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

Argonne National Laboratory (ANL)

Feng Qiu

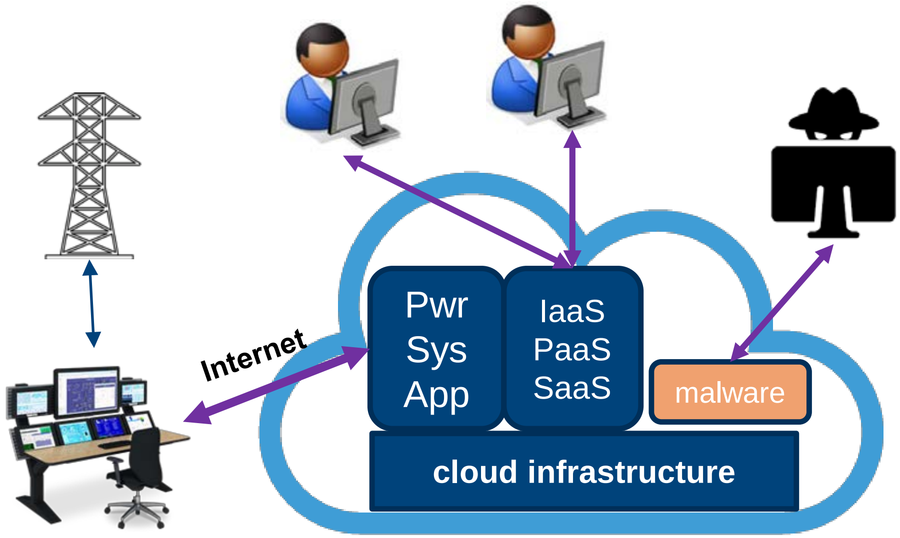
Cybersecurity for Energy Delivery Systems Peer Review

November 6-8, 2018

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

Objective

- **Background:** Cloud computing provides powerful computational capacity, scalability, and high cost-effectiveness
- **Challenges:** Confidentiality of grid data; vulnerabilities in data transmission and cloud data storage; time criticality
- **Opportunity:** Build a trustworthy and secured cloud computing framework for power grid applications to facilitate cloud computing in power industry
- **Benefits:** Provide highly secured encryption framework for power system computing (on cloud or other outsourcing scenarios)



Schedule

- Started in August 2016, ends August 2021
- Key deliverables and dates met
  - Design of an attack-resilient framework, Y1 Q2
  - Deployment of SCED & SCUC on cloud, Y2 Q4
- Capabilities to be transitioned to energy sector
  - Attack-resilient framework for power system applications on cloud computing and other outsourced platforms
  - Privacy-preserving methodologies and software packages for a set of power system applications

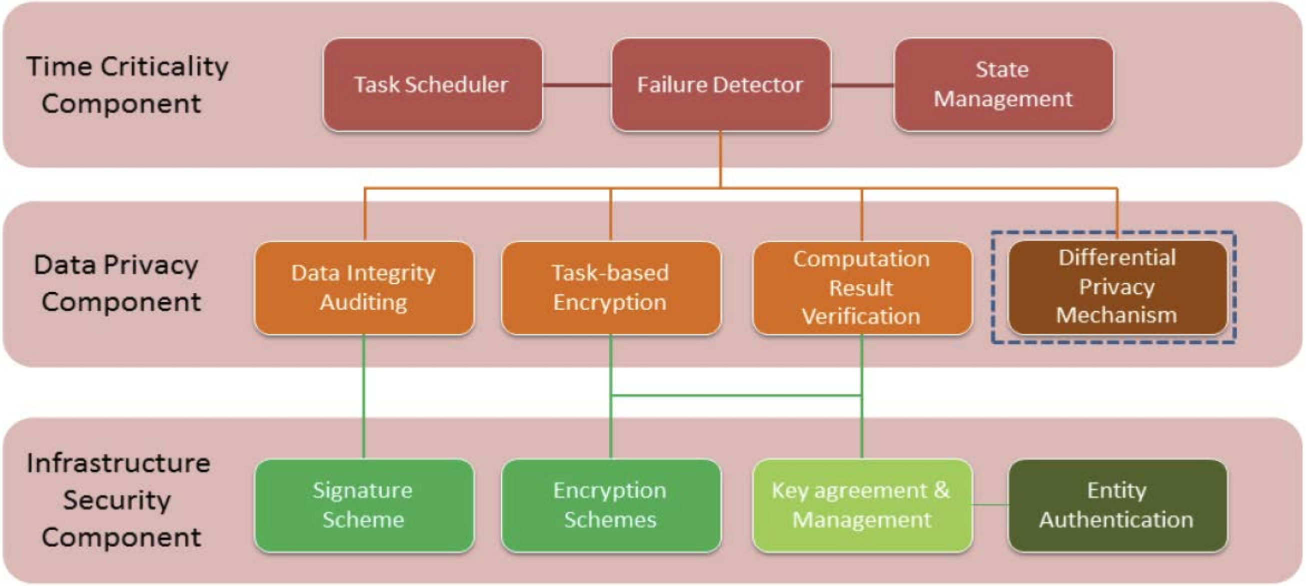
Total Value of Award:	**$1,500,000**
Funds Expended to Date:	**%40**
Performer:	**Argonne National Lab**
Partners:	**University at Buffalo, Illinois Institute of Technology**

