A Lightweight and Privacy-Preserving Data Aggregation for Dynamic Pricing-based Billing in Smart Grids

Prosanta Gope
National University of Singapore
21 Lower Kent Ridge Rd, Singapore 119077
Email: dcsprg@nus.edu.sg

Biplab Sikdar
National University of Singapore
21 Lower Kent Ridge Rd, Singapore 119077
Email: bsikdar@nus.edu.sg

***Abstract*—Smart grids are expected to enhance the efficiency of current power grids by using advanced digital information and communication technology. However, as the power grid is extended to network of networks, it not only becomes smarter, but also more vulnerable to several security and privacy threats. One of the major concerns with the scale of data collection in smart grids, and in particular smart meters, is that of privacy. While several solutions have been introduced to address this issue, they are computationally complex and introduce large overheads, making them infeasible for resource constrained smart meters. In addition, given the large scale of most smart grids, the computational burden at the aggregator of smart meter data is also a challenging issue. In this article, we propose a lightweight and privacy-preserving data aggregation (LPDA) scheme for dynamic electricity pricing based billing for smart grids using the concept of lightweight single-pass authenticated encryption (AE). Security and performance analyses show that our proposed scheme offers better privacy protection for electricity meter reading aggregation and computational efficiency, as compared to the existing solutions.**

***Index Terms*—Data aggregation, dynamic pricing, security, privacy, integrity, smart grid**

I. Introduction

A smart grid is an evolved grid system that manages electricity demand in a sustainable, reliable and economic manner, built on advanced infrastructure and tuned to facilitate the integration of all involved. The combined volatility of both power supply and power demand creates a growing problem that needs to be solved by smart grids. To enable the envisioned energy management in the smart grid, information on current power consumption and the availability of power needs to be exchanged between power consumers and the power supplier. Hence, devices that monitor and report the power consumption and generation in a smart-grid are required to be connected using a communication network. However, this interconnection of grid technology with information and communication technology (ICT) leads to various security challenges in a power grid [1]. One of the key challenges and major obstacles in the widespread development of the smart grid is user privacy.

In general, for pricing and feedback purposes, a smart grid relies heavily on the usage of smart metering infrastructure. Fine granular readings of power consumption generated by the metering infrastructure are transmitted to the power supplier. These power consumption profiles are used to enable a precise prediction of power demand for managing power production accordingly. However, these profiles also allow the creation of usage profile of a specific person, household, or a company, and that may cause several privacy issues. For analyzing the personal behavior of users or to evaluate the business activity in enterprises, such profiles can be deeply analyzed. In other words, the recording and transmission of power consumption profiles may introduce serious privacy issues. For instance, a long-time analysis on the consumers' data can reveal their private information related to their daily routines. In this regard, an outside adversary or a third-party utility company may use this information to deduce consumers' living habits and lifestyle. Therefore measures have to be taken to ensure the required level of privacy by considering all the aforesaid issues.

A. Related Work

In recent years, several privacy-preserving data aggregation schemes have been proposed for addressing various privacy issues in smart grids. For example, Lu et al. designed a privacy-preserving data aggregation protocol [2] by using Pailler homomorphic crypto-system [3], which results in high computational overhead on the entities like smart-meters. Liang et al. proposed a usage-based dynamic pricing scheme [4] for smart grids by using the fully homomorphic technique devised by Naehring et al. [5]. As a fully homomorphic technique is difficult to implement with the current computing resources, this scheme is regarded as a unrealistic one. Chia-Mu et al. [6] introduced a ring signature based scheme to protect an individual's usage profile. However, the

This research is 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.

978-1-5386-4505-5/18/$31.00

computational cost increases with the size of the ring. Liu et al. [7] have proposed a aggregation scheme based blind signature. However, this scheme cannot protect the privacy of the consumers' usage data profile [8]. Zhang et al. [8] proposed a self-certified signature scheme and Sui et al. [9] designed an incentive-based anonymous authentication scheme. These are constructed with the assumption of an anonymity network, where the sources of usage reports are anonymous. Therefore, it is hard to identify smart meter or any communication failure. Li et al. [10-11] introduced a different technique of data aggregation for smart grid in a hop-by-hop way. However, it is still unclear how to construct the aggregation tree, and how to ensure aggregation in case of failure. Besides, public key signatures used in these schemes cause higher computation cost. Recently, several other smart metering schemes were proposed [27-29]. However, most of these schemes are also based on the homomorphic encryption, which may incur much higher computational overhead on resource-limited smart meters and some of them do not ensure data integrity and sender authentication. Nevertheless, none of the existing schemes has considered the privacy of a smart meter. In that case, an outside attacker may target one of the particular HANs and through human-factor-aware data aggregation (HDA) attacks [30] they can reveal the consumer's activity.

