An Efficient Data Aggregation Scheme for Privacy-Friendly Dynamic Pricing-based Billing and Demand-Response Management in Smart Grids

Prosanta Gope and Biplab Sikdar, *Senior Member, IEEE*

Abstract—**Smart grids take advantage of information and communication technologies to achieve energy efficiency, automation and reliability. These systems allow two-way communications and power flow between the grid and consumers. However, these bidirectional communications introduce several security and privacy threats to consumers. One of the open challenges in this context is user privacy when smart meters are used to capture fine-grained energy usage information. Although considerable research has been carried out in this direction, most of the existing solutions invariably introduce computational complexity and overhead, which makes them infeasible for resource constrained smart meters. In this paper, we propose a privacy-friendly and efficient data aggregation scheme (EDAS) for dynamic pricing based billing and demand-response management in smart grids. To the best of our knowledge, this is the *first paper* to address privacy in the context of billing under dynamic electricity pricing. Security and performance analyses show that the proposed scheme offers better privacy protection for electric meter reading aggregation and computational efficiency, as compared to existing schemes.**

Index Terms—**Privacy, data aggregation, smart grids**

I. Introduction

Smart-grids represent the next generation of power grids which use extensive monitoring and measurements to manage the operation of the grid, and achieve greater efficiency and cost reduction. The combined volatility of both power supply (e.g. with renewables) and power demand creates a growing problem that needs to be resolved by smart grids. To enable the envisioned energy management in smart grids, information on current power consumption and the availability of power needs to be exchanged between power consumers and power suppliers. Hence, smart grids need a framework of interconnected smart monitoring and measurement devices. Besides, with the recent development in smart grids, many endeavours have started to introduce the Internet of Things (IoT) as an enabling technology for smart grids since each device in the grid can be considered as a connected object [1]. In this regard, devices in the smart grid such as smart meters act as IoT devices that autonomously report their data to the grid infrastructure by using information and communication technology (ICT). However, this interconnection of grid technology with information and communication technologies leads to various security challenges in a power grid [2]. A key challenge and major obstacle in the widespread deployment of smart grids is privacy, which is a primary concern from the customer's point of view.

In general, for pricing and feedback purposes, a smart grid relies heavily on the usage of a smart metering infrastructure. For instance, smart meter data is useful for load forecasting, demand-response management, and dynamic pricing. However, the recording and transmission of power consumption profiles may cause serious privacy issues. For example, fine-grained power consumption data of a smart meter can be exploited for revealing a consumer's private information related to their daily routines or the appliances in the house. This can lead to personalized advertisements or be used extract information on when a house is empty. In [2], it is shown that complex usage patterns can be extracted from the high-resolution consumption information using simple off-the-shelf statistical tools, and the extracted information can be used to profile and monitor users for various purposes. Thus, energy usage data must be protected for privacy in a smart grid. Furthermore, the computational resources at the consumer's side are usually very limited. Solutions for preserving user privacy should thus be computationally inexpensive.

A. Related Work

In order to address the privacy issues, several privacy-preserving data aggregation protocols have been proposed in recent years. Lu et al. designed a privacy-preserving data aggregation protocol [3] by using the Paillier homomorphic crypto-system [4], which results in a high computation overhead on the entities like smart meters. Liang et al. proposed a usage-based dynamic pricing scheme for smart grids [5] by using the fully homomorphic technique devised by Naehring et al. [6]. As fully homomorphic techniques are difficult to implement with current computing resources, this scheme is impractical. Chia-Mu et al. [7] introduced a ring signature based scheme to protect usage profiles. However, its computational cost increases with the size of the ring. In [8], a mesh-network-based privacy-preserving data aggregation scheme has been proposed using elliptic curve cryptography (ECC). However, this scheme requires higher setup and computation cost. Zhang et al. have proposed a self-certified signature scheme [9] and Sui et al. have designed an incentive-based anonymous authentication scheme [10]. These are constructed with the assumption of an anonymity network, where the sources of

P. Gope, is with Department of Computer Science, National University of Singapore, 21 Lower Kent Ridge Rd, Singapore 119077. (E-mail: prosana.nitdgp@gmail.com/prosanta@comp.nus.edu.sg)

B. Sikdar is with Department of Electrical and Computer Engineering, National University of Singapore, 21 Lower Kent Ridge Rd, Singapore 119077. (Email: bsikdar@nus.edu.sg)

Corresponding author: P. Gope

usage reports are anonymous. Therefore, it is hard to identify any smart meter or communication failure. Li et al. introduced a different technique for data aggregation in smart grids in a hop-by-hop way [11], [12]. But it is still unclear how to construct the aggregation tree, and how to ensure aggregation in case of failure. Besides, the public key signatures used in these schemes result in higher computational cost. Apart from the schemes above, there are few more data aggregation protocols that have been introduced in recent years [13], [14], [15], [16]. In [13] a discrete logarithm problem (DLP)-based data aggregation scheme is introduced, in which the authors allows a substation to access private data using a shared key. Hence, this scheme cannot ensure strong privacy. In [14], Kursawe et al. suggested a set of masking-based schemes for privacy in smart grids. In their schemes, the authors utilized the concept of Decisional Diffie-Hellman (DDH) group and Bilinear mapping for checking the correctness of the shared masking value, which are computationally expensive and ill-suited for resource constrained smart meters. Knirsch et al. have also proposed a masking-based approach for data aggregation [15]. Their scheme utilizes the concept of homomorphic hashing for checking the correctness of the shared secrets. However, this construction has a couple of issues. First, it is complicated to implement and computationally expensive to execute. Second, it cannot ensure security of the hashed data, and an attacker can compute the original message block by taking the logarithm of the hash for that block. In [16] a Paillier homomorphic encryption based data aggregation protocol is proposed. However, in the proposed scheme, the usage reports transmitted by each smart meter SM_i reveals it's identity ID_{SM_i}, which is fixed for all transactions. Therefore, an adversary can easily understand that the usage data is from the same consumer's end and can easily link the ID_{SM_i} to an actual user. Thus, the scheme presented in [16] cannot ensure anonymity of a consumer. Mohammed et al. have proposed a multi-hop based data aggregation scheme [17]. However, in their scheme the usage report is transmitted without any integrity protection. Besides, during data aggregation, a smart meter is not authenticated. Consequently, a dishonest or fake smart meter may falsify the data, which will cause an inaccurate aggregated result. Apart from [3-17], recently two more interesting data aggregation schemes have been proposed [25-26]. However, these schemes are designed upon the computationally inefficient operations (such as EC-ElGamal cryptosystem and complex parabolic function). Hence, they would be infeasible for the resource constrained smart meters.

B. Problem Statement and Motivation

The collection of fine-grained energy consumption data is necessary for a number of smart-grid features and applications. For example, implementing dynamic electricity pricing based on time-of-day schedules, demand-side management through financial incentives, and energy demand-response management requires the collection of meter readings multiple times a day. Also, consumers may wish to know their energy usage information on a given day or period in order to adjust their energy consumption. Therefore, the utility or its designated data aggregator needs the ability to collect smart meter readings at arbitrary intervals or periods. Although several existing techniques have been proposed for privacy-preserving data aggregation for billing or demand-response management of energy in smart grids, most of the existing schemes are based on computationally expensive operations such as Paillier crypto system, lattice-based encryption, ElGamal encryption etc. On the other hand, in the existing masking-based schemes, for verifying the correctness of the masking secrets, they also use the computationally expensive operations such as DDH group and Bilinear mapping, or homomorphic hashing, which are not suitable for the resource-limited smart meters. For example, a smart meter from Atmel's family with ARM Cortex-M4 processor can provide a maximum CPU speed of 720 MHz [20]. As such, this smart meter may not be suitable to perform any computationally expensive operations. Also, since smart grid systems are mostly operated in a large scale, computationally expensive operations may impair the efficiency of the system. Furthermore, existing billing solutions in the literature consider a constant tariff price rate throughout the day (even for the whole month), which is not suitable for the *dynamic electricity pricing-based billing model* used in many counties (such as Finland, Estonia, Norway, etc.) [22]. For instance, in Portugal, tariff price rate varies four times in a day based on peak (3 hours/day), half-peak (14 hours/day), normal off-peak (3 hours/day) and super off-peak (4 hours/day). For that, we need a dynamic pricing-based billing model.

