An Ultra-Lightweight Data-Aggregation Scheme with Deep-Learning Security for Smart-Grid

Prosanta Gope, *Senior Member, IEEE*, Pradip Kumar Sharma, *Senior Member, IEEE*, and Biplab Sikdar, *Senior Member, IEEE*

***Abstract*—Various smart meter data aggregation protocols have been developed in literature to address the rising privacy threats against customers' energy consumption data. However, most of these protocols require the smart meter (installed at the consumer's end) to either maintain a secret-key or to run an authenticated key-establishment scheme for interacting with the aggregator. Both these approaches create additional requirements for the system. To address this issue, this paper first proposes a machine-learning based ultra-lightweight data aggregation scheme for smart-grids that does not require a secret-key to be maintained for communicating with the aggregator. In particular, unlike existing data aggregation schemes, in the proposed data aggregation scheme, neither the server nor the smart meter need to store any secret. Instead, for every round of data aggregation, each smart meter uses an embedded PUF for generating an unique random response for a given challenge. On the other hand, the server maintains a PUF-model for each smart meter for producing the same random response. This unique secret key is used to ensure the privacy of the metering data. Next, we propose an optimized data aggregation scheme using collaborative learning to enhance the performance of the proposed scheme.**

***Index Terms*—Smart meters, Data aggregation, Train-PUF-model (TPM), Collaborative learning.**

I. Introduction

Future energy systems are expected to be increasingly complex systems that will deeply integrate information and communication technologies in their operations to optimize system performance, reduce costs, and facilitate the integration of new technologies and services. Instrumentation and automation facilitated by enhanced monitoring and measurement tools will play a critical role in such power systems. Smart meters, in particular, will play an important role in smart grids by providing fine-grained power consumption data of a home or enterprise. Such data is imperative for grid operations such as demand-supply management, load forecasting, integration of distributed generation and electric vehicles, and the implementation of energy demand management techniques (a.k.a. demand-side management (DSM) or demand-side response (DSR)).

P. Gope is with Department of Computer Science, University of Sheffield, Regent Court, Sheffield S1 4DP, United Kingdom. (E-mail: prosanta.nitdgp@gmail.com/p.gope@sheffield.ac.uk)

P. Sharma is with Department of Computer Science, University of Aberdeen, Aberdeen AB24 3FX, United Kingdom. (E-mail: pradip.academic@gmail.com)

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: Prosanta Gope

While the integration of technologies that facilitate the real-time monitoring and control of power grids have various advantages, they also introduce the possibility of a wide range of cyber attacks that can adversely affect the operation of the grid and its consumers. While attacks such as false data or command injection target the grid infrastructure, individual consumers may be targeted through attacks on their privacy. The power consumption data provided by smart meters are particularly vulnerable to privacy attacks and it has been shown than they can used by adversaries to extract private information such as household occupancy, behavioral patterns, and economic status [1]. Thus, any techniques that are based on the use of smart meter data (e.g., meter data aggregation for load prediction) must be designed with considerations for privacy. While the problem of privacy-preserving data aggregation for smart grids has been considered in literature, a specific consideration for such techniques is their computational and communication overhead. This paper addresses this problem by developing an ultra-lightweight data aggregation scheme for smart grids.

A. Related Work and Motivation

Aggregation protocols in smart grids aim at privately summing the readings from a given set of smart meters. Several methods of aggregation have been proposed in literature and they can be divided into two categories: public-key-based schemes and masking-based schemes. In this context, most of the public-key-based data aggregation schemes are either based on additive homomorphic encryption [2], [3], [4] or multiparty computation with secure secret sharing [5], [6]. On the other hand, most of the masking-based data-aggregation schemes are based on the approach of addition of random values [7-8] or noisy statistics with the meter readings. Apart from these two types, there exist some papers that have considered faulty smart meters or non-working communication links [9]. Also, public-key-based data aggregation schemes [13-15] have been proposed where multiple dimensions of the meter data have been considered. The major problem with public-key-based schemes (such as [2], [3], [4]) is that they cause a large computational overhead on the resource-limited smart meters. In addition, they also have various security issues. For instance, the data aggregation scheme presented in [4] is susceptible to the middle-man attack. In contrast, although existing masking-based approach may have lower computational overhead, they need to run a secure authenticated key-establishment process for establishing a secret-key

