Security and Cloud Outsourcing Framework for Economic Dispatch

Mushfiqur R. Sarker, *Member, IEEE*, Jianhui Wang, *Senior Member, IEEE*, Zuyi Li, *Senior Member, IEEE*, and Kui Ren, *Fellow, IEEE*

***Abstract*—The computational complexity and problem sizes of power grid applications have increased significantly with the advent of renewable resources and smart grid technologies. The current paradigm of solving these issues consist of in-house high performance computing infrastructures, which have drawbacks of high capital expenditures, maintenance, and limited scalability. Cloud computing is an ideal alternative due to its powerful computational capacity, rapid scalability, and high cost-effectiveness. A major challenge, however, remains in that the highly confidential grid data is susceptible for potential cyberattacks when outsourced to the cloud. In this work, a security and cloud outsourcing framework is developed for the Economic Dispatch (ED) linear programming application. The security framework transforms the ED linear program into a confidentiality-preserving linear program, that masks both the data and problem structure, thus enabling secure outsourcing to the cloud. Results show that for large grid test cases the performance gain and costs outperforms the in-house infrastructure.**

***Index Terms*—Cloud computing, economic dispatch, high-performance computing**

I. Introduction

With the advent of renewable resources and smart grid technologies, power grid applications, e.g., economic dispatch (ED), have increased in computational complexity and problem size. As a solution, high-performance computing (HPC) infrastructure is a necessity for system operators (SO) to solve such intensive power grid applications. Traditionally, however, HPC infrastructure is hosted by SOs in local computing environments (e.g., by ISO New England [1]), which mandate high capital expenditures and maintenance, while limiting rapid scalability.

On the other hand, cloud computing is an ideal alternative to in-house HPC. Cloud computing provides powerful computational capacity, rapid scalability, and high cost-effectiveness [2]–[4]. Therefore, by outsourcing grid applications to the cloud, the SOs can potentially reduce computational solve time, reduce ongoing operating costs [5], and exploit enhanced applications (e.g., contingencies, uncertainty management, among others). The benefits and challenges associated with cloud computing for power grid applications have been studied extensively in the literature, such as in [3], [4], [6]. A major challenge remains in the confidential-nature of power grid data within the applications, which makes direct deployment in the cloud nonviable because of the potential for cybersecurity attacks [7]. If proper measures can be developed to safeguard applications from insider and outsider attackers, and even malicious cloud service providers (CSP), then it will offer significant benefits to the power system field.

ED [8] is a power grid application that is performed in the real time by SOs (e.g., PJM [9], ERCOT [10], ISO-NE [11], among others) to ensure the generation dispatch meets the demand requirements at the least cost, while ensuring transmission limits are met. However, the ED applications include confidential grid data, such as generation-specific and network-specific data, that must be safeguarded. Access to such data by malicious entities, i.e., those attempting to exercise market power for profitability [12], [13] or worst-case forcing system blackouts, may cause significant economic damages [14]. The challenge remains for these SOs to deploy frequently run ED into the cloud while assuring confidentiality of power grid data. Intensive research has been conducted on the potential adverse outcomes of cyberattacks on the grid. A series of works in [12], [13] looked at the potential profitability of malicious entities when false data injection attacks are performed on ED. Another work [15] studied the economic profitability of entities that conduct power grid network topology data attacks with virtual market bids. Such challenges in [12], [13], [15] will be even more imminent as ED is openly outsourced to the cloud. Therefore, it will be necessary that proper techniques are used to ensure the cloud is secured against cyberattacks.

From a security perspective, extensive research has focused on protecting data transfers and storage via various authentication and authorization approaches (e.g., encryption-based in [16], [17] and/or public key infrastructure in [18]). Although these types of work add a mandatory layer of security, they still present risks if a malicious entity is able to obtain the stream of data and authentication/authorization scheme information. On the other hand, these works do not hide the mathematical structure of the cloud application being solved. Other categories of research performed in [19]–[21] explored methods to transform linear programs (LP), which is the mathematical technique used to solve ED, to a masked LP outputting an identical optimal solution. Such approaches have dual benefits, where (1) the confidential power system data is masked to the extent that a malicious entity cannot discern the context, and (2) the LP problem itself is transformed in a way that does not reveal the specific application being solved.

Limited pioneering works exist on bridging the gap from a public to a confidentiality-preserving ED application in

This work was supported by the U.S. Department of Energy (DOE)'s Office of Electricity Delivery and Energy Reliability Cybersecurity for Energy Delivery Systems (CEDS) program. Authors are with Argonne National Laboratory, State University of New York at Buffalo, and Illinois Institute of Technology (email: mushfiqsarker@gmail.com, jianhui.wang.@anl.gov, kuiren@buffalo.edu, lizu@iit.edu).

[22]–[25]. In [22], a multi-party model is developed that is then masked to ensure each participating party does not obtain knowledge of another party. A distributed algorithm for solving ED was developed in [23] while considering a secure sum protocol to ensure power grid data confidentiality. The approach hides only the generator cost functions, limits, and power output from other generation companies in order to minimize market power. However, a more holistic approach is needed to hide all power grid data such that all malicious entities, whether that be a generation company or outside/inside attackers, have no access to confidential power grid data. The works in [24], [25] developed a data-masked OPF problem that preserves the power system structure. However, by revealing the structure, critical power grid information becomes public, which enables malicious entities to learn about the power system. An ideal solution method is to not only mask the sensitive power system data (e.g., system connectivity, generation limits, among others) but also the structure of the ED problem; i.e., problem constraints should not be easily distinguishable from one another.

The work in this paper focuses on implementing a holistic cloud security and outsourcing framework for the ED application. Within the security framework, the traditional ED is transformed into a confidentiality-preserving linear program (CPLP) formulation. This formulation is used to generate a set of masked random matrices with the classified power grid data in an offline manner. The process does not publicly reveal any confidential data or problem structure of the ED. Within the outsourcing framework, the SO transmits the masked matrix data to the cloud, where the CPLP problem is solved. The holistic framework ensures (1) the SO's computing infrastructure is reduced, (2) the grid data transmission and storage is highly secured, and (3) the SO invokes the cloud to provide the equivalent ED solution in a confidential manner.

The major contributions of this work are as follows:

- Development of a holistic cloud outsourcing and security framework for LP applications, such as ED,
- Development of a CPLP for the ED application that ensures security of sensitive power system data, and
- Assessment of computation times and costs when implementing the framework on cloud infrastructure.

The remainder of this paper is organized as follows. Section II describes the benefits and challenges of cloud computing, discusses the potential cyberattacks, and formulates the CPLP. Section III and Section IV discuss the security and cloud outsourcing framework, respectively. Section V presents the results of the framework applied on the cloud and Section VI concludes the paper.

