RESILIENT AND TRUSTWORTHY CLOUD SECURITY FRAMEWORK FOR POWER GRID APPLICATIONS

Feng Qiu (fqiu@anl.gov), **Alinson Santos Xavier** (axavier@anl.gov)
Center for Energy, Economic, and Environmental Systems Analysis (CEEESA)
Argonne National Laboratory

MOTIVATION

Cloud Computing

- Cloud computing is Powerful, Scalable, Cost-effective
- Nearly half of all companies claim 31% to 60% of their IT systems are cloud-based

Increasing demand for cloud computing in power industry and other sectors

- An example is ISO-NE (55000 simulation hrs/yr on a single machine, expected to grow)
- Global Smart Grid as a Service market expected to grow from $1.3B (2016) to $6B in 2025 [*Navigant Research,* 2016]
- US Department of Defense investing billions to transition to cloud

Weak Cloud Security for Computing

- 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 storage encryption
- Cloud computing is completely vulnerable to insider attacks
- Not suitable for power system computing

HOLISTIC CYBERSECURITY FRAMEWORK

Infrastructure Security

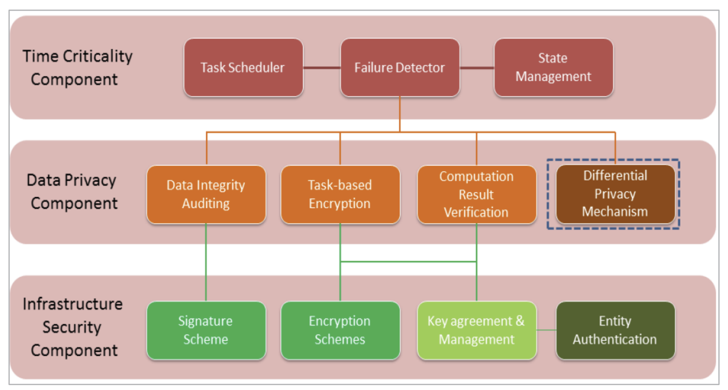
- High confidentiality of power grid data and insufficient cloud security
- Module-based cybersecurity system design for data transmission and storage