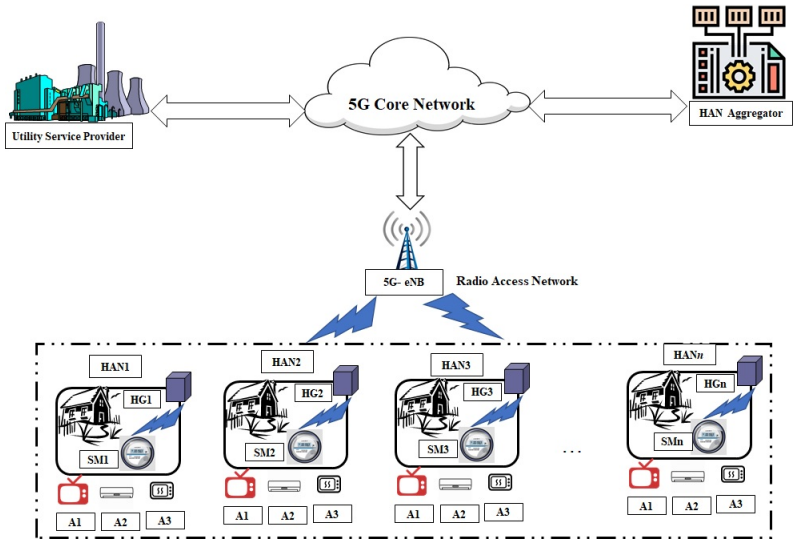

Figure 1. System architecture for smart grid metering.

with the aggregator. For instance, the data aggregation in [8] scheme first requires to execute an authenticated initialization phase for establishing a secret-key between the smart meter and the aggregator. After that, the key is used by the aggregator to send a randomly generated secret. Later, the smart meter uses the random-secret received from the aggregator for masking the meter readings. Therefore, such approaches not only introduce additional computational burden on the security solution but are also executed over several phases, which increases the communication costs. This paper seeks to address all the above issues by proposing a new machine learning (ML) based, ultra-lightweight data aggregation scheme. The proposed data aggregation scheme does not require any authenticated initialization phase for sharing the random-secret for masking. Instead, in the proposed scheme, the random-secret for masking is generated on-the-fly. In order to do that, here we utilize the PUF-technology, which will not only be able to generate a unique random-key-stream for a given challenge to ensure privacy of the metering data for each round of data aggregation but at same time it can also ensure the physical security of each smart meter. The major contributions of this paper can be summarized as follows:

- We introduce a *new* ML-based ultra-lightweight spatial data aggregation scheme for smart grids. The proposed solution has significantly lower computational cost due to masking.
- We propose an optimized version of the data aggregation scheme using collaborative learning.

II. System Architecture and Threat Model

We begin with a description of our system architecture, which is the foundation of the proposed ultra-lightweight data aggregation scheme. Subsequently, we present the attacker model and security goals of the proposed scheme.

A. System Architecture

Figure 1 represents our system architecture which consists of *five* major entities: an utility service provider (USP), a group of home area networks (HANs), a HAN aggregator (HA), a set of smart meters (SMs), and a set of home gateways (HGs). In this system architecture, each HAN consists of a group of appliances and receives utility services (e.g., electricity) from the USP. The HA is responsible for periodically aggregating the electricity consumption of a group of HANs in a geographical region, and provide the aggregated result to the USP. The aggregated result plays a vital role in maintaining balance between power production and demand, and any incorrect data may cause economic losses or even a blackout. In addition, the aggregated result may be used by the USP for demand-side management by providing time-varying pricing to HAN users. Each SM is installed at a HAN, which is composed of a set of home appliances, and a HG, which is basically an edge device. The HG is responsible for collecting meter readings from the SM installed in the HAN and then sending the readings to the HA through an in-home network (e.g. WiFi). The USP and HA interact via a 5G-enabled (as an example) dedicated secure channel.