This paper seeks to address all these issues by proposing an efficient data aggregation scheme (EDAS) for privacy-aware secure billing systems and facilitating applications such as balancing the power production and demand in smart grids. Our proposed scheme is based on symmetric key cryptographic primitives such as hash functions, which cause very limited computational overhead and data aggregation time and hence is suitable for the resource constrained devices in smart grids. The key contributions of this paper can be summarized as:

- An efficient *authentication and key establishment scheme* is developed for data aggregation for dynamic pricing-based billing.
- A computationally efficient, lightweight *data aggregation scheme*, EDAS, is proposed for dynamic pricing-based billing systems that ensures the privacy of the consumer's identity as well as the usage data. To the best of our knowledge, this is the *first paper* to address privacy in the context of billing under dynamic electricity pricing.
- A novel data aggregation scheme for a group of consumers (e.g. from a region/locality) is proposed that does not compromise the privacy of any individual customer.
- The proposed scheme provides a higher degree of efficiency. Specifically, the proposed scheme does not need to perform any asymmetric cryptographic operations.

The rest of the paper is organized as follows. In Section II, we present the underlying smart grid model, adversary model, and security goals that are relevant to this paper. Section III presents the proposed EDAS scheme and its security is analyzed in Section IV. A discussion on the performance of

TABLE I
NOTATIONS AND CRYPTOGRAPHIC FUNCTIONS

Symbol	Definition
SP	Service provider
HAN	Home area network
HG	Home gateway
SM	Smart meter
TPA	Third-party aggregator
SID_i	Shadow identity of the HG$_i$
TID_i	Temporary Identity of the HG$_i$
k_i	Secret key of the HG$_i$
K_{as}	Shared secret key between TPA and SP
k_{hi}	Shared integrity key between HG$_i$ and TPA
ENC$_k[x]$	Plaintext x encrypted using key k
M_{ij}	Meter reading of the smart meter SM$_i$ at time interval T_j

the proposed scheme is presented in Section V and Section VI concludes the paper. The symbols and cryptographic functions used in this paper are defined in Table I.

II. System and Adversary Model, and Security Goals

In this section, we first describe the network architecture of the proposed privacy-preserving data aggregation mechanism and present the underlying adversary model. Subsequently, we define the security goals of our proposed scheme.

A. System Model

Figure 1 shows our system model for the smart metering infrastructure which is used to develop the proposed scheme. Our system model consists of five major entities: a service provider (SP), a third-party aggregator (TPA) employed by the service provider, a set of smart meters (SMs), a set of home gateways (HGs), and numerous home area networks (HANs). In our system model, the SP is responsible for procuring electricity from the producers, supplying electricity to consumers, and sending billing notification to each HAN. The TPA is responsible for accumulating the power consumption data of each HAN. At the end of each day or any specific period, the TPA sends the aggregated data to the SP for billing purposes. In this way, the TPA assists the SP to implement dynamic pricing-based billing and also reduces the overhead of the SP. Next, each HAN is composed of a SM, a HG, and a set of home appliances (HAs). Each SM is connected with its HG through a trusted link. A HG periodically collects reading from the SM and sends it to the TPA. The communication between a SM and its HG is through WiFi. Each HG communicates with the TPA through a Long-Term-Evolution-Advanced (LTE-A) network. Note that while the network model is provided for completeness, the proposed EDAS scheme does not rely on any specific underlying networking technology.

B. Adversary Model

In our system model, the SP handles the billing process. Therefore, the SP has to know relevant information about the consumer such as the consumer's name and the mailing address etc. Hence, in our adversary model we consider the SP as a trusted organization (e.g. owned by the government, such as Singapore Power in Singapore and National Grid in United Kingdom). On the other hand, the TPA is owned by a private company whose main responsibility is to assist the SP. Therefore, in our system model we consider the TPA as a honest-but-curious entity, who may want to know the consumption data of each HAN and subsequently may try to sell the usage information to another company, e.g. for marketing materials for home appliances. Various elements inside the communication network may also act as adversaries and be interested in private details of the power consumption of each HAN. A compromised network and its various elements (like router or switch) can alter or fabricate the meters' consumption data. Hence, any communication through the network may not be secure. Usually, the TPA and the communication network (like LTE-A) are owned and operated by two different organizations, and therefore we assume that they do not collude with each other. Also, any HG may act as an adversary and be interested to know the consumption data of another HG from a different HAN. An outside attacker may try to impersonate as a legitimate entity that can be a HG, or the TPA, to send data under its name. For instance, a dishonest or fake HG could falsify the data for causing inaccurate aggregation result. In addition, the outside attacker may eavesdrop on the network transmission media for obtaining the power consumption data and also may try to alter or retransmit them.

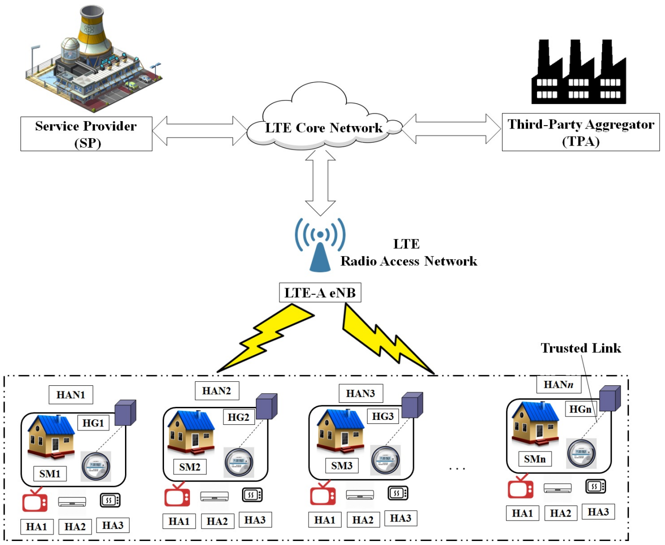

Fig. 1. System model for smart metering infrastructure.

C. Security Goals

- **Authentication:** Before aggregating any data, the TPA needs to authenticate each HG in order to prevent inaccurate aggregation results. On the other hand, before obtaining the aggregated data from the TPA through the insecure public communication channel, the SP needs to authenticate the TPA.
- **Usage Data Confidentiality**: The secrecy of the end-to-end communication is vital and the electricity consumption data should be kept secret from any third party for protecting the privacy of the customer. In this regard, if