II. Cloud Computing for Power Systems

Fig. 1 shows the connectivity scheme for the local in-house and the cloud infrastructure. The current computing paradigm for an SO is in-house HPC infrastructure, which has the benefit of data and infrastructure security because minimum outgoing communication of sensitive grid data is required under a local infrastructure. However, the flexibility to enhance computational capacity becomes a bottleneck, because marginal performance increases require high capital expenditures and maintenance. On the other hand, a paradigm shift to cloud computing introduces numerous benefits. The intensive computational capacity and rapid scalability available in the cloud opens new opportunities for SOs to perform complex grid simulations at a typically lower cost [1]. The interested reader is encouraged to refer to [1], [6] for the benefits of cloud computing.

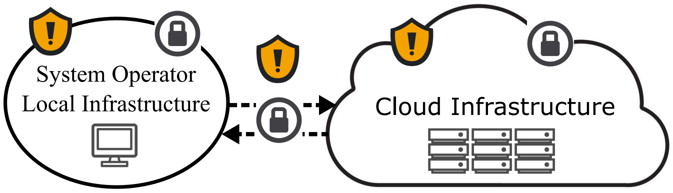


Fig. 1. Connectivity between SO's in-house computing infrastructure and the cloud. Individually, it is assumed each entity employs standard security protocols (e.g., encryption).

The major challenge of cybersecurity attacks exists when power grid applications are performed on the cloud. Attacks may occur in three distinct locations in the connectivity between the SO and the cloud: (1) at the local infrastructure, (2) the communication channel, and (3) on the cloud itself, as illustrated in Fig. 1. The worst-case attacks at all locations will occur from *outsiders* who are categorized as *passive* (i.e., only monitors the data throughput) or *active* (i.e., alters data maliciously) entities. The outsiders do not have system-level privileges to perform such tasks and are treated as malicious entities.

Other categories of attacks may originate from insiders, either passively or actively. These may include malicious local administrators in the computing infrastructure under the SO's jurisdiction. Alternatively, the CSP may passively (honestly yet curiously) monitor the data or even, in the worst case, actively alter data. However, active data manipulation by the CSP would drastically reduce trust in the provider and would violate data privacy policies (see [26], [27] for details on cloud policies and trust maintenance). In general, proper protocols must be enacted by the SO to protect against such attacks.

A holistic security and outsourcing framework must ensure appropriate mechanisms are established so that outsiders and insiders, either actively or passively, cannot gain proprietary knowledge or alter operations of the power grid, in this case ED. In general, it is assumed the local in-house infrastructure has basic security measures (e.g., data encryption, vetted administrators, and others) and the interested reader is encouraged to refer to [18], [28] for design of such secured infrastructure. On the other hand, and in general for the cloud, CSPs provide multilayer trust and security mechanisms within their services [26], [27]. The framework developed in this work is therefore an additional layer of security against potential cyberattacks for sensitive power grid data used in cloud-based ED.

A. Holistic Security and Outsourcing Framework

Fig. 2 shows the process of data transfer between the SO and the cloud, and the timeline. The holistic framework consists of two sub-frameworks: SO offline security and the online cloud outsourcing framework. Within the SO's offline security

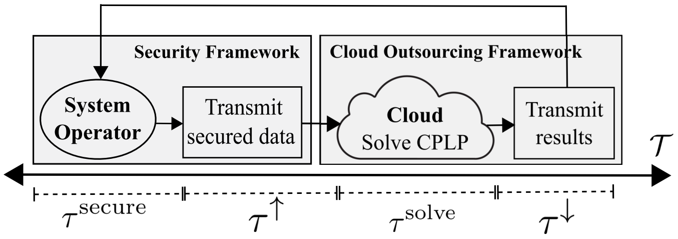


Fig. 2. Security and cloud outsourcing framework process.

framework, local computing infrastructure is used to secure the ED application demanding τ^{secure} time, and then the data is transmitted to the cloud demanding $\tau^{\uparrow}$ time. The benefits of the security framework are twofold. First, the sensitive grid data is stored on locally SO managed computing, and second, the sensitive data is masked so that it can be securely outsourced to the cloud. It is important to note that the security framework should be performed in advance (offline) of the actual real-time period when ED is to be solved. For example, the SO may perform the framework immediately after the real-time market closure. Such an option does not require alterations to the current market operating structure of the SO.

After processing the security framework and as the time approaches for ED initiation, the online outsourcing framework solves the CPLP in τ^{solve} time after receiving the secured data. The optimal results are then transmitted back to the SO in $\tau^{\downarrow}$ time. The CPLP model does not resemble the typical ED model, so malicious entities are unable to observe the type of simulation being performed, which is a major benefit of the cloud outsourcing framework. This process shown in Fig. 2 is repeated based on the specific market rules (*e.g.* every 5-minutes) set forth by the SO.

The total computation time for an instance of ED solved within the holistic framework is calculated as follows

$$\mathcal{T} = \left[\tau^{\text{secure}} + \tau^{\uparrow}\right] + \left[\tau^{\text{solve}} + \tau^{\downarrow}\right] \tag{1}$$

where the first and second bracket represents the computation time for the security and cloud framework, respectively, as illustrated in Fig. 2.

The following section will introduce the basis of the CPLP problem, which is then applied to the ED problem under the security framework, and then followed by the process of cloud outsourcing.

B. Confidentiality-Preserving Linear Program (CPLP)

In linear programs, the variables, parameters, and problem structure are visible. However, such visibility can enable malicious entities (e.g., outsider/insider attackers) to curiously monitor, extract data, or perform false data injections. For example, exposing the ED problem structure can enable malicious entities to understand (1) the specific power system application being solved at that time instance, and (2) the connectivity of generators and transmission lines in a network (i.e., via the power balance constraints). Such open disclosure will enable the malicious entities to recreate the transmission network and effectively learn about its vulnerabilities.