B. Threat Model

In our threat model, we consider the both the USP and HA as trusted entities. Consumers are considered as honest-but-curious entities that follow the protocol but can collude and share their data to infer information about others. A malicious consumer may also try to perform physical attacks [10] on the smart meter to send falsified usage data. In this regard, the consumer may try to change the settings of the HG or try to manipulate the readings collected from the smart meter. Recall that the communication link between the smart meter and the HG is assumed to be secure and authenticated. However, an outside attacker may compromise the communication between a HG and the HA. For example, the adversary may intercept the messages communicated between an HG and the HA, and then may try to modify the meter reading or the intercepted message. Additionally, an outside attacker may also try to

impersonate as a legitimate entity (e.g., a HG) to send data under its name.

C. Security Goals

- **Privacy of the Usage Data:** Privacy of of the usage data in an aggregation protocol is preserved as long as no adversary is able to infer anything about the individual measurements. It is expected that if an adversary intercepts the communication between a HG and the HA, then he/she must not be able to learn anything about the usage data. Therefore, we need to maintain the secrecy of the end-to-end communication between the HG and HA.
- **Integrity of the Usage Data:** Any changes in the individual measurements are directly reflected on the aggregated result. Therefore, when the HA receives any usage data from a HG, the integrity of the usage data must be verified.
- **Authentication:** If an adversary can successfully masquerade as a legitimate HG and send wrong information about the individual measurements, it will lead to an inaccurate aggregation result. Therefore, it is important that before aggregating any usage data, the HAN aggregator HA needs to authenticate each HG.
- **Protection against any Physical Attacks**: A malicious consumer may try to change the settings of the SM to manipulate its readings. This will result not only in incorrect billing, but also in inaccurate decisions related to demand and supply management. Therefore, it is highly important to maintain physical security of each SM installed in a HAN.

III. Proposed Ultra-lightweight Data Aggregation Scheme

In this section, we present our ultra-lightweight data aggregation scheme. The proposed scheme consists of *two* phases: meter enrollment phase, and the data aggregation phase.

A. Meter Enrollment Phase

Each smart meter needs to enroll with the HA, which is an integral part of the USP. We assume that each smart meter is embedded with a PUF-circuit [10].

- **Step E1**: The HG (installed at the home) sends an enrollment request to the HA through a secure channel.
- **Step E2**: Upon receiving the enrollment request, the HA collects a sufficient numbers of CRPs (Challenge-Response pairs) from the PUF embedded with the smart meter via the HG. In this regard, the HA generates a set of challenges and sends them to the smart meter via the HG and then receives a response corresponding to each challenge. After collecting a sufficient numbers of CRPs, the HA builds a ML-based train-PUF-model (TPM), where the number of CRPs may vary for different PUFs. For instance, in case of a four-stage arbiter PUF, approximately 40,000 CRPs are needed to build a machine-learning model, whereas only 5129 CRPs are required in the case of slender PUF [12]. After collecting the CRPs, a ML algorithm such as Naive Bayes, or LR (Linear Regression)-based algorithm is applied to estimate the internal characteristics of the original PUF (e.g., its linear delay vector) that are needed to model the PUF behavior. Here, the simulated-PUF model (i.e., the TPM) is expected to behave identically as the original PUF embedded with the smart meter. That means, for a given challenge $\mathcal{C}$, both the TPM and the original PUF are expected to generate the same response $\mathcal{R}$. The response of a PUF may be noisy, and this in turn may impact the accuracy of the train-PUF model that is trained on noisy data. To address this issue, an error connection code (such as Golay codes) can be applied. Alternatively, a preselection and filtering mechanism can also be applied. At the end of this step, the HA generates an unique meter_id for the smart meter and stores the TPM and the meter_id in it's secure NVM (non-volatile memory) for further communication and also sends a copy of the meter_id to the HG via the secure channel. After receiving the meter_id, the HG asks the smart meter to disable the internal fuse in the IC with the PUF, so that anyone with access to the IC afterwards will not be able to model the PUF.

