

SPHERE - Security and Privacy Heterogeneous Environment for Reproducible Experimentation

University of Southern California Information Sciences Institute,
Northeastern University, University of Utah

Presented by: David Balenson, Outreach Director <balenson@isi.edu>

SPHERE is based upon work supported by the National Science Foundation under Grant #2330066. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

SPHERE Project Team



Jelena Mirkovic
USC-ISI
Lead PI



Erik Kline
USC-ISI
Co-PI, Tech Lead



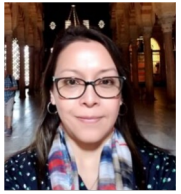
David Choffnes
NEU
Co-PI



Daniel Dubois
NEU
Tech Lead



David Balenson
USC-ISI
Outreach Director



Alba Regalado
USC-ISI
Project Manager



Terry Benzel
USC-ISI



Geoff Lawler
USC-ISI



Joseph Barnes
USC-ISI



Lincoln Thurlow
USC-ISI



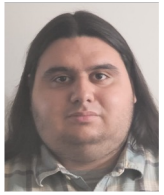
Yuri Pradkin
USC-ISI



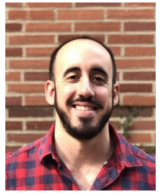
Srivatsan Ravi
USC-ISI



Nandan Desai
NEU



Kevin Aldana
NEU



Luis Garcia
Utah



Erika Bobbitt
USC

Government Team



Kevin Thompson
Cognizant PD
NSF/CISE/OAC



Deep Medhi
PD
NSF/CISE/CNS

SPHERE Advisory Board



Eric Eide

Research Associate Professor, University of Utah



Inder Monga

Executive Director of ESNet and Division Director of Scientific Networking



Kate Keahey

Senior Fellow, Computation Institute, University of Chicago; and Computer Scientist, Mathematics and Computer Science Division, Argonne National Laboratory



Margaret Martonosi

Hugh Trumbull Adams '35 Professor of Computer Science, Dept. of Computer Science, Princeton University



Patrick Traynor

John and Mary Lou Dasburg Preeminence Chair in Engineering, Herbert Wertheim College of Engineering, University of Florida



Raheem Beyah

Dean of the College of Engineering and Southern Company Chair, Georgia Institute of Technology