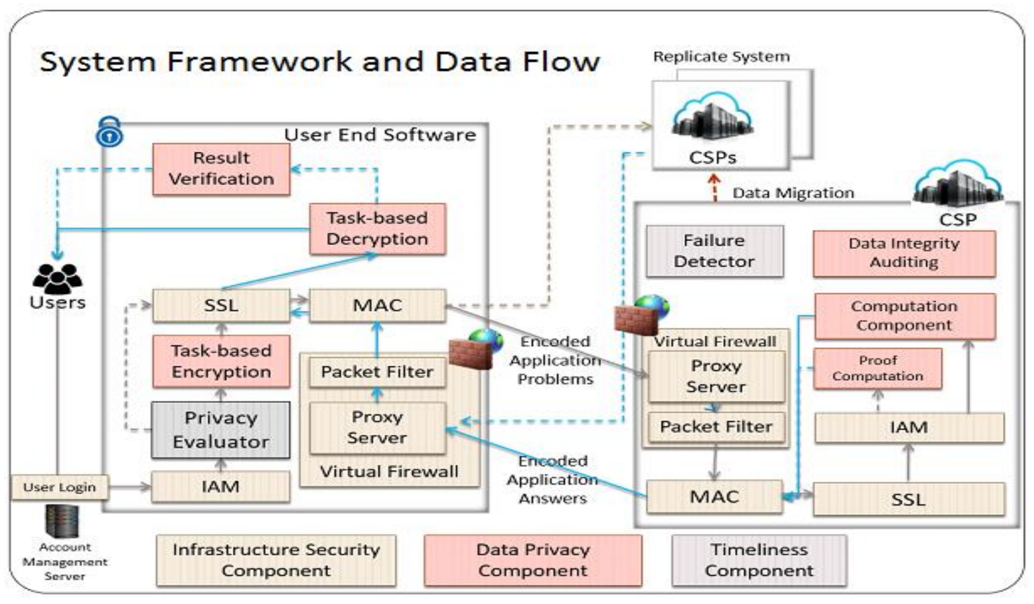
Data Integrity

- 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





TRANSFORMATION-BASED PRIVACY PRESERVING METHOD

Cloud Computing with Privacy-Preserving Security Framework

(1) Transform (encrypt) problems into a "fake" problem; (2) Send "fake" problem to cloud and solve; (3) Fetch "fake" solution; (4) Transform into true solution at local . *Data confidentiality preserved even if cloud security is breached and data are leaked.*

Privacy-Preserving (PP) Transformations

- Multiplying from left/right, scaling and perturbation, shifting
- Privacy-Preserving (PP) transformation ensures correctness of computing, optimality of solutions

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

→ Perturbation/Scaling, Variable shifting →

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

Q a positive monomial matrix

→ Add slack variables, Turn ineq. into eq. →

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

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

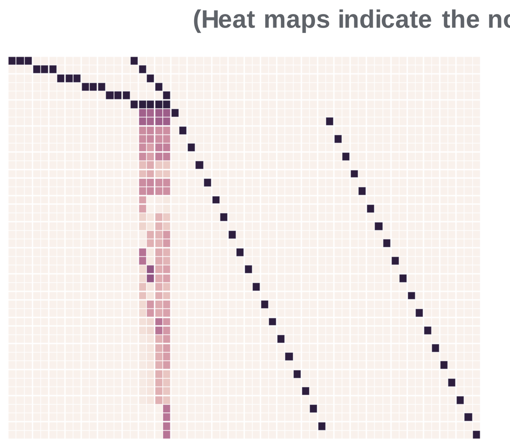
→ Multiplying by random non-singular matrix →

$$\begin{aligned} \min \quad & c_s^{\prime T} z \\ \text{s.t.} \quad M'' z_s &= b'' \\ z_s &\geq 0 \\ M'' &= P * M' \\ b'' &= P * b' \end{aligned}$$

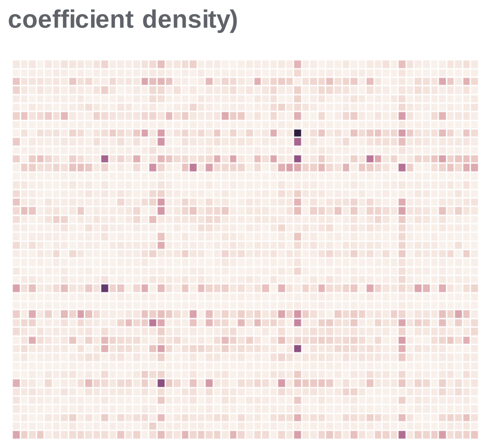
P: non-singular matrix

PP-Security Constrained Economic Dispatch –An Illustration

(Heat maps indicate the no-zero coefficient density)



Original formulation

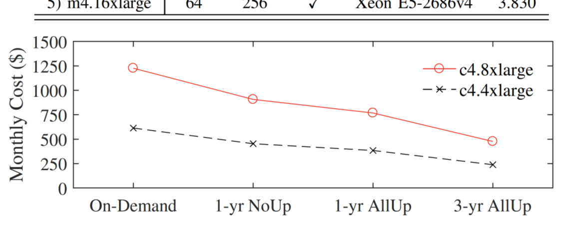


PP Transformation

Cost Comparison AWS Cloud vs HPC

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

Tradeoff Between Computational Performance vs. Security

- SCUC: Computational performance of integer programming is very sensitive to constraint matrix density
- PP transformation can significantly increase computational complexity