As a solution, the research work in [19] introduced the notion of a CPLP with equality constraints, and then in [20] the approach was enhanced to include inequality constraints. In [19], [20], the CPLP was developed for hiding confidential data from multiple entities participating in a linear program. However, this work assumes a single entity (i.e., an SO) initiates the solution process of the CPLP in the form of ED. The following notations are used in the CPLP problem formulation:

Parameters	
M	Number of constraints
V	Number of variables
$\mathbf{A}$	Constraint coefficient matrix with $\mathbf{R}^{M\times V}$
$\mathbf{b}$	Right-hand side vector with $\mathbf{R}^{M\times 1}$
$\mathbf{c^T}$	Price row vector with $\mathbf{R}^{1\times M}$
$\mathbf{H}, \mathbf{U}$	Diagonal monomial matrix with $\mathbf{R}^{M\times M}$
$\mathbf{I}$	Identity matrix
Variables	
x	Main decision variables
x^s	Auxiliary slack variables used for transformation

C. Formulation

Consider a LP in the form of

$$\min \quad \mathbf{c^T}x \tag{2a}$$

where $\mathbf{c^T}$ is the price vector and x is the variable. The objective function is subject to

$$\mathbf{A}x \leq \mathbf{b} \tag{2b}$$

$$x \geq 0 \tag{2c}$$

where $\mathbf{A}$ is the constraint coefficient matrix with M by V elements (i.e., $\mathbf{R}^{M\times V}$) and $\mathbf{b}$ is the right-hand side (RHS) column vector with M elements (i.e., $\mathbf{R}^{M}$) where M represents the number of constraints and V is the number of decision variables in the LP. Note that in the ED application, the $\mathbf{A}$ matrix holds the variable coefficients of the generator outputs and voltage angles, and $\mathbf{b}$ holds the generator, line, and voltage limits, and the demand at each bus. This standard LP problem in (2a)–(2c) must be transformed into the CPLP structure in order to mask the coefficient matrix $\mathbf{A}$ and RHS vector $\mathbf{b}$, which hold confidential data.

The standard LP problem includes inequality constraints as shown in (2b), which are transformed into equality constraints with the introduction of slack variables, x^s. Note that each constraint requires a single slack variable, such that M slack variables are needed. The constraint is now formulated as

$$\mathbf{A}x + \mathbf{I}x^s = \mathbf{b}.$$

The slack variables x^s in this constraint are multiplied by an identity[1] matrix, $\mathbf{I}$. However, by observing the structure of the problem, it is straightforward for a malicious entity to differentiate exactly the variables which are tied to the $\mathbf{A}$ coefficients, which must remain secure, and those that are for transformation purposes with the identity $\mathbf{I}$ coefficients. To

[1] An identity matrix is a square matrix in which all the elements of the main diagonal are ones and all other elements are zeros.

amend this, as discussed in [20], a privately held and diagonal monomial matrix[2] $\mathbf{U}$ is generated with M by M elements (i.e., $\mathbf{R}^{M\times M}$). The elements of $\mathbf{U}$ are randomly chosen positive real numbers. This matrix is multiplied by the slack coefficients and variable, x^s.

The *transformed yet not confidential LP* can be rewritten as

$$\begin{aligned} \min \quad & \mathbf{c^T} x \\ s.t. \quad & \mathbf{A}x + \mathbf{UI}x^s = b \\ & x, x^s \geq 0 \end{aligned}$$

To mask the data, the entity locally generates a privately held and random diagonal monomial[2] matrix $\mathbf{H} \in \mathbf{R}^{M\times M}$. Similar to $\mathbf{U}$, the elements of $\mathbf{H}$ are randomly chosen positive real numbers. All coefficients ($\mathbf{c^T}$, $\mathbf{A}$, $\mathbf{UI}$, $\mathbf{b}$) of the transformed LP are now multiplied by the random matrix $\mathbf{H}$.

Such multiplication transforms the problem into the CPLP structure and is formulated as follows:

$$\min \quad \mathbf{c^T H} x \tag{3a}$$

$$s.t. \quad \mathbf{HA}x + \mathbf{HUI}x^s = \mathbf{Hb} \tag{3b}$$

$$x, x^s \geq 0 \tag{3c}$$

In this formulation, the entity (SO) only makes public the secured matrices $\mathbf{HA}$, $\mathbf{Hb}$, $\mathbf{c^T H}$, $\mathbf{HU}$. Therefore, the original data in $\mathbf{c^T}$, $\mathbf{A}$, and $\mathbf{b}$ is kept confidential when transmitting and performing the CPLP on the cloud. Without knowledge of the underlying monomial matrices $\mathbf{H}$ and $\mathbf{U}$, the data is secured from potential cyberattacks.

Implementation of the CPLP has three distinct benefits:

1) The CPLP structure includes M randomly generated constraints with random coefficients in each constraint. Therefore, from the perspective of malicious entities, it is not possible to distinguish what type of problem is being solved.
2) Although the output solutions (values of x and x^s) are not masked, it is not possible for a malicious entity to depict the context of each variable without the underlying data in $\mathbf{A}$ and $\mathbf{b}$, which in turn is confidential because of $\mathbf{H}, \mathbf{U}$.
3) The optimal solution obtained under CPLP is the same as under standard LP. This is because the feasible region of the original LP (2a)–(2c) is equivalent to that of the CPLP (3a)–(3c). The objective function, while scaled, produces the same optimal solution.

III. Offline Security Framework Design

To safeguard sensitive grid data when transmitting data or performing the CPLP on the cloud, offline pre-processing of ED data must take place in a local in-house computing environment. The basis of the offline security framework design is shown in Fig. 3. The local computing environment of the SO is assumed to be secured from potential cyberattacks. The interested reader is encouraged to refer to [18] for discussion regarding local computing security.

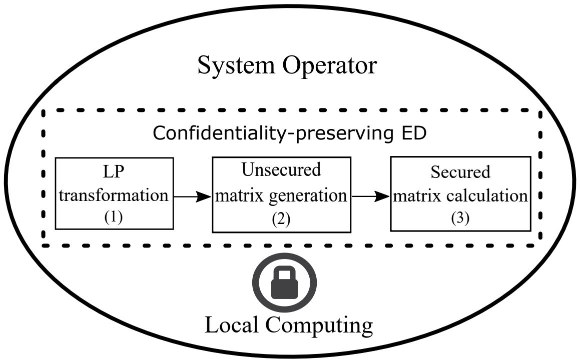

System Operator
Confidentiality-preserving ED
LP transformation (1)
Unsecured matrix generation (2)
Secured matrix calculation (3)
Local Computing

Fig. 3. Offline security framework is performed at the in-house computing infrastructure prior to ED being solved. A three-step process is established to perform an LP transformation, generate the unsecured matrices, and then calculate the secured matrices. It is assumed the in-house infrastructure has preexisting security measures to safeguard against cyberattacks.