Advancing the State of the Art (SOA)

- **Cloud Computing**
  - Powerful: Amazon EC2 96 vCPUs 345 GB memory
  - Scalable: Hundreds or even thousands of instances simultaneously
  - Cost-effective: $0.0016/hr (spot pricing)
  - Nearly half of all companies claim 31% to 60% of their IT systems are cloud-based
  - Global Smart Grid as a Service market expected to grow from $1.3 billion in 2016 to $6 billion in 2025 ["Smart Grid as a Service," *Navigant Research,* 2016]
- **Weak Cloud Security**
  - Shared Security Responsibility Model
    - Secure only certain layers of infrastructure and software
    - Customer is ultimately responsible for how data are accessed/used
  - Data breaches on cloud
    - AWS, Microsoft, Apple, Yahoo . . .
    - Malware injection, side channel, wrapping, Spectre, and Meltdown (shared memory)
- **Commonly Used Cloud Cybersecurity Methods**
  - Communication encryption, data encryption
  - Cloud computing is completely vulnerable to insider attacks
  - Not suitable for power system computing
- **Privacy-Preserving (PP) Methodologies**
  - "Fake" problems solved on cloud; real data always on local
  - Data confidentiality is preserved even if data breach occurs
  - Ensuring correctness, optimality, and performance of solution

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

- **A Holistic Security Framework for Cloud Computing**
  - Infrastructure security
  - Data confidentiality (privacy-preserving)
  - Application-specific encryption for higher security: Security-constrained economic dispatch (SCED), security-constrained unit commitment (SCUC), stochastic unit commitment (UC), etc.
- **Benefits to Cyber Resilience of Energy Delivery Systems**
  - Establish cybersecurity framework/methodologies for power system cloud computing
  - Pave the way (cybersecurity) to facilitate cloud computing application in power industry



Challenges to Success

Infrastructure Security

- High confidentiality of power grid data and insufficient cloud security
- Module-based cybersecurity system design for data transmission and storage

Data Integrity

- Power system computations completely vulnerable on cloud (leaking and manipulation)
- Set of encryption and validation methodologies ensure data confidentiality, accuracy, and consistency in computing

Time Criticality

- Applications must be completed in a timely manner to ensure continuous operation; time cost of encryption
- Highly efficient and effective privacy-preserving methods