Sujata Banerjee

Partner Research Manager, Microsoft



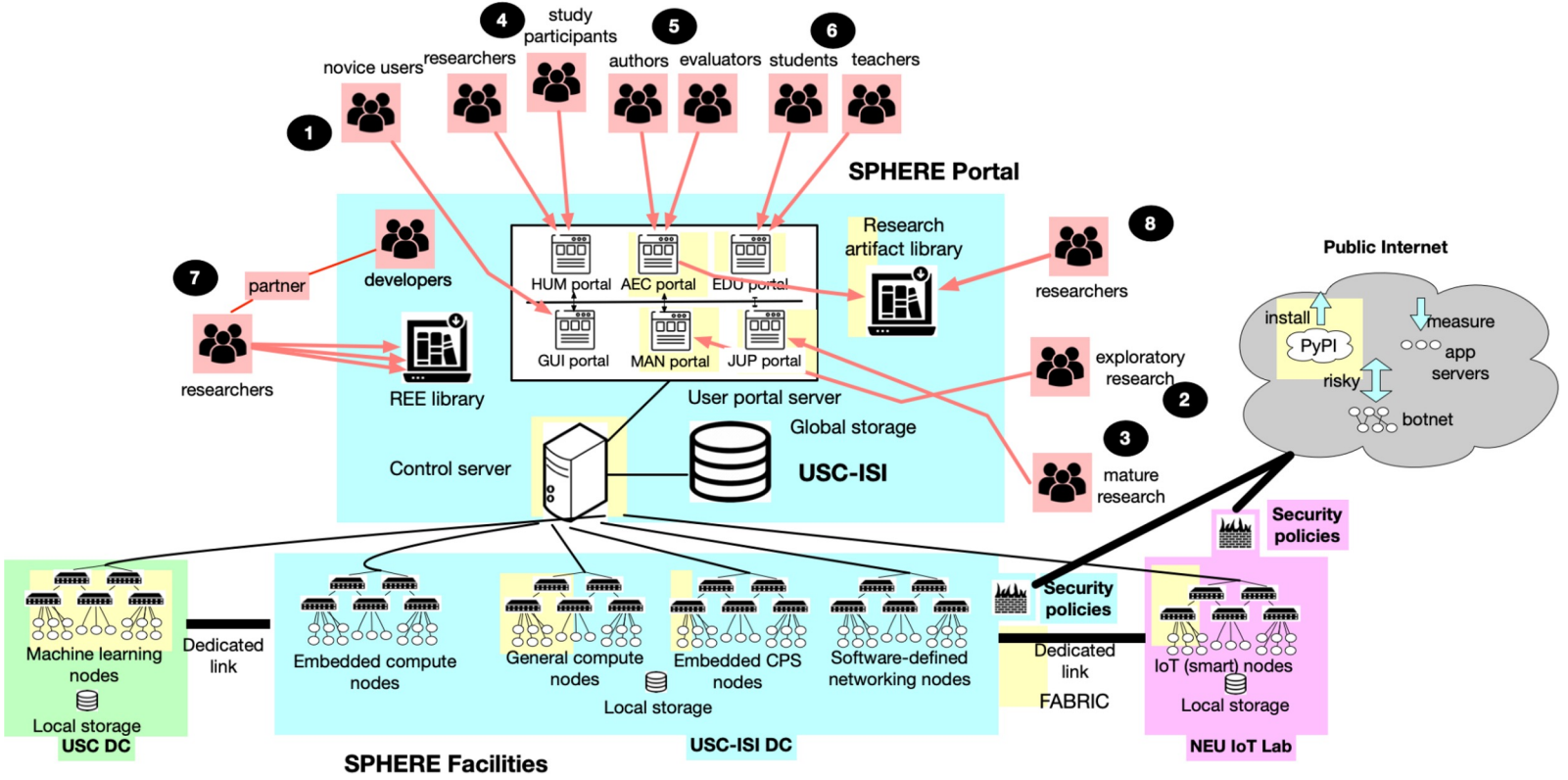
Tingting Chen

Professor, Computer Science Department, College of Science, Cal Poly Pomona

Motivation and Need

- **Motivation:** Cyber threats affect every aspect of our daily lives, critical infrastructure, science, and government. Research solutions are simplistic, piecemeal, and opportunistic, and slow to reach the market
- **Community need:** Common, rich, representative research infrastructure, which meets the needs across all members of the community and facilitates reproducible and open science → vertical progress, integrated research, and more sophisticated solutions
- **Proposed:** SPHERE research infrastructure
  - Heterogeneous resources to meet 90% of research needs in the community
  - Multiple user portals to meet the unique needs of different classes of users
  - Processes/incentives for the community to create representative experimentation environments (REEs) on SPHERE
  - Integrated reproducibility support and processes/incentives for stakeholders to share/reuse research artifacts

