



SPHERE: A Global Testbed for Reproducible Cybersecurity and Privacy Research



Jelena Mirkovic, David Balenson, and Erik Kline (USC-ISI), David Choffnes and Daniel Dubois (Northeastern University), Geoff Lawler, Joe Barnes, Yuri Pradkin, Christopher Tran, Srivatsan Ravi, Terry Benzel, and Alba Regalado (USC-ISI), Luis Garcia (U. Utah), and Ganesh Chennimalai Sankaran (RENCI)

Societal Need

- **Advancing research in cybersecurity and privacy** is of critical global importance for safeguarding people, infrastructure, and data worldwide.
- As societies grow increasingly interconnected and reliant on digital systems, **robust and reproducible research** is essential to counter evolving threats and strengthen the security, privacy, and resilience of our shared global community.

Research Need

- The global cybersecurity and privacy research community needs a **common, comprehensive, and representative research infrastructure** that meets the needs of all its members and enables reproducible science.
- Such an infrastructure must support **realistic experimentation**, foster **widespread collaboration**, and accelerate the **development of solutions** that enhance cybersecurity and privacy worldwide.

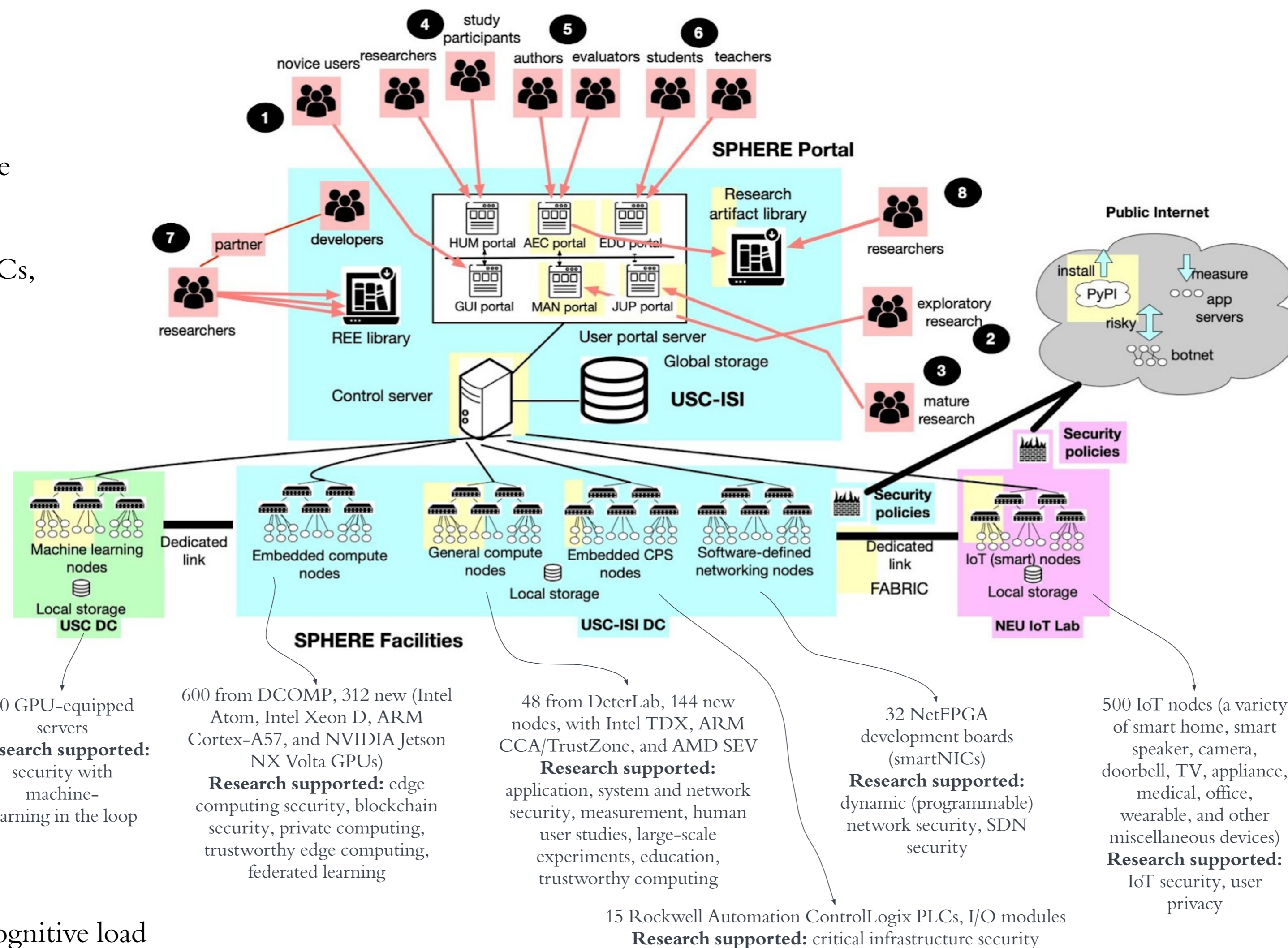
SPHERE Architecture and Capabilities

- **Diverse hardware to support diverse research needs (nearly 90% of today's publications):**
 - General and embedded compute nodes with trusted hardware, PLCs and IoT devices, programmable switches and NICs, and GPU-equipped nodes

- **Six user portals supporting:**
 - Exploratory research (MAN)
 - Novice users (GUI)
 - Mature research (JUP)
 - Education (EDU)
 - Human user studies (HUM)
 - Artifact evaluation (AEC)

- **Libraries of artifacts**
 - Realistic experimentation environments (REEs) and other artifacts
 - Easy reuse on SPHERE

- **Reproducibility support**
 - User action logging to alleviate cognitive load
 - Help package artifacts on SPHERE (including workflows)
 - Automatically verify completeness of an artifact
 - Support stability, consistency of results, and portability



- **Flexible security policies:**
 - Full isolation
 - Measurement research