B. Data Aggregation Phase

To ensure proper demand-response management in a power grid, it is important to balance the power production and demand. To support this objective, the HA periodically (say, every 30 or 45 mins) needs to know the power consumption of any group of *n* HANs. This phase of the proposed aggregation scheme consists of the following steps:

- **Step DA1:** For a specific session j, a smart meter SM_i randomly generates a challenge C_{ij}, a timestamp t_j, and then uses C_{ij} as an input to the PUF attached with the smart meter to obtain the PUF response k_{ij} (we call it the PUF-Key). Hereafter, the smart meter collects the meter-reading of that period (*j*-th session) (i.e., m_{ij}), encrypts m_{ij}, C_{ij} and t_j with the PUF-Key k_{ij}, and then sends them to the HG. After that, the HG attaches the meter_id and composes a message M_{ij} consisting of the encrypted m_{ij}, C_{ij}, t_j, along with the meter_id, and subsequently sends the message M_{ij} to the HA (as shown in Fig. 2).
- **Step DA2:** After receiving the M_{ij} $(i = 1, 2, \cdots, n)$ from each of the respective HGs, for each M_{ij}, the HA first loads the respective TPM and generates the PUF-key k_{ij} and then uses the key to decrypt the message M_{ij} and check the timestamp and the challenge. If both of them are valid, then the aggregator obtains the meter-reading m_{ij} and after obtaining all the meter readings, the HA computes the summation of all readings, i.e., $Sum_j = \sum_{i=1}^{n} m_{ij}$. Details of this phase are shown in Fig. 2.

C. Optimized Ultra-lightweight Data Aggregation Scheme Using Collaborative Learning

To optimize the proposed model by minimizing the number of communications between HGs and HA, we develop a

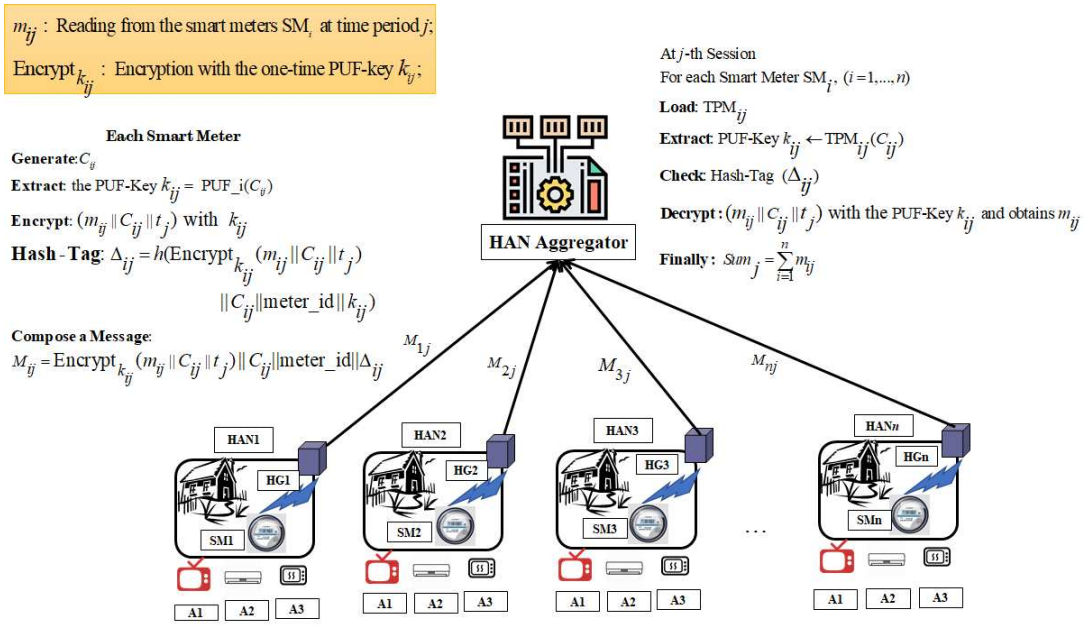

Figure 2. Proposed Ultra-lightweight Data Aggregation Scheme.