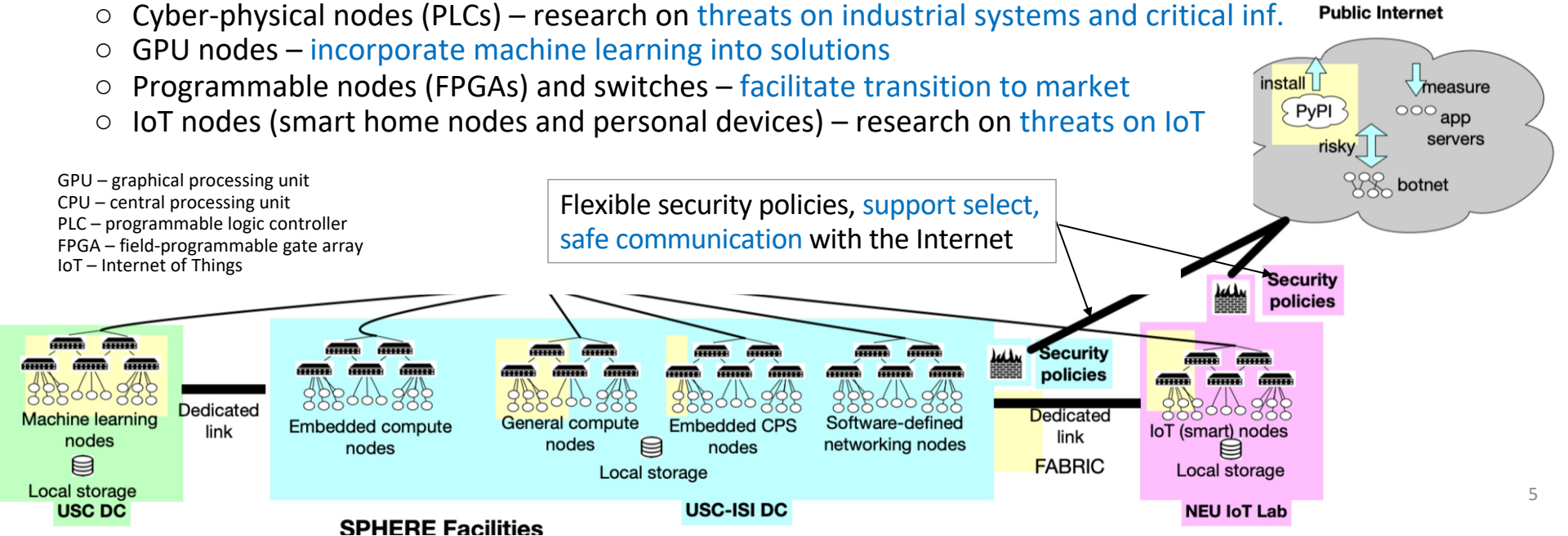
High-Level Architecture



Multiple Types of Resources

- **Multiple** types of resources, needed for **emerging cybersecurity and privacy research**:
  - General compute nodes with trusted computing technology – research on network, cloud computing and system threats
  - Embedded compute nodes (e.g., in phones, tablets, etc.) – research on distributed threats, threats on distributed computing, attacks on specific CPU architectures
  - Cyber-physical nodes (PLCs) – research on threats on industrial systems and critical inf.
  - GPU nodes – incorporate machine learning into solutions
  - Programmable nodes (FPGAs) and switches – facilitate transition to market
  - IoT nodes (smart home nodes and personal devices) – research on threats on IoT

GPU – graphical processing unit
CPU – central processing unit
PLC – programmable logic controller
FPGA – field-programmable gate array
IoT – Internet of Things



NEU IoT Lab

Remote access to a set of 500 consumer IoT devices

- Device reservation (individual devices or groups of devices)
- Network isolation and management:
  - Remote network access to the devices (VPN / VLANs)
- Remote sensor access
  - Cameras, microphones
- Remote actuator access
  - Speakers, button pushers, robotic arms, power control, infrared control
- Companion apps on physical/virtualized phones
- Logging and access to network traffic and sensor/actuator data

