SAFE: Secure Appliance Scheduling for Flexible and Efficient Energy Consumption for Smart Home IoT

Sai Mounika Errapotu, *Student Member, IEEE*, Jingyi Wang, *Student Member, IEEE*, Yanmin Gong, *Member, IEEE*, Jin-Hee Cho, *Senior Member, IEEE*, Miao Pan, *Member, IEEE*, and Zhu Han, *Fellow, IEEE*

***Abstract*—Smart homes (SHs) aim at forming an energy optimized environment that can efficiently regulate the use of various Internet of Things (IoT) devices in its network. Real-time electricity pricing models along with SHs provide users an opportunity to reduce their electricity expenditure by responding to the pricing that varies with different times of the day, resulting in reducing the expenditure at both customers' and utility provider's end. However, responding to such prices and effectively scheduling the appliances under such complex dynamics is a challenging optimization problem to be solved by the provider or by third party services. As communication in SH-IoT environment is extremely sensitive and private, reporting of such usage information to the provider to solve the optimization has a potential risk that the provider or third party services may track users' energy consumption profile which compromises users' privacy. To address these issues, we developed a homomorphic encryption-based alternating direction method of multipliers approach to solve the cost-aware appliance scheduling optimization in a distributed manner and schedule home appliances without leaking users' privacy. Through extensive simulation study considering real-world datasets, we show that the proposed secure appliance scheduling for flexible and efficient energy consumption scheme, namely SAFE, effectively lowers electricity cost while preserving users' privacy.**

***Index Terms*—Alternating direction method of multipliers (ADMMs), appliance scheduling, Paillier cryptosystem, smart home (SH).**

Manuscript received November 1, 2017; revised May 22, 2018; accepted July 31, 2018. Date of publication August 24, 2018; date of current version January 16, 2019. This work was supported by the U.S. National Science Foundation under Grant CNS-1801925, Grant CNS-1343361, Grant CNS-1350230 (CAREER), Grant CNS-1717454, Grant CNS-1646607, Grant CNS-1702850, Grant CNS-1731424, and Grant ECCS-1547201. *(Corresponding author: Miao Pan.)*

S. M. Errapotu, J. Wang, and M. Pan are with the Department of Electrical and Computer Engineering, University of Houston, Houston, TX 77204 USA (e-mail: serrapotu@uh.edu; jwang86@uh.edu; mpan2@uh.edu).

Y. Gong is with the Department of Electrical and Computer Engineering, Oklahoma State University, Stillwater, OK 74074 USA (e-mail: yanmin.gong@okstate.edu).

J.-H. Cho was with the U.S. Army Research Laboratory, Adelphi, MD 20783 USA. She is now with the Department of Computer Science, Virginia Polytechnic Institute and State University, Falls Church, VA 22043 USA (e-mail: jicho@vt.edu).

Z. Han is with the University of Houston, Houston, TX 77004 USA, and also with the Department of Computer Science and Engineering, Kyung Hee University, Seoul 02447, South Korea (e-mail: zhan2@uh.edu).

Digital Object Identifier 10.1109/JIOT.2018.2866998

I. Introduction

THE ENERGY demand is exponentially increasing due to the technological advances worldwide. Accordingly, energy efficiency has become one of the major concerns in today's life that significantly affects almost all human activities. This necessity leads to the development of "smart grid" an integration of advanced power system electronics, networking and communication technologies that allows accurate real-time monitoring, ensures the optimization of power flows, facilitates real-time troubleshooting, and enables two-way communication between the utility and customer sides [1]–[4]. These grids are capable of handling uncertainties, incorporating renewable sources, managing and resolving operations during unpredictable events. "Smart homes (SHs)" integrate the smart grids, which report recorded energy consumption through "smart meters" to the grid, while allowing effective household energy monitoring and control [5]. The evolution of Internet of Things (IoT) has further enhanced the actual implementation of networked SHs.

IoT extends the interactions between humans and applications to a new dimension of machine to machine communication. Development of new communication technologies and advanced electrical gadgets operated by understanding signals enhanced the opportunities to control various types of devices in a home. SH-IoT environment enables everyday household objects, electronics and smart appliances to communicate with each other locally or via Internet. The devices in SH are capable of storing data, responding to user commands and sending alerts. Along with flexibility in home management and surveillance, SH-IoT aims at forming an energy optimized environment through connectivity between devices.

Recent studies suggest that residential sector accounts for 37% of total power consumption in the United States. The households of the future need to be significantly smarter and more energy-aware. SHs are expected to dynamically adjust their energy profile according to dynamic prices along with the use of renewable energy sources at home. This reduces the energy consumption, while providing their owners with the opportunity for remote device monitoring and low cost benefits. The data collected from SHs can be integrated with external data, allowing the SH system to make better decisions or provide optimized services. SH-IoT along

with the real time pricing (RTP)/time of use (TOU) tariffs varying throughout the day can significantly reduces the per device energy consumption of users, laying ground for much greener consumption [6], [7]. This is because a residential customer's daily activities are characterized by a list of tasks to be scheduled at preferred time intervals. Some of these tasks are persistent, e.g., the use of a refrigerator, while others can be scheduled according to the user-specified constraints and the variable tariffs offered by the utility company to achieve cost savings by peak demand reduction [6] and by participating in the demand response (DR) programs [8], [9].

Even though the use of RTP in SHs has numerous advantages, there are certain challenges associated with its efficient implementation. In SHs, for efficient energy consumption, the owner decides on appliance scheduling based on the fluctuating electricity price (i.e., whether appliance needs to be used at that particular time, or if renewable energy at home should be used at that time instead). Accordingly, time varying prices along with SHs' flexibility to schedule appliances provide numerous benefits; but optimally scheduling the appliances to reduce the consumption cost is complex for users and utility providers due to the nature of a large scale optimization problem. The utility providers can either solve the problem or leverage such computation to third party services to solve the optimization problem. However, constant reporting of SH' usage information to the utility provider can pose serious concerns to the user's privacy as traffic over SH-IoT is sensitive to timeliness, security, and privacy. Such usage information provides detailed consumption about the home with which they are connected and the devices being used. Collection of such sensitive usage information over time can allow third parties to strongly infer a lot about a user's lifestyle like its presence at home or its day-to-day routine that can breach user's privacy. Since communication and information exchange play an important role in the efficient monitoring and control of SHs and smart grid, smart endpoints introduced in this dynamic network can become portals for intrusion and malicious attacks, leaking sensitive user data over time either during computation or transmission. Due to the increased use of renewable energy at home with the advantage of dynamic pricing, this can be a potential problem in the future.

Despite security and privacy being critical concern in developing smart grid, the research on SH and smart grid security/privacy issues is still in its infant stage [10], [11]. As a result, we are motivated to further investigate these issues in SH environments and their impact on smart grid. Our aim is to contribute to the current state-of-the-art by providing a more comprehensive view of privacy in the SH environment that considers its persistent interaction with the provider for computation. In this paper, we consider the cost minimization for optimal appliance scheduling to be a convex optimization problem.

The optimization problem is solved using the alternating direction method of multipliers (ADMMs) since it has strong convergence properties and its decomposability property of dual ascent. Many existing approaches have addressed optimization problems in SH [8], [9], [12], but little has used the ADMM to solve optimization problems considering privacy issues in SH environments. For this reason, our adopted approach identifies threats that can arise in SH environment due to its interactions with the utility provider and between various entities of the smart grid environment. To address the privacy issues in the SH environment, we propose secure appliance scheduling for flexible and efficient energy consumption (SAFE) for SH-IoT, where the user's sensitive usage information is protected using Paillier cryptosystem. The key contributions of proposed SAFE include the following.

1) We identify the interactions between various entities in SH and smart grid environments; and then classify the risks that threaten these interactions and evaluate their impact on overall system security and user privacy.
2) We solve the optimization problem for SH's efficient energy consumption in fog using ADMM in a distributed manner while preserving the privacy of the home owner based on Paillier cryptosystem.
3) Our simulation results show the advantages of our privacy preserving scheme with dynamic pricing compared to the fixed pricing scheme. Further, we provide the analysis of the observed trends in the results in terms of security, privacy, and performance of the proposed scheme.