Progress to Date

Major Accomplishments

- Diverse Industry Advisory Board
  - Xiaochuan Luo, ISO-NE; Jianzhong Tong, PJM
  - Alex Rudkevich, Newton Energy Group; Tobias Whitney, EPRI (Cyber Security for the Electric Sector)
- Important Milestones Accomplished (progress on track)
  - Design of an attack-resilient framework that comprehensively captures all common cyber and physical properties across power grid monitoring, protection, and control applications
  - Model of attacks against cloud-based power grid applications
  - Deployment of SCED and SCUC on GovCloud (AWS)
  - Initial results on privacy-preserving methods on SCED and SCUC
- Publications
  - M. R. Sarker, J. Wang, Z. Li and K. Ren, “Security and Cloud Outsourcing Framework for Economic Dispatch,” *IEEE Transactions on Smart Grid*, vol. 9, no. 6, pp. 5810–5819, 2018.
  - “A Resilient and Trustworthy Cloud and Outsourcing Security Framework for Power Grid Applications,” ANL/ESD-18/14, Lemont, IL, Argonne National Laboratory.
  - “Cyberattacks Against Cloud-based Power System Applications,” ANL/ESD-18/16, Lemont, IL, Argonne National Laboratory.
  - “Privacy-preserving Transformations for Security Constrained Unit Commitment” (in preparation).

Collaboration/Technology Transfer

Plans to Transfer Technology/Knowledge to End User

- Reduce Technology Adaption Difficulty
  - Modular design for flexible implementation and deployment
  - Thorough test on publicly accessible clouds
- Stick to Industrial Needs
  - Select widely used power system applications to develop cloud security enhancement
  - Emphasize practicality and scalability (large-scale systems will be thoroughly tested)
  - Industry advisory board with various potential customers
- End-users Include but not Limited to:
  - System Operators: Directly implement on cloud services
  - Software as a service (SaaS): Entity can host and maintain the technology framework for a usage/service fee
- Testing and Demonstrate Plan
  - Demonstration to industry with realistic instances (PJM, etc.)