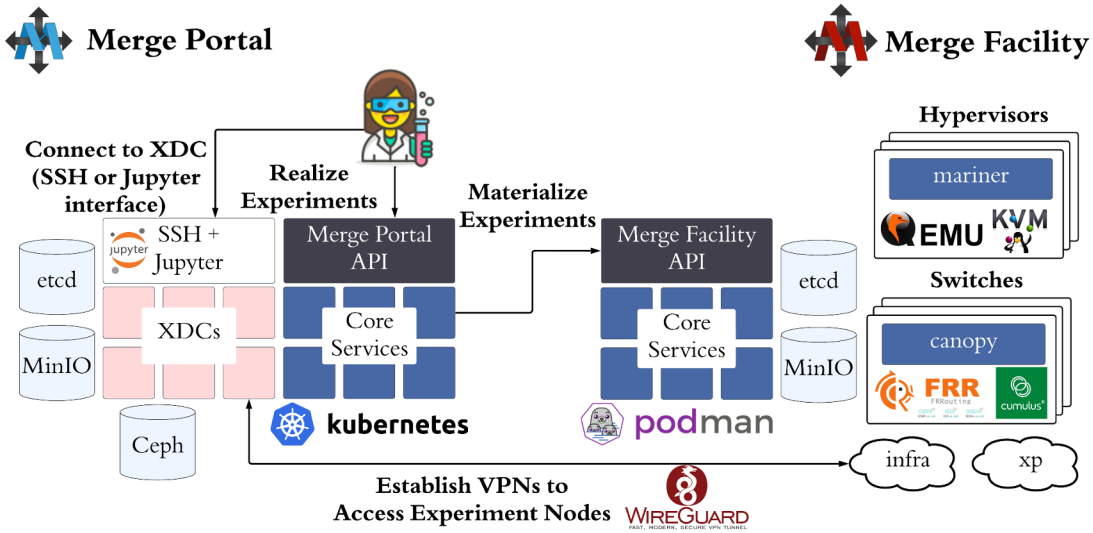


MERGE Control Software

Microservice Architecture for Modularity and Resilience

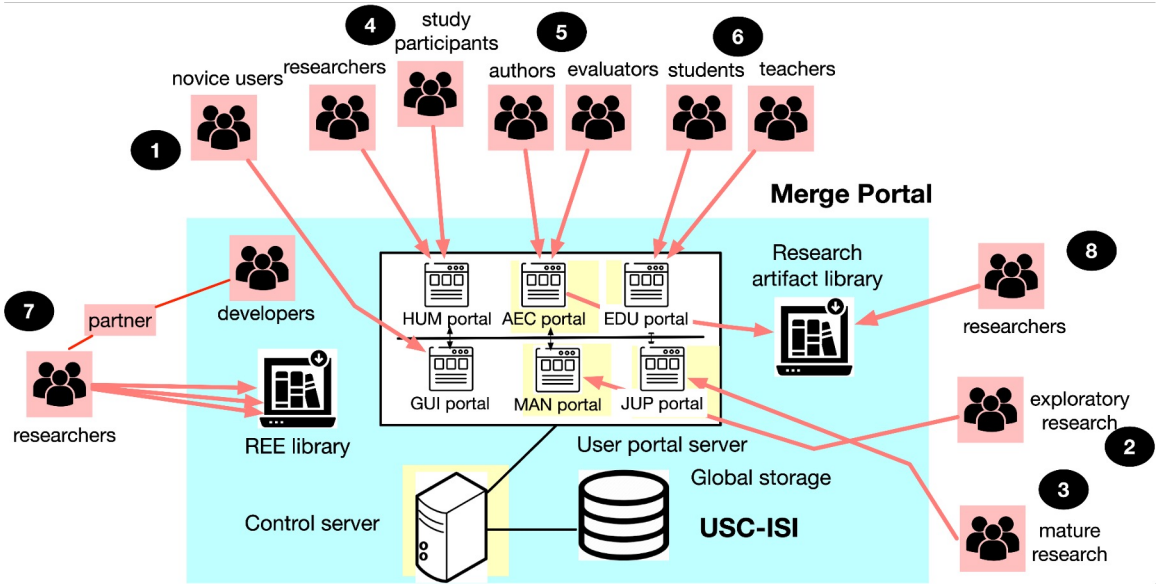
The Merge Portal and Facilities codebases use microservice architectures to flexibly integrate homegrown and third-party services to implement the Merge APIs

Merge supports multiple facilities, which may be managed by different teams and contain different hardware and software



Any compute/network infrastructure implementing the Merge Facility API can be commissioned as a Merge testbed facility

User Portals



- Multiple user portals, supporting different types of users and use modalities
  - Manual, scripted, and GUI-only use support exploratory, mature, and novice research
  - Dedicated support for AECs, education, Internet measurement, and human user studies

GUI – graphical user interface
AEC – artifact evaluation committee

REEs and Research Artifacts



Representative Experimentation Environments (REEs)

- Make research more relevant, vertical and sophisticated
- “Standard” for experimentation in each CS&P area
- Integrated by their authors into SPHERE (funded)

Research Artifacts

- Make research more vertical and reproducible
- Acquired via partnership with artifact evaluation committees (AECs)
- Integrated by their authors into SPHERE as part of artifact evaluation for a conference

CS&P – cybersecurity and privacy
AEC – artifact evaluation committee

Using SPHERE for Artifact Evaluation (1)

