Jianhui Wang
Argonne National Laboratory (ANL)

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

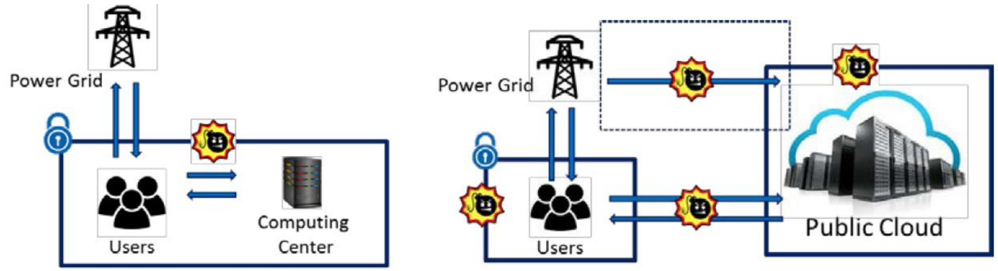
Cybersecurity for Energy Delivery Systems Peer Review

December 7-9, 2016

Summary

Objective

- The computational complexity of power grid applications is increasing
- Cloud computing provides *powerful computational capacity*, *scalability*, and *high cost-effectiveness*
- **Goal:** Develop a secure and trustworthy cloud computing and outsourcing framework for power grid applications



Traditional Scenario vs. Cloud Scenario

Performer:	**ANL**
Partners:	**University at Buffalo, Illinois institute of Technology**
Federal Cost:	**$1,500,000**
Cost Share:	**N/A**
Total Value of Award:	**$1,500,000**
Funds Expended to Date:	**5%**

Schedule

- August 2016 – July 2021
- Framework and white paper (Q2 2017)

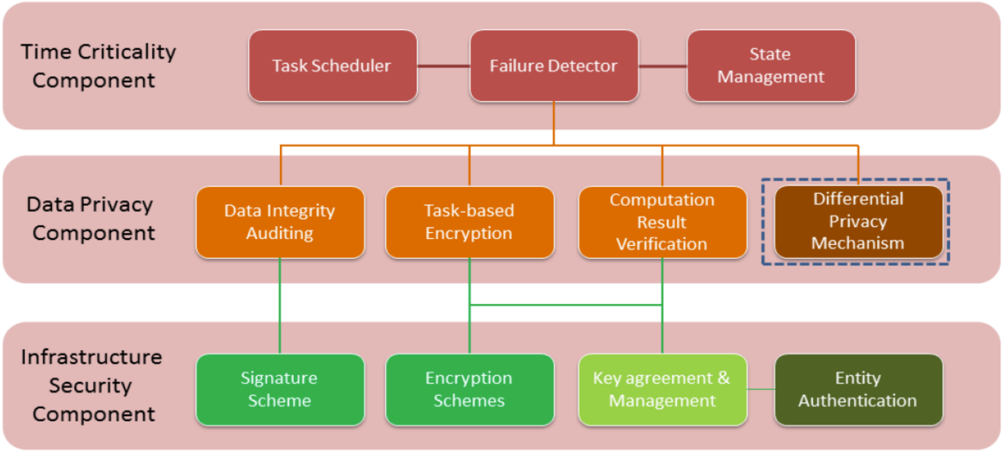
Advancing the State of the Art (SOA)

Current versus new SOA

- System Operators currently exploit High Performance Computing (HPC) on local computing infrastructures
  - Requires high-capital expenditures and maintenance
  - Limits rapid scalability for power grid applications
- Transition to cloud computing can save time and manpower, while unveiling new opportunities

Enhanced Cloud Cybersecurity

- Module-based cybersecurity system design
- Flexible based on the specific power grid application

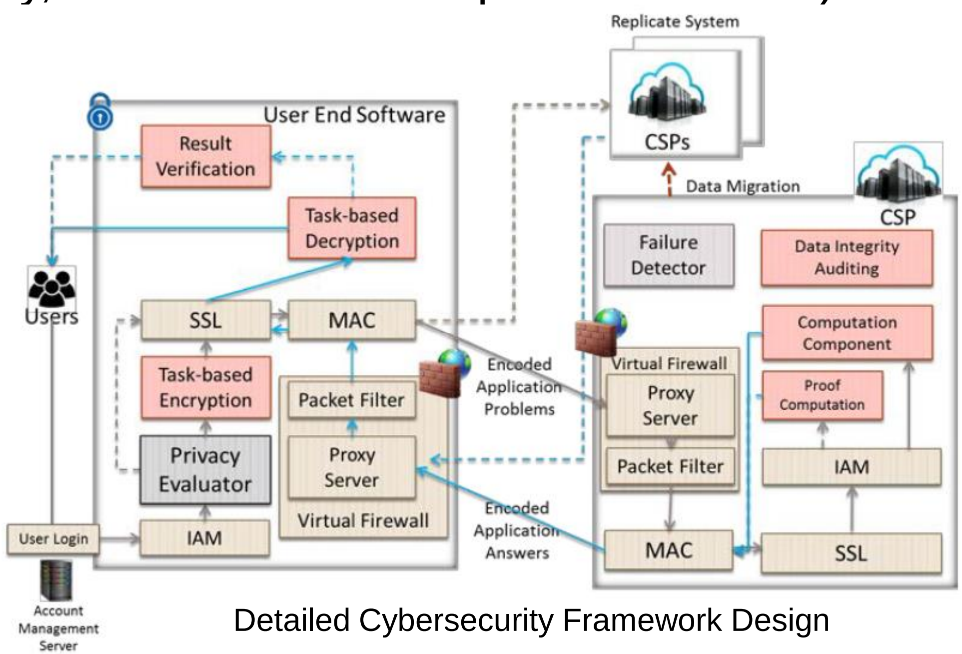


Advancing the State of the Art (SOA) (cont.)