Within this offline framework, the SO performs the (1) ED LP transformation, (2) unsecured matrix generation of $\mathbf{A}$, $\mathbf{b}$, $\mathbf{c^T}$, and (3) matrix calculations to secure such matrices against cyberattacks. As a benefit of implementing the holistic framework, the in-house computing infrastructure is not expected to be as powerful as the cloud or currently deployed HPC infrastructure. This is because the ED will be solved in the cloud, and only matrix calculations are performed locally and offline before the actual real-time period when ED must be solved, according to the SO's market rules. Sections III-A through III-C will discuss each of the steps in Fig. 3 in further detail. The notation used for the ED formulation is stated below for reference:

Sets	
S	Set of buses with index b and m
R	Set of all generators with index r
R_b	Set of generators connected to bus b
L	Set of lines connecting bus b to m
ED Parameters	
$B_{b,m}$	Admittance of line connecting bus b to m
C_r	Marginal price of generator r
D_b	Demand at bus b
$F^{\max}_{\{b,m\}}$	Power limit of line connecting bus b to m
π	Voltage angle limit
$I_{\lvert R\rvert}, I_{\lvert S\rvert}$	Square identity matrix (1,0) of size $\lvert R\rvert$ and $\lvert S\rvert$, respectively
N	Arc-node network incidence matrix of size $\lvert S\rvert$ by $\lvert S\rvert$
Variables	
p_r	Power output of generator r
θ_b	Voltage angle of bus b

A. ED LP transformation

For the SO to understand the structure of the CPLP matrices, the ED formulation must be transformed into the LP form shown in (2a)–(2c). The transformed model is formulated as follows:

$$\min \quad \sum_{r\in R} C_r \cdot p_r \tag{4a}$$

[2] A monomial matrix is a matrix where in each row and column there is only one nonzero element. $\mathbf{U}$ and $\mathbf{H}$ are diagonal monomial matrices, where only the main diagonal elements include a nonzero element.

where C_r is the marginal price and p_r is the power dispatch of generator r. The objective function (4a) minimizes the cost of dispatching the generators and is subject to the following constraints:

$$-\left[\sum_{r\in R_b} p_r - \sum_{\{b,m\}\in L|m\geq b} B_{b,m}\cdot(\theta_b-\theta_m) + \sum_{\{b,m\}\in L|m\leq b} B_{b,m}\cdot(\theta_m-\theta_b)\right] \leq -D_b \qquad \forall b\in S \tag{4b}$$

$$p_r \leq P_r^{\max} \qquad \forall r\in R \tag{4c}$$

$$-p_r \leq -P_r^{\min} \qquad \forall r\in R \tag{4d}$$

$$B_{b,m}\cdot(\theta_b-\theta_m) \leq F_{\{b,m\}}^{\max} \qquad \forall \{b,m\}\in B \tag{4e}$$

$$-B_{b,m}\cdot(\theta_b-\theta_m) \leq F_{\{b,m\}}^{\max} \qquad \forall \{b,m\}\in B \tag{4f}$$

$$\theta_b \leq \pi \qquad \forall b\in B \tag{4g}$$

$$-\theta_b \leq \pi \qquad \forall b\in B \tag{4h}$$

In (4c), the system attempts to dispatch generators to meet demand D_b at each bus b, while also considering the power flow through the network. Note that in traditional formulations the power balance constraint is formulated as an equality; however, without altering the solution, it can be formulated as an inequality to conform to the CPLP structure. The next set of constraints in (4c) and (4d) are the maximum and minimum power limits of the generators. The transmission lines within the network have maximum power limits that are modelled as in (4e) and (4f). Similarly, each bus has limits to its voltage angles, which are modelled as shown in (4g) and (4h).

Note that the SO does not solve this transformed ED LP in-house as would be done in the current paradigm. This step in the security framework (Fig. 3) is used to assist in the matrix generation discussed in the following subsection.

B. Unsecured matrix generation for ED

The constraint structure shown in (4b)–(4h) identifies the coefficients of the variables (p_r and θ_b) and the RHS (e.g., D_b, $P_r^{\max}$, among others). With this, the coefficient matrix $\mathbf{A}$ and RHS vector $\mathbf{b}$ are generated for the CPLP problem in the context of ED. The size of these matrices is determined as follows,

$$M = 2\cdot|R| + |R_b| + 2\cdot|L| + 2\cdot|B|, \tag{5}$$

$$V = |R| + |B| \tag{6}$$

where equation (5) calculates the total number of constraints, M, and equation (6) does the same for the total number of variables, V. Note in (5)–(6), the cardinality operator is used to determine the number of elements in each set. To illustrate with an example, for a three-bus system with three lines and two generators, $M = 19$ and $V = 5$, and thus matrix $\mathbf{A}\in\mathbf{R}^{19\times 5}$ and $\mathbf{b}\in\mathbf{R}^{19\times 1}$. The general matrices can be represented as follows:

$$\begin{array}{ccccc} & & \begin{array}{cc} p_r\cdots p_{|R|} & \theta_b\cdots\theta_{|B|} \end{array} & & \text{RHS} \\ \mathbf{A} = \text{Constraints} & \begin{array}{c} \text{(4b)} \\ \text{(4c)} \\ \text{(4d)} \\ \text{(4e)} \\ \text{(4f)} \\ \text{(4g)} \\ \text{(4h)} \end{array} & \left[\begin{array}{cc} \mathrm{R}_{\boldsymbol{b}} & \mathrm{B} \\ \mathrm{I}_{|\mathrm{R}|} & 0 \\ -I_{|R|} & 0 \\ 0 & -B\cdot N \\ 0 & B\cdot N \\ 0 & I_{|S|} \\ 0 & I_{|S|} \end{array}\right], & \mathbf{b} = & \left[\begin{array}{c} -D \\ P^{\max} \\ -P^{\min} \\ F^{\max} \\ F^{\max} \\ \pi \\ \pi \end{array}\right] \end{array} \tag{7}$$

where for the purpose of clarity, each row is labelled with the ED problem constraints (4b)–(4h) that are represented by the coefficients. The matrix $\mathbf{A}$ includes two columns that correspond to the decision variables' coefficients. The first column represents the coefficients of the generator power outputs, p_r, whereas the second column is tied to the voltage bus angles, θ_b. The price row vector is also created as shown in (8), where each element represents the marginal price of generator r.

$$\mathbf{c^T} = \left[C_r \cdots C_{|R|}\right] \tag{8}$$

An advantage of this approach is that the data involved in the matrices ($\mathbf{A}$, $\mathbf{b}$, and $\mathbf{c^T}$) are preexisting in the current operating paradigm of the SO. The matrices, however, hold sensitive data regarding the power grid and generator operating conditions. To conform to the security framework, the matrices must be secured.

C. Secured matrix calculation for ED

Under the CPLP structure, the privately held random matrices $\mathbf{H}$ and $\mathbf{U}$ are constructed by the SO as shown in (9).

$$\mathbf{H} = \begin{bmatrix} h_{1,1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & h_{M,M} \end{bmatrix}, \; \mathbf{U} = \begin{bmatrix} u_{1,1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & u_{M,M} \end{bmatrix} \tag{9}$$

To mask the sensitive matrices, the SO calculates the following: $\mathbf{HA}$, $\mathbf{Hb}$, $\mathbf{c^T H}$, and $\mathbf{HU}$. The communication between the SO and the cloud consists of only these secured matrices, which to malicious entities appear as random sets of data with no distinguishable characteristics to the power system. Without knowledge of $\mathbf{H}$ and $\mathbf{U}$, attackers cannot obtain the grid data, and therefore the SO must privately safeguard these original random matrices.