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 in smart grids, most of the existing schemes are based on computationally expensive operations such as Pailler crypto system, lattice-based encryption, ElGamal encryption etc. These are not suitable for resource constrained smart meters, which typically have limited computational capability. For example, a smart meter from Atmel's family with ARM Cortex-M4 processor can provide a maximum CPU speed of 720 MHz [12]. 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 only 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, Portugal etc. [13-14]). For instance, in Portugal, tariff price rate varies four times in a day

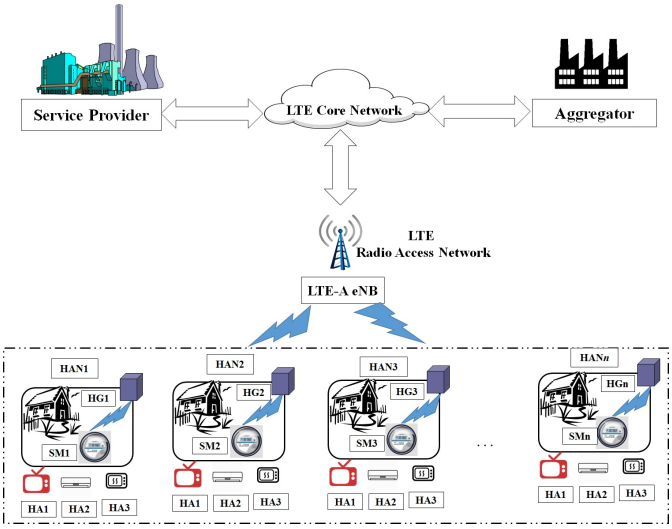

Fig. 1. System Model for Smart Metering.

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 article seeks to address these issues by proposing a lightweight and privacy-preserving data aggregation (LPDA) scheme for dynamic electricity pricing based billing systems in smart grids. To the best of our knowledge, we are first to propose a lightweight solution for privacy preserving data aggregation that also allows the use of dynamic pricing in the electricity grid. Our proposed scheme is based on symmetric key cryptographic primitives such as hash functions, and single-pass lightweight authenticated encryption (AE) [16], which will cause limited computational overhead and data aggregation time and hence is suitable for the resource constraint devices in smart grids.

The rest of the paper is organized as follows. In Section II, we explain the underlying smart metering model, security goals, and the preliminaries that are relevant to this article. In Section III, we present our LPDA scheme. A relevant discussion based on security and computational analyses of the proposed scheme is given in Section IV. Finally, the conclusion is drawn is Section V.

II. System and Adversary Model, Security Goals, and Preliminaries

In this section, we first briefly describe the network architecture of privacy-preserving data aggregation for smart grids and also present the underlying adversary model. This section concludes with a brief introduction to the concept of single-pass authenticated encryption mode, which is necessary to understand our work.

A. System Model

As shown in Fig. 1, our system model for the smart grid consists of four major entities: a service provider (SP), a third-party aggregator employed by the service provider, a set

of smart meters (SMs), and a set of home gateways (HGs). In our system model, the SP is responsible for supplying electricity and sending billing notification to each home-area-network (HAN) consumer. The aggregator is responsible for accumulating and aggregating the power consumption data of each HAN. At the end of each month, the aggregator sends the aggregated data to the SP for billing purposes. Each HAN is composed of a tamper resistant SM, a HG, and a set of home appliances (HAs). The SM sends its periodic readings to its HG. At the end of each day, the HG sends its aggregated result to aggregator. The communication between a SM and its HG is through WiFi. Each HG communicates with aggregator through, for example, a LTE-A network. In this case, the HG connects and sends its data to a LTE-A evolved node B (LTE-A eNB) through the radio access network. Then, the LTE-A eNB sends the data to the high-speed LTE core network to send to the aggregator. Note that, while the network model using a LTE network is provided for completeness, the proposed LPDA scheme does not rely on any specific underlying network.