The remainder of this paper is organized as follows. Section II briefly describes the related work done. Section III introduces the architecture of the SH environment and interactions with the provider for computation. In addition, the key concerned security goals are addressed along with the identification of threats under representative scenarios of interactions between SH and the provider. Section IV discusses Paillier cryptosystem used to preserve privacy and ADMM used to solve the optimization problem that aims to minimize the cost. Section V describes our model that allows an efficient appliance scheduling while preserving the privacy of a home owner. Section VI provides the security and performance analysis of our scheme. Section VII concludes this paper and suggests future work directions.

II. Related Work

The advent of smart grid, smart meters, low-cost sensors, and smart appliances has led to innovative residential energy management techniques that involve communication and interactions between users, devices and the grid. Such interactions of energy-aware SHs with smart grid ensure the smart grid to meet its major goals, such as managing and resolving demand under uncertainties, load shedding, and/or effective feedback on energy consumption. The interaction not only benefits smart grid, but also allows energy providers and users to incorporate small scale renewable resources for energy generation to keep the electricity demand in line with the supply during peak hours of usage. Such an ability to control the usage is called demand side management (DSM) or DR. DR is essentially an agreement between the utility and its users, promising low tariffs or discounts in their monthly consumption bill, provided that they agree to reduce their consumption in response to signals received by the grid. In the study of dynamic DSM, many different techniques and

algorithms have been proposed, where the underlying rationale was to reduce the energy bill corresponding to the RTP/TOU tariffs incentives offered by the energy provider [6]. TOU tariffs vary throughout the day according to the supply and demand [7]. Most of the utility companies release day-ahead pricing which allows users to schedule appliances in advance. Users can generate renewable energy, consume some portion of it locally, and sell the excess energy to the utility companies when permitted or participating in DR programs to receive incentives or discounts [8], [9], [13]. For example, the Ontario government's micro feed-in tariff program in Canada allows home owners to sell locally generated energy [13], thereby conserving less and having enough power for everyone.

Some existing works [8], [12] investigated these energy consumption problems in SHs to be solved as optimization problems. In [8], a single objective optimization problem was proposed to minimize the total cost of electricity usage at home, considering four appliances based on two competitive optimization algorithms. In [12], optimization of the appliances in a single home is examined based on a convex programming framework whose objective is to minimize both cost and user dissatisfaction. Since the estimated binary status of appliances (i.e., on or off) can relax decision variables from integer to continuous values, the mixed integer linear programming problem can be formulated as a new convex programming problem.

In TOU tariffs, pricing signals indicate the electricity tariff at any time which allow devices to instantly inform the amount of energy (in money) to be spent when switched on at the moment. This mechanism has highly impacted in ensuring a stable and optimal operation of a power system. A residential user's daily activities are characterized by a certain list of tasks that need to be scheduled at preferred time intervals. Some of these tasks are persistent, as they consume electricity throughout the day (e.g., the use of a refrigerator is persistent while others can be scheduled according to the user-specified constraints). Such variable tariffs, offered by the utility company, allow customers to benefit from lower rates when using energy during off-peak hours, resulting in a better distribution of demand due to peak demand reduction [6].

Flexibility, associated with appliances and time varying prices, can achieve numerous benefits for customers. In order to facilitate the users to participate in the DR program and regulate their consumption pattern through pricing signals, studies have suggested employing automated household energy management strategies [14]–[16] in the SH-IoT environments. Therefore, a centrally located automated intelligent device is required to optimize the appliances and load operation on behalf of users. Users of centralized controllers should be able to schedule appliances remotely according to its priority as well as to report the updated usage information to the utility provider in order to minimize its expenditure. But sending such sensitive information to the provider, which may leverage such usage information to third party services for reducing its cost, causes privacy issues. Optimization enables users to efficiently manage the energy consumption at home, but these issues during computation should be addressed to preserve the user's privacy.

In the literature, most of the works focused on the security of the grid servers. Many techniques were proposed to prevent attacks aiming to take down or control servers or to steal data from the servers. As the connectivity amongst different entities of the smart grid and/or the SH increases, the challenges also increase especially those related to system security and user privacy. Some works [10], [17] described the threats of interactions and updates between SH meters and smart grid. However, various interactions between SH entities could also become targets for cyber attacks. In the literature, little has addressed such security and privacy issues in SH-IoT along with personalized home energy management to help the grid meet the demand.

Although many works investigated on SH energy management and security aspects of smart grids separately, privacy issues have not been much investigated in SH energy management which is highly required to meet the growing energy demand. In this paper, we focus on effective and efficient home energy management of users while addressing the security and privacy issues the users encounter to optimize the consumption cost when sending the usage data to the provider. We describe the threat model in Section III. This paper effectively prevents the attacks from targeting various SH entities in the SH-IoT environments and preserves the privacy of users from the considered threats (see Section III), which allows more users to participate in DSM and DR programs.

III. System Architecture and Threat Model

In this section, we first outline the system architecture for SAFE, i.e., secure appliance scheduling for flexible and efficient energy consumption for SH-IoT in Section III-A and discuss the optimization problem in Section III-B. Then, we provide the threat model in Section III-C. Finally, we discuss the design goals we aim to achieve in SAFE in Section III-D.

A. System Architecture

We formulate an optimization problem that aims to reduce expenditures by both customers (i.e., home owners) and utility providers. The problem considers that the home owners need to update their usage information to the utility provider while achieving the goals of their individual subproblems. We consider a set of SH owners $\mathcal{I}$ in a community, indexed by $i = 1, \ldots, I$ that timely updates their usage information to the utility provider for solving the energy consumption cost minimization problem. Each user's home consists of a set of $\mathcal{J}$ of appliances, indexed by $j = 1, \ldots, J$ whose usage information is updated. We consider utility provider P_u aiming to minimize the energy consumption cost. Fig. 1 describes the overall system model. We also have a trusted coordinator, assumed to be a trusted third party (e.g., a government agency or trusted key generation center) [18], [19] that is responsible for public-key-infrastructure-based key management by issuing public key-private key pairs for each utility provider, respectively, and sending only the public keys to the utility providers. The utility providers publish their respective public key to their customers. The home owner resorts to encryption for preserving its privacy by having secure usage data

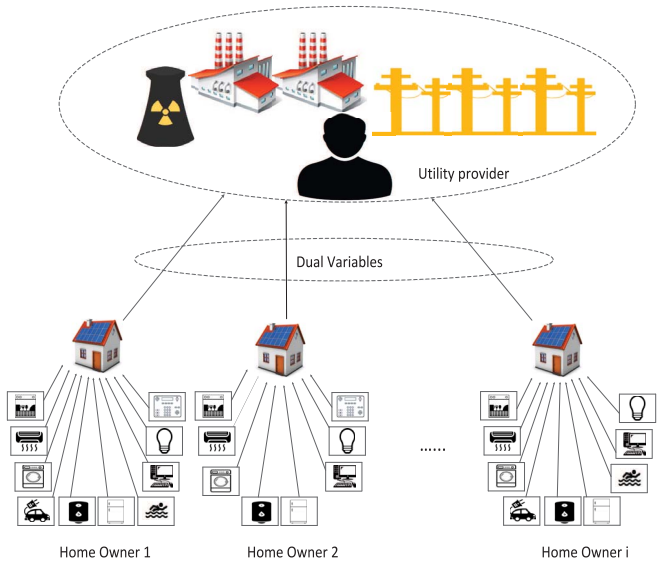

Fig. 1. System architecture of SAFE.

transmission. We consider the home owner to be the centralized controller in a considered SH network. Whenever the energy provider wants to solve the optimization problem, the owner sends the encrypted appliance usage data encrypted with energy provider's public key to the energy provider.