D. Enhancements to ED-based CPLP

The unique structure of ED enables enhancements to be made on the CPLP to improve computations and security. Four enhancements are discussed below.

1) Reduced matrix generation and calculations

Depending on the size of the ED problem (i.e., M and V), frequent instantiation of the coefficient, RHS and cost matrices, and random matrice calculations may be computationally intensive. Data in $\mathbf{A}$ consists of the power grid network (generator, line, and bus connectivity, and line admittance), which do not change for ED. Similarly in the RHS matrix $\mathbf{b}$, the bottom portion (line flow and voltage angle limits) does not change, but the upper portion (D and $P^{\max}/P^{\min}$) varies in every instance of ED. On the other hand, the price row vector $\mathbf{c^T}$ is based on the generator bids that change in every instance of ED as well. Given these facts, the instantiation of the non-variable $\mathbf{A}$ and bottom portions of $\mathbf{b}$ should be performed once by the SO, unless changes are made to the overall grid network, and updates can be made as needed to the variable portion of $\mathbf{b}$ and the price vector $\mathbf{c^T}$. Therefore, secured matrix calculations for $\mathbf{HA}$ and $\mathbf{HU}$ do not need to occur in every instance of ED. However, frequent generation of the random $\mathbf{H}$ and $\mathbf{U}$ matrices will lead to a more secure outsourcing framework because each instance will be different from the previous one.

2) Improving security with randomly ordered $\mathbf{A}, \mathbf{b}$

The overall security can be increased by randomly or systematically sorting the rows of the $\mathbf{A}$ and $\mathbf{b}$ matrices prior to multiplying them with $\mathbf{H}$. According to (7), the structure shown presents all power balance coefficients followed by generator limits coefficients, and so on, which may lead to possible pattern detection by attackers. Sorting the rows (e.g., a single bus power balance coefficients can be followed by a single generator limit coefficients, and so on) adds another layer of obscurity to the data without a distinguishable pattern.

3) Improving security with randomly ordered $\mathbf{HA}$*,* $\mathbf{HU}$*,* x^*

Since the output solutions (x and x_s) are not masked, malicious entities can still obtain the solutions to the optimization problem. To remedy this, a column-based randomization of the masked matrices can occur locally by the SO prior to outsourcing the problem to the cloud. After creation of $\mathbf{HA}$ and $\mathbf{HU}$, these both can be augmented and instead of two variables (x and x_s), a single representative variable x^* can be used. This transforms equation (3b) as follows

$$(\mathbf{HA}|\mathbf{HU}) \cdot x^* = \mathbf{Hb}$$

where as-is with no randomization, the order of $x^* = \left(\begin{smallmatrix} x \\ x^s \end{smallmatrix}\right)$, which remains similar to equation (3b) where the terms are separate instead of augmented. To ensure security of the optimal solutions, however, column-based randomization is performed on the augmented matrix $\mathbf{HA}|\mathbf{HU}$ and its corresponding variable x^* column vector.

For example, assume an LP with two constraints $M = 2$ and two decision variables $V = 2$. With the CPLP transformation, an additional two auxiliary variables are required for masking. Therefore, the augmented matrix has a size of 2-by-4 and x^* is a column vector with 4 variables (i.e., two decision and auxiliary variables, respectively). Without randomization $x^* = [x_1 \quad x_2 \quad x_1^s \quad x_2^s]^{\mathrm{T}}$ and thus the malicious entity knows the first two columns correspond to decision variables. With randomization, x^* can be randomized, e.g., $x^* = [x_1^s \quad x_2 \quad x_4^s \quad x_1]^{\mathrm{T}}$, with a similar corresponding column order in the augmented matrix. Given this, the malicious entities now have no knowledge of which variables are related to the optimal decisions.

4) Enhanced ED problems

The standard ED problem can be further enhanced to consider contingencies (i.e., security-constrained ED) by expanding the data matrix $\mathbf{A}$ and $\mathbf{b}$ with each contingency data. The benefit is that the SO can use the CPLP structure developed in Section III-A to perform the standard or enhanced versions of ED.

The following section discusses the cloud outsourcing framework based on the secured matrices and the CPLP problem residing on the cloud.

IV. Cloud Outsourcing Framework Design

The SO outsources the simulation process of the CPLP problem to the cloud to exploit its powerful computational capacity, scalability, and cost-effectiveness. The outsourcing process can be separated into secure data transmission to and from the cloud, and solving the optimization in the cloud.

As discussed, the SO only transmits the secured random matrices ($\mathbf{HA}$, $\mathbf{Hb}$, $\mathbf{c^TH}$, $\mathbf{HU}$) developed in Section III-C. The SO transmits the secured matrices by leveraging existing Internet-based communication channels (e.g., File Transfer Protocol (FTP)). An illustration of the communication connectivity between the SO and the cloud is shown in Fig. 1. The cloud holds the ready-to-solve standard CPLP in equations (3a)–(3c) and waits for the SO to transmit the matrices and invoke the simulation. The cloud solves the CPLP with the given matrices and the solutions are then transmitted back to the SO.

V. Simulation Results

The proposed framework is applied to the 2383-bus Polish system, which is a portion of the greater European system. The system includes 327 generators connected to 2383 buses, with 2896 lines supplying 24,558 MWh of total demand. The data for this system was obtained from the MatPower library [29]. The test case was studied in a local in-house environment under Argonne National Laboratory's Blues HPC (ANLBlues) [30]. On the other hand, four types of Amazon EC2 instances were employed to showcase the proposed cloud-based framework similar to [1]. Amazon EC2 is an elastic cloud computing infrastructure that provides rapid scalability with various cost-effective pricing structures [26]. Note the ED framework was performed on one computing cloud instance; however, different families of instances were tested to determine the one that provides the best performance. The local and cloud infrastructures are summarized in Table I. The data for Amazon EC2 instances (c4.2xlarge, c4.4xlarge, c4.8xlarge, and m4.16xlarge) and the ANLBlues was obtained from [31]–[32] and [30], respectively. The hourly usage price for a local in-house infrastructure (e.g., ANLBlues) was obtained from a total cost analysis performed in [5], while assuming the 16 central processing units (CPUs) were being used to full capacity at all times, thus providing the least-cost estimate.

The Amazon C4 instances are equipped with high-performance processors ideal for computationally intensive applications, whereas the M4 instances provide an overall balance of computing, memory, and network resources. Note that it is not in the scope of this work to compare and contrast the architectures of the infrastructures; instead, the purpose of this work is to present the benefits of cloud computing for power grid applications in terms of computational times and costs. In general for ED, the data transmission times $\tau^{\uparrow}$, $\tau^{\downarrow}$ in

TABLE I
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

equation (1) are negligible[3] compared to the matrix generation and/or solve times. For simplicity, the data transmission times are ignored in consequent computational analysis.