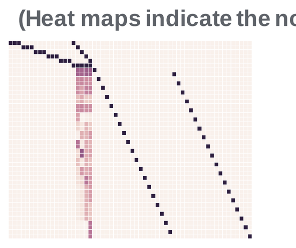
Instances	Instance	Nz Before	Nz After
SCUC(no contingency)	case188	46,976	6,410,880
	case300	73,966	13,524,000

A Shuffling and Scaling Method

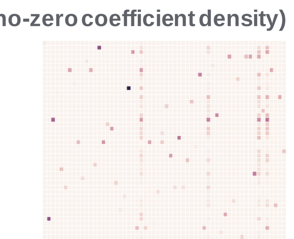
$$\begin{aligned} \text{minimize} \quad & \sum_{t\in T}\sum_{g\in G}\left[c_g^U y_{gt} + c_g^D z_{gt} + c_g^{\min} x_{gt} + \sum_{k\in K} c_g^k p_{gt}^k\right] \\ \text{subject to} \quad & p_{gt} = P_{gt}^{\min} x_{gt} + \sum_{k\in K} p_{gt}^k \\ & p_{gt}^k \leq P_{gt}^k x_{gt} \\ & p_{gt} \leq p_{g,t-1}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

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

(Heat maps indicate the no-zero coefficient density)



Original formulation



Shuffling & Scaling

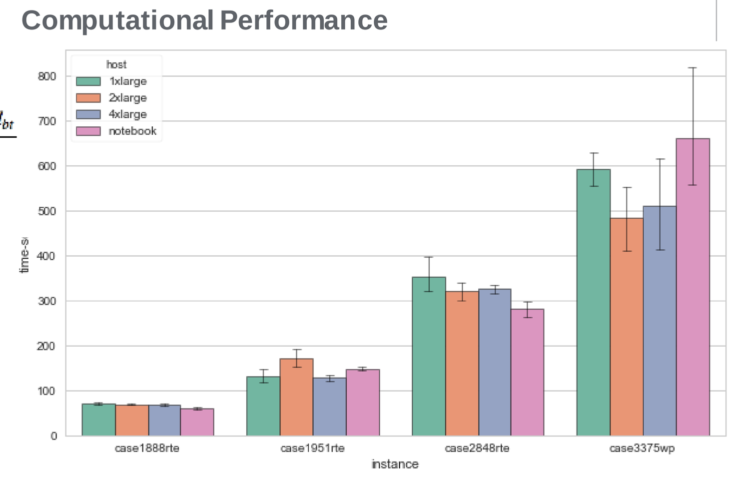
instance	host	t-key	t-enc	t-solve	t-comm	t-total	obj
Case2848	1xlarge	0.36	1.44	352.91	1.36	356.06	53631900
	2xlarge	0.36	1.37	320.33	1.35	323.41	53634704
	4xlarge	0.37	1.45	325.05	1.3	328.16	53634044
	notebook	0.39	1.14	282.3	2.21	286.03	53630267
Case3375	1xlarge	0.12	2.75	592.33	1.97	597.17	46532888
	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

Encryption, communication, and solution time

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

Computational Performance



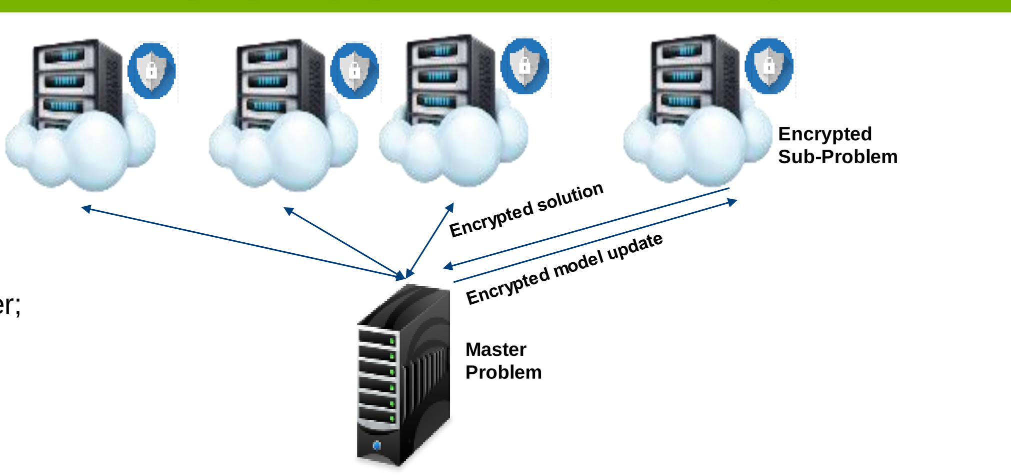
DISTRIBUTED PRIVACY PRESERVING SECURITY ENHANCEMENT