B. Adversary Model

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 aggregator is owned by a private company whose main responsibility is to assist the SP. Therefore, in our system model we consider the aggregator 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. The networks 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. As the aggregator and the communication network (like LTE-A) are owned and operated by two different authorities, we assume that they do not collude each other. Also, any legitimate HG may be the adversary and be interested to know the consumption data of some other HG. An outside attacker may try to impersonate as a legitimate entity such as a HG or the aggregator to send data under its name. For instance, a dishonest or fake HG could falsify the data for causing inaccurate aggregation result. An outside attacker may eavesdrop on the network transmission media for obtaining the power consumption data and also may try to alter or retransmit them.

C. Security Goals

In our proposed system model for smart grid data aggregation, the SP is trusted by all participants. Here, we aim to accomplish the following security goals:

- **Authentication:** Before aggregating any data, the aggregator needs to authenticate each HG. This will prevent any inaccurate aggregation results. On the other hand, before obtaining the aggregated data from the aggregator through the insecure public communication channel, the SP needs to authenticate the aggregator.
- **Data Confidentiality:** The secrecy of the end-to-end communication is vital. For example, if an adversary can know power consumption data from a HAN, then he can determine its occupancy. This information can be used by robbers to determine the best day or time to break into a home. Therefore, the electricity consumption data is required to be kept secret from any third party for protecting the privacy of the customer. In this regard, if an outsider or an inside adversary (like other HGs or the aggregator) obtains the messages with electricity consumption information, he/she should not be able to comprehend the encrypted message.
- **Data Integrity:** The aggregator should be able to verify the integrity of the data received from each HG of a HAN. On the other hand, the SP needs to check the integrity of the aggregated data received from the third party aggregator.
- **User Privacy:** The aggregator 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 real identity, and their electricity usage. This is necessary for the actual electricity supply determination and proper billing services.

D. Preliminaries

In this subsection, we describe the concept of single-pass authenticated encryption (AE). In general, if we want to achieve privacy or integrity of any message using symmetric key cryptographic primitives, then one of the possible solutions would be to encrypt the data by using an encryption mode like Cipher Block Chaining (CBC), and for integrity we need another primitives, like CBC-MAC or hash function. If there are *n* blocks of data in the message, to ensure both privacy and integrity we need $2n + 4$ encryptions [17]. AE is a type of encryption, which can ensure both the privacy and integrity of data in a single pass with only $n + 1$ encryptions. Assume that $\mathcal{D}$ is a data of arbitrary length that needs to be encrypted and authenticated, $\mathcal{K}$ is the encryption key, and $\mathcal{N}$ is a non-repeating random nonce. AE takes $\mathcal{D}$, $\mathcal{K}$, $\mathcal{N}$ as inputs and generates a cipher $\mathcal{C}$ and tag $\mathcal{T}$ of length ω, where ω is defined such that an adversary is only able to forge a valid cipher-text with probability of $2^{-\omega}$. Syntactically, an authenticated encryption scheme is just a symmetric encryption scheme, which can be denoted as AE = $E(\mathcal{D}, \mathcal{K}, \mathcal{N}) \Longrightarrow \mathcal{C} + \mathcal{T}$. By considering the limited computational abilities of the resource constrained devices (such as sensors, smart meters, home gateway, etc.), several AE modes have been proposed [16-19] in recent years. These AE modes are capable to ensure both INDistinguishability under Chosen Plain-text Attack (IND-CPA) and INDistinguishability under Chosen Cipher-text Attack (IND-CTXT) properties, and hence they can fulfill the requirements of strong data privacy and integrity support with reasonable computational overhead and execution time.