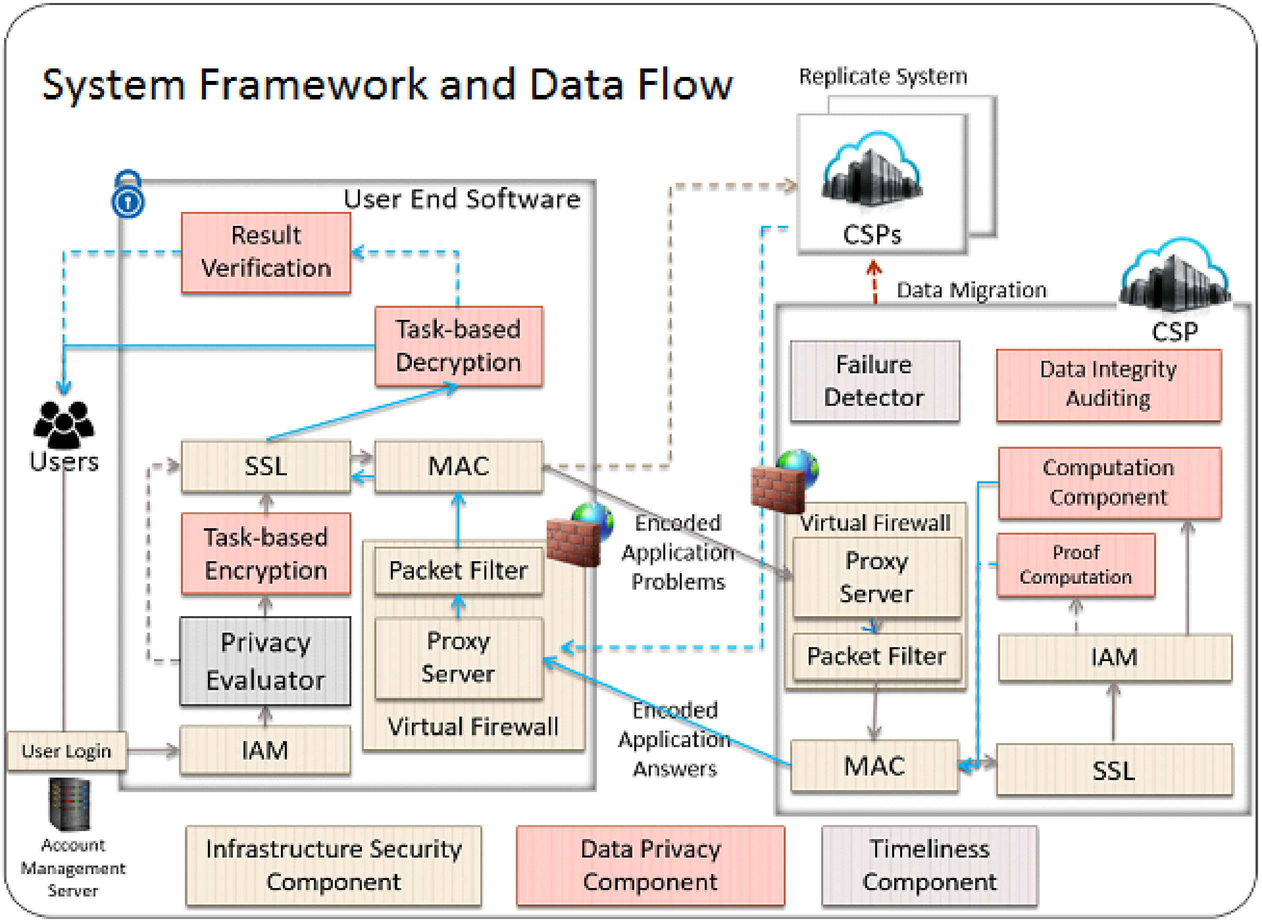
Next Steps for this Project

Approach for the Next Year or to the End of Project

- Sparse Transformation for SCUC
  - Sparse transformation for integer programming
  - Selectively secure certain data (e.g., topology) to achieve higher performance
- Distributed Cyber Security Framework
  - Enhanced security by distributing data and computations on multiple machines
  - Enhanced computational performance by parallel computing
- Security Enhancement for Stochastic UC on Cloud
  - One of the applications that can benefit most from cloud computing
  - Utilizing a large pool of computers on cloud
- Implementation and Test for Industrial Adaption
  - Scalability and technology transferability

Infrastructure Security Framework

System Framework of Resilient and Trustworthy Cloud and Outsourcing Framework



- Identity and Access Management
- Confidentiality evaluator
- Communication security and authentication
- Virtual firewall
- CSP components
- Data audit protocols
- Result verification schemes

Transformation-Based Privacy-Preserving

Desired Security Definition

- Assumption: Attackers know the model but not the data
- The number of values in this domain is infinite, or the number of values in this domain is so large that a brute-force attack is computationally infeasible.
- The range of the domain (the difference between the upper and lower bounds) is acceptable for the application.

Transformations

- Multiplying from left/right, scaling and perturbation, shifting

$$\begin{array}{lccc} & \min & c^T x & \\ \text{s.t.} & Mx & \leq & B \\ & x & \geq & 0 \end{array}$$

→ Perturbation/Scaling
Variable shifting

$$\begin{array}{rcl} \min c^T Q(Q^{-1}x + r) & & \\ M_1 Q(Q^{-1}x + r) & = & b_1 + M_1 Qr \\ M_2 Q(Q^{-1}x + r) & \leq & b_2 + M_2 Qr \\ (Q^{-1}x + r) & \geq & r \end{array}$$

Q a positive monomial matrix

→ Add slack variables
Turn ineq. into eq.

$$\begin{array}{lccc} & \min & c_s'^T z_s & \\ \text{s.t.} & M' z_s & = & b' \\ & z_s & \geq & 0 \end{array}$$

$$M' = \begin{pmatrix} M_1 Q & 0 \\ M_2 Q & \mathrm{A} \\ -S & \end{pmatrix} b' = \begin{pmatrix} b_1 + M_1 Qr \\ b_2 + M_2 Qr \\ -Sr \end{pmatrix}$$

→ Multiplying by random non-singular matrix

$$\begin{array}{lccc} & \min & c_s'^T z & \\ \text{s.t.} & M'' z_s & = & b'' \\ & z_s & \geq & 0 \end{array}$$