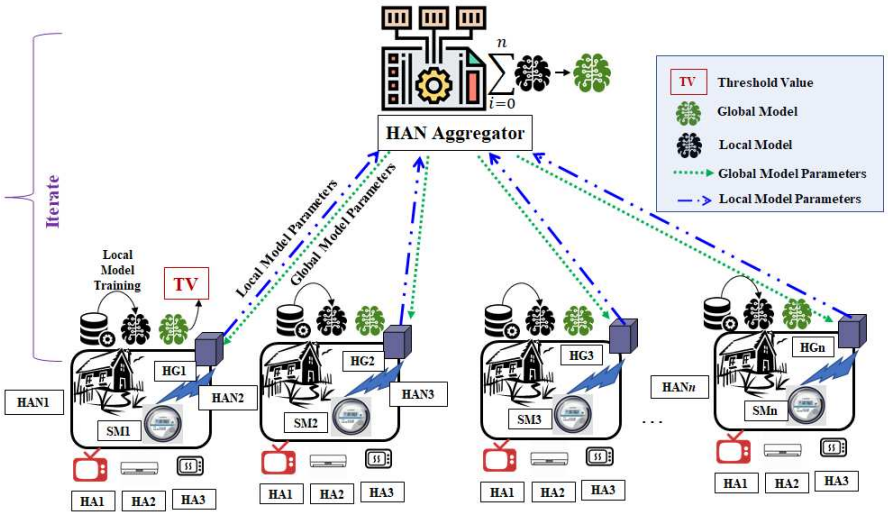

Figure 3. Collaborative-Learning-based Optimized Ultra-lightweight Data Aggregation Scheme.

collaborative learning based mechanism that uses and defines a Threshold Value (TV) at each HAN. In this optimized aggregation mechanism, each HG sends the consumption update to the HA when the consumption data exceeds the set threshold value. Each HAN collects its usage data samples and the samples across HANs share the same set of features and labels. Thus, they can choose to train models separately and set the TV individually. Along with the consumption data, demographics or weather data that have an impact on power consumption may also be used to set the TV. However, individual models are susceptible to cyber-attacks where the adversary may inject poisoned data to comprise the local model to set the TV. This may result in a degradation of the overall accuracy and effectiveness of the decision-making process for supply-demand management. In addition, information about consumption patterns can be extracted from individual TVs that pose a risk of sensitive user information being leaked.

To address such issues, we propose a federated, collaborative learning scheme to set the TV, as shown in Fig. 3. We consider a scenario where the data collected by each HAN follows the same format and has the same information fields. Instead of training local models to set the TV individually, the proposed model using federated learning greatly enriches the training set, contributing to a high generalization performance of the resulting model to set the TV. The use of federated

Table I
PERFORMANCE COMPARISON BASED ON SECURITY GOALS

Schemes↓and Goals→	SG1	SG2	SG3	SG4	SG5
Zuo et al. [2]	Yes	Yes	No	No	No
Sui et al. [3]	Yes	No	No	No	Yes
Xue et al. [4]	Yes	Yes	No	No	Yes
Mustafa et al. [5]	Yes	No	No	No	No
Kursawe et al. [7]	Yes	Yes	No	No	Yes
Gope and Sikdar [10]	Yes	Yes	Yes	No	No
Ming et al. [13]	Yes	Yes	No	No	No
Mohammadali et al. [14]	Yes	Yes	Yes	No	Yes
Zuo et al. [15]	Yes	Yes	No	No	No
Proposed Scheme	Yes	Yes	Yes	Yes	Yes
SG: Security Goals; **SG1:** Data Confidentiality; **SG2:** Data Integrity; **SG3:** Smart-meter Authentication;					
SG4: Security against physical attacks; **SG5:** Does not require to run any authenticated key-establishment scheme					

Table II
PERFORMANCE COMPARISON BASED ON METHODOLOGIES

Schemes	Aggregation Method	Computational Overhead
Zuo et al. [2]	Additive homomorphic encryption with noisy statistics	Very High
Sui et al. [3]	Signcryption with Computational and Decisional Diffie-Hellman	High
Xue et al. [4]	Additive homomorphic encryption and) Threshold secret sharing	Very High
Mustafa et al. [5]	Multiparty computation with secure secret sharing	Very High
Kursawe et al. [7]	Decisional Bilinear Diffie-Hellman	Very High
Gope and Sikdar [10]	AKE + Addition of random values (generated from PRNG)	Low
Ming et al. [13]	Elliptic curve discrete logarithm problem (ECDLP)	High
Mohammadali et al. [14]	Additive homomorphic encryption with Nyberg's Accumulator [11]	Very High
Zuo et al. [15]	Additive homomorphic ELGamal cryptosystem with Bilinear aggregated signature	Very High
Proposed Scheme	Encryption with One-time-Key (generated from PUF/TPM)	Very Low