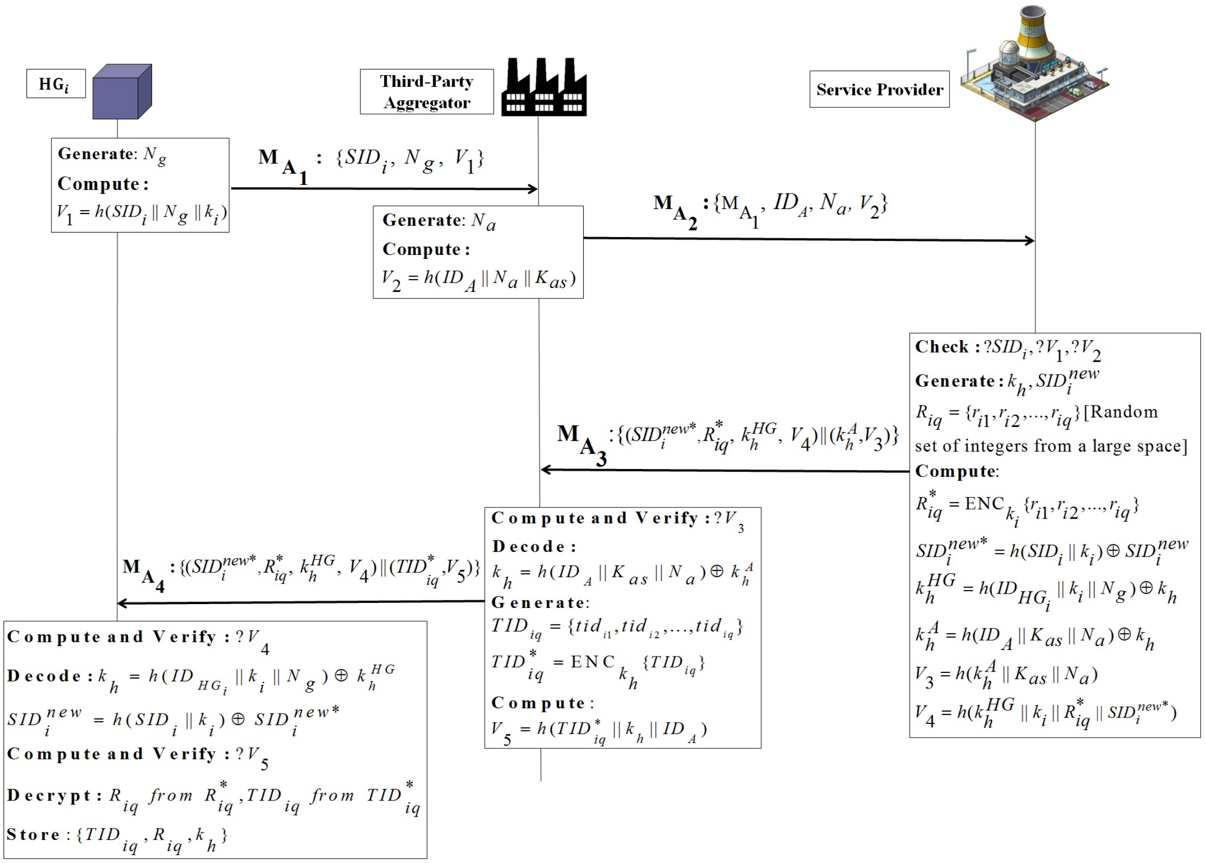
HG_i
Third-Party Aggregator
Service Provider
Generate: N_g
Compute:
$V_1 = h(SID_i \| N_g \| k_i)$
M_{A_1} : $\{SID_i, N_g, V_1\}$
Generate: N_a
Compute:
$V_2 = h(ID_A \| N_a \| K_{as})$
M_{A_2} : $\{M_{A_1}, ID_A, N_a, V_2\}$
Check : $?SID_i, ?V_1, ?V_2$
Generate : k_h, SID_i^{new}
$R_{iq} = \{r_{i1}, r_{i2}, ..., r_{iq}\}$ [Random set of integers from a large space]
Compute:
$R_{iq}^* = \text{ENC}_{k_i}\{r_{i1}, r_{i2}, ..., r_{iq}\}$
$SID_i^{new*} = h(SID_i \| k_i) \oplus SID_i^{new}$
$k_h^{HG} = h(ID_{HG_i} \| k_i \| N_g) \oplus k_h$
$k_h^A = h(ID_A \| K_{as} \| N_a) \oplus k_h$
$V_3 = h(k_h^A \| K_{as} \| N_a)$
$V_4 = h(k_h^{HG} \| k_i \| R_{iq}^* \| SID_i^{new*})$
M_{A_3} : $\{(SID_i^{new*}, R_{iq}^*, k_h^{HG}, V_4) \| (k_h^A, V_3)\}$
Compute and Verify : $?V_3$
Decode : $k_h = h(ID_A \| K_{as} \| N_a) \oplus k_h^A$
Generate:
$TID_{iq} = \{tid_{i1}, tid_{i2}, ..., tid_{iq}\}$
$TID_{iq}^* = \text{ENC}_{k_h}\{TID_{iq}\}$
Compute:
$V_5 = h(TID_{iq}^* \| k_h \| ID_A)$
M_{A_4} : $\{(SID_i^{new*}, R_{iq}^*, k_h^{HG}, V_4) \| (TID_{iq}^*, V_5)\}$
Compute and Verify : $?V_4$
Decode : $k_h = h(ID_{HG_i} \| k_i \| N_g) \oplus k_h^{HG}$
$SID_i^{new} = h(SID_i \| k_i) \oplus SID_i^{new*}$
Compute and Verify : $?V_5$
Decrypt : R_{iq} from R_{iq}^*, TID_{iq} from TID_{iq}^*
Store : $\{TID_{iq}, R_{iq}, k_h\}$

Fig. 2. Authenticated initialization and refilling process.

an outsider or an inside adversary like other HGs from different HANs or the TPA obtains the messages with electricity consumption information, then he/she should not be able to comprehend the encrypted message.

- **Usage Data Integrity:** The TPA should be able to verify the integrity of the data received from each HG of a HAN. Similarly, the SP needs to check the integrity of the aggregated data received from the TPA.
- **Consumer Privacy:** The TPA should not be able to extract any private information (e.g, name, address, contact number, etc.) of a HAN user. Only the SP should have the ability to know a consumer's real identity, and their electricity usage. This is necessary for determining the actual electricity consumption and proper billing services. In addition, after eavesdropping the usage data, an outside adversary should not be able to comprehend that the data is from a particular consumer's end.
- **Forward Secrecy:** Forward secrecy is extremely important since cryptographic computations, e.g., encryption, and authentication, are often carried out during data aggregation. In a scheme with forward secrecy, secret keys are evolved at regular time periods. Exposure of a secret key corresponding to a given time period does not enable an adversary to break the scheme for any prior time period. In other words, forward secrecy ensures that the messages of prior time periods are confidential even if the current time period's key has been compromised. To improve the security level of smart meters, forward secrecy should be considered. Now, to ensure forward secrecy in our proposed scheme, it is important that the exposure of shared secret keys of HG_i, TPA, and SP should not enable the adversary to obtain the aggregated meter reading and billing information of each user in the previous time periods.

III. Proposed Energy-Efficient Data Aggregation Scheme - EDAS

In this section we present our EDAS which consists of three phases: *authenticated initialization and refilling*, *data aggregation for dynamic pricing-based billing*, and *data aggregation for demand-response management*. In the authenticated initialization and refilling phase, a home gateway HG_i and the aggregator TPA mutually authenticate each other with the help of the SP and subsequently establish an integrity key k_{hi}, a set of random integers, and temporary identities between them. In addition, through this phase, both the HG_i and the TPA can update their integrity key and establish a new set of temporary identities. In the data aggregation for dynamic pricing-based billing phase, the TPA anonymously accumulates the usage data and eventually sends it to the SP for billing. In the final phase of EDAS, the TPA anonymously accumulates and aggregates the usage data of a group of HANs in order to assists the SP with demand-response management.

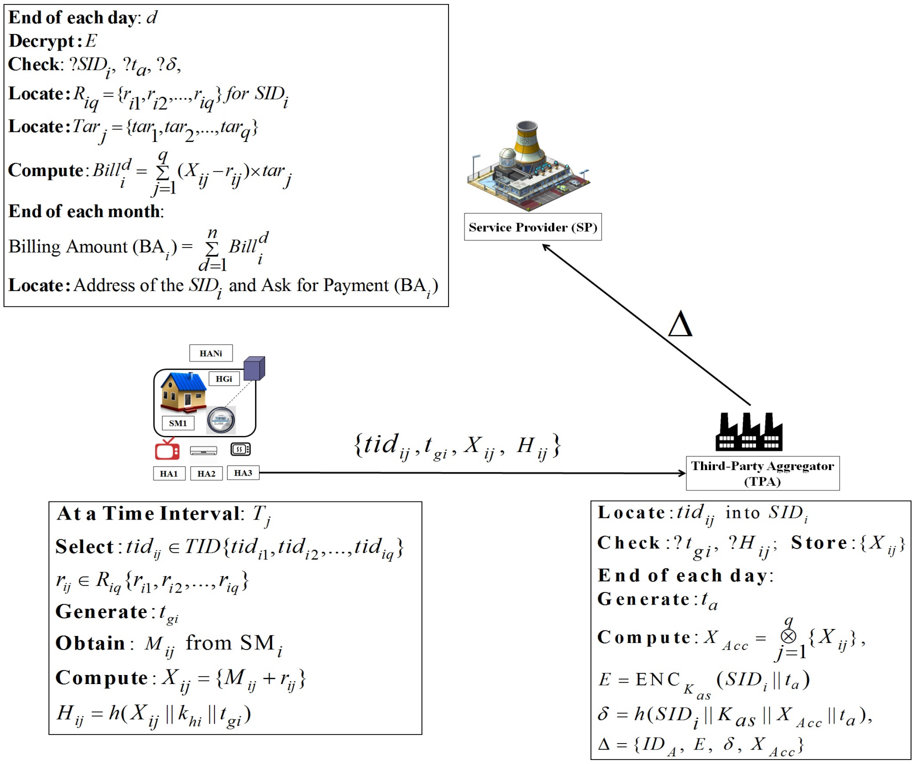
End of each day: d
Decrypt: E
Check: $?SID_i$, $?t_a$, $?\delta$,
Locate: $R_{iq} = \{r_{i1}, r_{i2}, \ldots, r_{iq}\}$ *for* SID_i
Locate: $Tar_j = \{tar_1, tar_2, \ldots, tar_q\}$
Compute: $Bill_i^d = \sum_{j=1}^{q} (X_{ij} - r_{ij}) \times tar_j$
End of each month:
Billing Amount (BA_i) = $\sum_{d=1}^{n} Bill_i^d$
Locate: Address of the SID_i and Ask for Payment (BA_i)
Service Provider (SP)
Δ
HANi
HGi
SM1
HA1
HA2
HA3
$\{tid_{ij}, t_{gi}, X_{ij}, H_{ij}\}$
Third-Party Aggregator (TPA)
At a Time Interval: T_j
Select: $tid_{ij} \in TID\{tid_{i1}, tid_{i2}, \ldots, tid_{iq}\}$
$r_{ij} \in R_{iq}\{r_{i1}, r_{i2}, \ldots, r_{iq}\}$
Generate: t_{gi}
Obtain: M_{ij} from SM_i
Compute: $X_{ij} = \{M_{ij} + r_{ij}\}$
$H_{ij} = h(X_{ij} || k_{hi} || t_{gi})$
Locate: tid_{ij} into SID_i
Check: $?t_{gi}$, $?H_{ij}$; **Store**: $\{X_{ij}\}$
End of each day:
Generate: t_a
Compute: $X_{Acc} = \bigotimes_{j=1}^{q} \{X_{ij}\}$,
$E = \mathrm{ENC}_{K_{as}}(SID_i || t_a)$
$\delta = h(SID_i || K_{as} || X_{Acc} || t_a)$,
$\Delta = \{ID_A, E, \delta, X_{Acc}\}$

