NSF Campus Cyberinfrastructure PI and Cybersecurity Innovation for Cyberinfrastructure PI Workshop

September 24 – 26, 2018 | University of Maryland, College Park, MD

NSF Program (either CC or CICI): CICI

Program Area:
Resilient Security Architecture

Award Number: 1738929

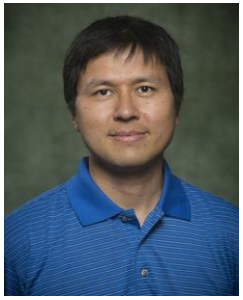
PI: Ping Yang
co-PIs: Shiyong Lu, Guanhua Yan, Fengwei Zhang

Project Title: CICI: RSARC: Infrastructure Support for Securing Large-Scale Scientific Workflows

Ping Yang
Binghamton University (SUNY)
pyang@binghamton.edu

Shiyong Lu
Wayne State University
shiyong@wayne.edu

Fengwei Zhang
Wayne State University
fengwei@wayne.edu



Guanhua Yan
Binghamton University (SUNY)
ghyan@binghamton.edu

NSF Campus Cyberinfrastructure PI and
Cybersecurity Innovation for Cyberinfrastructure PI Workshop
September 24 – 26, 2018 | University of Maryland, College Park, MD

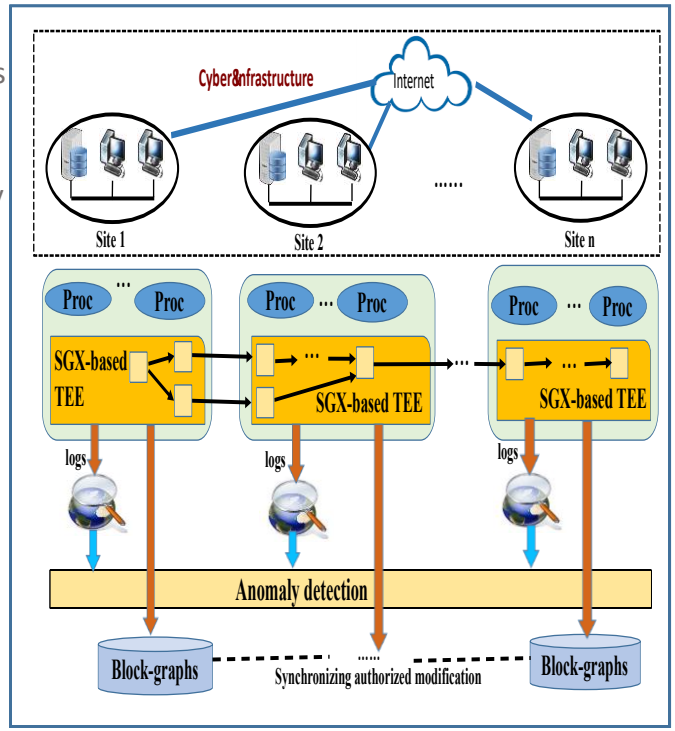
Quad Chart for: CICI: RSARC: Infrastructure Support for Securing Large-Scale Scientific Workflows

Challenge

- The correctness of scientific discoveries relies on the trustworthiness and reliability of the data processed by scientific workflows and the underlying cyberinfrastructure.
- Existing scientific workflow systems lack strong infrastructure support for trustworthy execution of scientific workflows and for protecting the workflow data.

Solution

- Develop a trusted execution environment for scientific workflows.
- Develop SciBlock, a tamper-proof and non-repudiable provenance storage that enables scientists to verify the trustworthiness of scientific data.
- Develop a machine-learning based technique to detect anomalous execution flows in scientific workflows.



Broader Impact

- Support secure scientific discovery processes for a wide range of science and engineering disciplines.
- Involve women and underrepresented minorities in research and education.
- Collaborate with domain scientists in Ford Motor and Department of Physiology at Wayne State university

Metadata Tag

- http://www.cs.binghamton.edu/~pyang/workflow.html
- *Intel Software Guard Extension (SGX)*
- *Blockchain*
- *Machine learning*