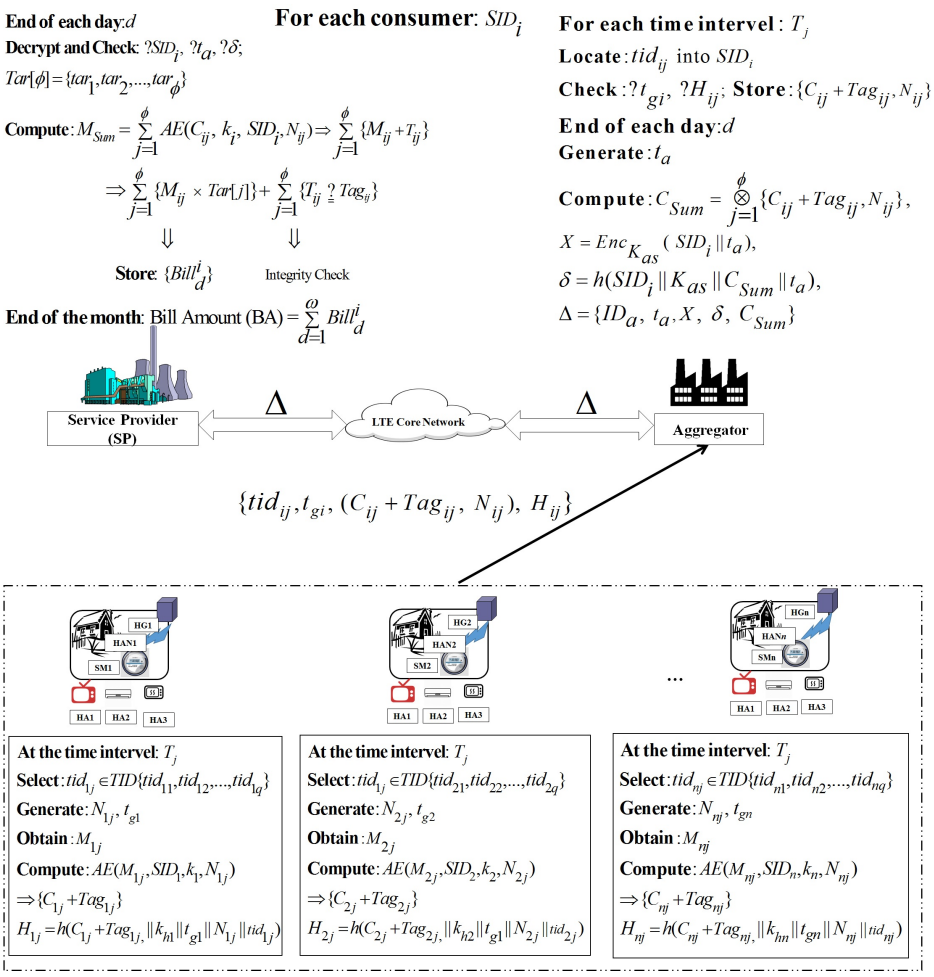

Fig. 2. Proposed LPDA Scheme for Dynamic Pricing-based Billing in Smart Grid

III. Proposed LPDA Scheme for Dynamic Pricing-based Billing

In this section, we present our LPDA scheme, which consists of three phases: Initialization, Data Aggregation, and Billing Processing.

A. Initialization Phase

Assume that there are n HANs in a locality which obtain their 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. Next, to ensure secure communication with the aggregator who is responsible for accumulating the power consumption data of HAN_i, each HG_i executes any three-party lightweight key establishment protocol such as in [15], where the SP helps both HG_i and the aggregator to establish a integrity key k_{hi} between them. Here it is assumed that both the SP and the aggregator maintain a secret key K_{as} between them for secure communication. Now, the aggregator generates a set of temporary identities $TID_i = \{tid_{1i}, tid_{2i}, \cdots, tid_{ni}\}$ and sends $Enc_{k_{hi}}(TID_i)$ (i.e., TID_i encrypted with key k_{hi}) to HG_i. Finally, for each HG_i the aggregator stores (TID_i, k_{hi}) and the HG_i stores $\{(SID_i, k_i), (TID_i, k_{hi})\}$ in its memory for secure interaction with the aggregator and the SP.