learning to train the model without sharing consumption data also makes it easier to address cyber-security issues [10] and each HAN operated by the same USP has little curious or malicious intent towards each other. The motivation for using federated learning is to create a generic model to define a TV more robustly. For example, while some users may have few data points, others may have many more. Also, in general, different homes have different consumption patterns. However, when it comes to defining the TV, we put more emphasis on locality, area, and geographic aspects (e.g., consumption in the industrial areas is comparatively higher than in commercial and residential areas). Finally, since privacy requirements may differ from HAN to HAN, the proposed method covers the local and global models' privacy with respect to all HGs in the HAN networks. As shown in Fig. 3, each HG trains the local model based on the local dataset and sends the local model updates to HA. All local model updates received from the HANs will be aggregated by the HA to generate a global model. This global model is then disseminated to all HANs and each HG sets the TV based on the global model to send consumption updates to the HA. This process can be iterated to generate the global model to tune the TV based on the accuracy, standard deviation, and degree of heterogeneity of local data samples.

IV. DISCUSSION

This section starts with a security analysis of the proposed ultra-lightweight data aggregation scheme. Subsequently, we present a comparative analysis to show its effectiveness.

A. Security Analysis

This section describes how the security goals defined in Section II.C are achieved by the proposed scheme.

- **Privacy of usage data:** To ensure the privacy of the usage data in the proposed ultra-lightweight data aggregation scheme, each HG encrypts the meter reading. In this context, only the HA with a valid TPM will be able to extract the PUF-key k_{ij}. Therefore, if an eavesdropper intercepts a message M_{ij}, he/she will not be able to decrypt the message. In this way, we grantee the privacy of any usage data.
- **Integrity of usage data:** To ensure the integrity of the usage data, we can simply use a key-hash function for generating a hash-tag, e.g., Δ_{ij} in Fig. 2, where the hash outputs will be generated based on the PUF-key, message M_{ij}, and the timestamp. Now, if an adversary $\mathcal{A}$ intends to modify any part of the message M_{ij}, the aggregator will be able detect such attempts using the hash-tag value of Δ_{ij}. It should be noted that if the aggregator detects any issue in the hash-tag value of Δ_{ij}, it will stop the decryption of message M_{ij} and will ask the respective smart meter to re-send its reading. In this way, we can also reduce the computation overhead at the aggregator's end.
- **Authentication:** To provide the authentication feature in the proposed scheme, the challenge C_{ij} is sent in both encrypted and unencrypted ways. Therefore, after receiving the message M_{ij}, the HA needs to check the challenge C_{ij} with its unencrypted form, which is also encrypted using the PUF-key. In this regard, for a given

Table III
MODELING ACCURACY RESULT FOR APUF

Challenge Size (in bits)	Number of CRPs	Training Time	Prediction Accuracy (in %)
64-bits	4890	11.89 sec	99.72 %
128-bits	8680	35.94 sec	99.65 %

challenge, only a legitimate PUF device (smart meter) will be able to generate the same PUF-key response as the TPM. Nevertheless, the HAN aggregator can also use the parameter Δ_{ij} to validate any smart meter.

- **Protection against physical attacks**: In the proposed scheme, each smart meter is embedded with a PUF. Therefore, if an adversary tries to do physical attacks (e.g., change the settings of the smart meter to influence the bill) on a smart meter, then the behavior of the PUF will be changed. In such cases, the PUF will not be able generate the same response for a given challenge as the TPM. In our system architecture, the HA will be be able to detect such issues and report them to the USP to take necessary actions. This ensures security against any physical attacks.