- Artifact evaluation committees (AECs) can use SPHERE to evaluate any artifact, even ones unrelated to cybersecurity and privacy research
- There are three ways SPHERE can support AECs:

(1) HotCRP integration

- We have integrated SPHERE support into the HotCRP
  - You can install the code from https://github.com/STEELISI/hotcrp
  - Follow the instructions from README
- At most, one allocation per paper is allowed - the allocation may contain one or more resources (e.g., VMs), and they may be connected or not
- All interaction with SPHERE is via the HotCRP interface
- AE accounts are anonymous on SPHERE, though they can be fully set up in HotCRP

Using SPHERE for Artifact Evaluation (2)

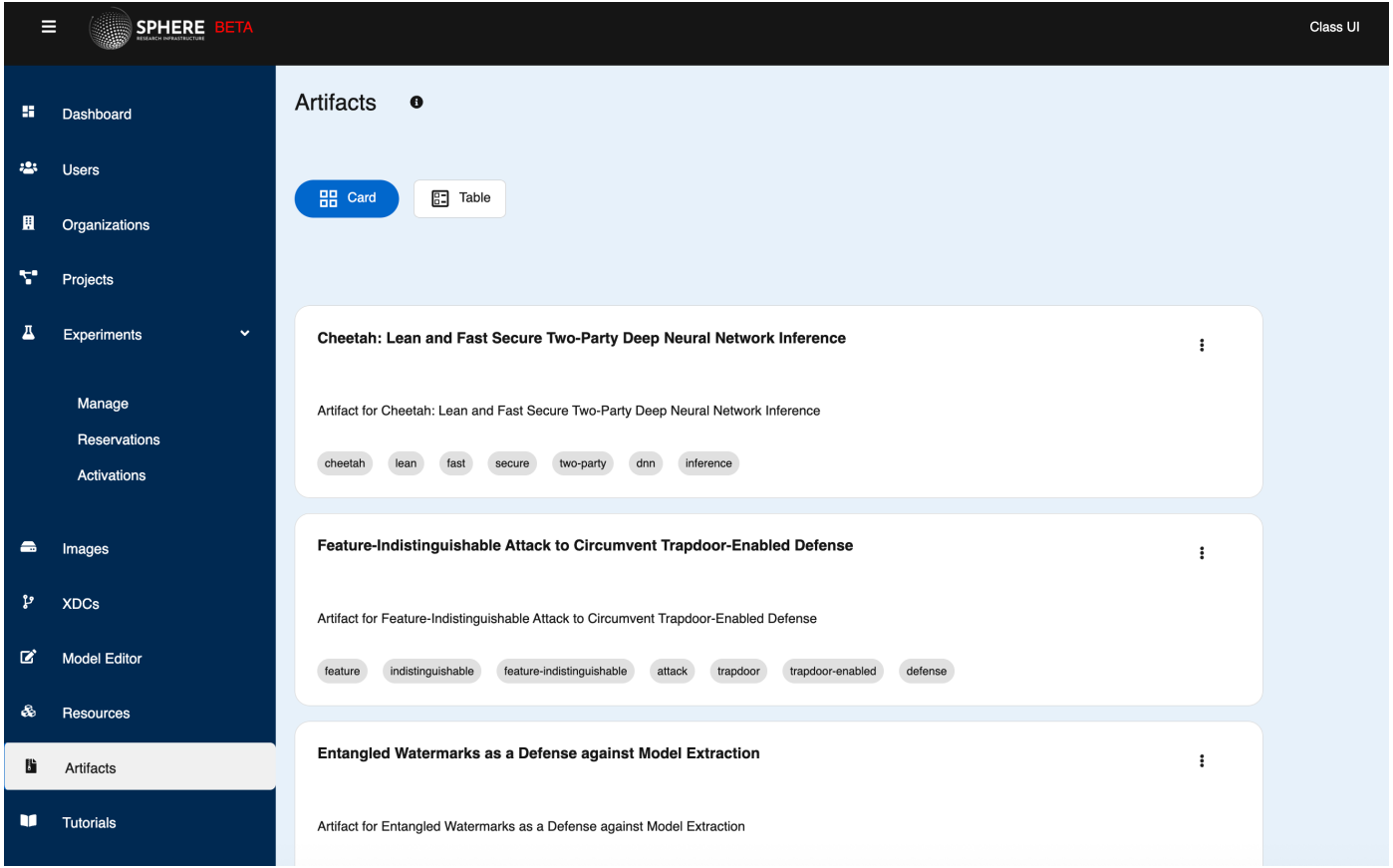
(2) SPHERE creates accounts for AEC chair