B. Data Aggregation Phase

After a pre-defined time interval T_j, each home gateway HG_i collects the meter reading M_{ij} from the smart meter SM_i of HAN_i and then securely sends the reading to the aggregator. For that, after accumulating the reading, the HG_i first randomly selects an unused temporary identity $tid_{ij} \in TID_i = \{tid_{1i}, tid_{2i}, \cdots, tid_{ni}\}$ and then generates a random number N_{ij} and a timestamp t_{gi}. Hereafter, HG_i invokes the authenticated encryption oracle of [16] and computes $AE(M_{ij}, k_i, SID_i, N_{ij}) \Longrightarrow \{C_{ij} + Tag_{ij}\}$, and $H_{ij} = h(C_{ij} + Tag_{ij} || k_{hi} || t_{gi} || N_{ij} || tid_{ij})$. Finally, HG_i sends $\{tid_{ij}, t_{gi}, C_{ij} + Tag_{ij}, N_{ij}, H_{ij}\}$ to the aggregator and deletes tid_{ij} from its memory. Once all the temporary identities are used up, the aggregator will generate a new set of temporary identities TID_i^{new} and sends $Enc_{k_{hi}}(TID_i^{new})$ to HG_i.

After receiving the aggregated result, the aggregator first maps tid_{ij} into SID_i and then validates the timestamp t_{gi} and the key-hash integrity output H_{ij}. If the validation is successful then the aggregator stores $\{C_{ij} + Tag_{ij}, N_{ij}\}$ in its database

in a sequential order. Otherwise, the aggregator terminates the accumulation process and asks HG_i to send the data again. At the end of the day, the aggregator generates a valid timestamp t_a and then computes $C_{Sum} = \otimes_{j=1}^{\phi}\{C_{ij} + Tag_{ij}, N_{ij}\}$, $X = Enc_{K_{as}}(SID_i||t_a)$, $\delta = h(SID_i||K_{as}||C_{Sum}||t_a)$. Here $\otimes$ denotes the accumulation of ciphertext with the respective tags and nonces in a sequential order i.e., $\{(C_{i1} + Tag_{i1}, N_{i1})||(C_{i2} + Tag_{i2}, N_{i2})||\cdots||(C_{i\phi} + Tag_{i\phi}, N_{i\phi})\}$ and ϕ represents the time interval index. Finally, the aggregator composes a message $\Delta = \{ID_a, t_a, X, \delta, C_{Sum}\}$ and sends it to the SP for billing.

C. Billing Processing Phase

Upon receiving the aggregated power consumption information Δ, the SP first validates t_a and then decrypts and checks SID_i and δ. If the validation is successful, then the SP locates the array of the list of tariff prices $Tar[\phi] = \{tar_1, tar_2, \cdots, tar_\phi\}$ and then computes $M_{Sum} = \sum_{j=1}^{\phi} AE(C_{ij}, k_i, SID_i, N_{ij}) \implies \sum_{j=1}^{\phi}\{M_{ij} + T_j\} \implies \sum_{j=1}^{\phi}\{M_{ij} \times Tar[j]\} + \sum_{d=1}^{\phi}\{T_{ij} \stackrel{?}{=} Tag_{ij}\}$. Here the first term ($\sum_{j=1}^{\phi}\{M_{ij} \times Tar[j]\}$) is for billing while the second term ($\sum_{d=1}^{\phi}\{T_{ij}$) is for integrity check. If any of the above validation processes is unsuccessful, the SP terminates the billing process and asks the aggregator to resend the usage data Δ. Otherwise, after calculating the billing amount $Bill_d^i = \sum_{j=1}^{\phi}\{M_{ij} \times Tar[j]\}$ for each day *d*, SP stores $Bill_d^i$ in its database. At the end of the month, the SP calculates the bill amount $BA = \sum_{d=1}^{\omega} Bill_d^i$, where ω is the number of days in a month. Next, the SP finds the consumer information (e.g., name and mailing address) of HAN_i in its database and sends a mail with the BA to the owner of HAN_i. Note that to enhance the performance of the proposed scheme, the aggregator may accumulate the usage data for a long interval like for two-three days, and then send it to the SP.

IV. Discussions

In this section, we first analyze our proposed scheme with respect to the security goals listed in Section II. Subsequently, we demonstrate that our proposed solution has reasonable computational overhead and is suitable even for the resource constraint entities in a smart-grid.