Distributed Security Framework

- Distributed information storage
- Distributed computing

Distributed security workflow

(1) Partition grid application into a set of smaller sub-problems and a master problem
(2) Encrypt each sub-problem (with PP) and send to 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, solve on different servers
- Hard to recover valuable information: distributed information; encrypted independently

Computation features

- Scalability by parallel computing

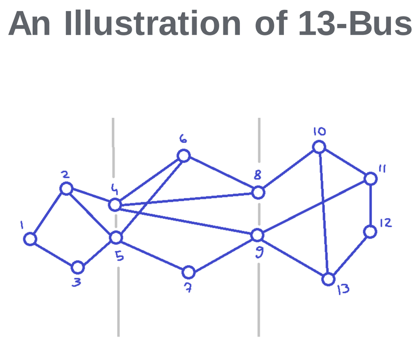
Challenges

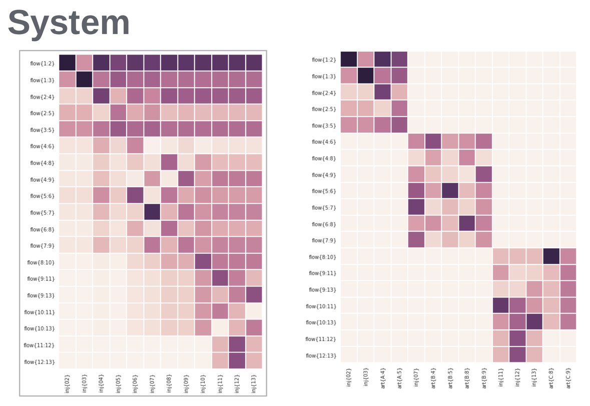
- Decomposable structure and sparsity
- Convergence, solution time, parallel implementation

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

An Illustration of 13-Bus System





Experiments of a 3375-Bus System

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

REFERENCES

- [1] 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.
- [2] "A Resilient and Trustworthy Cloud and Outsourcing Security Framework for Power Grid Applications," ANL/ESD-18/14, Lemont, IL, Argonne National Laboratory.
- [3] "Cyberattacks Against Cloud-based Power System Applications," ANL/ESD-18/16, Lemont, IL, Argonne National Laboratory.
- [4] X. Luo, S. Zhang and E. Litvinov, "Practical Design and Implementation of Cloud Computing for Power System Planning Studies," in *IEEE Transactions on Smart Grid*.
- [5] J. Dreier, F. Kerschbaum. Practical Secure and Efficient Multiparty Linear Programming Based on Problem Transformation. [Technical Report] IACR Cryptology ePrint Archive. 2011.

ACKNOWLEDGMENTS

This project is led by Argonne National Laboratory with support from the US Department of Energy's division of Cybersecurity for Energy Delivery Systems (CEDS) within the office of Cyber Security, Energy Security and Emergency Response (CESER).

THE UNIVERSITY OF CHICAGO
U.S. DEPARTMENT OF ENERGY
Argonne National Laboratory is a U.S. Department of Energy laboratory managed by UChicago Argonne, LLC.
Argonne NATIONAL LABORATORY