- The AEC chair can ask artifact evaluators for their resource needs, collect them in a Google doc, and then share them with the SPHERE team
- We will create the accounts, allocate the needed resources, and put the information into the document (the AE accounts are anonymous)

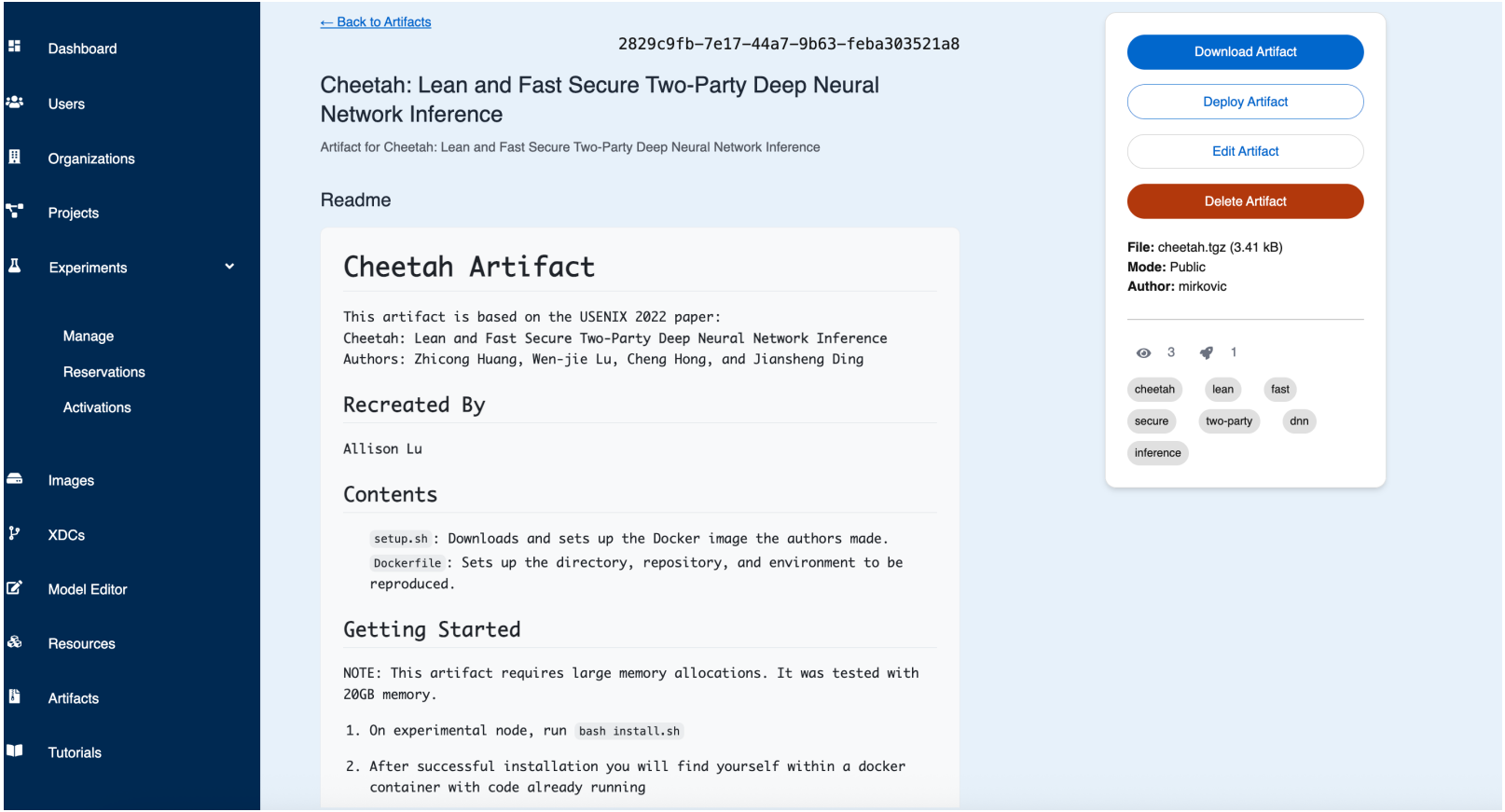
(3) Artifact evaluators creates their own accounts

