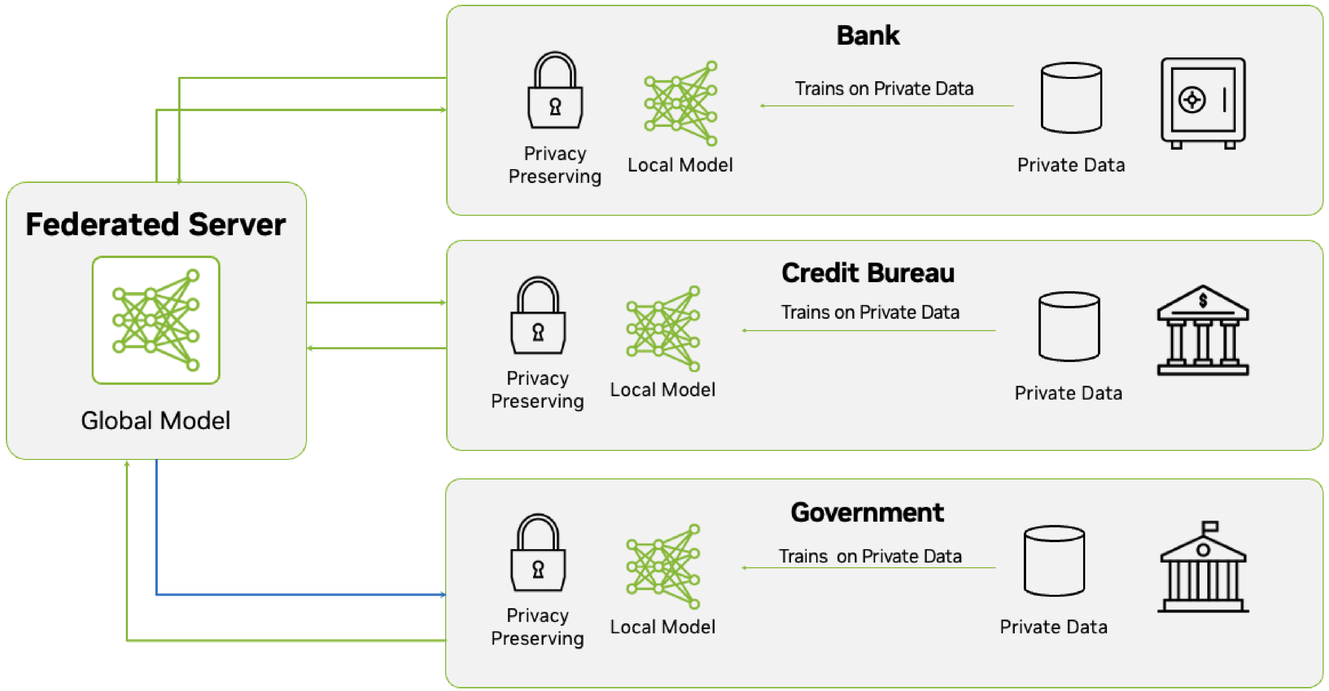
Participants collaborate to train a global model
Implicit trust often established through business relationship

Threat Model

- One of the participating machine is attacked (Physical Hardware attack or hypervisor attack)
- Infrastructure admin or machine owners ssh into the system and modify or leak data / model

