Sadaf Alam

Session 5

Title:

Exascale AI Research Resources Federation and Security: Yesterday, Today and Tomorrow

Abstract:

This talk overviews the rapidly evolving landscape of AI supercomputing research platforms for compliance, cybersecurity, and user accessibility (single sign-on or SSO) and privacy using UK AI Research Resource (AIRR) as deployment instances across two supercomputing sites at Bristol and Cambridge. I will highlight significant changes that we have observed since 2023 UK AI Safety Summit, within the AI RR ecosystem and its national regulatory and compliance framework. Using standard protocols and open-source solutions from community including public cloud platforms for our federated SSO and zero trust architecture deployment, we have (so far) managed to provide service continuity with minimal disruptions to our AIRR user communities. Furthermore, this agility would not have been possible without the development of key skills across technical teams and necessary structural changes to incorporate DevSecOps processes.

Bio:

Dr. Sadaf Alam is chief technology officer (CTO) for Bristol Centre for Supercomputing (BriCS), home to Isambard 3 and Isambard-AI, part of the national AI Research Resource (AIRR). She is also director of strategy and academia in the Advanced Computing Research Centre (ACRC). Across both roles, she is responsible for digital transformation of research computing and data services. Prior to joining Bristol, Alam was the CTO at CSCS, the Swiss National Supercomputing Centre. She was chief architect for two generations of the Piz Daint innovative flagship supercomputing facilities and the MeteoSwiss operational weather forecasting platforms. From 2004 to 2009, Alam was a computer scientist at Oak Ridge National Laboratory (ORNL) and a staff scientist at the ORNL Leadership Computing Facility (OLCF). She studied computer science at the University of Edinburgh, UK, where she received her PhD.