Fig. 3. Proposed computationally efficient and lightweight data aggregation scheme for secure dynamic pricing-based billing process in smart grids.

A. Authenticated Initialization and Refilling

Assume that there are n HANs in a locality which obtain power supply from the SP. During meter installation of a home HAN_i, the SP randomly generates a shadow identity SID_i and a secret key k_i and assigns them to the HG of HAN_i. This phase of the proposed scheme consists of the following steps:

Step 1: HG_i generates a nonce N_g and computes $V_1 = h(SID_i||N_g||k_i)$. Then, HG_i composes a request message $\mathrm{M}_{\mathrm{A}_1} : \{SID_i, N_g, V_1\}$ and sends it to the TPA. Since, a particular shadow identity SID_i cannot be used twice, the request message $\mathrm{M}_{\mathrm{A}_1}$ cannot be replayed. Moreover to address the loss of synchronization issue or denial of service (DoS) attack [19], both HG_i and the SP can maintain a set of pseudo identities $PID_i = \{pid_1, pid_2, \cdots, pid_n\}$, where each identity can be used only once and after that it must be deleted by both sides.

Step 2: Upon receiving the request message $\mathrm{M}_{\mathrm{A}_1}$, the TPA generates a random number N_a and computes $V_2 = h(ID_A||N_a||K_{as})$. Subsequently, the TPA creates a message $\mathrm{M}_{\mathrm{A}_2} : \{\mathrm{M}_{\mathrm{A}_1}, ID_A, N_a, V_2\}$ and sends it to the SP.

Step 3: After receiving the message $\mathrm{M}_{\mathrm{A}_2}$, the SP first tries to identify SID_i and then checks V_1 and V_2. If these parameters are valid, then the SP randomly generates an integrity key k_h, a new shadow identity SID_i^{new}, and picks a set of q random integers $R_{iq} = \{r_{i1}, r_{i2}, \cdots, r_{iq}\}$ drawn uniformly from $[a, b]$, where a and b are chosen to be orders of magnitude larger than the typical meter value. For instance, in the USA the average power consumption of a house is about 15 kWh each day. In this scenario, a and b may be chosen as 10^6 and 10^8, respectively. To ensure better privacy, the choice of a and b should be changed regularly. Now, the SP computes $R_{iq}^* = \mathrm{ENC}_{k_i}\{r_{i1}, r_{i2}, \cdots, r_{iq}\}$, $SID_i^{new*} = h(SID_i||k_i) \oplus SID_i^{new}$, $k_h^{HG} = h(ID_{HG_i}||k_i||N_g) \oplus k_h$, $k_h^A = h(ID_A||K_{as}||N_a) \oplus k_h$, $V_3 = h(k_h^A||K_{as}||N_a)$, and $V_4 = h(k_h^{HG}||k_i||R_{iq}^*||SID_i^{new*})$. It then composes a message $\mathrm{M}_{\mathrm{A}_3} : \{(SID_i^{new*}, R_{iq}^*, k_h^{HG}, V_4)||(k_h^A, V_3)\}$ and sends it to the TPA. Here, ENC denotes symmetric-key-based encryption using the Advanced Encryption Standard (AES).

Step 4: On receiving $\mathrm{M}_{\mathrm{A}_3}$, the TPA first validates V_3. If the validation is successful, then the TPA decodes $k_h = h(ID_A||K_{as}||N_a) \oplus k_h^A$ and generates a set of q unique temporary identities $TID_{iq} = \{tid_{i1}, tid_{i2}, \cdots, tid_{iq}\}$. Next, the TPA derives $TID_{iq}^* = \mathrm{ENC}_{k_h}(TID_{iq})$, $V_5 = h(TID_{iq}^*|| k_h||ID_A)$ and creates a message $\mathrm{M}_{\mathrm{A}_4} : \{(SID_i^{new*}, R_{iq}^*, k_h^{HG}, V_4)||(TID_{iq}^*|| V_5)\}$ and sends it to HG_i.

Step 5: Upon receiving the message $\mathrm{M}_{\mathrm{A}_4}$, HG_i first computes and verifies V_4 and then decodes $k_h = h(ID_{HG_i}||k_i||N_g) \oplus k_h^{HG}$ and $SID_i^{new} = h(SID_i||k_i) \oplus SID_i^{new*}$. Hereafter, HG_i verifies the parameter V_5. If all the validations are successful, HG_i decrypts R_{iq} from R_{iq}^*, and TID_{iq} from TID_{iq}^*, and stores $\{TID_{iq}, R_{iq}, k_h\}$ for data aggregation. Details of this phase are also depicted in Fig. 2.

B. Data Aggregation for Dynamic Pricing-based Billing

In this subsection, we present our privacy-friendly and efficient data aggregation scheme for dynamic pricing-based billing, where we consider the variations in tariff prices throughout the day according to the time-of-day period schedules. After a pre-defined schedule of the time interval T_j, HG_i collects the meter reading of SM_i, selects the next