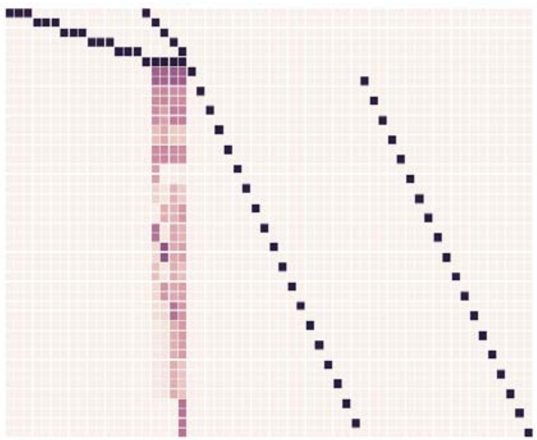
$$M'' = P * M'$$
$$b'' = P * b'$$

P: non-singular matrix

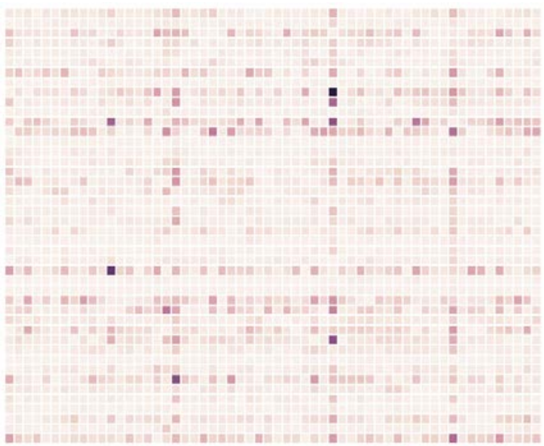
Privacy-Preserving SCED

PPSCED–An Illustration (Heat maps indicate the no-zero coefficient density)

Original formulation



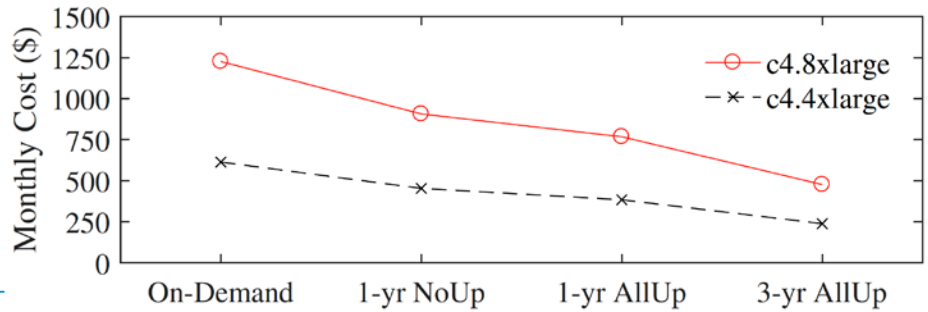
PP Transformation

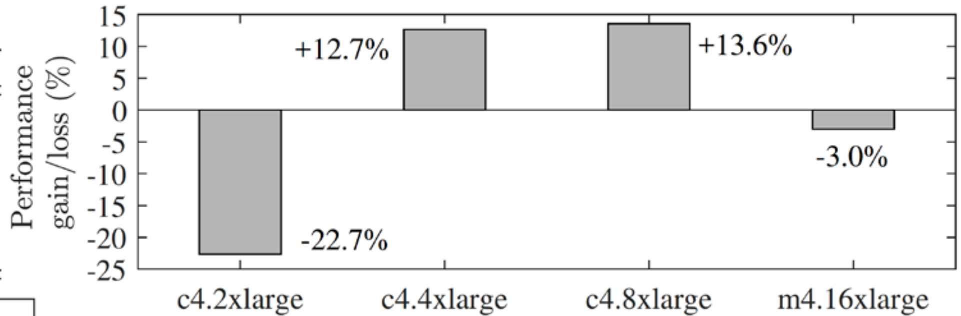


Comparing AWS Cloud with In-house HPC (ANL Blues)