B. Comparison

In this section, we compare the proposed scheme with other state-of-the-art data aggregation schemes for smart grids. From Table I, we can see that the data aggregation scheme presented in [5] cannot ensure most of the important security goal that are vital for smart grid security. In most of the existing data aggregation schemes (such as [2-5], [13-15]) the smart meters are not authenticated, making them vulnerable to several attacks. For instance, the data aggregation scheme presented in [4] operates without a trusted authority. Regretfully, this work is also susceptible to the man-in-the-middle attack. On the other hand, even though the data aggregation scheme presented in [10] can accomplish most the security goals, it requires the execution of an authenticated key-establishment (AKE) scheme that leads to additional overhead on the resource limited smart meters. Finally, since smart meters are installed at the customer end, they can be easily tampered by a malicious consumer for influencing the bill. However, none of the existing data aggregation schemes have considered the security against physical attacks. In contrast, Section IV.A has already shown how the proposed scheme ensures all the security goals. One of the major differences between the proposed scheme and the scheme presented in [10] is that unlike [10], the proposed scheme can achieve all the security goals without running a authenticated key-establishment scheme. Next, we compare the proposed scheme with other state-of-the-art data aggregation schemes in terms of the aggregation method and computational overhead. From Table II, we can see that most of the state-of-the-art data aggregation schemes are public-key-based, where additive homomorphic encryption, with accumulator or multiparty computation with secure secret sharing are used. For instance, the scheme presented in [14] requires additive homomorphic encryption (Paillier Crypto-system) with Nyberg's Accumulator [11]). Similarly, in [15], the proposed data aggregation scheme is based on additive homomorphic ELGamal cryptosystem with Bilinear aggregated signature. This results in very high computational overhead at the resource-limited smart meters. Besides, the execution of such approaches takes longer time as compared to any masking-based approach (as shown in [10]). In contrast, the proposed scheme is based on lightweight symmetric-key encryption, where the one-time-key is generated *on-the-fly* just before encryption/decryption.

C. Experimental Evaluation

To validate the effectiveness of the proposed modeling-based data aggregation scheme and also to show how to model a PUF's behavior, we built simulation models of two different Arbiter PUFs (64-bit and 128-bit APUFs) using Matlab. We then collected CRPs from the Matlab simulation models by considering that all stage delay parameters of each PUF are independent and identically distributed. For each PUF, the generated CRP set was divided into two parts: the training set consisted of 80% of the total CRPs, while the test set consisted of the remaining 20%. Here, we implemented a modeling setup for Deep Feed-forward Neural Networks using Python 2.7 and the Keras 2.1.5 framework, with TensorFlow backend, and executed the model on a Linux workstation with 64 GB RAM and a 3.3 GHz, 4-core Intel Xeon processor. All the experiments were conducted without explicitly parallelizing the code across the cores. For classification of APUFs, we found that the necessary deep learning architectures were particularly simple, e.g., only one hidden layer with two nodes was sufficient to model the 64-bit APUF. Table III shows the results obtained on modeling APUFs. As expected, the modeling accuracy achieved is very high with relatively small training sets.

V. Conclusion

Smart meters play a vital role in smart grids by providing user power consumption data at regular time intervals for use cases such as billing, forecasting and supply-demand management. In this paper, we first presented an efficient ultra-lightweight data aggregation scheme for smart girds. To enhance the performance of the proposed scheme, we utilized a collaborative learning mechanism. Unlike existing data aggregation schemes, the proposed solution does not require to store any secret-key but can still ensure a higher-level of security. Also, to the best of our knowledge, this is first aggregation scheme that can ensure physical security of the smart meter.

References

[1] M. R. Asghar, G. Dan, D. Miorandi and I. Chlamtac, "Smart Meter Data Privacy: A Survey," *IEEE Communications Surveys & Tutorials,* vol. 19, no. 4, pp. 2820-2835, Fourth quarter 2017.

[2] A. Abdallah and X. S. Shen, "A lightweight lattice-based homomorphic privacy-preserving data aggregation scheme for smart grid," *IEEE Transactions on Smart Grid*, vol. 9, no. 1, pp. 396-405, Jan 2019.

[3] Z. Sui and H. d. Meer, "An Efficient Signcryption Protocol for Hop-by-Hop Data Aggregations in Smart Grids," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 1, pp. 132-140, Jan. 2020.

[4] K. Xue, B. Zhu, Q. Yang, et al., " An Efficient and Robust Data Aggregation Scheme Without a Trusted Authority for Smart Grid." *IEEE Internet Things J.*, vol. 7, no. 3, pp. 1949-1959, Mar. 2020.

