Problem

How to secure data in use at HPC centers?
- without significant performance degradation
- without large application changes
- supporting the sensor, edge, and HPC facility

Trusted Execution Environments (TEEs) can help!

However, existing TEEs
- don't span across nodes, accelerators, or the edge
- incur high slowdowns for large data workloads
- have unsuitable programming model for HPC

Data Centric TEE -- DESC

We propose DESC that
- spans sensor → edge → HPC facility nodes
- focuses on data rather than compute
- requires minimal app changes
- does not require a full OS in the TCB