COMPUTING INFRASTRUCTURE CHARACTERISTICS

	CPU	RAM	SSD	Intel Processor	$/h
1) ANLBlues	16	64	✓	Xeon Nehalem	2.880
2) c4.2xlarge	8	16	✓	Xeon E5-2666v3	0.419
3) c4.4xlarge	16	30	✓	Xeon E5-2666v3	0.838
4) c4.8xlarge	36	60	✓	Xeon E5-2666v3	1.675
5) m4.16xlarge	64	256	✓	Xeon E5-2686v4	3.830





- Simulating SCED on 2383-bus Polish system, run every 5 minutes, compare performance and costs
- Shuffling and scaling
- Cost effective: 77-85% saving over ANL Blues
- Cloud provide a variety of performance options

Privacy-Preserving Transformation for SCUC

Performance vs. Security

- SCUC: Computational performance of integer programming is very sensitive to constraint matrix density

Instances	Instance	Nz Before	Nz After
SCUC(no contingency)	case188	46,976	6,410,880
	case300	73,966	13,524,000

A Shuffling and Scaling Method

$$
\begin{aligned}
\text{minimize} \quad & \sum_{t\in T}\sum_{g\in G}\left[c_g^U y_{gt} + c_g^D z_{gt} + c_g^{\min} x_{gt} + \sum_{k\in K} c_g^k p_{gt}^k\right] \\
\text{subject to} \quad & p_{gt} = P_{gt}^{\min} x_{gt} + \sum_{k\in K} p_{gt}^k \\
& p_{gt}^k \le P_{gt}^k x_{gt} \\
& p_{gt} \le p_{g,t-1} + R_{gt}^U \\
& p_{gt} \ge p_{g,t-1} - R_{gt}^D \\
& \sum_{g\in G} p_{gt} = D_t \\
& x_{gt} - x_{g,t-1} = y_{gt} - z_{gt} \\
& -F_l - \sum_{b\in B} \delta_b^l d_{bt} \le \sum_{b\in B}\sum_{g\in G_b} \delta_b^l p_{gt} \le F_l + \sum_{b\in B} \delta_b^l \\
& p \ge 0 \\
& x_{gt}, y_{gt}, z_{gt} \in \{0,1\}
\end{aligned}
$$

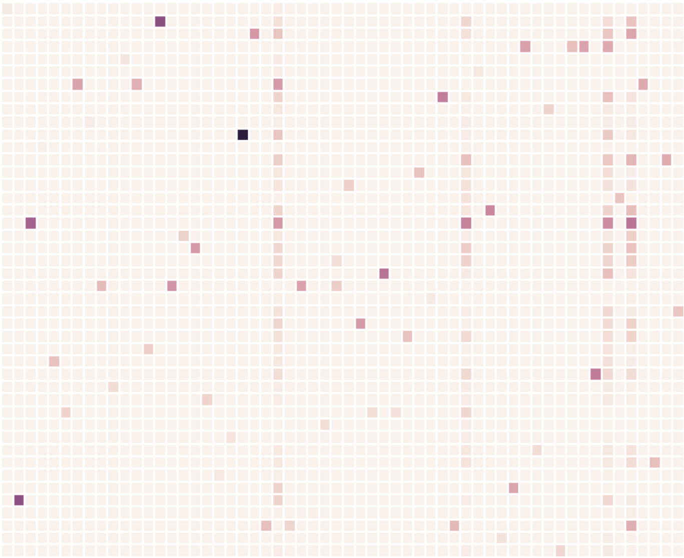
$$
\begin{aligned}
\text{minimize} \quad & \sum_{t\in T}\sum_{g\in G}\left[\gamma c_g^U y_{gt} + \gamma c_g^D z_{gt} + \gamma c_g^{\min} x_{gt} + \sum_{k\in K} \gamma c_g^k D_t p_{gt}^k\right] \\
\text{subject to} \quad & p_{gt} = \frac{P_{gt}^{\min}}{D_t} x_{gt} + \sum_{k\in K} p_{gt}^k && \forall t, g \\
& p_{gt}^k \le \frac{P_{gt}^k}{D_t} x_{gt} && \forall t, g, k \\
& p_{gt} \le \frac{D_{t-1}}{D_t} p_{g,t-1} + \frac{R_g^U}{D_t} && \forall g, t \\
& p_{gt} \ge \frac{D_{t-1}}{D_t} p_{g,t-1} - \frac{R_g^D}{D_t} && \forall g, t \\
& \sum_{g\in G} p_{gt} = 1 && \forall t \\
& x_{gt} - x_{g,t-1} = y_{gt} - z_{gt} && \forall g, t \\
& -\frac{\alpha_l F_l}{D_t} - \sum_{b\in B} \frac{\alpha_l \delta_b^l d_{bt}}{D_t} \le \sum_{b\in B}\sum_{g\in G_b} \alpha_l \delta_b^l p_{gt} \le \frac{\alpha_l F_l}{D_t} + \sum_{b\in B} \frac{\alpha_l \delta_b^l d_{bt}}{D_t} && \forall l, t \\
& p \ge 0 \\
& x_{gt}, y_{gt}, z_{gt} \in \{0,1\} && \forall g, t
\end{aligned}
$$