A. Security Analysis

- **Authentication:** In the proposed data aggregation scheme, the aggregator authenticates the home gateway HG_i by using the parameter H_{ij}, which must be equal to $h(C_{ij} + Tag_{ij}||k_{hi}||t_{gi}||N_{ij}||tid_{ij})$. Only a legitimate HG_i can generate the valid key-hash output H_{ij} using the secret key k_{hi} and fresh timestamp t_{gi}. On the other hand, in our proposed scheme the SP authenticates the aggregator by using the timestamp t_a and the hash-response δ, where the security of these parameters is ensured by the secret key K_{as}. Furthermore, in the proposed data aggregation scheme, if an adversary tries to perform any replay attempt, the receiving end can easily comprehend such activities by using the timestamps t_{gi}, and t_a. Therefore, our proposed scheme is also secure against replay attacks [20-21].
- **Data Confidentiality:** The amount of electricity usage in HAN_i is encrypted using the secret key k_i. Hence, except for the service provider, no one can decrypt and get the usage information. AE supports the IND-CPA property [22-23], and hence, even if the usage of electricity for two consecutive days is the same, an adversary (even the aggregator) cannot comprehend that from the ciphertext. Thus, the pattern of the electricity consumption is protected from detection by any eavesdropper [25].
- **Data Integrity:** In our proposed scheme, we ensure two levels of data integrity. In the first level, the aggregator checks whether it has received the same data as that was sent by the home gateway HG_i. For that, the aggregator needs to compute $H_{ij}^* = h(C_{ij} + Tag_{ij}||k_{hi}||t_{gi}||N_{ij}||tid_{ij})$ and check whether H_{ij}^* is equal to H_{ij} or not. Similarly, in the second level, the service provider SP invokes the AE oracle and checks the integrity of the electricity consumption data for each interval T_j by $\sum_{j=1}^{\phi}\{T_{ij} \stackrel{?}{=} Tag_{ij}\}$. This approach facilitates the detection of any manipulation on the aggregated usage data.
- **User Privacy:** In our proposed scheme, 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).

B. Security Comparisons

In this subsection, we compare our proposed scheme with respect to related data aggregation schemes that support billing in terms of the desired security requirements. Table II shows the security properties that each scheme supports, where we can see that our proposed scheme and the schemes presented in [4], [10], [27], and [29] guarantee data confidentiality and usage data integrity support. However, in [4], [10], [27], and [29] sender is not authenticated during data aggregation process.Therefore, a dishonest or fake smart meter may falsify the data, which will cause an inaccurate aggregated result. Furthermore, these schemes allow to send the identity of the smart meter in plain-text form. In this way, an outside attacker can target the smart meter of a particular HAN and through human-factor-aware data aggregation (HDA) attacks they can reveal the consumer's behavior.

TABLE I
PERFORMANCE BENCHMARKING BASED ON SECURITY PROPERTIES

Scheme	Data Confidentiality	Data Integrity	Sender Authentication	Consumer's Privacy
Paillier-based Billing Schemes [4][10][29]	Yes	Yes	No	No
Elgamal-based Billing Schemes [7-8][27]	Yes	Yes	No	No
Proposed Scheme	Yes	Yes	Yes	Yes

TABLE II
COMPUTATION COST OF DIFFERENT CRYPTOGRAPHIC OPERATIONS

	Paillier Enc. [4][10][29]	**Paillier Dec. [4][10][29]**	**EC-Elgamal Enc.[7-8][27]**	**EC-Elgamal Dec.[7-8][27]**	**ALE-Enc./Dec.(AE) [Proposed Scheme]**	**AES-CBC Enc.+CBC-MAC[Possible Alternative]**	**AES-CBC Dec.+CBC-MAC[Possible Alternative]**
Intel Core i5	29.2 ms	34.8 ms	23.7 ms	28.6 ms	14.8 $\times 10^{-4}$ ms	52.7$\times 10^{-4}$ ms	87.4$\times 10^{-4}$ ms
AMD E450	-	-	33.8 ms	41.6 ms	-	-	-
HTC One X	89.4 ms	141.6 ms	71.6 ms	83.4 ms	26.6$\times 10^{-4}$ ms	83.1$\times 10^{-4}$ ms	112.8$\times 10^{-4}$ ms