We use $e_{i,j}$ as home owner's usage information that needs to be sent to the provider for solving the problem. The allocation decision variables of user i are denoted by $e_i = (e_{i,1}, \ldots, e_{i,J})$. The owner updates the usage of all the appliances in its SH. In reality, appliances can be devices that have interaction features and can be monitored remotely. For example, if certain appliances cannot be controlled remotely, such access can be enabled using static devices like smart switches. The provider may be limited in its computational capacity CL. Once the utility provider obtains a solution of the optimization problem, the response traffic will be routed back to the home owner. A propagation latency $L_{i,p}$ is observed for transmission between user i and the provider. For simplicity, we interchangeably use the following terms: 1) home owner, user, or customer; 2) trusted coordinator or key generator; and 3) utility provider or resource.

We consider that the energy usage of SH owner comprises of two types of loads: 1) inelastic energy loads and 2) elastic energy loads. *Inelastic energy loads* include lights, microwaves, or computers whose energy requests must be met at the time of need. *Elastic energy loads* (i.e., loads that can be controlled) include smart appliances like air conditioners, dehumidifiers, or electric vehicles which can adjust their time of operation. Elastic loads can be scheduled to operate when the electricity price is low, significantly reducing the energy consumption cost. SH owners may possess distributed renewable generator like roof top solar panels installed at their site. Note that the power generation from renewable sources is lower than the normal power consumption of the households and the households are connected to the utility provider for back-up power. The energy consumption of the SH owner from the utility provider is the additional amount of energy he/she requires to meet the elastic and inelastic loads after utilizing the renewable energy generated at home.

The performance objective of the user is formulated based on the user's utility function, denoted by $U_i(\cdot)$ based on the scheduling of appliances. In this paper, $U_i(\cdot)$ is designed to be a nondecreasing, non-negative and concave function in e_i. A simple example is shown as

$$U_i(e_i) = \sum_{j \in \mathcal{J}} e_{i,j}\left(L_{\max} - L_{i,p}\right) \tag{1}$$

where $L_{\max}$ is the maximum tolerable latency for service requested, or can be a general class of functions that represent the elasticity of the service request or determine the fairness of resource allocation. $L_{i,p}$ is the transmission latency between user i and provider.

We characterize the performance objective of the provider in terms of the energy consumption cost given by function $C_p(\cdot)$ that changes due to the varying RTPs. Here, we consider the consumption cost to be a nondecreasing, non-negative, and concave function in $e_{i,j}$. A simple example can be given by

$$C_p(e_i) = \Pr_t \times \left[P_{\text{idle}} + \left(P_{\text{peak}} - P_{\text{idle}}\right) \sum_{i \in \mathcal{I}} e_i \right] \tag{2}$$

where $\Pr_t$ is the spot electricity price at time t, P_{idle} is the degree of idle power, and P_{peak} is the degree of peak power.

The price $\Pr_t$ changes over time and is usually high during the peak hour, while solving the optimization problem the price at that time point is considered. This consumption cost also scales with the number of appliances at home. If we have renewable energy resources at home, this total consumption cost also includes the cost pertaining to the renewable resources while solving individual subproblems. The cost for using renewable resources accounts for installation, i.e., usually one time investment which lasts for a longer period of time. We do not consider the cost for the installation of renewable resources (e.g., solar panels) in our total consumption cost as a subproblem.

B. Efficient Energy Consumption Problem

The efficient energy consumption can be regulated by formulating the optimization problem with the aim of minimizing the cost of the provider as follows:

$$\underset{\{e_i\}_{i=1}^{N}}{\text{minimize}} \sum_{i \in \mathcal{I}} C_p(e_i) - \alpha \sum_{i \in \mathcal{I}} U_i(e_i) \tag{3}$$

subject to

$$\lambda_{i,j} \leq L_{\max} \quad \forall j \tag{4}$$

$$\lambda_{i,p} \leq L_{\max} \quad \forall i \tag{5}$$

$$\sum_{i \in \mathcal{I} j \in \mathcal{J}} e_{i,j} \leq \text{CL} \quad \forall i, j \tag{6}$$

$$e_{i,j} \geq 0 \quad \forall i, j \tag{7}$$

where, $\lambda_{i,j}$ is the propagation latency observed for transmission of update between appliance and user, $\lambda_{i,p}$ is the propagation latency observed for transmission of update between provider

TABLE I
NOTATION TABLE

Symbol	Descriptions
e_i	Energy consumption of user i
$e_{i,j}$	Energy consumption of appliance j of user i
$U_i(\cdot)$	Utility function of user
$C_p(\cdot)$	Consumption cost of utility provider
CL	Computational limit of utility provider
L_{max}	Maximum tolerable latency
$L_{i,p}$	Transmission latency between user and provider
$\lambda_{i,j}$	Propagation latency between device and user
$\lambda_{i,j}$	Propagation latency between user and provider
$a_{i,j}$	Auxiliary variables
$\mu_{i,j}$	Dual variables
$E(\cdot)$	Paillier cryptosystem encrypted message

and user, and (6) is a provider's computational capacity constraint, where CL refers to a given computational capacity constraint. The problem is not readily solvable in a distributed manner due to coupling of $e_{i,j}$ between users in a community. In the next section, ADMM is utilized to decouple those constraints and to design a distributed approach. We listed all the notations in this paper in Table I.

C. Threat Model

To solve the energy consumption optimization problem, the appliances' energy usage information is updated to P_u. Since such usage information, e_i, provides detailed energy consumption information about the home they are connected with and the devices being used, updating such sensitive information to the utility provider can pose serious privacy concerns. Such development is synonymous to the collection and transmission of large volumes of energy consumption data from SH appliances, that can be a serious concern to customer privacy [11], [20]–[22]. While sending this data from appliances to the utility provider, through an eavesdropping attack [17], the adversary can infer a lot about a customer's lifestyle from the leaked consumption data. Passing such data through a load profiling algorithm, an adversary can know what devices are on at any given time since each device has a distinctive load signature [23]. Through a mode detection algorithm [24], specific information about the operation of the devices can also be learnt by the adversary. Traffic analysis attack can also allows the attacker to learn the present information, where it does not reveal the data as such but exposes the sending patterns [25]. By consistent collection of such sensitive information, an adversary can intrude into a customer's private life. For example, it can disclose when the customer wakes up and goes to sleep, when the customer leaves to and returns from work, what room the customer is in at any given moment, when the home is vacant, even where the customer travels to (by collecting charging data from the customer's plug-in electric vehicle). This information can help an adversary plan more severe attacks against a customer (e.g., burglary, theft, and kidnapping). Other types of attacks can also occur during the SH optimization. With device impersonation attack, the customer believes he/she is remotely controlling one device but in reality might be controlling another. For example, instead of setting the temperature of oven to 120 °C, the sauna's temperature can be set to 120 °C risking the lives of anyone in it.

In this paper, we consider the adversary to be an active attacker trying to learn the home owner's usage data and lifestyle for its benefit. And P_u, while solving the optimization problem, is assumed to be honest-but-curious. That is, the utility provider will solve the optimization problem honestly but can try to infer the user's usage data. It is critical to keep the transmission data between the SH and the utility provider highly protected from external adversaries and from the utility provider that solves the problem.

D. Design Goal

The goal is to minimize the total consumption cost for efficient energy management in SH environments as well the utility provider. To address the above privacy concerns, we design a privacy preserving scheme that can efficiently schedule the appliances while minimizing the total cost under varying TOU tariffs. Since we assume the communication between is not trustworthy, i.e., various adversaries, such as eavesdroppers and tampers may be present, to ensure data privacy the home owner can use data encryption used to encrypt the data before outsourcing to prevent unauthorized entities from prying into the data. The major design goal is that the scheme should achieve maximum efficiency of computational and communication overhead, compared to the existing counterparts.

IV. PRELIMINARIES AND PROBLEM FORMULATION

In this section, we first introduce the background of the ADMM and Paillier cryptosystem. Then we present our distributed method to solve the appliance scheduling optimization problem.

A. Paillier Cryptosystem Preliminaries

In this paper, we adopt Paillier encryption [26], [27] which is an indistinguishable, additive homomorphic public key encryption scheme. In public key encryption, anyone can encrypt data with the public key (here $<n, g>$), but can be decrypted only by the one having secret/private key ($<\lambda, \mu>$).

Parameters: p, q.