Zero Trust Security

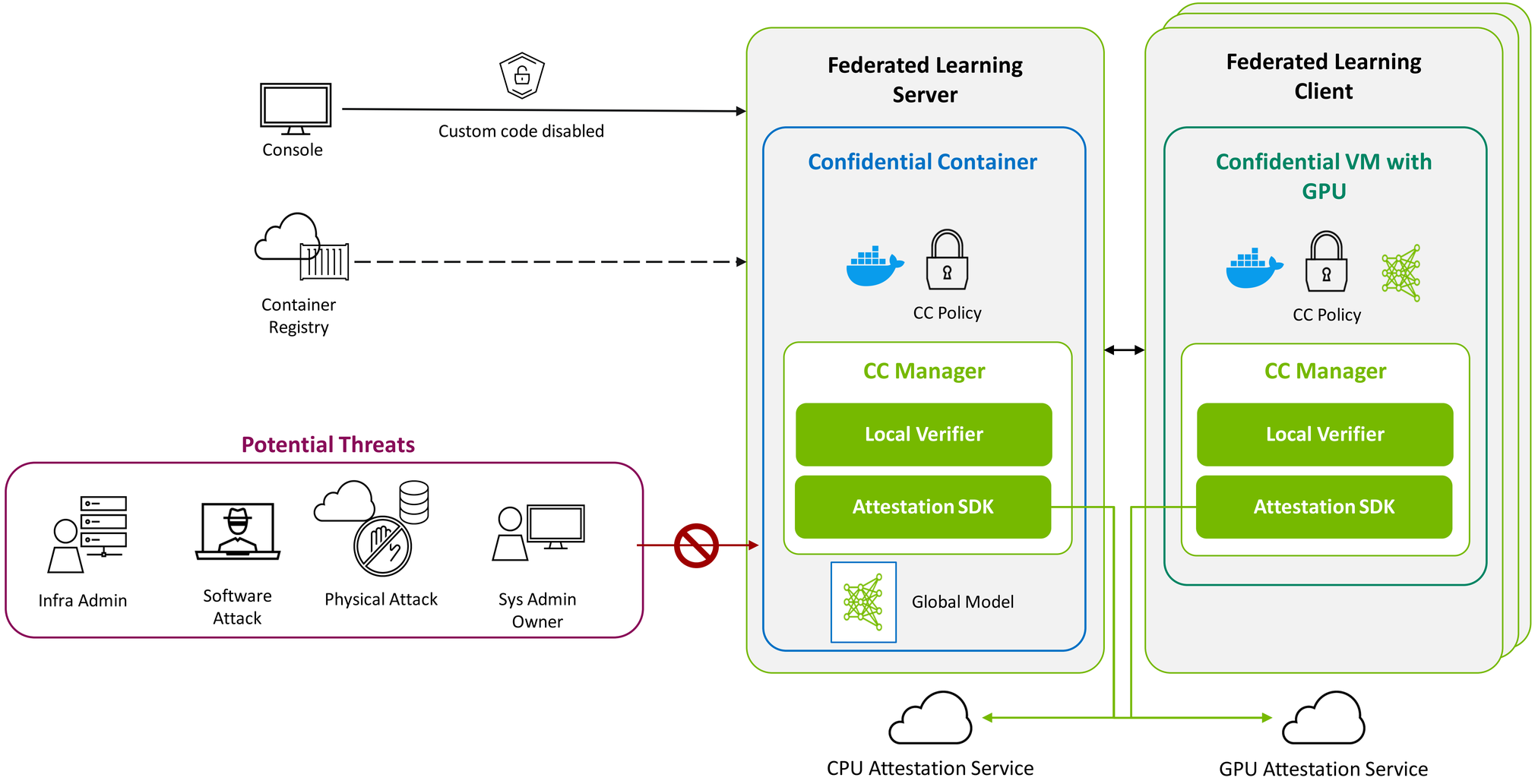
- FL Server does not trust FL Clients
- FL Clients do not trust FL Server
- FL Clients do not trust each other



Before a job starts and while a job is running, establish explicit trust among all participants

Building Trust in FL with Confidential Computing (CC)

Hardware-Based Security to Protect Data In Use



Demo

DEMO: NVIDIA FLARE with Confidential Computing (CC)

NVIDIA FLARE + Azure Confidential Computing

Infrastructure setup:

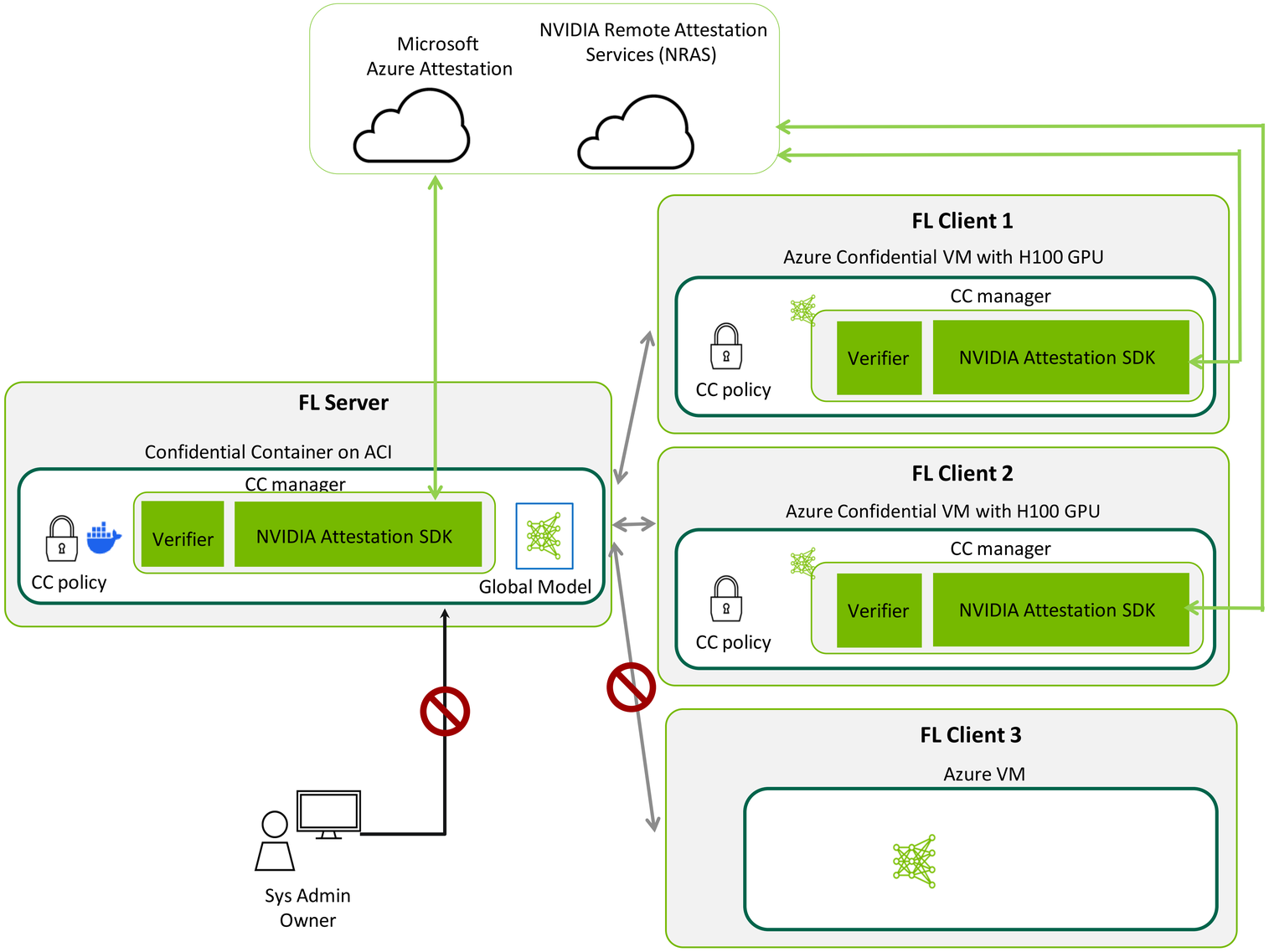
- **FL Clients: Azure Confidential GPU**
  - AMD CPU + NVIDIA H100 GPU
- **FL Server: Confidential Container on ACI**
  - AMD CPU

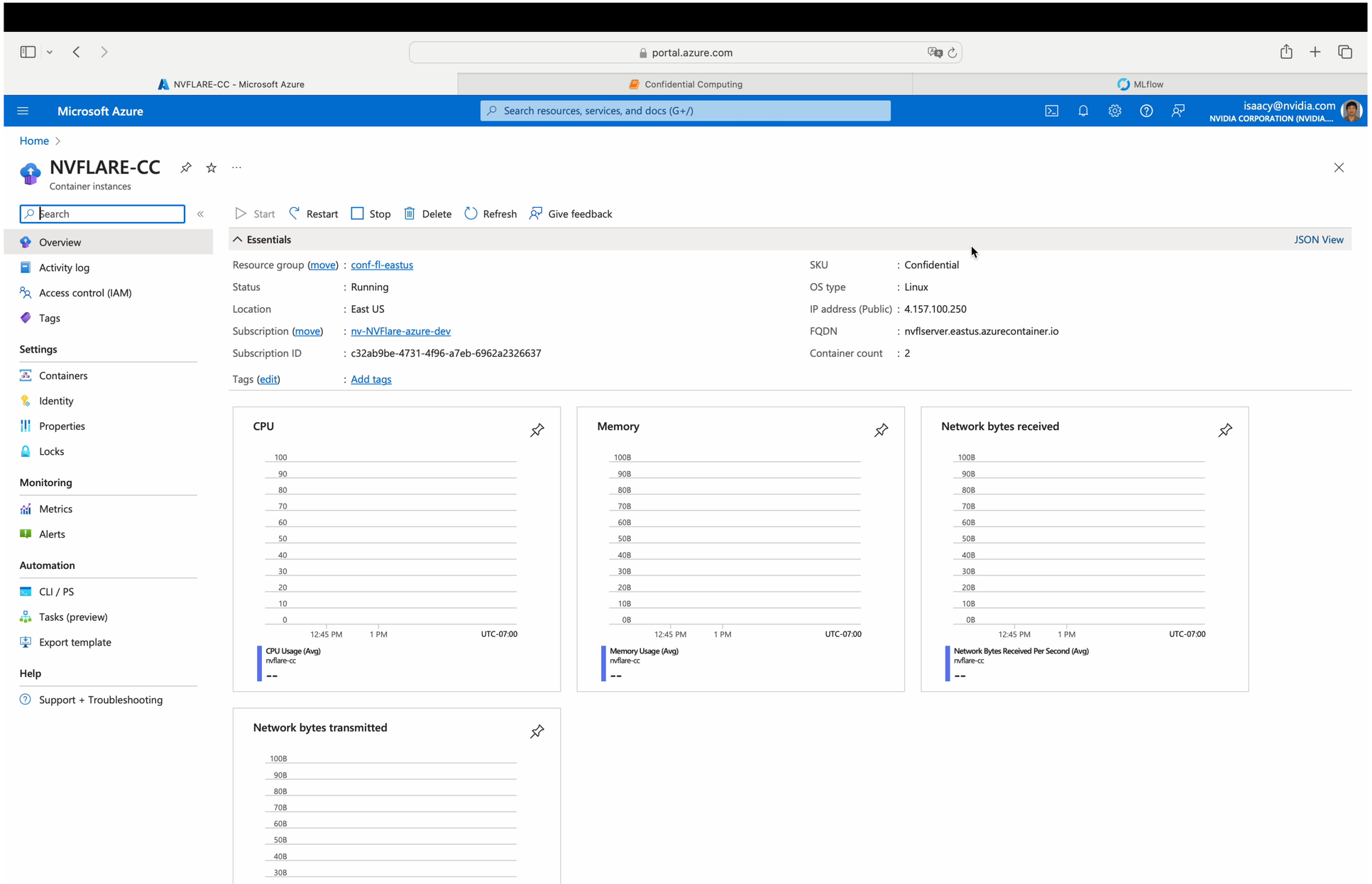
Demo job setup:

- **Credit card fraud detection with XGBoost**
- **Dataset:** Credit Card Fraud Detection
- **Approach:** horizontal federated learning using histogram-based collaboration (see NVFLARE examples)

What we expect to see:

- No one can SSH into FL server
- Use CC policy to verify attestation results of FL Server and FL Clients
- Credit card fraud detection job can be completed with expected results
- FL Clients or FL Server CC token verification failure will cause the job to fail or system shutdown




portal.azure.com
NVFLARE-CC - Microsoft Azure
Confidential Computing
MLflow
Microsoft Azure
Search resources, services, and docs (G+/)
isaacy@nvidia.com
NVIDIA CORPORATION (NVIDIA....
Home
NVFLARE-CC
Container instances
Search
Start
Restart
Stop
Delete
Refresh
Give feedback
Overview
Activity log
Access control (IAM)
Tags
Settings
Containers
Identity
Properties
Locks
Monitoring
Metrics
Alerts
Automation
CLI / PS
Tasks (preview)
Export template
Help
Support + Troubleshooting
Essentials
JSON View
Resource group (move) : conf-fl-eastus
Status : Running
Location : East US
Subscription (move) : nv-NVFlare-azure-dev
Subscription ID : c32ab9be-4731-4f96-a7eb-6962a2326637
Tags (edit) : Add tags
SKU : Confidential
OS type : Linux
IP address (Public) : 4.157.100.250
FQDN : nvflserver.eastus.azurecontainer.io
Container count : 2
CPU
100
90
80
70
60
50
40
30
20
10
0
12:45 PM
1 PM
UTC-07:00
CPU Usage (Avg)
nvflare-cc
--
Memory
100B
90B
80B
70B
60B
50B
40B
30B
20B
10B
0B
12:45 PM
1 PM
UTC-07:00
Memory Usage (Avg)
nvflare-cc
--
Network bytes received
100B
90B
80B
70B
60B
50B
40B
30B
20B
10B
0B
12:45 PM
1 PM
UTC-07:00
Network Bytes Received Per Second (Avg)
nvflare-cc
--
Network bytes transmitted
100B
90B
80B
70B
60B
50B
40B
30B

If You Enjoyed This Talk…

Attend Other CC Talks at NVIDIA GTC 2024

- **CWE62185- Connect With the Experts: Real-World Federated Learning Production with NVFLARE: Easily Transition from DL to FL, Keep Data Local, Preserve Data Privacy, and Build Better Models**
  - Tuesday, Mar 19 | 2:00PM - 2:50PM PDT
  - Location: CWE Pod D (LL)

- **S62427: Confidential Computing: New Features and NVIDIA Hardware Attestation**
  - Thursday, Mar 21 | 8:00 AM - 8:50 AM PDT
  - Location: SJCC 210B (L2)