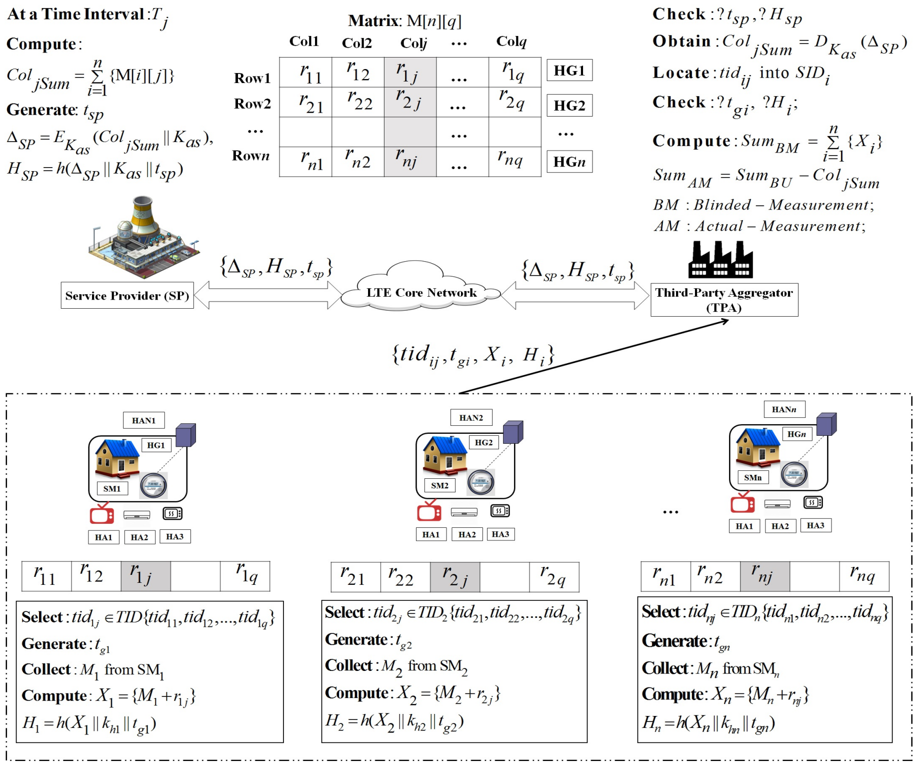
At a Time Interval: T_j
Compute:
$Col_{jSum} = \sum_{i=1}^{n} \{M[i][j]\}$
Generate: t_{sp}
$\Delta_{SP} = E_{K_{as}}(Col_{jSum} \| K_{as})$,
$H_{SP} = h(\Delta_{SP} \| K_{as} \| t_{sp})$
Matrix: M[n][q]
Col1
Col2
Col$j$
...
Col$q$
Row1
Row2
...
Row$n$
r_{11} r_{12} r_{1j} ... r_{1q}
r_{21} r_{22} r_{2j} ... r_{2q}
r_{n1} r_{n2} r_{nj} ... r_{nq}
HG1
HG2
HGn
Check: ?t_{sp}, ?H_{sp}
Obtain: $Col_{jSum} = D_{K_{as}}(\Delta_{SP})$
Locate: tid_{ij} into SID_i
Check: ?t_{gi}, ?H_i;
Compute: $Sum_{BM} = \sum_{i=1}^{n} \{X_i\}$
$Sum_{AM} = Sum_{BU} - Col_{jSum}$
BM : $Blinded - Measurement$;
AM : $Actual - Measurement$;
$\{\Delta_{SP}, H_{SP}, t_{sp}\}$
Service Provider (SP)
LTE Core Network
$\{\Delta_{SP}, H_{SP}, t_{sp}\}$
Third-Party Aggregator (TPA)
$\{tid_{ij}, t_{gi}, X_i, H_i\}$
HAN1
HG1
SM1
HA1
HA2
HA3
HAN2
HG2
SM2
HA1
HA2
HA3
...
HANn
HGn
SMn
HA1
HA2
HA3
r_{11} r_{12} r_{1j} r_{1q}
r_{21} r_{22} r_{2j} r_{2q}
r_{n1} r_{n2} r_{nj} r_{nq}
Select: $tid_{1j} \in TID\{tid_{11}, tid_{12}, ..., tid_{1q}\}$
Generate: t_{g1}
Collect: M_1 from SM$_1$
Compute: $X_1 = \{M_1 + r_{1j}\}$
$H_1 = h(X_1 \| k_{h1} \| t_{g1})$
Select: $tid_{2j} \in TID_2\{tid_{21}, tid_{22}, ..., tid_{2q}\}$
Generate: t_{g2}
Collect: M_2 from SM$_2$
Compute: $X_2 = \{M_2 + r_{2j}\}$
$H_2 = h(X_2 \| k_{h2} \| t_{g2})$
Select: $tid_{nj} \in TID_n\{tid_{n1}, tid_{n2}, ..., tid_{nq}\}$
Generate: t_{gn}
Collect: M_n from SM$_n$
Compute: $X_n = \{M_n + r_{nj}\}$
$H_n = h(X_n \| k_{hn} \| t_{gn})$

Fig. 4. Proposed computationally efficient and lightweight data aggregation scheme for demand-response management in smart grids.

unused masking value $r_{ij} \in R_{iq}$, and calculates the blinded measurement $X_{ij} = \{M_{ij} + r_{ij}\}$, where it is assumed that $r_{ij} \ggg M_{ij}$. Then, HG$_i$ selects an unused temporary identity $tid_{ij} \in TID\{tid_{i1}, tid_{i2}, \cdots, tid_{iq}\}$, generates a timestamp t_{gi}, and computes $H_{ij} = h(X_{ij}||k_h||t_{gi})$. Finally, HG$_i$ composes a message $\{tid_{ij}, t_{gi}, X_{ij}, H_{ij}\}$ and sends it to the TPA. Then, HG$_i$ deletes the pair of used (r_{ij}, tid_{ij}) from the respective lists. Note that once all the masking values $R_{iq} = \{r_{i1}, r_{i2}, \cdots, r_{iq}\}$ and temporary identities $tid_{ij} \in TID\{tid_{i1}, tid_{i2}, \cdots, tid_{iq}\}$ are used up, HG$_i$ needs to execute Phase 1 again.

Now, upon receiving the usage data, the TPA first locates and validates the temporary identity tid_{ij}, along with the timestamp t_{gi} and key-hash integrity output H_{ij}. If the validation is successful, the TPA stores X_{ij} in its database. Otherwise, the TPA terminates the accumulation process and asks HG$_i$ to send the reading again. At the end of the day (or any desired interval), the TPA generates a timestamp t_a and then computes $X_{ACC} = \bigotimes_{j=1}^{q}\{X_{ij}\}$, $E = \text{ENC}_{K_{as}}(SID_i||t_a)$, and $\delta = h(SID_i||K_{as}||X_{ACC}||t_a)$. Here, $\bigotimes$ denotes the accumulation of the blinded measurements, i.e., $\{X_{i1}||X_{i2}||\cdots||X_{iq}\}$. Finally, the TPA composes a message $\Delta = \{ID_A, E, \delta, X_{ACC}\}$ and sends it to the SP. After receiving the power consumption information Δ, the SP first decrypts E and then validates the timestamp t_a, and δ. If the validation is successful, the SP locates $R_{iq} = \{r_{i1}, r_{i2}, \cdots, r_{iq}\}$ and the list of tariff prices $Tar[q] = \{tar_1, tar_2, \cdots, tar_q\}$ for each interval and subsequently computes the bill amount for the day d, i.e., $Bill_i^d = \sum_{j=1}^{q}(X_{ij} - r_{ij})Tar[j]$ and stores $Bill_i^d$ in its database. Thus, the consumer can see his/her energy usage for each day. At the end of the month, the SP calculates the billing amount $BA_i = \sum_{d=1}^{n} Bill_i^d$. After calculating BA_i, the SP locates the consumer information and sends the bill to the owner of HAN$_i$. Details of this phase are depicted in Fig. 3.

Note that for the correctness of the proposed scheme, both the SP and HG$_i$ should sequentially use the masking values from $R_{iq} = \{r_{i1}, r_{i2}, \cdots, r_{iq}\}$. For instance, if it is assumed that there are five different tariff prices throughout the day, then HG$_i$ needs to send the usage information of HAN$_i$ five times $(T_1, T_2, \cdots, T_5)$ in a day. Now, we further assume that after the execution of each *authenticated initialization and refilling phase*, HG$_i$ receives five masking values, i.e., $R_{i5} = \{r_{i1}, r_{i2}, \cdots, r_{i5}\}$. Therefore, both the SP and HG$_i$ are required to use R_{i5} in the following way: $\{r_{i1}$ (at T_1), r_{i2} (at T_2), $\cdots$, r_{i5} (at T_5)$\}$. However, for better performance of the proposed scheme, we assume that after execution of each *authenticated initialization and refilling phase*, HG$_i$ receives the masking values for two to three days.

C. Data Aggregation for Demand-Response Management

For maintaining balance between power production and demand, the SP needs to know the electricity usage of its users or any sub-group of its users (e.g. from a specific geographic region) on a regular basis (say, every one or two hours). Consider a group of n users for aggregation. In this regard, the SP maintains a $n \times q$ matrix (P) of random integers, whose i-th row comprises of the vector $R_{iq} = \{r_{i1}, r_{i2}, \cdots, r_{iq}\}$ that was generated for and shared with HG$_i$ during the execution of the *authenticated initialization and refilling phase*. All HGs are synchronized with respect to their vector R_{iq} and for any time period T_j specified by the SP or the TPA, each HAN uses the j-th element of its vector of random variables (i.e., r_{ij} for HG_i). Our data aggregation process then consists of the following steps:

Step AG1: At a particular time interval T_j, the SP selects the corresponding column of M and calculates $Col_{jSum} = \sum_{i=1}^{n} P[i][j]$. It then generates a time stamp t_{sp} and computes $\Delta_{SP} = \mathrm{ENC}_{K_{as}}(Col_{jSum}||K_{as})$, $H_{SP} = h(\Delta_{SP}||K_{as}||t_{sp})$, and subsequently sends $\{\Delta_{SP}, H_{SP}, t_{sp}\}$ to the TPA.

