U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

A Resilient and Trustworthy Cloud and Outsourcing Security Framework for Power Grid Applications

Making cloud computing for power grid applications cyber-secure and resilient

Background

Power grid applications, such as wide-area state estimation, contingency analysis, security-constrained economic dispatch (SCED), security-constrained unit commitment (SCUC), and faster-than-real-time grid dynamics simulation and analysis, are complex enough to pose significant processing and networking challenges to the computers and networking equipment available to power system operators.

As a consequence, more computing and networking capabilities are needed for operations, and cloud computing is an attractive prospect. Since applications in a power grid have to be secured, due to the sensitivity and proprietary nature of the data used, the concerns over cloud security are impeding the migration of power grid applications from local computing centers to public clouds.

Some major challenges to cloud computing for power grid applications include:

- Vulnerability of virtual machine (VM) in a cloud server
- Continuous evolution of adversaries' targets, methods, and tools
- Encryption-based techniques can suffer from high computation overhead and may be difficult to apply

Objectives

- Deploy power grid applications with different time criticality requirements in the cloud, with strong cybersecurity
- Develop resilient and trustworthy cloud and outsourcing security framework for power grid applications
- Deploy security enhancements to cloud-based power grid applications
- Demonstrate best practices in cybersecurity for cloud-based power grid applications in a real power system

Project Description

Cloud computing can be used to optimize operations of the power grid. This project will identify risks to the cloud computing model with the intent of removing or mitigating these risks by:

- Modeling and quantifying different types of attacks against cloud-based power grid applications
- Modeling and quantifying the security and time criticality requirements of different types of power grid applications

Benefits

- New business models based on cyber-secure cloud computing for the power generation and distribution industry
- Commercial cyber-secure cloud computing tools for the energy sector
- Outreach to the energy sector on strengthening cybersecurity of the power grid

Partners

- Argonne National Laboratory (ANL) (lead)
- Idaho National Laboratory (INL)
- SUNY-Buffalo
- Illinois Institute of Technology (IIT)
- Commonwealth Edison (ComEd)
- PJM Interconnection (PJM)

Period of Performance

October 2015 – September 2021

Total Project Cost

$900,000

Content last updated: May 2016

Cybersecurity for Energy Delivery Systems (CEDS)

CEDS projects are funded through the Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) Research and Development (R&D) program, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of emergency disruptions due to cyberattacks.

For more information: https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/cybersecurity-research-development-and

Initial Leads

Carol Hawk
Program Manager

Jianhui Wang
Principal Investigator
Argonne National Laboratory
630-252-1474
jianhui.wang@anl.gov

Current Contact as of Aug. 2020

Akhlesh Kaushiva
Program Manager
DOE CESER
202-287-6062
akhlesh.kaushiva@hq.doe.gov

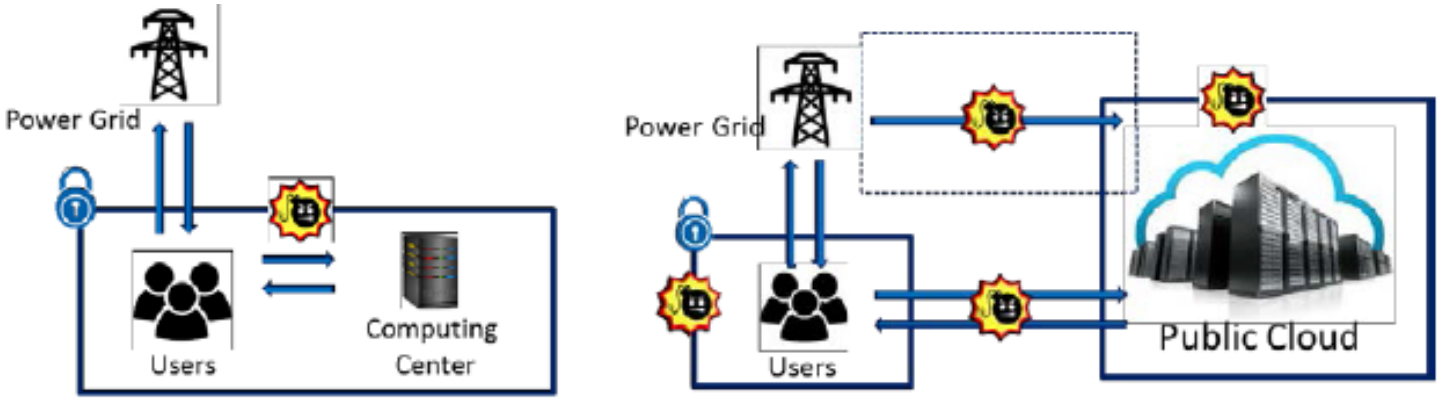

Figure 1: Traditional Scenario vs. Cloud Scenario

Technical Approach

The project is designing and implementing cyber-secure cloud-based power grid software tools, and testing them on three power grid applications: SCED, SCUC, and stochastic SCUC.

Tasks

- Establish an attack-resilient cloud and outsourcing security framework for power grid applications, emphasizing defense-in-depth.
- Model and quantify attacks against cloud-based power grid applications.
- Quantify the security and time criticality requirements of the three major cloud-based power grid applications.
- Deploy the three power grid applications on a cloud computing platform, and compare the results with local server based solutions.
- Compare performance of three applications with and without security enhancements.
- Deploy security enhancements to the three cloud-based power grid applications implemented in the previous task.
- Quantify the security and time criticality guarantees of cloud-based power grid applications.
- Recommend improvements to current cloud capabilities for resilient and trustworthy grid applications.
- Recommend best practices for cloud-based power grid applications.

Anticipated Results

Project results will include the following:

- Attack-resilient and trustworthy cloud computing and outsourcing security framework for the energy sector
- Three case studies of operation, one with standard IEEE bus configuration, one in ComEd subregion of PJM, and one on model of PJM grid
- Recommendations for cybersecurity improvements for cloud-based power grid applications