[5] M. A. Mustafa, S. Cleemput, A. Aly, et al., "A Secure and Privacy-Preserving Protocol for Smart Metering Operational Data Collection," in *IEEE Trans. Smart Grid*, 2vol. 10, no. 6, pp. 6481-6490, Jun. 2020.

[6] K. Bonawitz, V. Ivanov, B. Kreuter, A. Marcedone, H. B. McMahan, S. Patel, D. Ramage, A. Segal, and K. Seth, "Practical Secure Aggregation for Privacy-Preserving Machine Learning," in *ACM CCS*, 2017.

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

[8] P. Gope and B. Sikdar, "Lightweight and privacy-friendly spatial data aggregation for secure power supply and demand management in smart grids," *IEEE Transactions on Information Forensics and Security*, 14 (6). pp. 1554-1566, 2019.

[9] F. Knirsch, G. Eibl and D. Engel, "Error-Resilient Masking Approaches for Privacy Preserving Data Aggregation," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 3351- 3361, Jul. 2018.

[10] P. Gope, and B. Sikdar, "A Privacy-Aware Reconfigurable Authenticated Key Exchange Scheme for Secure Communication in Smart Grids,," *IEEE Transactions on Smart Grid* DOI: 10.1109/TSG.2021.3106105, 2021.

[11] K. Nyberg, et al., "Fast accumulated hashing," *Fast Software Encryption*, 1996.

[12] M. Majzoobi, et al., "Slender PUF Protocol: A Lightweight, Robust, and Secure Authentication by Substring Matching," *IEEE Symposium on Security and Privacy Workshops*, 2012.

[13] Y. Ming, X. Zhang, and X. Shen, "Efficient privacy-preserving multidimensional data aggregation scheme in smart grid," *IEEE Access*, vol. 7, pp. 32 907-32 921, 2019.

[14] A. Mohammadali et al., "A Privacy-Preserving Homomorphic Scheme with Multiple Dimensions and Fault Tolerance for Metering Data Aggregation in Smart Grid," *IEEE Transactions on Smart Grid*, DOI: 10.1109/TSG.2021.3049222, Jan. 2021

[15] X. Zuo, L. Li, H. Peng, et al., "Privacy-Preserving Multidimensional Data Aggregation Scheme Without Trusted Authority in Smart Grid," in *IEEE Syst. J.*, vol. 15, no.1, pp. 395-406, Mar. 2021.

Prosanta Gope (M'18-SM'21) is currently working as an Assistant Professor in the Department of Computer Science (Cyber Security) at the University of Sheffield, UK. Dr. Gope served as a Research Fellow in the Department of Computer Science at National University of Singapore (NUS). Primarily driven by tackling challenging real-world security problems, he has expertise in lightweight anonymous authentication, authenticated encryption, access control, security of mobile communications, healthcare, Internet of Things, Cloud, RFIDs, WSNs, SmartGrid and hardware security of the IoT devices. He has authored more than 100 peer-reviewed articles in several reputable international journals and conferences and has four filed patents. He received the *Distinguished Ph.D. Scholar* Award 2014 by National Cheng Kung University (Taiwan). Several of his papers have been published in high impact journals such as IEEE TIFS, IEEE TDSC, IEEE TIE, IEEE TSG, etc. Dr. Gope has served as TPC member/Chair in several reputable international conferences such as IEEE TrustCom, IEEE GLOBECOM (Security-track), ARES, etc. He currently serves as an Associate Editor for the IEEE INTERNET OF THINGS JOURNAL, IEEE SYSTEMS JOURNAL, IEEE SENSORS JOURNAL, *Security and Communication Networks*, and the *Journal of Information Security and Applications (Elsevier)*.

Pradip Kumar Sharma is an Assistant Professor in Cybersecurity in the Department of Computing Science at the University of Aberdeen, UK. Currently, he is Associate Editor of Peer-to-Peer Networking and Application (PPNA), Human-centric Computing and Information Sciences (HCIS), Electronics (MDPI), and Journal of Information Processing Systems (JIPS) journals. He has been serving as a Guest Editor for international journals of certain publishers such as IEEE, Elsevier, Springer, MDPI, JIPS, etc. His current research interests are focused on the areas of Cybersecurity, Blockchain, Edge computing, SDN, and IoT security.

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.