Step AG2: Upon receiving $\{\Delta_{SP}, H_{SP}, t_{sp}\}$, the TPA first checks whether the time stamp t_{sp} and H_{SP} are valid or not. If they are valid, the TPA decrypts and obtains Col_{jSum} from Δ_{SP}. Then the TPA asks the HGs to return their reading for that interval.

Step AG3: Next, each gateway HG_i picks an unused temporary identity $tid_{ij} \in TID$ and selects the predefined random integer r_{ij} from its array, which was assigned for that particular interval. The HG_i then collects the meter reading M_i for that interval from SM_i and generates a time stamp t_{gi}. HG_i then calculates its blinded measurement $X_i = M_i + r_{ij}$, computes $H_i = h(X_1||k_{hi}||t_{gi})$, composes a message $\{tid_{ij}, t_{gi}, X_i, H_i\}$, and sends it to the TPA.

Step AG4: After receiving the meter reading from each home gateway HG_i, the TPA first checks t_{gi} and H_i, and then maps tid_{ij} into SID_i. It then computes the sum of the blinded measurement $Sum_{BM} = \sum_{i=1}^{n} X_i$, and obtains the aggregated result of the actual measurement by $Sum_{AM} = Sum_{BM} - Col_{jSum}$. Thus the TPA obtains the aggregated power consumption data of the HANs, which may be used as an input for demand-response management.

Note that in our system if any of the checks in the steps above fails, this phase of the proposed scheme is aborted. Besides, to expedite the performance of the above data aggregation scheme, the SP can pre-compute Δ_{SP} and H_{SP} for several sessions and send them to the TPA. Finally, in order to ensure forward secrecy in the proposed scheme, at the end of each interaction, all the three entities (HG_i, the TPA, and the SP) need to update their shared secret keys. For example, after sending/receiving the aggregated data of each day, both HG_i and the TPA need to update the hash-integrity key with $k^*_{hi} = h(k_{hi}||t_{gi})$. In case of loss of synchronization or denial of service (DoS) attack [19], both HG_i and the TPA need to execute the *authenticated initialization and refilling phase* of the proposed scheme. Details of this phase are depicted in Fig. 4.

IV. Security Analysis

In this section, we demonstrate that the proposed scheme can achieve all the security goals listed in Section II.

1) Accomplishment of Authentication: In the *authenticated initialization and refilling* phase of EDAS, the SP authenticates HG_i by verifying the shadow identity SID_i and V_1 in the request message $\mathrm{M}_{\mathrm{A}_2}$, where only a legitimate HG_i can generate the valid key-hash output V_1. Besides, the SP authenticates the TPA by using the request parameter V_2, which must be equal to $h(ID_A||N_a||K_{as})$. On the other hand, both HG_i and the TPA authenticate the SP by using the response parameters V_3 and V_4, respectively. Now, in the *data aggregation for billing phase* of EDAS, before accumulating any usage data, the TPA authenticates HG_i by using the time-stamp t_{gi} and the response H_{ij}. Moreover, in this phase of EDAS, the SP authenticates the TPA by using the hash-response parameter δ. On the other hand, in the *data aggregation for balancing demand-response phase* of EDAS, the TPA authenticates HG_i by using the time-stamp t_{gi} and the response H_i. Finally, in EDAS, if an adversary tries to perform any replay attempt, the receiving end can easily comprehend such attacks by using the timestamps $\{t_{gi}, t_a\}$. Therefore, the proposed scheme is also secure against replay attacks.

2) Accomplishment of Usage Data Confidentiality: The amount of electricity usage in HAN_i is blinded with the random integer r_{ij}. Hence, the TPA can only see the blinded measurement of a HAN or the summation of the usage data of a group of HANs. As each element of R_{iq} is unique and random, even if two consecutive readings from a HAN or the readings from two HANs are the same, an adversary (even the TPA) cannot comprehend that from the blinded measurements. Thus, the pattern of the electricity consumption is protected from detection by any eavesdropper.

3) Accomplishment of Usage Data Integrity: In the *data aggregation for billing phase*, we ensure two levels of data integrity. In the first level, the TPA checks whether it has received the same data as that was sent by HG_i. For that, the TPA computes H^*_{ij} and checks whether H^*_{ij} is equal to H_{ij} or not. Similarly, in the second level, the SP invokes the key-hash oracle and computes δ^* to check the integrity of the aggregated electricity consumption by comparing δ^* with δ. This approach facilitates the detection of any manipulation of the aggregated usage data during communication. On the other hand, in the *data aggregation for balancing demand-response phase* of EDAS, the TPA checks the integrity of the usage data by using the parameter H_i, which helps to prevent the generation of an inaccurate aggregated result.

4) Accomplishment of Consumer Privacy : In EDAS, except for the SP, no one can gain knowledge of any private information of a HAN user. The TPA only knows the shadow identity SID_i and uses that to accumulate the readings for each HAN. Besides, while sending the usage data, HG_i is not allowed use the same temporary identity tid_{ij} twice. No one except the TPA can recognize the mapping between tid_{ij} and SID_i. Therefore, an outsider cannot guess whether the usage data for two consecutive days are from the same HAN user. This approach of the proposed scheme is quite useful for achieving privacy against eavesdropper (PAE) [21].

5) Accomplishment of Forward Secrecy : EDAS uses a regular update of the shared keys k_{hi} and K_{as}. For instance, after sending/receiving the usage data of each day, both HG_i and the TPA need to update the hash-integrity key k_h with k^*_h. Now, even if the integrity key k^*_h is revealed, an attacker cannot obtain k_h from k^*_h since the hash function $h(\cdot)$ is one-way. In this way, EDAS can prevent an attacker from obtaining any previous aggregated usage data and billing information.

TABLE II
PERFORMANCE BENCHMARKING BASED ON SECURITY PROPERTIES (NOTATION: A: AUTHENTICATION; DC: DATA CONFIDENTIALITY; DI: DATA INTEGRITY; CP: CONSUMER PRIVACY; FS: FORWARD SECRECY).

Scheme	A	DC	DI	CP	FS
Li et al. [12]	No	Yes	Yes	No	Yes
Fouda et al. [13]	Yes	No	Yes	No	Yes
Kursawe et al. [14]	No	Yes	Yes	No	No
Knirsch et al. [15]	No	Yes	Yes	No	Yes
Jo et al. [16]	Yes	Yes	Yes	No	Yes
Mohammed et al. [17]	No	Yes	No	Yes	Yes
EDAS	Yes	Yes	Yes	Yes	Yes

TABLE III
PERFORMANCE BENCHMARKING BASED ON COMPUTATION AND COMMUNICATION COST (NOTATION: H: HASH OPERATION; ASE/D: ASYMMETRIC ENCRYPTION/DECRYPTION; SE/SD: SYMMETRIC ENCRYPTION/DECRYPTION; MEO: MODULAR EXPONENTIATION OPERATION).

Performance Matrices	Fouda et al. [13]	EDAS
Key-establishment Cost	2ASE+2ASD +4MEO+2H	2SE+2SD +15H
Computation Cost at HG	1SE+1H	1H
Computation Cost at TPA	1SD+1H	1SE+1H
Computation Cost at SP	-	1SD+1H
Communication Cost (HG-TPA)	56 bytes	72 bytes
Communication Cost (TPA-SP)	-	80 bytes

V. PERFORMANCE ANALYSIS AND COMPARISONS

The objective of EDAS is not only to fulfill several security requirements in smart grids, but also to ensure that the computational and communication overhead is reasonable during the data aggregation process. To manifest the advantages of EDAS, we compare EDAS with recently proposed data aggregation schemes for smart grids: [12], [13], [14], [15], [16], and [17]. We also demonstrate that EDAS is well suited for resource limited smart grid devices (like smart meters and home gateways). In order to analyze the performance of EDAS, particularly on the security front, our scheme has been compared with five state-of-the-art protocols [12], [13], [14], [15], [16], and [17] (shown in Table II), by considering all the security goals listed in Section II. From Table II we see that EDAS can ensure *all* the security goals listed in Section II, in contrast to the protocols presented in [12], [13], [14], [15], [16], and [17] that only guarantee a *subset* of the requirements. For instance, in [12], [14], [15], and [17], while data aggregation the identity and the legitimacy of the smart meters are not verified. Consequently, a dishonest or fake smart meter may falsify the data, which will cause an inaccurate aggregated result. On the other hand, in [12], [13], [14], [15], [16], and [17], the smart meters reveal their fixed identity while transmitting the usage data. As a consequence, an adversary can easily comprehend that the usage data is from the same HAN. Therefore, [12], [13], [14], [15], [16], and [17] cannot ensure consumer privacy.