Encryption: $c = E(m, r) = g^m r^n \bmod n^2$, where $r \in Z_n^*$ is a random number, $n = pq$ and random number $g \in Z_{n^2}^*$.

Decryption: $m = L(c^\lambda \bmod n^2)\mu \bmod n$, where $\lambda = lcm((p-1),(q-1))$ and $\mu = (L(g^\lambda \bmod n^2))^{-1} \bmod n$, and $L(u) = [(u-1)/n]$.

The properties of Paillier encryption include the following.

1) *Indistinguishability:* In Paillier encryption, $E(M)$ is computed using random number r. Thus, if the same plain text is encrypted twice using different random numbers,

these two cipher texts look different and we cannot know whether the original plain texts are the same or not without decrypting them.

2) *Additive Homomorphism:* Encryption E is additively homomorphic if

$$E(M_1)\Delta E(M_2) = E(M_1 + M_2) \tag{8}$$

where Δ refers to any operation. If we define the product of cipher texts $E(M_1)$ and $E(M_2)$ by

$$\begin{aligned} E(M_1)E(M_2) &= \left(g^{M_1} r^n \bmod n^2\right)\left(g^{M_2} r^n \bmod n^2\right) \\ &= g^{M_1+M_2} r^n \bmod n^2 \end{aligned} \tag{9}$$

then, decrypting this result gives the sum of $M1$ and $M2$, i.e., M_1+M_2. Therefore, Paillier encryption has the property of homomorphic addition. By this property, we can obtain the sum of two plain texts by computing the product of two cipher texts. The result would be the same as the sum of two plain texts after decryption.

B. ADMM

The ADMM, is an algorithm that solves a convex optimization problem by breaking them into subproblems, each of which are then easier to handle. ADMM has been widely applied in various research domains [28]–[31]. It is a variant of the augmented Lagrangian scheme that uses partial updates for the dual variables. The generic form of the optimization problem using ADMM can be described as

$$\min_{x,z} \quad f(x) + g(z) \tag{10}$$

subject to

$$Ax + Bz = c \tag{11}$$

where $x \in R^n, z \in R^m$, $c \in R^p$ and matrices $A \in R^{p\times n}$ and $B \in R^{p\times m}$. Functions f and g are convex, close and proper. The scaled augmented Lagrangian can be expressed as

$$L_\rho(x, z, \mu) = f(x) + g(z) + \frac{\rho}{2}\|Ax + Bz - c + \mu\|_2^2 \tag{12}$$

where $\rho > 0$ is the penalty parameter and μ is the scaled dual variable. x and z are updated in a Gauss–Seidel fashion using the scaled dual variable. At each iteration k, the update process can be expressed as

$$x^k = \underset{x}{\operatorname{argmin}}\ f(x) + \frac{\rho}{2}\|Ax + Bz^k - c + \mu^k\|_2^2 \tag{13}$$

$$z^k + 1 = \underset{z}{\operatorname{argmin}}\ g(z) + \frac{\rho}{2}\|Ax^{k+1} + Bz - c + \mu^k\|_2^2. \tag{14}$$

Finally, the scaled dual variable is updated as

$$\mu^{k+1} = \mu^k + Ax^{k+1} + Bz^{k+1} - c. \tag{15}$$

The advantage of ADMM is that the objective function is separable in x and z. The dual update requires solving a proximity function in x and z at the same time; the ADMM technique allows this problem to be solved by first solving for x with z fixed, and then solving for z with x fixed. Rather than iterating until convergence, the algorithm proceeds directly to updating the dual variable and then repeating the process. Even though it is not equivalent to the exact minimization, it shows that this method converges to the optimum under some assumptions.

C. Distributed ADMM for Home Appliance Scheduling

By introducing a set of auxiliary variables for a user's appliances $a_j = (a_{1,j}, \ldots, a_{N,j})^T$ for $j \in \mathcal{J}$ and enforcing $a_{i,j} = e_{i,j}$, the optimization problem can be formulated in a distributed manner as

$$\underset{\{e_i\}_{i=1}^N}{\text{minimize}} \sum_{i\in\mathcal{I}} C_p(a_j) - \alpha \sum_{j\in\mathcal{J}} U_i(e_i) \tag{16}$$

subject to

$$\lambda_{i,j} \le L_{\max} \quad \forall j \tag{17}$$

$$\lambda_{i,p} \le L_{\max} \quad \forall i \tag{18}$$

$$\sum_{i\in\mathcal{I} j\in\mathcal{J}} e_{i,j} \le \mathrm{CL} \quad \forall i, j \tag{19}$$

$$e_{i,j} = a_{i,j} \quad \forall i, j \tag{20}$$

$$e_{i,j} \ge 0, a_{i,j} \ge 0 \quad \forall i, j. \tag{21}$$

Now a distributed approach can be designed to solve the optimization problem which is shown in (16). Specifically, the decision variables e_i and a_j are arranged into two groups, which correspond to the provider updates and user updates, respectively. During the optimization, the variables of each group are optimized in a distributed and parallel fashion. In particular, each user i solves e_i and the provider obtains a_j, and those two groups of decision variables are coordinated through auxiliary variables.

For compactness, we define sets $A_i = \{e_i | \sum_{j\in\mathcal{J}} e_{i,j} = \lambda_i, e_{i,j} \ge 0, \forall j \in \mathcal{J}\}$ and $B_j = \{a_j | \sum_{i\in\mathcal{I}} a_j \ge 0, \forall i \in \mathcal{I}\}$. Accordingly, $A = \{\cup A_i\}_{i=1}^I$ and $B = \{\cup B_j\}_{j=1}^J$. By applying ADMM to solve the optimization problem, we first calculate the partial Lagrangian, which introduces the Lagrange multipliers only for the constraint in (20)

$$L_\rho\left(\{e_i\}_{i=1}^N, \{a_j\}_{j=1}^J, \{\mu_{i,j}\}_{i=1,j=1}^{N,J}\right) \tag{22}$$

$$= \sum_{i\in\mathcal{I}} C_p(a_j) - \alpha \sum_{i\in\mathcal{I}} U_i(e_i) + \frac{\rho}{2}\sum_{i\in\mathcal{I}}\sum_{j\in\mathcal{J}} \|e_{i,j} - a_{i,j} + \mu_{i,j}\|_2^2 \tag{23}$$

where $\mu_{i,j}$ is the scaled Lagrangian multiplier. The decision variables e_i and a_j are arranged into two groups and updated in an iterative fashion.

Home Owner Updates: At iteration k, e_i is updated by

$$\underset{\{e_i\}_{i=1}^N \in A}{\text{minimize}} \quad \frac{\rho}{2}\sum_{i\in\mathcal{I}}\sum_{j\in\mathcal{J}} \|e_{i,j} - a_{i,j}^k + \mu_{i,j}^k\|_2^2 - \alpha \sum_{i\in I} U_i(e_i). \tag{24}$$

In (23), the optimization is performed to maximize the utility at the user's side under a square regularization term. The optimization problem can be handled at independent computing unit locally. Each computing unit i solves a stochastic optimization problem as follows:

$$\underset{\{e_i\}\in A_i}{\text{minimize}} \quad \frac{\rho}{2}\sum_{j\in\mathcal{J}} \|e_{i,j} - a_{i,j}^k + \mu_{i,j}^k\|_2^2 - \alpha U_i(e_i). \tag{25}$$

Provider Update: The decision variables a_j at provider are updated by

$$\underset{\{a_j\}_{j=1}^{J}\in B}{\text{minimize}} \quad \sum_{j\in\mathcal{J}} C_p(a_j) + \frac{\rho}{2}\sum_{i\in\mathcal{I}}\sum_{j\in\mathcal{J}} \|e_{i,j}^{k+1} - a_{i,j}^{k+1} + \mu_{i,j}^{k}\|_2^2. \tag{26}$$

The provider will determine a_j independently by solving the following optimization problem:

$$\underset{\{a_j\}\in B_j}{\text{minimize}} \quad C_p(a_j) + \frac{\rho}{2}\sum_{i\in\mathcal{I}} \|e_{i,j}^{k+1} - a_{i,j}^{k+1} + \mu_{i,j}^{k}\|_2^2. \tag{27}$$

Finally, the dual variables are updated as

$$\mu_{i,j}^{k+1} = \mu_{i,j}^{k} + e_{i,j}^{k+1} - a_{i,j}^{k+1}. \tag{28}$$

We decompose the optimization problem into $N + 1$ optimization problems, first associated with provider corresponding to the primal variables and the rest corresponding to the home owners with the dual variables. Detailed description of the proposed distributed workload management is given in Algorithm 1. ADMM is an iterative algorithm, where each computing unit solves its own subproblem, the variations to constraint in (20) are systematically penalized at certain prices through the scaled dual variable to each individual subproblem. In the ADMM framework for distributed computing the dual variables, or price, are not uniformly set for all nodes, which will require synchronization. For the convex optimization problem, ADMM geometrically converges to the optimum [32].