Holistic Cloud Outsourcing and Security Framework

The developed framework will incorporate:

- **Application-specific features:** security-constrained economic dispatch (SCED), unit commitment (SCUC), and stochastic SCUC
- Security framework for confidential power grid data transfer
- Outsourcing framework specific to classes of applications (*e.g.*, mathematically, SCUC is more complex than SCED)



Detailed Cybersecurity Framework Design

Challenges

Infrastructure Security

- Power grid data requires high confidentiality
- Ensure security during transmission to/from and storage on the cloud

Data Integrity

- Cyberattacks, *e.g., false data injections*, during transmission, storage, and even the simulation process are probable
- Ensure grid data and application results remain accurate and consistent

Time Criticality

- Applications must be completed in a timely manner to ensure continuous operation of the grid
- Ensure the holistic cloud framework meets with the time requirements of the system operator

Technical Approach

Cyberattacks may result from two groups - *insiders* and *outsiders*

Within the insider group are passive and active entities

- **Passive**: monitor communication channel between the user and the cloud
- **Active**: attacks to alter system resources, *e.g.,* flood attack, spoofing attack

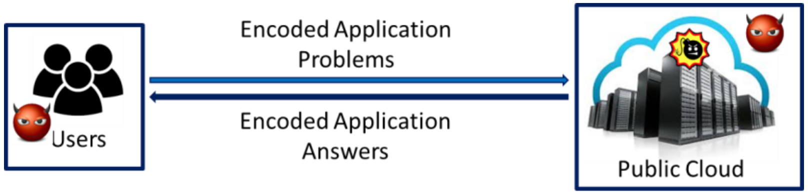


Illustration of Insider Attackers

Within the insider group are compromised users and cloud providers, or malicious administrators

- **User**: compromise infrastructure security
- **Cloud provider**: compromise data privacy
- **Administrator**: obtain sensitive data

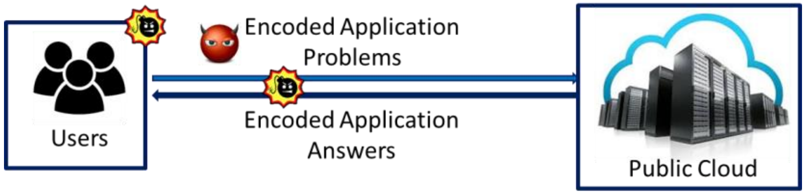


Illustration of Outsider Attackers

Technical Approach

Develop methods to secure SCED and SCUC

- For example, SCED as a linear program (LP), can be formulated as:

Objective Function:	$\min \ \mathbf{c}^{\mathbf{T}}\mathbf{x}$
Equality Constraints:	$\mathbf{A}\mathbf{x} = \mathbf{b} \ \ (\boldsymbol{\lambda})$
Inequality Constraints:	$\mathbf{B}\mathbf{x} \geq \mathbf{0} \ \ (\boldsymbol{\mu})$

- Two distinct approaches can be implemented

  1. **Formulate** LP locally based on the raw grid data, **transfer** and **solve** the problem to the cloud, and then **transfer** results back to end-user
  2. **Transfer** raw grid data to the cloud, **formulate** and **solve** LP on the cloud, and **transfer** results back to end-user

- Two approaches have different implications for data confidentiality
  - *Approach #1* is **more secure** than *Approach #2*
  - *Approach #2* is **more efficient** than *Approach #1*

- Trade-offs exist. Develop techniques that holistically consider both efficiency and security

Technical Approach

Solution methods must consider Infrastructure Security, Data Integrity, and Time Criticality

- Possible solution methods include a combination of efforts from various fields in Operational Research, Communications, Data Science, etc.

- Infrastructure security can be performed via techniques in cryptography (*e.g.,* SSL) and/or data encryption (*e.g.,* AES)

- Data Integrity can be performed via techniques to check if the data in-transit are authentic

- To ensure SCED and SCUC solve timely, model transformations will be enacted while ensuring
  - Problem sizes do not grow out of proportion
  - Optimal solutions are exact to their original problem

Progress to Date

Major Accomplishments

- Industry Advisory Board consisting of a diverse group of individuals applying cloud computing:
  - Xiaochuan Luo, ISO-NE
  - Alex Rudkevich, Newton Energy Group
  - Jianzhong Tong, PJM
  - Tobias Whitney, NERC
- Invited to attend NERC Emerging Technologies Roundtables on Nov 15-16
  - Opening remark and presentation
- Two papers under preparation
  - Security and Cloud Outsourcing Framework for Security-Constrained Economic Dispatch
  - Fast Encryption Scheme for Cloud-based SCUC Problem Outsourcing System
- Framework report and white paper

Collaboration/Technology Transfer

Plans to transfer technology/knowledge to end user

- Technology will conform to operating paradigms of system operators
  - Enable ease of implementation and high impact to business processes
- Technology testing will occur on large-scale datasets to ensure applicability and scalability
  - PJM and ComEd grid datasets will be used
- End-users may be but not limited too:
  1. **System Operators:** directly implement on cloud services (*e.g.,* Amazon EC2, Microsoft Azure, among others)
  2. **Software-as-a-Service (SaaS)**: entity can host and maintain the technology framework for a usage/service fee
  3. **Software-as-a-Product (SaaP)**: entity can sell licenses of the technology to practicing users

Thank You!

Jianhui Wang Ph.D.
Section Lead – Advanced Power Grid Modeling
Energy Systems Division
Argonne National Laboratory
9700 S. Cass Avenue, Bldg. 362
Argonne, IL 60439, USA
Jianhui.wang@anl.gov