Next, we consider the computation and communication costs for analyzing the performance of the *data aggregation for billing phase* in EDAS with respect to other existing schemes. To ensure fairness, we compare EDAS with the scheme in [13] because both of these schemes use symmetric-key crypto systems to ensure privacy and integrity of the usage data for billing process. Before data aggregation, both the schemes require the establishment of a shared secret key between the HG and the TPA through an authenticated key-exchange protocol. However, it should be noted that unlike [13], for maintaining forward security EDAS does not need to execute the authenticated key-establishment protocol for each transaction. Instead, once all the random integers R_{iq} are used up, EDAS executes the key-establishment protocol of the *authenticated initialization and refilling* phase for obtaining the new set of random integers (the results presented here use sets of 10 random integers). On the other hand, the key establishment protocol in [13] is based on the computationally expensive Diffie-Hellman key exchange scheme. In contrast, EDAS is based on the lightweight cryptographic primitives like one-way hash function, exclusive-OR, etc. (shown in Table III).

Next we present experimental results to analyze the performance of the proposed scheme more comprehensively. Table IV presents the experiential specifications, including the hardware, computational, and communication specifications. For measuring the computation time of different cryptographic operations used in [13] and/or EDAS, we conducted simulations of their cryptographic operations on an Intel Core i5-2500 processor with CPU speed 3.3 GHz (operating as the SP), an AMD E450 processor with 1.65 GHz CPU speed (operating as the TPA), and a HTC One X with ARM Cortex-A9 MPCore processor with 890 MHz CPU speed (operating as a HG). Moreover, the scheme presented in [13] uses asymmetric encryption during its key-establishment process and both EDAS and [13] use symmetric key encryption and hash operations during data aggregation. Hence, we emulate the Advance Encryption Standard with Cipher Block Chaining (AES-CBC) mode, the Elliptic Curve Integrated Encryption Scheme (ECIES), and SHA-256, as the symmetric encryption, asymmetric encryption, and hash operation, respectively. The simulation uses Java Cryptography Extension (JCE) [25] to evaluate the execution time of different cryptographic operations.

Based on our experimental results, the key-establishment process in [13] takes 147.48 ms on an average. Besides, for securely transferring 56 bytes of usage data, the protocol incurs 5.32 ms of communication cost. In our experiments, we consider the size of the usage data for each transactions to be 8 bytes, and the size of the identity of a HG and the hash integrity outputs to be 128 bits and 256 bits, respectively. Ensuring privacy and integrity of the usage data in [13] incurs 0.0075 ms of computation cost. Overall, the average computation and communication cost for data aggregation and billing process in [13] for an entire month is $N \times 152.9$ ms, where N denotes the number of times the aggregated usage data is sent from a HG to the TPA in a month. One the other hand, the key-establishment process in EDAS takes 57.03 ms. In addition, transferring 72 bytes of data (including usage data of 8 bytes) between a HG and the TPA takes 6.49 ms. At the end, for transferring billing information to the SP, EDAS takes 9.63 ms. Overall, the entire computation and communication costs for the data aggregation and billing process for each

TABLE IV
EXPERIMENTAL SPECIFICATIONS

Specification	**HG**	**TPA**	**SP**
Hardware Specification	HTC One X with ARM Cortex-A9 MPCore processor	AMD E450 processor	Intel Core i5-2500 processor
Computation Cost of the Cryptographic Operations Used in [13] and EDAS			
Computational Specification	**HG**	**TPA**	**SP**
SHA-256	0.00067 ms	0.00042 ms	0.00037 ms
AES-CBC-256 Encryption	0.0027 ms	0.0012 ms	0.00097 ms
AES-CBC-256 Decryption	0.0043 ms	0.0031 ms	0.0019 ms
Modular Exponentiation Operation	13.56 ms	8.93 ms	-
Elliptic Curve Integrated Encryption (ECIE)	17.37 ms	11.54 ms	-
Communication Cost			
Communication Specification	**HG-TPA**	**TPA-SP**	
Link Type	One-hop Wireless (802.11)	Wired (Internet)	
Average Transmission Time for 896-bits	12.32 ms	16.19 ms	

month in EDAS is $x \times 57.03 + N \times 6.49 + d \times 9.63$ ms, where x is the number of executions of the *authenticated initialization and refilling phase* in a month and d is the number of days in a month. Fig. 5 shows the total cost with respect to the number of HG data transmissions in a month. From Fig. 5, we see that if a HG sends it's meter reading twice in every day to the TPA (i.e. $N = 60$), $d = 30$ and $x = 15$ (i.e., one execution of the *authenticated initialization and refilling phase* every two days), then the scheme presented in [13] takes 9174 ms, whereas EDAS takes only 1533.3 ms. Finally, we consider the performance of the *demand-response management phase* in EDAS with the existing schemes. For this, we conducted simulations of the cryptographic operations used by the existing data aggregation schemes and by the proposed scheme on an AMD E450 processor with 1.65 GHz CPU speed (operating as the TPA or SP), and a HTC One X with ARM Cortex-A9 MPCore processor with 890 MHz CPU speed (operating as a HG). The simulations used the JPBC library Pbc-0.5.14 [23], JCE [25], and the Pailler library libpaillier-0.8 [24] to evaluate the execution time of different cryptographic operations. Table V shows the variation in the aggregation time for different numbers of SMs in the proposed scheme, and others. It can be seen from Table V that the aggregation time for the Pailler encryption based Li et al.'s scheme is higher than others. On the other hand, the data aggregation time for the proposed scheme is significantly lower as compared to the others. Hence, the proposed scheme is better suited for efficient data aggregation in smart-grids.

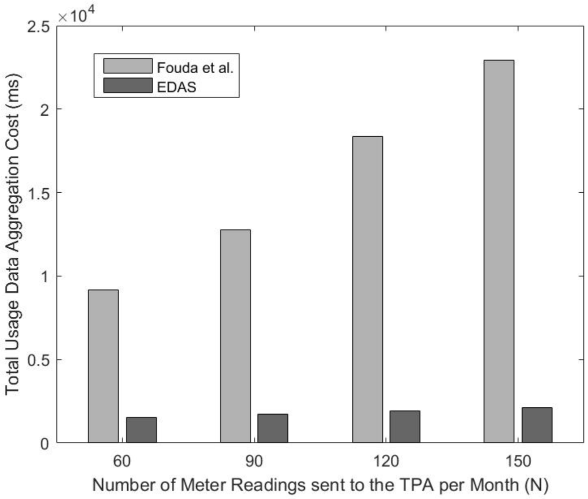

Fig. 5. Performance comparison between Fouda et al.'s scheme [13] and EDAS-based Billing Approach in terms of total data aggregation time.

TABLE V
VARIATION OF AGGREGATION TIME FOR VARIOUS NUMBER OF SMS

Schemes	**No of Smart Meters**	**Aggregation Time**
Li et al. [12]	200	3216 ms
	400	5829 ms
	500	7210 ms
Fouda et al. [13]	200	1.87 ms
	400	3.73 ms
	500	4.65 ms
Kursawe et al. [14]	200	2364 ms
	400	4698 ms
	500	5880 ms
Knirsch et al. [15]	200	89.6 ms
	400	123.45 ms
	500	165.97 ms
Jo et al. [16]	200	1247 ms
	400	2189 ms
	500	2685 ms
Mohammed et al. [17]	200	875 ms
	400	1546 ms
	500	2317 ms
EDAS	200	0.185 ms
	400	0.37 ms
	500	0.56 ms

VI. CONCLUSION

In this paper, we proposed an efficient data aggregation scheme (EDAS) for secure and privacy-aware dynamic pricing-based billing, and demand-response management in smart-grids. It is designed using lightweight symmetric-key-based cryptographic primitives. We analyzed the security of the proposed scheme and it was shown that EDAS can ensure several security properties like authentication, data privacy, data integrity, etc., which are highly important for smart grid security. Moreover, it was shown that EDAS has significantly lower computation and communication cost as compared to other data aggregation schemes. Hence, we argue that EDAS is efficient, practical, and more suitable for applications with real time requirements than other similar approaches for smart grid security.