C. Performance Evaluation

In this section, we analyze the performance of our proposed scheme in terms of the computation time of different cryptographic operations used in various data aggregation schemes. For that, we conduct simulations of several 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 aggregator), and HTC One X with ARM Cortex-A9 MPCore processor and 890 MHz CPU speed (operating as a HG). To evaluate the execution time of different cryptographic operations used in several data aggregation schemes and in our proposed scheme, we use the Bouncy Castle Library [24] to emulate EC-Elgamal encryption scheme [25], ALE (Authenticated Lightweight Encryption) [16], and AES-CBC with CBC-MAC. Furthermore, we also use the Pailler library libpaillier-0.8 [26] for Paillier-based encryption schemes.

Table 1 shows the computation time of the cryptographic operations for aggregating 1024-bits of data. To measure the computational time of our data aggregation process, we adopt ALE as a lightweight AE. It should be noted that during decryption, ALE does not require to call any decryption oracle, while decryption of AES takes more time than encryption. From Table 1, we can see that our AE-based approach needs smaller computation time as compared to others. The EC-Elgamal encryption scheme [24] has lower computation overhead than Paillier encryption. However, this approach has higher computational cost as compared to our scheme.

Note that in our proposed scheme and Paillier based solutions, the aggregator need not perform any encryption/decryption. Hence, we do not consider the simulation outcomes of the ALE and Paillier encryption/decryption operations on the AMD E450 machine. Table 1 also shows AES-CBC encryption mode with CBC-MAC as a possible alternative for accomplishing privacy and integrity of the power consumption data in smart grids. However, this approach requires significantly more execution time as compared to our proposed technique.

V. CONCLUSION

In this article, we proposed a lightweight data aggregation scheme called LPDA for dynamic pricing-based billing systems in smart grids. It is designed based on the concept of single-pass authenticated encryption. We analyzed the security of the proposed scheme and it was shown that the proposed LPDA scheme can ensure several security properties like authentication, data privacy, data integrity etc., which are greatly important for smart grid security. Moreover, we also analyzed the computational cost of the proposed scheme. It was shown that the proposed LPDA scheme has significantly lower computational cost as compared to other data aggregation schemes. Hence, we argue that our LPDA scheme is efficient, practical, and more suitable for 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] U.S. NIST, "Guidelines for smart grid cyber security," NIST IR-7628, Aug. 2010, available at: http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628.

[2] 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 Distrib. Syst.* vol. 23, no. 9, pp. 1621–1631, 2012.

[3] 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.

[4] X. Liang, X. Li, R. Lu, X. Lin and X. Shen, " UDP: usage based dynamic pricing with privacy perservation for smart grid," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 141–150, 2013.

[5] 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.

[6] Y. Chia-Mu, C-Y. Chen, S-Y. Kuo, and H-C Chao, "Privacy-preserving power request in smart grid networks," *IEEE Syst. J*. vol. 8, no.2, pp. 441–449, 2014.

[7] X. Liu, Y. Zhang, B. Wang, and H. Wang, "An anonymous data aggregation scheme for smart grid systems, "*Secur. Commun. Netw.* vol. 7 no. 3, 602–610, 2014.

[8] J. Zhang, L. Liu, Y. Cui, and Z. Chen, " SP2DAS: self-certified PKC-based privacy-preserving data aggregation scheme in smart grid,". *Int. J. Distrib. Sens. Netw*. 2013, pp. 1–11.

[9] Z. Sui, A. Alyousef, and H. de Meer, "IAA: incentive-based anonymous authentication scheme in smart grids," *In: Tiropanis, T*., Vakali, A., Sartori, L., Burnap, P. (eds.) Internet Science. LNCS, vol. 9089, pp. 133–144. Springer, Heidelberg (2015)

[10] F. Li, and B. Luo, "Preserving data integrity for smart grid data aggregation," *In: Third International Conference on Smart Grid Communications (SmartGridComm)*, Tainan pp. 5–8 November, pp. 366–371, 2012

[11] F. Li, B. Luo, and P. Liu, "Secure information aggregation for smart grids using homomorphic encryption,"*in First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Gaithersburg, USA, 4–6 October, pp. 327–332, 2010

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

[13] 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)

[14] I. Apolinario, N. Felizardo, A. L. Garcia, P. Oliveira, A. Trinidad and P. Verdelho, "Determination of time-of-day schedules in the Portuguese electric sector," *IEEE Power Engineering Society General Meeting*, Montreal, Que., 2006, pp. 8 pp.-. doi: 10.1109/PES.2006.1709487, 2006.