 - Software download
 - Risky experiments with malware

- **Sample use cases:**
 - Studying ICS security in a realistic environment
 - Studying IoT behavior and privacy implications
 - Studying AI-enhanced network attack detection and mitigation
 - Evaluation at different levels of fidelity

- **Current/planned REEs:**
 - Tier 1 ML security paper artifacts (UFL)
 - Tier 2 security paper artifacts (UFL)
 - CensorLab (UMass)
 - Reconstructed attack dataset (NU)
 - Heavy-duty vehicle CAN bus (CSU)

Collaborate with Us

- **Graduate Students and Faculty Researchers** can use SPHERE to conduct new innovative research
- **Student Interns** can apply for a summer internship to work with SPHERE teams, or apply for a virtual internship to port REEs to SPHERE
- **Other Research Infrastructure** can merge their resources with SPHERE
- **Teachers** can use SPHERE's educational modules, including for homework assignments, graduate and undergraduate classes, demos for K-12 students, and CTFs
- **Government PMs** can use SPHERE (or other Merge testbeds) to support their research programs
- **Artifact Evaluation Committees:** authors can package and share their artifacts and reviewers can evaluate shared artifacts in a common environment



TAKE OUR ANONYMOUS SURVEY TO SHARE YOUR NEEDS
<https://bit.ly/SPHERE-Needs-Survey>

Current Status

- Starting third of four funded years
- Developing general-purpose, ML, and IoT enclaves
- Approx. one-third of general-purpose nodes and 100+ IoT devices available to beta users
- Designing CPS, embedded, and programmable enclaves
- Running control infrastructure and MAN, JUP, and EDU portals
- Piloting AEC portal, used for part of NDSS; working on artifact libraries
- Hosted 25 summer interns and several virtual interns
- Serving approx. 150 research beta users and approx. 1,000 educ. beta users

	Dev Started	Available for Use	
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	Aug 2025	
Embedded compute nodes	May 2025	Jan 2026	
IoT nodes	Oct 2023	Aug 2025	
Programmable nodes	Sep 2025	Mar 2026	* NICs available Fall 2025

Citation: 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>

Visit us at <https://sphere-project.net>