- Let $\gamma > 0$ be a secret number
- Let $\alpha_l > 0$ be a secret number, for every transmision line l
- Let $p_{gt} \leftarrow D_t \bar{p}_{gt}$
- Let $p_{gt}^k \leftarrow D_t \bar{p}_{gt}^k$

Privacy-Preserving Transformation for SCUC

Security

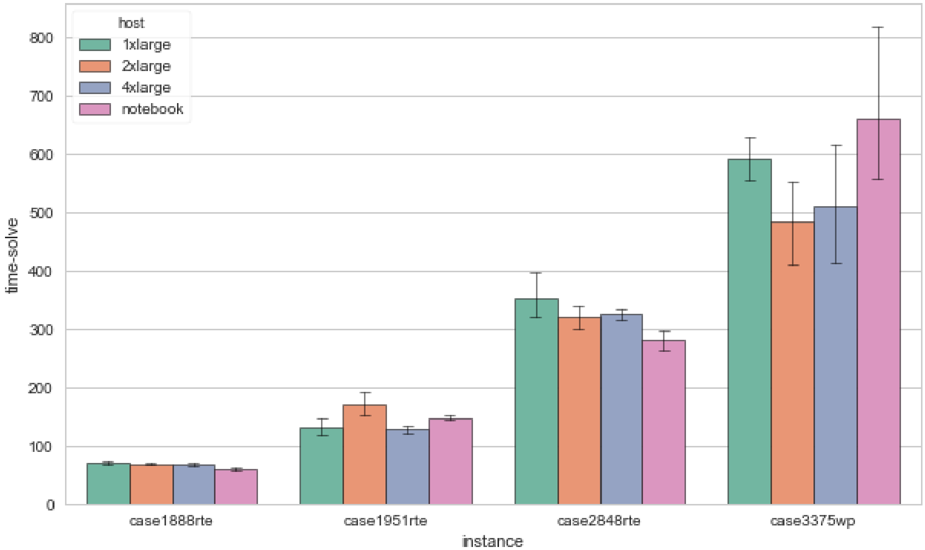
- Partially secured (absolute values protected but not relative values)
  - Start-up, shutdown, production costs, generation capacities, ramping rates, demands
- Perfectly secured
  - Network topology (PTDF matrix) and thermal limits
- Implementation
  - Julia 0.6.4, JuMP 0.18.4, CPLEX 12.8.0
  - GovCloud, SSH