V. SAFE

In this section, we describe the formulation and overview of the proposed SAFE scheme, energy consumption for SH-IoT. The overview of the computation in our scheme without privacy preservation is shown in Algorithm 1. In this section, we describe the computation with privacy preservation. Initially, the home owner generates its public key pk_u and private key pair sk_u. The user also receives the public key of the provider. The user can either choose tariffs on that particular day or choose day ahead pricing tariffs released by the utility providers for appliances scheduling. The user can monitor and control the appliance usage information from its mobile device. Every time the provider wants to solve the optimization problem the user updates usage information to the utility provider for solving the problem. Each appliance's usage information is encrypted with provider's public key before sending it to the provider for solving the optimization problem. The user can have a predefined algorithm to encrypt appliance data whenever it sends to the provider. The user can sign the updated information with its private key that can be verified by the provider to know the source is a legitimate customer not an external adversary. Only the trusted coordinator can decrypt the optimization end data, but the utility provider can solve the problem without decrypting the data. The utility provider solves on the ciphertexts from all the users and obtains the optimal energy consumption. The user then schedules the appliances accordingly.

Algorithm 1: Distributed ADMM for Home Appliance Scheduling

Input: $C_p(.), \{U_i(...)\}_{i=1}^{N}, L_{max}, CL, k = 0$
Initialize: $\{e_i\}_{i=1}^{N}, \{a_j\}_{j=1}^{J}, \{\mu_{i,j}\}_{i=1,j=1}^{N,J} = 0$;
while not converge **do**
    At the home owner:
    Parallel for i;
    $\underset{\{e_i\}\in A_i}{\text{minimize}} \quad \frac{\rho}{2}\sum_{j\in\mathcal{J}} \|e_{i,j} - a_{i,j}^{k} + \mu_{i,j}^{k}\|_2^2 - \alpha U_i(e_i)$;
    At the provider:
    Wait until receive $e_{i,j}$, $\mu_{i,j}$ from all the home owners
    $\underset{\{a_j\}\in B_j}{\text{minimize}} \quad C_p(a_j) + \frac{\rho}{2}\sum_{i\in\mathcal{I}} \|e_{i,j}^{k+1} - a_{i,j}^{k+1} + \mu_{i,j}^{k}\|_2^2$
    and obtain optimal solution $e_{i,j}^{k+1}, a_{i,j}^{k+1}$;
    $\mu_{i,j}^{k+1} = \mu_{i,j}^{k} + e_{i,j}^{k+1} - a_{i,j}^{k+1}$;
    Broadcast optimal solution to all home owners
    Adjust penalty parameter ρ if necessary;
    Set $k = k + 1$;
end while
return $\{e_i\}_{i=1}^{N}, \{a_j\}_{j=1}^{J}$;
Output: $\{e_i\}_{i=1}^{N}, \{a_j\}_{j=1}^{J}$.

We describe the entire mechanism along with the problem formulation in the following sections including five steps: 1) pricing; 2) encryption; 3) efficient energy consumption optimization; 4) cost minimization in appliances scheduling; and 5) decryption.

A. Pricing

In this phase, the user either decides on RTP or day ahead pricing and then decides to solve the optimization problem for scheduling the appliances.

B. Encryption

In this phase, the user encrypts the appliance's usage information as described in Section III before sending it to the provider, i.e.,

$$c_{e_i} = E(e_{i,j}) \tag{29}$$

$$c_{a_j} = E(a_{i,j}). \tag{30}$$

C. Efficient Energy Consumption Optimization

The optimization problem is solved in a distributed manner over the ciphertexts of the usage information as follows:

$$\underset{\{e_i\}_{i=1}^{N}}{\text{minimize}} \sum_{i\in\mathcal{I}} C_p(c_{a_j}) - \alpha\sum_{i\in\mathcal{I}} U_i(c_{e_i}) \tag{31}$$

subject to

$$\lambda_{i,j} \le L_{\max} \quad \forall j \tag{32}$$

$$\lambda_{i,p} \le L_{\max} \quad \forall i \tag{33}$$

$$\sum_{i\in\mathcal{I},j\in\mathcal{J}} e_{i,j} \le \text{CL} \quad \forall i,j \tag{34}$$

$$e_{i,j} = a_{i,j} \quad \forall i,j \tag{35}$$

$$e_{i,j} \ge 0, a_{i,j} \ge 0 \quad \forall i,j. \tag{36}$$

The decision variables corresponding to user updates and provider updates are updated in an iterative fashion. Initially, all the users update and then the provider updates, followed by the update of the dual variable μ, as described in (28). This procedure continues until it converges to the optimum.

D. Cost Minimization in Appliances Scheduling

The provider needs to find the minimum cost for appliance scheduling. In this scenario, the provider has m values taken at discrete points $a_1, \ldots, a_m$ encrypted under its secret key that key generator holds and wants to know the argmin over these values (the index of the lowest value), but the provider should not learn anything else. For example, if a provider P_u has values $E[1]$, $E[10]$ and $E[2]$ then the provider during computation with the key generator should learn that the first one is the lowest value, but learn nothing else. In particular, the P_u should not learn the order relations between the a_i's.

To prevent the utility provider from learning the order relations, at each iteration once the key generator determines which is the maximum of the compared two values and returns the index of the lowest value, the key generator should randomize the encryption of this minimum in such a way that the utility provider cannot link this value to one of the compared values. The trusted coordinator, the key generator, uses the refresh procedure for the randomization of Paillier ciphertexts. In the case, where the "refresher" knows the secret key, this can be seen as a decryption followed by a re-encryption. Otherwise, it can be seen as a multiplication by the encryption of 0.

During the optimization process, the utility provider does not manipulate or randomize the end or intermediate optimization results since we assume the utility provider to be honest-but-curious while following the protocol in our threat model.

E. Decryption

After converging to the optimum, the end optimization result is decrypted as described in Section III and the appliances are scheduled accordingly for that day or the following day.

VI. Privacy and Performance Analysis

In this section, we discuss the privacy properties and the performance analysis of the appliances scheduling optimization scheme.

A. Privacy Analysis

In this section, we describe the security and privacy properties of the proposed SAFE algorithm.

1) *Privacy Preservation From External Adversaries:* In this algorithm, the confidentiality and data privacy are achieved by encrypting the home owner's energy usage information and any other sensitive information using the homomorphic encryption scheme, Paillier cryptosystem. It is worth noting that since all messages are encrypted, an outside eavesdropper cannot learn anything by intercepting the messages.
2) *Resistance to Attacks:* Due to the existence of random value r in the encryption of our protocol, the ciphertexts encrypted under Paillier cryptosystem are resistant to the dictionary attack. Given a plaintext p, the primitive most frequently used by our protocol is the generation of multiple encryptions of p in such a way that they are statistically indistinguishable in the indistinguishabilty under chosen-plaintext attack model. Therefore, from ciphertexts $x = E(p)$ and $y = E(p)$ encrypted under different random numbers, it is difficult to distinguish that they decrypt to the same plaintext p. The semantic security of the Paillier cryptosystem effectively protects the energy profiles of users from such attacks.
3) *Privacy Preservation From Provider and Trusted Coordinator:* The home owner's private information or intermediate information cannot be inferred by the honest-but-curious utility provider solving the optimization problem. *Honest-but-curious adversaries* are agents who follow all protocol steps correctly but are curious and collect input/output or intermediate information in an attempt to learn some information about the participating parties. The home owner's privacy is protected from the honest-but-curious utility provider which solves the optimization problem since it cannot learn about usage information during the procedure. Even though the usage information is encrypted by the user with its public key, it can decrypted only by the key generator, which secures it from the provider and other malicious adversaries. Although the trusted coordinator holds the secret key, he/she has no access to the detailed energy consumption of the user.
4) *Privacy Preserving Optimization:* The homomorphism of Paillier cryptosystem that allows computation over ciphertext enables the correctness of the proposed privacy preserving ADMM-based optimization. The input/output and intermediate information are effectively protected from the honest-but-curious provider while solving the cost-minimization problem.