In ANLBlues, the model was fully developed in GAMS [33] and solved using IBM's CPLEX [34]. For the cloud-based framework, Matlab R2016b [35] was first used to develop the secured matrices (see Fig. 3) on local in-house computing infrastructure. It was then outsourced to Amazon EC2, where the CPLP model was developed under GAMS and solved using IBM's CPLEX. Regardless of the computing paradigm, the optimal solution to ED is equivalent in all cases.

A. *Computational analysis of the security framework*

In the typical operating paradigm, the ED application is fully processed and solved using commercial solvers (*e.g.* CPLEX) on locally based HPC infrastructure. However, with the proposed holistic framework, additional matrix calculations within the security framework (see Fig. 3) are mandatory before being outsourced to the cloud and solved using CPLEX. Thus, it is crucial to ensure the additional computational burden of the security framework is minimal for the SO.

Based on the unique ED problem structure, secured matrix calculations for $\mathbf{HA}$ and $\mathbf{HU}$ do not need to take place in every ED instance. The remaining matrices ($\mathbf{Hb}$ and $\mathbf{c^T H}$), however, must be calculated prior to every ED solve, in other words, after real-time market closure. Note that further details regarding this enhancement were discussed in Section III-D1. Table II categorizes the matrices based on one-time and variable calculations and then presents their dimensions, computational complexities, and calculation time for the 2383-bus test system. The breakdown of the calculation time shows the total variable calculations (1.326 seconds) are an order of magnitude less than the total one-time calculations (51.47 seconds). Furthermore, performing the optional security enhancements discussed in Section III-D2 and Section III-D3 requires an additional 1.24 and 0.98 seconds for the row-based and column-based randomization, respectively. Note that the best practice is to perform the data randomization frequently, such that the variable time shown in Table II will require an additional 2.22 seconds thus totaling 3.546 seconds. Given this, the security framework adds minimal computational burden to the operations of the SO prior to cloud outsourcing.

B. *Computational analysis for outsourcing framework*

To be viable, the performance gain in terms of the solve time τ^{solve} for the online outsourcing framework must outperform the same framework applied to a in-house HPC (ANLBlues). To obtain an average solve time, Monte Carlo simulations of the framework were performed over 1000 trials of the same ED data. Numerous trials are needed for accurate time estimates, because cloud infrastructures are multi-user facilities with shared resources. Note that such a study should be performed by the SO to compare performance gains of their specific local computing environment and the cloud.

TABLE II
SECURITY FRAMEWORK MATRIX CALCULATIONS FOR CPLP ED

		Dimensions		Complexity	Time (s),
		M	V		τ^{secure}
One-time	$\mathbf{HA}$	13595	2710	$O\left(M^2 V\right)$	9.390
	$\mathbf{HU}$	13595	13595	$O\left(M^3\right)$	42.08
	Total				51.47
Variable	$\mathbf{Hb}$	13595	—	$O\left(M^2\right)$	1.230
	$\mathbf{c^T H}$	—	13595	$O\left(V\right)$	0.096
	Total				1.326

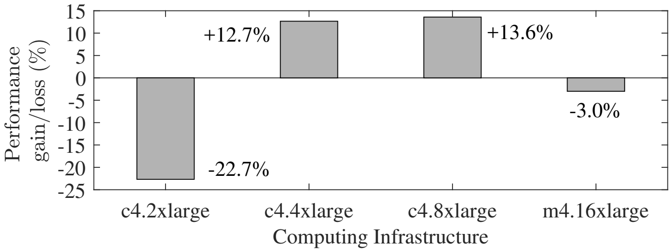


Fig. 4. Performance gain or loss (%). For each instance, the percent change was determined using the average computation time over all trials on Amazon EC2 against the average computation time on ANLBlues.

Fig. 4 shows the performance gain or loss for each cloud instance. The average time was obtained over all the trials, and then the percent change was calculated against the average time for ANLBlues. Compared to ANLBlues, the C4 family of instances from Amazon EC2 has a performance change of -22.7%, +12.7%, and +13.6% for c4.2xlarge, c4.4xlarge, and c4.8xlarge, respectively. The c4.2xlarge instance exhibits a large loss in performance (-22.7%) due to the 50% decrease in CPUs available for processing as compared to ANLBlues (see Table I). On the other hand, even though the M4 family (m4.16xlarge) is equipped with the largest number of CPUs (64) and RAM (256 GB), it performs at a loss of -3.0% compared to ANLBlues, and consequently at a loss compared to the other EC2 instances. This is because the M4 instances are characterized as general purpose, whereas C4 instances are compute-optimized, featuring high-performance processors. The typical ED problem size does not require extensive RAM, as compared to more dynamic grid applications, and instead benefits from high-performing CPUs. CPLEX exploits CPUs by performing concurrent optimization, where different algorithms (such as primal simplex, dual simplex, and barrier, among others) are deployed on multiple CPU threads to solve the LP, which is terminated as soon as a CPU obtains the optimal solution [34]. With this, the C4 instances, specifically c4.4xlarge and c4.8xlarge, outperform M4 instances because the tradeoff between high-performance CPUs outweighs the

[3] Maximum file size that includes the secured matrices for the 2383-bus data is 740 kB, which can be transmitted in milliseconds, especially with C4 and M4 network limits of 4 Gbps [31].

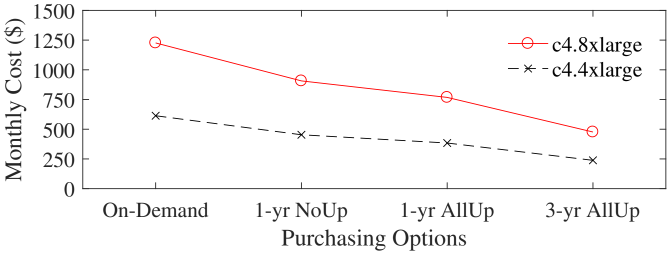


Fig. 5. Effective EC2 monthly usage costs under various purchasing options

larger number of CPUs and RAM.

C. Usage cost analysis

Amazon EC2 has four pricing mechanisms: on-demand pricing, reserved instances, spot instances, and dedicated hosts. The spot instance is a market that allows end-users to bid on spare EC2 capacity at significant discounts, with the drawback that applications should have flexible start/end times and can tolerate interruptions. Such instances are not ideal because ED is time critical for the proper operations of the grid. On the other hand, dedicated EC2s come at a price premium over traditional on-demand EC2s. For the proposed framework, on-demand and reserve instances will be analyzed because they provide the structures that fit ideally with ED.