[15] P. Gope and T. Hwang, "Lightweight and Energy-Efficient Mutual Authentication and Key Agreement Scheme with User Anonymity for Secure Communication in Global Mobility Networks," *IEEE Syst. J.*, vol. 10, no. 4, pp. 1370–1379, 2016.

[16] A. Bogdanov, F. Mendel, F. Regazzoni, V. Rijmen, and E. Tischhauser, "ALE: AES-Based Lightweight Authenticated Encryption,"*Fast Software Encryption*, pp. 447–466, 2013.

[17] P. Rogaway P, M. Bellare, J. Black, "OCB: a block-cipher mode of operation for efficient authenticated encryption," *ACM Transactions on Information and System Security (TISSEC*) vol. 6, no. 3, pp. 365–403, 2003.

[18] C. Beierle, J. Jean, S. Klbl, G. Leander, A. Moradi, T. Peyrin, Y. Sasaki, P. Sasdrich and S. M. Sim, "The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS," Advances in Cryptology – CRYPTO 2016: 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016.

[19] CryptoLUX Research Group - University of Luxembourg, "Lightweight Block Ciphers," 2016. [Online]. Available: https://www.cryptolux.org/index.php/Lightweight_Block_Ciphers. [Accessed on 10 July 2017].

[20] P. Gope and T. Hwang, "A Realistic Lightweight Anonymous Authentication Protocol for Securing Real-Time Application Data Access in Wireless Sensor Networks," *IEEE Transactions on Industrial Electronics*, vol. 63, no. 11, pp. 7124–7132, Nov. 2016.

[21] P. Gope et al. "Lightweight and Practical Anonymous Authentication Protocol for RFID Systems Using Physically Unclonable Functions," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 11, pp. 2831–2843, 2018.

[22] M. Bellare, C. Namprempre, "Authenticated encryption: relations among notions and analysis of the generic composition paradigm," *Journal of Cryptology*, vol. 21, no. 4, pp. 469-491, Jun. 2008.

[23] M. Bellare, A. Desai, E. JokiPii, P. Rogaway. " A concrete security treatment of symmetric encryption: analysis of the DES modes of operation," *Proceedings of the 38th IEEE Symposium on Foundations of Computer Science*, 1997; A revised version is available online at http://www-cse.ucsd.edu/users/mihir

[24] Bouncy Castle crypto library, [Online]. Available: http://www.bouncycycastle.org/ (accessed on 16 April 2017).

[25] E. Mykletun, J. Girao, D. Westhoff, "Public key based cryptoschemes for data concealment in wireless sensor networks," *In: IEEE International Conference on Communications*, Istanbul, 11-15 June, vol. 5, pp. 2288-2295, 2006.

[26] libpaillier-0.8. Tech. rep. http://hms.isi.jhu.edu/acsc/libpaillier/ (accessed on 8 August 2017).

[27] P. Gope, and B. Sikdar, "An Efficient Data Aggregation Scheme for Privacy-Friendly Dynamic Pricing-based Billing and Demand-Response Management in Smart Grids," *IEEE Internet of Things Journal* DOI:10.1109/JIOT.2018.2833863, 2018.

[28] P. Deng, L.Yang, "A Secure and Privacy-preserving communication scheme for Advanced Metering Infrastructure," *In Proceedings of the IEEE PES Innovative Smart Grid Technologies*, Washington, DC, USA, 16–20 January 2012; pp. 1–5.

[29] X-F Wang, Y. Mu, R-M Chen, "An efficient privacy-preserving aggregation and billing protocol for smart-grid," *Secur. Commun. Netw*. 2016, 9, pp. 4536–4547.

[30] W. Jia, H. Zhu, Z. Cao, X. Dong, and C. Xiao, "Human-Factor-Aware privacy-preserving aggregation in smart-grid," *IEEE Systems Journal*, vol. 8(2), 2014.