- Artifact evaluators can create their own accounts on SPHERE
- If they want to remain anonymous to the SPHERE team they can use SPHERE-provided fake information during account creation

Artifact Repository – Listing of Artifacts



Artifact Repository – View of One Artifact



Unique Research Capabilities

- **Relevance:** Experiments with emerging technology and specialized hardware, not currently available to many researchers, support 90%
- **Realism:** Experiments that combine different hardware devices to create realistic scenarios
  - e.g., IoT nodes with GPU nodes and programmable switches to filter attacks
- **Reproducibility:** Experiments on common RI, with extensive support for artifact sharing and reuse, facilitate vertical development
- **BPC:** Different experimentation portals cater to users with different abilities and interests, lowering barrier to entry
- **Impact:** Faster pace of innovation in CS&P and faster technology transition to practice

IoT – Internet of Things
GPU – graphical processing unit
RI – research infrastructure

BPC – Broadening Participation in Computing
CS&P – cybersecurity and privacy

Open to Beta Users

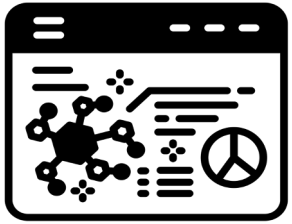
- These users help us grow and improve before we open to larger audience
- Currently around 130 researchers and 200-1000 students per semester
- Users get access to cool new hardware and features
  - Log in remotely via browser, create custom topologies of general purpose VMs (control VM resources, network topology, bandwidth and delay)
  - Access nodes via SSH w/ sudo privileges
  - Experiment directly on nodes or via Jupyter notebooks
  - Able to reach into the Internet, can also support incoming connections
  - Chat-based user support

Component	Dev Started	Available for Use	Notes
SPHERE Infrastructure	Oct 2023	Mar 2024	
General purpose nodes	May 2024	Oct 2025	* Old nodes available now
GPU nodes	Nov 2024	Apr 2025	
CPS nodes	Nov 2024	Oct 2025	
Embedded compute nodes	May 2025	Jan 2026	
IoT nodes	Oct 2023	Aug 2025	
Programmable nodes	Sep 2025	Mar 2026	

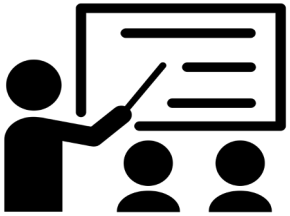
How You Can Help!

Promote and leverage SPHERE at your organizations!

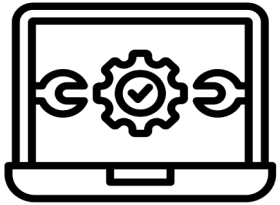
Researchers can use SPHERE to conduct new, innovative research



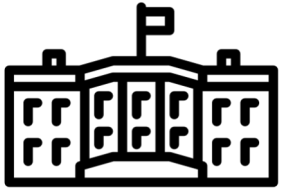
Faculty and students can use SPHERE for educational purposes



IT staff can use SPHERE to test and evaluate new solutions and technologies



Govt PMs can use SPHERE (or other Merge testbeds) to support their programs



Thank you!

If you use SPHERE in your research and a publication, we would appreciate a citation. Currently, the best reference for SPHERE is:

Jelena Mirkovic, David Balenson, Brian Kocoloski. Enabling Reproducibility through the SPHERE Research Infrastructure. USENIX ;login: Online, USENIX Association. December 16, 2024.
https://www.usenix.org/publications/loginonline/enabling-reproducibility-through-sphere-researchinfrastructure

https://sphere-project.net

contact@sphere-project.net