Acknowledgment

This research was supported by the National Research Foundation, Prime Minister's Office, Singapore under its Corporate Laboratory@University Scheme, National University of Singapore, and Singapore Telecommunications Ltd.

References

[1] Y. Li, X. Cheng,Y.Cao, "Smart Choice for the Smart Grid:Narrowband Internet of Things (NB-IoT)," *IEEE Internet of Things Journal*, DOI: 10.1109/JIOT.2017.2781251,2017.

[2] R. Anderson and S. Fuloria,"Who controls the off switch?" *in Proc. IEEE SmartGridComm*, pp. 96-101, 2010.

[3] R. Lu, X. Liang, X.L Li, and X. Shen, "Eppa: an efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Trans. Parallel Distributed System,* vol. 23(9), pp. 1621–1631, 2012.

[4] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," In: Stern, J. (ed.) *EUROCRYPT* 1999. LNCS, vol. 1592, pp. 223–228. Springer, Heidelberg 1999.

[5] X. Liang, X. Li, R. Lu, X. Lin and X. Shen, "UDP: usage based dynamic pricing with privacy preservation for smart grid," *IEEE Transactions on Smart Grid*, vol. 4(1),pp. 141–150, 2013.

[6] M. Naehrig, K. Lauter and V. Vaikuntanathan, "Can homomorphic encryption be practical?," *In Proc. the 3rd ACM Cloud Computing Security Workshop*, pp. 113–124, 2011.

[7] Y. Chia-Mu, C.-Y. Chen, S.-Y. Kuo, H.-C. Chao, "Privacy-preserving power request in smart grid networks," *IEEE Syst. J*. vol. 8(2), pp. 441–449, 2014.

[8] S. Tonyali, O. Cakmak, K. akkaya, M. Mahmoud, and I. Guvenc, "Secure Data Obfuscation Scheme to Enable Privacy-Preserving State Estimation in Smart Grid AMI Networks,"*IEEE Internet of Things Journal*, vol. 3(5), OCTOBER 2016.

[9] J. Zhang, L. Liu, Y. Cui, Z. Chen, "SP 2 DAS:self-certified PKC-based privacy-preserving data aggregation scheme in smart grid," *Int. J. Distrib. Sens. Netw*, DOI: https://doi.org/10.1155/2013/457325, 1–11, 2013.

[10] Z. Sui, A. Alyousef, H. de Meer, "IAA: incentive-based anonymous authentication scheme in smart grids," *Internet Science* vol. 9089, pp. 133–144. Springer, Heidelberg (2015)

[11] F. Li, B. Luo, "Preserving data integrity for smart grid data aggregation," *in Proc. IEEE SmartGridComm*, pp. 366-371, Tainan, Taiwan, November 2012.

[12] F. Li, B. Luo, P. Liu, "Secure information aggregation for smart grids using homomorphic encryption," *in Proc. IEEE SmartGridComm*, pp. 327-332, Gaithersburg, USA, November 2010.

[13] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. Shen, "A lightweight message authentication scheme for smart grid communications," *IEEE Transactions on Smart Grid,* vol. 2(4), pp. 675–685, Dec. 2014.

[14] K. Kursawe, G. Danezis, and M. Kohlweiss, "Privacy-friendly aggregation for the smart grid,"*in Proc. Privacy Enhanced Technology Symposium*, pp. 175–191, 2011.

[15] F. Knirsch et al. "Error-resilient Masking Approaches for Privacy Preserving Data Aggregation," *IEEE Transactions on Smart Grid,* DOI 10.1109/TSG.2016.2630803, 2016.

[16] H. J. Jo, I. S. Kim and D. H. Lee, "Efficient and Privacy-Preserving Metering Protocols for Smart Grid Systems," in *IEEE Transactions on Smart Grid*, vol. 7, no. 3, pp. 1732-1742, doi: 10.1109/TSG.2015.2449278, May 2016.

[17] H. Mohammed, S. Tonyali, K. Rabieh, M. Mahmoud, and K. Akkaya, ""Efficient Privacy-Preserving Data Collection Scheme for Smart Grid AMI Networks"," in *IEEE Globecom 2016,*, Washington DC, USA, December 2016.

[18] Oracle Technology Network. Java Cryptography Architecture (JCA). [Online]. Available: http://docs.oracle.com/javase/6/docs/technotes/guides/crypto/CrypoSpec.html, accessed Apr. 20, 2017.

[19] P. Gope, J. Lee, and T~Q. S. Quek, "Resilience of DoS attack in designing anonymous user authentication protocol for wireless sensor networks," *IEEE Sensors Journal*, vol. 17, no. 2, pp. 498–503, Jan. 2017.

[20] Atmel's family of smart power meters. http://www.atmel.com/products/smart-energy/power-metering/ (accessed on 28 May 2017).

[21] P. Gope, J. Lee, and T~Q. S. Quek, "Lightweight and Practical Anonymous Authentication Protocol for RFID Systems Using Physically Unclonable Functions," *IEEE Transactions on Information Forensics and Security,* 2018.

[22] Dynamic pricing in electricity supply. http://www.eurelectric.org/media/309103/dynamic_pricing_in_electricity_supply-2017-2520-0003-01-e.pdf (accessed on 28 August 2017).

[23] libpaillier-0.8. Tech. rep. http://hms.isi.jhu.edu/acsc/libpaillier/ (accessed on 16 April 2017).

[24] Pbc library. Tech. rep. http://crypto.standford.edu/pbc/, (accessed on 16 April 2017).

[25] Y. Liu, W. Guo, C. Fan, L. Chang, and C. Cheng, "A Practical Privacy-Preserving Data Aggregation (3PDA) Scheme for Smart Grid," *IEEE Transactions on Industrial Informatics*, DOI: 10.1109/TII2018.2809672, 2018.

[26] T. Jiang, Y. Cao, L. Yu, and Z. Wang, "Load Shaping Strategy Based on Energy Storage and Dynamic Pricing in Smart Grid,"*IEEE Transactions on Smart Grid*, vol.5(6), pp.2868-2876, 2014.

Prosanta Gope received the M.Tech. degree in computer science and engineering from the National Institute of Technology (NIT), Durgapur, India, in 2009, and the PhD degree in computer science and information engineering from National Cheng Kung University (NCKU), Tainan, Taiwan, in 2015. He is currently working as a Research Fellow in the department of computer science at National University of Singapore (NUS). Prior to this, Dr. Gope served over one year as a Postdoctoral Research Fellow at Singapore University of Technology and Design (SUTD) established in collaboration with Massachusetts Institute of Technology (MIT). His research interests include lightweight authentication, authenticated encryption, access control system, and security in mobile communication and hardware security of the IoT devices. He has authored over 40 peer-reviewed articles in several reputable international journals and conferences, and has three filed patents. He received the Distinguish Ph.D. Scholar Award in 2014 given by National Cheng Kung University, Tainan, Taiwan.

Biplab Sikdar (S'98-M'02-SM'09) received the B.Tech. degree in electronics and communication engineering from North Eastern Hill University, Shillong, India, in 1996, the M.Tech. degree in electrical engineering from the Indian Institute of Technology, Kanpur, India, in 1998, and the Ph.D. degree in electrical engineering from the Rensselaer Polytechnic Institute, Troy, NY, USA, in 2001. He was on the faculty of Rensselaer Polytechnic Institute from 2001 to 2013, first as an Assistant and then as an Associate Professor. He is currently an Associate Professor with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore. His research interests include computer networks, and security for IoT and cyber physical systems. Dr. Sikdar is a member of Eta Kappa Nu and Tau Beta Pi. He served as an Associate Editor for the IEEE Transactions on Communications from 2007 to 2012. He currently serves as an Associate Editor for the IEEE Transactions on Mobile Computing.