To make the scheme more secure, the key can be generated by multiple trusted coordinators in a distributed way. Each distributed trusted coordinator has only a share of secret key. So, this scheme guarantees that coordinators cannot learn any usage information while performing decryption. Since the utility provider is assumed to be passive while following the protocol, our approach using Paillier encryption for optimization effectively preserves user's privacy.

B. Performance Analysis

In this section, we evaluate the performance of our proposed scheme based on real-world electricity price data sets. The scheduling horizon is divided into discrete time periods with 5 min at each period. We first describe the real world electricity data set and average solar radiance data used in this paper. Then, we illustrate the improved cost minimization of our scheme for a day and a week in comparison with the fixed price schemes.

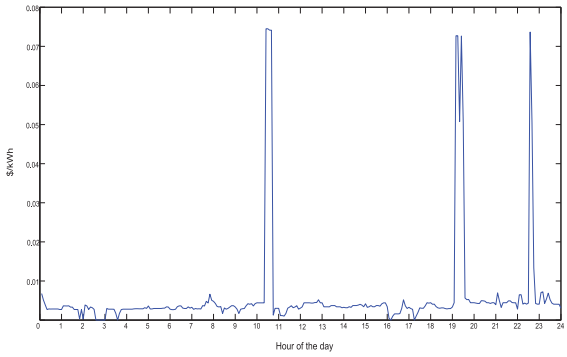

Fig. 2. 5-min real-time electricity price at Palo Alto in a day.

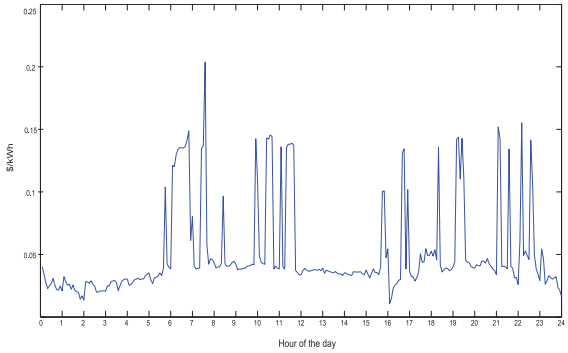

Fig. 3. 5-min average real-time electricity price at Palo Alto in a week.

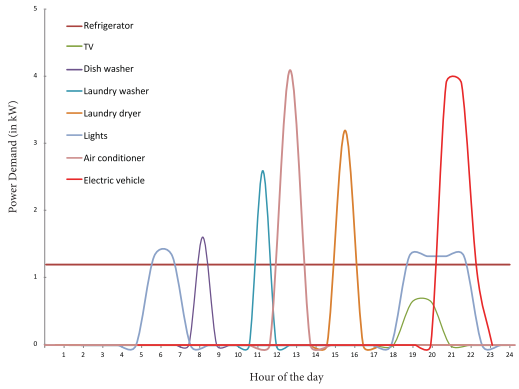

Fig. 4. Aggregated power demand of appliances.

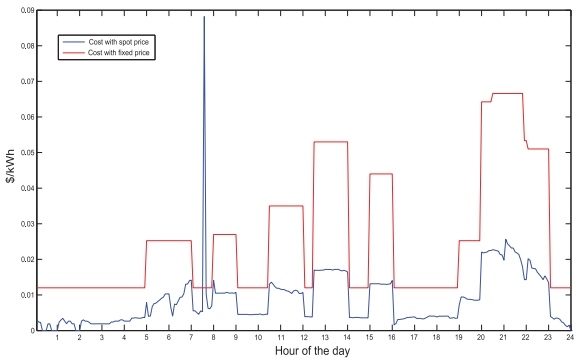

Fig. 5. Consumption cost comparison with spot price in a day.

1) Electricity Price Data: We use the 5-min locational marginal prices in real-time electricity markets at Palo Alto, CA, USA [33]. The data set is obtained from publicly available government sources. Based on this raw data, we calculate the average electricity price over a week. The time horizon we consider in this paper is from January 1 to January 7, 2011. In total, this duration includes 1 week or 2016-min periods. The electricity price variation during a day is plotted in Fig. 2. The average 5-min real-time electricity price during the first week of January 2011 is plotted in Fig. 3. The electricity price is in unit of $\$/kWh$. For renewable energy generation, we used the hourly average solar radiance data for the first week of January 2011, from Measurement and Instrumentation Data Center [34] at the National Renewable Energy Laboratory. The control interval is chosen to be 1 h. In total, this duration includes one week or 168 1-h slots. We analyze the performance of the proposed scheme with and without the use of renewable energy in fixed price scheduling and spot price scheduling.

2) Simulation Results: We analyze the simulation results of our scheme, where the optimization problem's objective is to minimize the utility costs at both owner and provider sides while protecting users' sensitive private information. The aggregated power demand of all the appliances at a dwelling can be scheduled as shown in Fig. 4 after solving the optimization problem based on ADMM. This varies for different households in a provider's community. In order to analyze the performance improvements in terms of cost minimization, we compare our scheduling scheme using spot electricity price with scheduling using fixed retail electricity price priced at 0.1 \$/kWh.

In Fig. 5, we compare the electricity consumption cost of our scheduling scheme with the fixed price scheduling scheme during a day. We considered eight appliances that are scheduled according to the day ahead energy prices to reduce the consumption cost. In the figure, we notice that the fixed retail price has fixed minimum cost of \$0.12 at any time, since certain appliances (e.g., refrigerators) need to be on the whole day, whereas the spot price minimum cost changes with the varying electricity price. We also notice that for most parts of the day, the consumption cost is higher in the fixed price plan than the spot price. In Fig. 5, the total consumption cost for that day using the fixed price plan is \$7.565 which is 3.05 times higher than the varying electricity price plan, i.e., \$2.479.

In the spot price plans, since the electricity price varies 24×7 throughout the year, we considered the average of every day electricity prices over a week for analyzing the consumption cost. In Fig. 3, we notice that the electricity price varies much more drastically in a week's average than a day. In Fig. 6, we see that the electricity consumption cost for the spot price plan is higher in some parts of the day when the average spot price over a week is considered. However, in Fig. 6, we see that the total consumption cost for that day using the spot price plan is \$4.088 which is still less than \$7.565 which reduces the consumption cost by a factor of 1.85. From the simulation results in Fig. 6, we conclude that the spot price plans with optimal energy usage reduces the

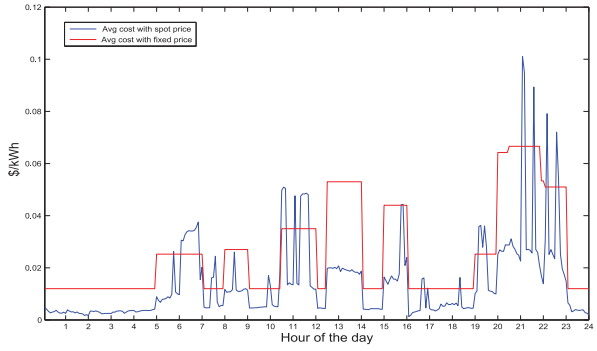

Fig. 6. Consumption cost comparison with average spot price over a week.