Constraint Matrix after PP Transformation

Performance

solution time comparison

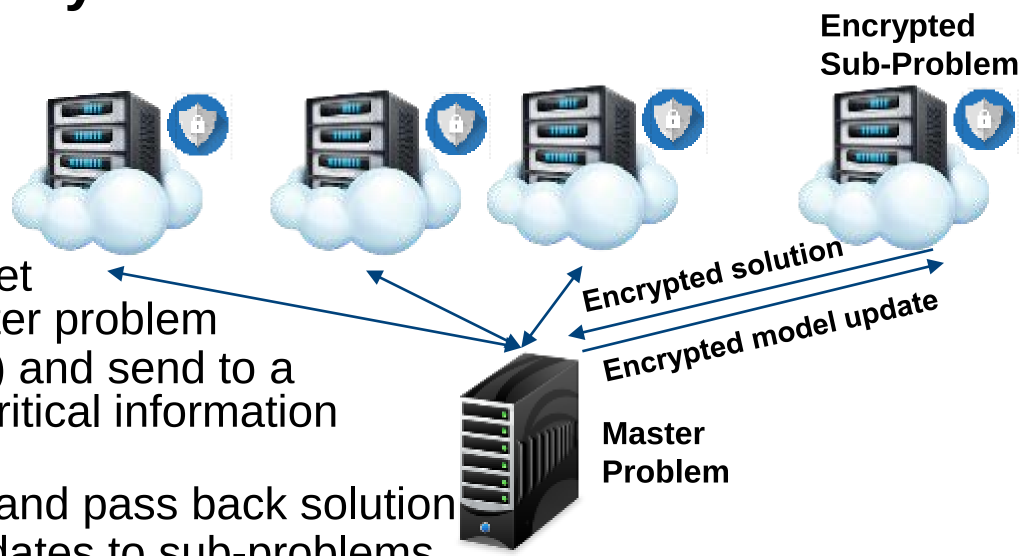


instance	host	t-key	t-enc	t-solve	t-comm	t-total	obj
Case1951	1xlarge	0.08	1.32	131.82	1.32	134.54	52660765
	2xlarge	0.07	1.26	171.42	1.29	174.04	52644059
	4xlarge	0.08	1.33	128.02	1.32	130.74	52676234
	notebook	0.08	1.09	147.73	1.78	150.69	52676234
Case2848	1xlarge	0.36	1.44	352.91	1.36	356.06	53631900
	2xlarge	0.36	1.37	320.33	1.35	323.41	53634704
	4xlarge	0.37	1.45	325.05	1.3	328.16	53634044
	notebook	0.39	1.14	282.3	2.21	286.03	53630267
Case3375	1xlarge	0.12	2.75	592.33	1.97	597.17	46532888
	2xlarge	0.11	2.71	483.33	1.9	488.04	46531362
	4xlarge	0.12	2.77	511.61	1.85	516.35	46525589
	notebook	0.13	2.13	660.2	2.93	665.38	46525413

Distributed Security Enhancement Framework

Advantages of distributed security framework

- Scalability by parallel computing
- Stronger security framework



Distributed security workflow

1) partition the grid application into a set of smaller sub-problems and a master problem
2) Encrypt each sub-problem (with PP) and send to a cloud server; master problem with critical information kept on local
3) Solve each encrypted sub-problem and pass back solution
4) Solve master problem and send updates to sub-problems
5) Iterate until convergence criteria met

Security features

- Hard to track: each time use different partitions, solved on different servers
- Hard to recover valuable information: distributed information; encrypted independently
- Security at multiple levels

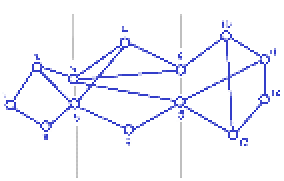
Distributed Security Enhancement Framework

Challenges

- Decomposable structure and sparsity
- Computational performance: convergence, solution time, parallel implementation

Novel decompositions for network constraints

- Reformulations of network constraints that have been used for decades in power engineering
- Sparse and decomposable structure
- Strong computational performance
- Working on distributed computing with security enhancement



Instance:

- Simplified version of Polish test system: 3375 buses, 596 units, 4076 branches and 9 zones

Results:

- 64% reduction in non-zeros
- 2.4x faster running time

Matrix	Reduced MIP nz	Running Time
Original Form.	2,924,357	430 s
Decomposable	1,029,175	178 s

Thank you !

Feng Qiu, PhD
Principle Computational Scientist
Energy Systems Division
Argonne National Laboratory
9700 S. Cass Ave, Lemont, IL 60439
fqiu@anl.gov