If an Amazon EC2 instance is launched, end-user billing occurs for all full hours regardless of whether the instance is stopped early due to an application completing in a fraction of an hour. Since ED is performed on a scheduled basis in real time (e.g., every 5 minutes), the EC2 instances are expected to be consistently running. Given this behavior, the total effective monthly usage costs under different purchasing options were analyzed as shown in Fig. 5 for EC2 instances c4.8xlarge and c4.4xlarge, since they both provide the largest performance gain compared to ANLBlues (see Fig. 4). Note that only the usage costs are analyzed because others include fixed costs (i.e., licensing, personnel, among others), which vary highly and will be reduced since CSPs manage the infrastructure.

Fig. 5 shows the costs for the on-demand payment option, in which the SO pays for each instance without long-term commitments. On the other hand, reserve instances, where the SO commits to a 1-year no upfront payment (1-yr NoUp), 1-year all upfront payment (1-yr AllUp), or a 3-year all upfront (3-yr AllUp) payment contract are also shown in Fig. 5. In comparison, the total monthly usage cost for ANLBlues is $2073.60. Therefore, it is evident that a switch to Amazon EC2's c4.4xlarge and c4.8xlarge provides maximum savings of 88.5% and 77.0%, respectively, if the longest term contract is used. On the other hand, the cost increase from c4.4xlarge to c4.8xlarge is approximately 50% for each of the purchasing options. Consequently, the performance gain compared to the in-house ANLBlues is 0.9% from c4.4xlarge to c4.8xlarge as shown in Fig. 4. Theoretically, the tradeoff between the cost and performance gain may not be worthwhile enough to justify the more powerful yet expensive c4.8xlarge over the c4.4xlarge instance.

The analysis presented in Fig. 5 presents an overview of specifically the usage cost. However, when making decisions whether to adopt cloud computing the SO must perform a total cost analysis [5] (i.e., considering facilities, utilities, manpower, among others) to explore the trade-off benefits from in-house computing. The SO must also consider the specific market timing rules, and the potential of other grid applications exploiting the same cloud instances if they are not being fully utilized.

VI. Conclusion and Perspectives

Cloud computing introduces numerous opportunities for power system entities, e.g., system operators (SO), to simulate computationally intensive power grid applications at relatively low costs. Two major challenges must be addressed to exploit the benefits of cloud computing. The first is for these entities to consider security measures to safeguard highly sensitive power grid data when outsourced to the cloud. Second, for typical applications, it is crucial to examine the availability, reliability, and privacy policies of the server instances provided by cloud service providers. It is important for entities to be vigilant in their decision-making process when evaluating the cloud computing paradigm.

In this work, a security and outsourcing framework is developed that enables system operators to take advantage of the powerful computational capacity, rapid scalability, and high cost-effectiveness of cloud computing infrastructure for Economic Dispatch (ED). However, in order to securely outsource ED to the cloud, the confidential power grid data (e.g., generator- and network-related data) must be secured from malicious entities attempting potential cyberattacks. To achieve this, a confidentiality-preserving linear program (CPLP) transformation is applied to ED within the security framework. This approach provides dual benefits, where (1) the confidential grid data is randomly masked so that no malicious entity can discern the context, and (2) the linear program is transformed in a manner that does not reveal the specific application being solved. With the completion of the security framework, the system operator then outsources the simulation process to the cloud. The SO may implement this framework without affecting the current operating paradigm.

The framework was applied to several Amazon EC2 instances and a local in-house high-performance computing infrastructure. Results show increased performance and decreased costs when employing Amazon EC2. Furthermore, it is economic to commit to long-term upfront contracts since costs decrease on average by 61% compared to on-demand usage. In general, the system operator must appropriately choose the specific cloud infrastructures that provide an ideal tradeoff between performance gain and operating costs.

References

[1] E. Litvinov, F. Ma, Q. Zhang, and X. Luo, "Cloud-based next-generation it paradigm for the operations of future power systems," in *2016 Power Systems Computation Conference (PSCC)*, June 2016, pp. 1–7.

[2] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the-art and research challenges," *Journal of Internet Services and Applications*, vol. 1, no. 1, pp. 7–18, 2010.

[3] M. Yigit, V. C. Gungor, and S. Baktir, "Cloud computing for smart grid applications," *Computer Networks*, vol. 70, pp. 312 – 329, 2014.

[4] S. Bera, S. Misra, and J. J. P. C. Rodrigues, "Cloud computing applications for smart grid: A survey," *IEEE Transactions on Parallel*

and Distributed Systems, vol. 26, no. 5, pp. 1477–1494, May 2015.

[5] W. Gentzsch, "A total cost analysis for manufacturers of in-house computing resources and cloud computing," UberCloud, Report, 2016.

[6] D. S. Markovic, D. Zivkovic, I. Branovic, R. Popovic, and D. Cvetkovic, "Smart power grid and cloud computing," *Renewable and Sustainable Energy Reviews*, vol. 24, pp. 566–577, 2013.

[7] K. P. Birman, L. Ganesh, and R. V. Renesse, "White paper - running smart grid control software on cloud computing architectures," Computational Needs for the Next Generation Electric Grid, Report, 2011.

[8] M. B. Cain, R. P. O'Neill, and A. Castillo, "History of optimal power flow and formulations," Federal Energy Regulatory Commission (FERC), Report, 2012.

[9] "How pjm operates & dispatches - pjm." [Online]. Available: www.pjm.com/Globals/Training/Courses/ol-gen-contrl.aspx

[10] "Real time market - ercot." [Online]. Available: www.ercot.com/mktinfo/rtm

[11] "Markets and operations - iso new england." [Online]. Available: www.iso-ne.com/markets-operations

[12] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Trans. on Smart Grid*, vol. 2, no. 4, pp. 659–666, Dec 2011.

[13] D. H. Choi and L. Xie, "Ramp-induced data attacks on look-ahead dispatch in real-time power markets," *IEEE Trans. on Smart Grid*, vol. 4, no. 3, pp. 1235–1243, Sept 2013.

[14] K. H. LaCommare and J. H. Eto, "Cost of power interruptions to electricity consumers in the united states (us)," *Energy*, vol. 31, no. 12, pp. 1845–1855, 2006.

[15] D. H. Choi and L. Xie, "Economic impact assessment of topology data attacks with virtual bids," *IEEE Trans. on Smart Grid*, vol. PP, no. 99, pp. 1–9, 2016.

[16] J. L. Tsai and N. W. Lo, "Secure anonymous key distribution scheme for smart grid," *IEEE Trans. on Smart Grid*, vol. 7, no. 2, pp. 906–914, March 2016.

[17] J. Baek, Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang, "A secure cloud computing based framework for big data information management of smart grid," *IEEE Trans. on Cloud Computing*, vol. 3, no. 2, pp. 233–244, April 2015.