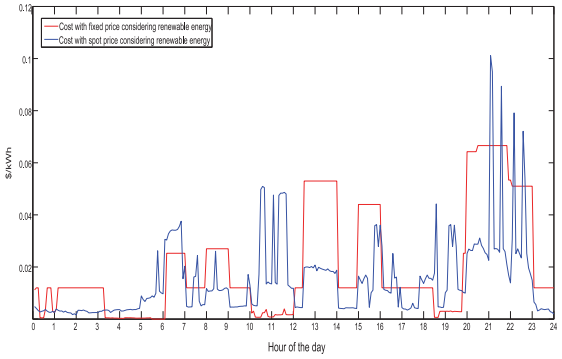

Fig. 7. Consumption cost comparison with renewable energy usage in a day.

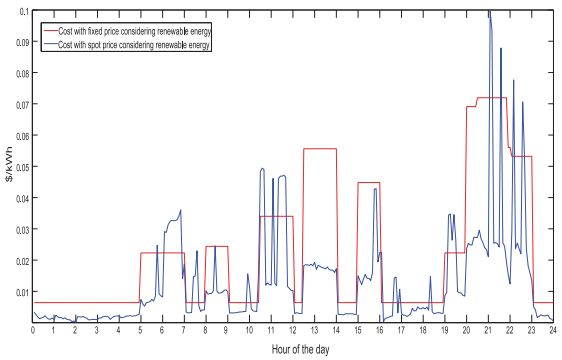

Fig. 8. Consumption cost comparison with renewable energy usage over a week.

consumption cost of the users, thereby minimizing the cost for the energy provider.

In Fig. 7, we compare the electricity consumption cost with fixed price scheduling scheme during a day considering usage of renewable energy. We notice that the consumption cost is higher in the fixed price plan than the spot price even when renewable energy usage is considered. In this figure, we see that the total consumption cost for that day using fixed price plan is \$5.998 which is 1.86 times higher than the varying electricity price plan, i.e., \$3.2256.

In Fig. 8, we compare the electricity consumption cost with renewable energy usage considering average spot price and renewable energy usage over a week. Even with consideration of the average spot price, the total consumption cost for that day using the spot price plan is \$3.6562 that is still less than consumption cost of \$6.7748 in the fixed price plan. From the

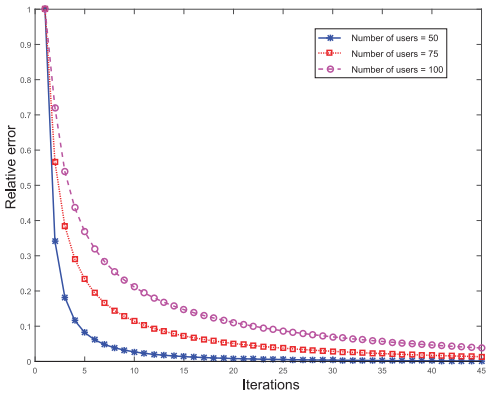

Fig. 9. Convergence performance.

simulation results, the spot price plans along with the usage of renewable resources allow optimal energy usage, reducing the consumption cost of the users, thereby minimizing the cost for the utility provider.

In Fig. 9, we analyze the convergence performance of ADMM which accounts for the communication overhead of our scheme. Here, a relative error is used to demonstrate the results which is the difference of the value at iteration k and the optimal value. When the number of home owners is 50, it took a moderate number of iterations to converge, similarly with 75 and 100. As the number of users increases, our scheme converges with only small increment of iterations, which proves the scalability of the proposed scheme and its associated overhead to solve the optimization problem. The proposed algorithm has good convergence performance and effectively reduces the consumption cost of the users and utility provider as evident from the simulation results.

VII. Conclusion

In this paper, we formulated the privacy preserving scheme, namely SAFE, energy consumption for SH-IoT environments, for appliances scheduling in SH-IoT as an optimization problem with the objective of minimizing utility cost at both users and utility provider sides. The problem for appliances scheduling was solved in a distributed manner by leveraging ADMM while the privacy of the user was preserved by using Paillier cryptosystem. The proposed scheme effectively preserves the user's usage information from malicious adversaries and honest-but-curious utility providers. Our simulation results show that the proposed SAFE is highly effective in lowering the electricity cost and computation overhead while preserving users' privacy.

References

[1] Y.-F. Huang, S. Werner, J. Huang, N. Kashyap, and V. Gupta, "State estimation in electric power grids: Meeting new challenges presented by the requirements of the future grid," *IEEE Signal Process. Mag.*, vol. 29, no. 5, pp. 33–43, Sep. 2012.

[2] "Final report on standards for smart grids," CEN/CENELEC/ETSI Joint Working Group, Brussels, Belgium, Rep. V1.12, 2011. [Online]. Available: http://www.etsi.org/WebSite/document/Report_CENCLCETSI_Standards_Smart%20Grids.pdf

[3] (2010). *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*. [Online]. Available: http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf

[4] Y. Guo, M. Pan, Y. Fang, and P. P. Khargonekar, "Decentralized coordination of energy utilization for residential households in the smart grid," *IEEE Trans. Smart Grid*, vol. 4, no. 3, pp. 1341–1350, Sep. 2013.

[5] M. R. Alam, M. B. I. Reaz, and M. A. M. Ali, "A review of smart homes—Past, present, and future," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 42, no. 6, pp. 1190–1203, Nov. 2012.

[6] Y. Ozturk, P. Jha, S. Kumar, and G. Lee, "A personalized home energy management system for residential demand response," in *Proc. IEEE 4th Int. Conf. Power Eng. Energy Elect. Drives (POWERENG)*, Istanbul, Turkey, May 2013, pp. 1241–1246.

[7] M. Erol-Kantarci and H. T. Mouftah, "TOU-aware energy management and wireless sensor networks for reducing peak load in smart grids," in *Proc. IEEE 72nd Veh. Technol. Conf.*, Ottawa, ON, Canada, Sep. 2010, pp. 1–5.

[8] M. Erol-Kantarci and H. T. Mouftah, "Wireless sensor networks for cost-efficient residential energy management in the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 314–325, Jun. 2011.

[9] F. Fernandes, H. Morais, Z. Vale, and C. Ramos, "Dynamic load management in a smart home to participate in demand response events," *Energy Build.*, vol. 82, pp. 592–606, Oct. 2014.

[10] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Comput. Netw.*, vol. 57, no. 5, pp. 1344–1371, Apr. 2013.

[11] X. Li *et al.*, "Securing smart grid: Cyber attacks, countermeasures, and challenges," *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 38–45, Aug. 2012.

[12] K. M. Tsui and S. C. Chan, "Demand response optimization for smart home scheduling under real-time pricing," *IEEE Trans. Smart Grid*, vol. 3, no. 4, pp. 1812–1821, Dec. 2012.

[13] A. Yatchew and A. Baziliauskas, "Ontario feed-in-tariff programs," *Energy Policy*, vol. 39, no. 7, pp. 3885–3893, Jul. 2011.

[14] A. Agnetis, G. de Pascale, P. Detti, and A. Vicino, "Load scheduling for household energy consumption optimization," *IEEE Trans. Smart Grid*, vol. 4, no. 4, pp. 2364–2373, Dec. 2013.

[15] C. Chen, J. Wang, Y. Heo, and S. Kishore, "MPC-based appliance scheduling for residential building energy management controller," *IEEE Trans. Smart Grid*, vol. 4, no. 3, pp. 1401–1410, Sep. 2013.

[16] X. Cheng, L. Fang, L. Yang, and S. Cui, "Mobile big data: The fuel for data-driven wireless," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1489–1516, Oct. 2017.

[17] I. Ghansah, "Smart grid cyber security potential threats, vulnerabilities and risks," PIER Energy-Related Environmental Research Program, California Energy Commission, Sacramento, CA, USA, Rep. CEC-500-2012-047, 2009.

[18] J. H. Seo and K. Emura, "Efficient delegation of key generation and revocation functionalities in identity-based encryption," in *Proc. CT-RSA*, vol. 7779. San Francisco, CA, USA, Jan. 2013, pp. 343–358.

[19] T. Perrin, L. Bruns, J. Moreh, and T. Olkin, "Delegated cryptography, online trusted third parties, and PKI," in *Proc. 1st Annu. PKI Res. Workshop*, vol. 14. Gaithersburg, MD, USA, Apr. 2002, pp. 97–116.