[18] A. R. Metke and R. L. Ekl, "Security technology for smart grid networks," *IEEE Trans. on Smart Grid*, vol. 1, no. 1, pp. 99–107, June 2010.

[19] O. L. Mangasarian, "Privacy-preserving linear programming," *Optimization Letters*, vol. 5, no. 1, pp. 165–172, 2011.

[20] W. Li, H. Li, and C. Deng, "Privacy-preserving horizontally partitioned linear programs with inequality constraints," *Optimization Letters*, vol. 7, no. 1, pp. 137–144, 2013.

[21] C. Wang, K. Ren, and J. Wang, "Secure and practical outsourcing of linear programming in cloud computing," in *INFOCOM, 2011 Proceedings IEEE*, April 2011, pp. 820–828.

[22] D. Wu, B. C. Lesieutre, P. Ramanathan, and B. Kakunoori, "Preserving privacy of ac optimal power flow models in multi-party electric grids," *IEEE Trans. on Smart Grid*, vol. 7, no. 4, pp. 2050–2060, July 2016.

[23] A. Mandal, *Privacy Preserving Consensus-Based Economic Dispatch in Smart Grid Systems*. Springer International Publishing, 2016, pp. 98–110.

[24] A. R. Borden, D. K. Molzahn, P. Ramanathan, and B. C. Lesieutre, "Confidentiality-preserving optimal power flow for cloud computing," in *2012 50th Annual Allerton Conference on Communication, Control, and Computing*, Oct 2012, pp. 1300–1307.

[25] A. R. Borden, D. K. Molzahn, B. C. Lesieutre, and P. Ramanathan, "Power system structure and confidentiality preserving transformation of optimal power flow problem," in *2013 51st Annual Allerton Conference on Communication, Control, and Computing*, Oct 2013, pp. 1021–1028.

[26] "Data privacy - amazon web services." [Online]. Available: aws.amazon.com/compliance/data-privacy-faq/

[27] K. M. Khan and Q. Malluhi, "Establishing trust in cloud computing," *IT Professional*, vol. 12, no. 5, pp. 20–27, 2010.

[28] S. Rusitschka, K. Eger, and C. Gerdes, "Smart grid data cloud: A model for utilizing cloud computing in the smart grid domain," in *2010 First IEEE International Conference on Smart Grid Communications*, Oct 2010, pp. 483–488.

[29] R. D. Zimmerman, C. E. Murillo-Sanchez, and R. J. Thomas, "Matpower: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Trans. on Power Systems*, vol. 26, no. 1, pp. 12–19, Feb 2011.

[30] "Anl laboratory computing resource center (lcrc)." [Online]. Available: www.lcrc.anl.gov

[31] "Amazon ec2 instances - documentation." [Online]. Available: docs.aws.amazon.com/AWSEC2/latest/UserGuide/Instances.html

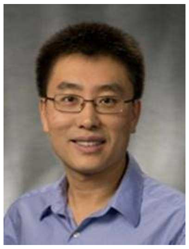
[32] "Amazon ec2 instances - on-demand pricing." [Online]. Available: aws.amazon.com/ec2/pricing/on-demand/

[33] "Gams - a user's guide." [Online]. Available: www.gams.com/dd/docs/bigdocs/GAMSUsersGuide.pdf

[34] "Ibm ilog cplex optimization studio user's manual," IBM, Report, 2015.

[35] MATLAB, *version 7.10.0 (R2010b)*. Natick, Massachusetts: The MathWorks Inc., 2016.

Mushfiqur R. Sarker (S'11) received his B.Sc and Ph.D. degree in electrical engineering from Oregon State University, Corvallis, OR, USA in 2012 and the University of Washington, Seattle, WA in 2016, respectively. He is currently a researcher at Argonne National Laboratories in Lemont, IL. His research interests are in the fields of power system economics, demand-side management, and power system cyber-security.

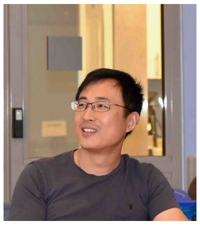


Jianhui Wang (M07-SM12) received the Ph.D. degree in electrical engineering from Illinois Institute of Technology, Chicago, Illinois, USA, in 2007.

Presently, he is an Associate Professor with the Department of Electrical Engineering at Southern Methodist University, Dallas, Texas, USA. He also holds a joint appointment as Section Lead for Advanced Power Grid Modeling at the Energy Systems Division at Argonne National Laboratory, Argonne, Illinois, USA.

Dr. Wang is the secretary of the IEEE Power & Energy Society (PES) Power System Operations, Planning & Economics Committee. He is an associate editor of Journal of Energy Engineering and an editorial board member of Applied Energy. He has held visiting positions in Europe, Australia and Hong Kong including a VELUX Visiting Professorship at the Technical University of Denmark (DTU). Dr. Wang is the Editor-in-Chief of the IEEE Transactions on Smart Grid and an IEEE PES Distinguished Lecturer. He is also the recipient of the IEEE PES Power System Operation Committee Prize Paper Award in 2015.

Zuyi Li (SM'09) received the B.S. degree from Shanghai Jiaotong University, Shanghai, China, in 1995, the M.S. degree from Tsinghua University, Beijing, China, in 1998, and the Ph.D. degree from the Illinois Institute of Technology (IIT), Chicago, in 2002, all in electrical engineering. Presently, he is a Professor in the Electrical and Computer Engineering Department at IIT. His research interests include economic and secure operation of electric power systems, cyber security in smart grid, renewable energy integration, electric demand management of data centers, and power system protection.



Kui Ren is a professor of Computer Science and Engineering and the director of UbiSeC Lab at State University of New York at Buffalo (UB). He received his PhD degree from Worcester Polytechnic Institute. Kui's current research interest spans Cloud & Outsourcing Security, Wireless & Wearable Systems Security, and Mobile Sensing & Crowdsourcing. His research has been supported by NSF, DoE, AFRL, MSR, and Amazon. He received IEEE CISTC Technical Recognition Award in 2017, UB Exceptional Scholar Award for Sustained Achievement in 2016, UB SEAS Senior Researcher of the Year Award in 2015, Sigma Xi/IIT Research Excellence Award in 2012, and NSF CAREER Award in 2011. Kui has published extensively in peer-reviewed journals and conferences and received several Best Paper Awards including IEEE ICNP 2011. He currently serves as an associate editor for IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Service Computing, IEEE Transactions on Mobile Computing, IEEE Wireless Communications, and IEEE Internet of Things Journal. Kui is a Fellow of IEEE, a Distinguished Lecturer of IEEE, a member of ACM, and a past board member of Internet Privacy Task Force, State of Illinois.