[20] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 998–1010, 4th Quart., 2012.

[21] S. Shapsough, F. Qatan, R. Aburukba, F. Aloul, and A. Al Ali, "Smart grid cyber security: Challenges and solutions," in *Proc. IEEE Int. Conf. Smart Grid Clean Energy Technol. (ICSGCE)*, Offenburg, Germany, Oct. 2015, pp. 170–175.

[22] Y. Cao *et al.*, "Smart meter data aggregation against wireless attacks: A game-theoretic approach," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kuala Lumpur, Malaysia, May 2016, pp. 1–6.

[23] S. Saponara and T. Bacchillone, "Network architecture, security issues, and hardware implementation of a home area network for smart grid," *J. Comput. Netw. Commun.*, vol. 2012, Nov. 2012, Art. no. 534512.

[24] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1933–1954, 4th Quart., 2014.

[25] G. Mantas, D. Lymberopoulos, and N. Komninos, "Security in smart home environment," in *Wireless Technologies for Ambient Assisted Living and Healthcare: Systems and Applications*. Hershey, PA, USA: IGI Glob., 2010, pp. 170–191.

[26] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.*, Prague, Czech Republic, 1999, pp. 223–238.

[27] M. Pan, J. Sun, and Y. Fang, "Purging the back-room dealing: Secure spectrum auction leveraging Paillier cryptosystem," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 4, pp. 866–876, Apr. 2011.

[28] J. F. C. Mota, J. M. F. Xavier, P. M. Q. Aguiar, and M. Püschel, "D-ADMM: A communication-efficient distributed algorithm for separable optimization," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2718–2723, May 2013.

[29] H. K. Nguyen, A. Khodaei, and Z. Han, "A big data scale algorithm for optimal scheduling of integrated microgrids," *IEEE Trans. Smart Grid*, vol. 9, no. 1, pp. 274–282, Jan. 2018.

[30] C. Song, S. Yoon, and V. Pavlovic, "Fast ADMM algorithm for distributed optimization with adaptive penalty," in *Proc. 30th Conf. Assoc. Adv. Artif. Intell. (AAAI)*, Phoenix, AZ, USA, Feb. 2016, pp. 753–759.

[31] L. Liu, Z. Han, H. V. Poor, and S. Cui, "Big data processing for smart grid security," in *Big Data Over Networks*. Cambridge, U.K.: Cambridge Univ. Press, 2016, ch. 8, pp. 217–244.

[32] W. Deng and W. Yin, "On the global and linear convergence of the generalized alternating direction method of multipliers," *J. Sci. Comput.*, vol. 66, no. 3, pp. 889–916, Mar. 2016.

[33] Y. Guo and Y. Fang, "Electricity cost saving strategy in data centers by using energy storage," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 6, pp. 1149–1160, Jun. 2013.

[34] *NREL: Measurement and Instrumentation Data Center*. Accessed: Jan. 2011. [Online]. Available: http:/www.nrel.gov/midc

Sai Mounika Errapotu (S'14) received the B.Tech. degree in electronics and communication engineering from Jawaharlal Nehru Technological University, Hyderabad, India, in 2013. She is currently pursuing the Ph.D. degree at the Department of Electrical and Computer Engineering, University of Houston, Houston, TX, USA.

Her current research interests include security and privacy in wireless networks and cyber physical systems, differentially private data analysis, privacy in IoT, and mobile crowd sourcing applications.

Jingyi Wang (S'16) received the B.S. degree in physics from Nankai University, Tianjin, China, in 2012, and the M.S. degree in electrical and computer engineering from Auburn University, Auburn, AL, USA, in 2015. She is currently pursuing the Ph.D. degree at the Department of Electrical and Computer Engineering, University of Houston, Houston, TX, USA.

Her current research interests include privacy preservation of cognitive radio networks, distributed spectrum trading, and wireless big data privacy.

Yanmin Gong (M'16) received the B.Eng. degree in electronics and information engineering from the Huazhong University of Science and Technology, Wuhan, China, in 2009, the M.S. degree in electrical engineering from Tsinghua University, Beijing, China, in 2012, and the Ph.D. degree in electrical and computer engineering from the University of Florida, Gainesville, FL, USA, in 2016.

She has been an Assistant Professor with the School of Electrical and Computer Engineering, Oklahoma State University, Stillwater, OK, USA, since 2016. Her current research interests include information security and privacy and mobile and wireless security and privacy, such as security in Internet-of-Things and privacy-preserving big data analytics.

Dr. Gong has served as a Technical Program Committee member for several conferences including IEEE INFOCOM and CNS. She is a member of the ACM.

Jin-Hee Cho (S'07–M'09–SM'14) received the B.A. degree from Ewha Woman University, Seoul, South Korea, the M.A. degree in social work from Washington University, St. Louis, MO, USA, and the M.S. and Ph.D. degrees in computer science from Virginia Polytechnic Institute and State University, Blacksburg, VA, USA, in 2004 and 2008, respectively.

She was a Computer Scientist with the U.S. Army Research Laboratory, Adelphi, MD, USA, since 2009. She has been an Associate Professor with the Department of Computer Science, Virginia Polytechnic Institute and State University, since 2018. She has authored or co-authored over 100 peer-reviewed technical papers in leading journals and conferences in the areas of trust management, cybersecurity, metrics and measurements, network performance analysis, resource allocation, agent-based modeling, uncertainty reasoning and analysis, information fusion/credibility, and social network analysis.

Dr. Cho was a recipient of the Best Paper Award of IEEE TrustCom'2009, BRIMS'2013, IEEE GLOBECOM' 2017, the 2017 ARL's Publication Award, and the IEEE CogSima 2018. She was a recipient of the 2015 IEEE Communications Society William R. Bennett Prize in the field of communications networking. She was selected for the 2013 Presidential Early Career Award for Scientists and Engineers in 2016, which is the highest honor bestowed by the U.S. Government on outstanding scientists and engineers in the early stages of their independent research careers. She is a member of the ACM.

Miao Pan (S'07–M'12) received the B.Sc. degree in electrical engineering from the Dalian University of Technology, Dalian, China, in 2004, the M.A.Sc. degree in electrical and computer engineering from the Beijing University of Posts and Telecommunications, Beijing, China, in 2007, and the Ph.D. degree in electrical and computer engineering from the University of Florida, Gainesville, FL, USA, in 2012.

He is currently an Assistant Professor with the Department of Electrical and Computer Engineering, University of Houston, Houston, TX, USA. He was an Assistant Professor of computer science with Texas Southern University, Houston, from 2012 to 2015. His current research interests include cognitive radio networks, cybersecurity, and cyber-physical systems.

Dr. Pan was a recipient of the Best Paper Award of Globecom 2017 and Globecom 2015, respectively. He is serving an Associate Editor for IEEE INTERNET OF THINGS JOURNAL from 2015 to 2018.

Zhu Han (S'01–M'04–SM'09–F'14) received the B.S. degree in electronic engineering from Tsinghua University, Beijing, China, in 1997, and the M.S. and Ph.D. degrees in electrical and computer engineering from the University of Maryland at College Park, College Park, MD, USA, in 1999 and 2003, respectively.

From 2000 to 2002, he was a Research and Development Engineer with JDSU, Germantown, MD, USA. From 2003 to 2006, he was a Research Associate with the University of Maryland at College Park. From 2006 to 2008, he was an Assistant Professor with Boise State University, Boise, ID, USA. He is currently a Professor with the Electrical and Computer Engineering Department, as well as with the Computer Science Department, University of Houston, Houston, TX, USA. His current research interests include wireless resource allocation and management, wireless communications and networking, game theory, big data analysis, security, and smart grid.

Dr. Han was a recipient of the NSF Career Award in 2010, the Fred W. Ellersick Prize of the IEEE Communication Society in 2011, the EURASIP Best Paper Award for the *Journal on Advances in Signal Processing* in 2015, the IEEE Leonard G. Abraham Prize in the field of communications systems (Best Paper Award in IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS) in 2016, and several Best Paper Awards in IEEE conferences. He is currently an IEEE Communications Society Distinguished Lecturer.