Learning Sparse Privacy-Preserving Representations for Smart Meters Data

Mohammadhadi Shateri
McGill University
Montreal, Canada

Francisco Messina
Universidad de Buenos Aires
Buenos Aires, Argentina

Pablo Piantanida
Laboratoire des Signaux et Systèmes (L2S)
CentraleSupélec CNRS Université Paris-Saclay
Gif-sur-Yvette, France

Fabrice Labeau
McGill University
Montreal, Canada

***Abstract*—Fine-grained Smart Meters (SMs) data recording and communication has enabled several features of Smart Grids (SGs) such as power quality monitoring, load forecasting, fault detection, and so on. In addition, it has benefited the users by giving them more control over their electricity consumption. However, it is well-known that it also discloses sensitive information about the users, i.e., an attacker can infer users' private information by analyzing the SMs data. In this study, we propose a privacy-preserving approach based on non-uniform down-sampling of SMs data. We formulate this as the problem of learning a sparse representation of SMs data with minimum information leakage and maximum utility. The architecture is composed of a releaser, which is a recurrent neural network (RNN), that is trained to generate the sparse representation by masking the SMs data, and an utility and adversary networks (also RNNs), which help the releaser to minimize the leakage of information about the private attribute, while keeping the reconstruction error of the SMs data minimum (i.e., maximum utility). The performance of the proposed technique is assessed based on actual SMs data and compared with uniform down-sampling, random (non-uniform) down-sampling, as well as the state-of-the-art in privacy-preserving methods using a data manipulation approach. It is shown that our method performs better in terms of the privacy-utility trade-off while releasing much less data, thus also being more efficient.**

I. Introduction

The Smart Grid (SG) aims at improving the efficiency, reliability, and security of the electric power systems by using intelligent transmission, control, and distribution networks [1]. One of the main components of the SG are smart meters (SMs), which are devices that enable data exchange between users and Utility Provider (UP) by recording the electricity data of the consumers [2]. This fine-grained electricity consumption data is used for billing, load forecasting, energy theft detection, and several other applications for improving the grid operation. However, the SMs data can be eavesdropped or be shared with a third-party, which can potentially infer sensitive information about users, including the behavioural patterns or even the type of appliances used in the dwelling [3], [4].

There are several privacy-preserving techniques that have been proposed to address the SMs data privacy issue, which can be divided in two main categories: Data Manipulation (DM) and Demand Load Shaping (DLS). The DM approaches modify the SMs using techniques such as data obfuscation/perturbation, anonymization, down-sampling, etc. [5]–[13]. Many of the most recent studies of this family, incorporated information theoretic measures such as Mutual Information (MI) or Directed Information (DI) to model the amount of information leaked about the sensitive attributes and used Machine Learning (ML) algorithms for their implementation. On the other hand, the DLS approaches use physical resources such as rechargeable batteries, electric vehicles, and even renewable energy resources, to shape the users' power consumption to mask the sensitive patterns [14]–[25]. Recently, Reinforcement Learning (RL) and Deep Reinforcement Learning (DRL) methods have been used to tackle this problem, showing good performance against strong ML based attackers.

One of the most simple and naive methods in the DM family is that of down-sampling. Although this is a straightforward and efficient mechanism that can reduce the stress on the communication channel and storage requirements, by communicating SMs data with lower rate, it has received less attention than other techniques. The motivation for this method is based on the fact that high granularity or temporal resolution of data can tremendously improve the accuracy of the electricity consumption disaggregation methods [26]. Therefore, by down-sampling the data, the performance of the disaggregation algorithms can be controlled, which means in turn that less sensitive information is shared with third-parties or UPs [27]–[30]. In the literature, however, there have been more efforts on motivating and analyzing down-sampling than presenting a comprehensive way for getting the most use out of this technique. In This work, we adopt a non-uniform down-sampling approach using deep neural networks for its implementation. Concretely, we pose the problem as that of learning a sparse representation of SMs data by decimating some of its samples with a learned probability distribution. Our framework includes three deep recurrent neural networks (RNNs): a releaser, a utility, and an adversary. The releaser is trained to generate a sparse representation of the SMs data by getting feedback from the utility and adversary networks regarding the reconstruction error of the original SM data, and privacy of the representation, respectively. Following our earlier study [12], DI between the sensitive data and its estimation (by the adversary network) is used as privacy measure and the mean squared error between SM data and its reconstructed version (by the utility network) is considered as the utility measure. Finally, the performance of the presented framework is tested using actual SM data and compared empirically with a state-of-the-art method [12], uniform down-sampling, and random (non-uniform) down-sampling in terms of privacy-utility trade-off, average released data rate, and the leakage of information about the sensitive attribute. To the best of our knowledge, this is the

first work where a down-sampling privacy-preserving approach is implemented using deep neural networks for SM data.

The rest of the paper is organized as follows. In Section II, the problem formulation of the SMs privacy-utility based on down-sampling is developed in relation with sparse representation of the SMs. Details of implementation of the proposed technique using deep RNNs are given in Section III. Empirical results for our method and comparisons with other approaches are presented and discussed in Section IV. Finally, some concluding remarks are presented in Section V.

II. Problem Formulation

Consider the electricity consumption of a household (useful data), denoted as a time series sequence $Y^T = \{Y_t\}_{t=1}^T$, that is recorded by SMs and needs to be communicated in real-time to the UP. To avoid violating the users' privacy, a privacy-preserving mechanism generates a representation of Y^T, denoted as $Z^T = \{Z_t\}_{t=1}^T$, which attempts to preserve the utility of Y^T while leaking minimum information about a private attribute $X^T = \{X_t\}_{t=1}^T$ that needs to be hidden. Therefore, instead of the actual SM data Y^T, its new representation Z^T would be released and shared with the UP. The scheme is shown in Fig.1.

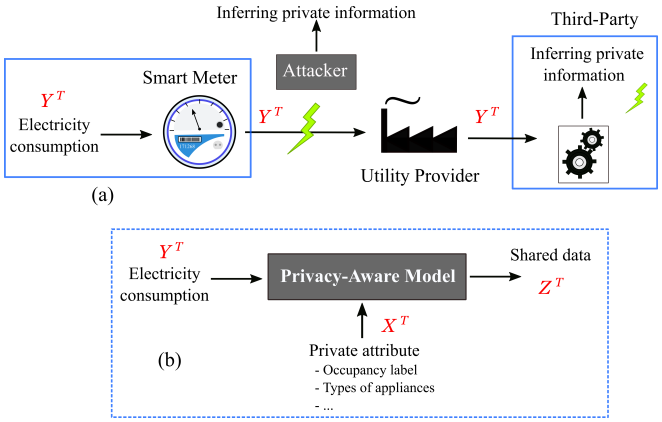

Fig. 1. (a) Smart meter data are communicated with the utility provider in real-time and could be attacked by either an eavesdropper or a third-party. (b) Sanitizing the smart meter data using a privacy-aware model before communicating it with the utility provider.

In this work, the mechanism used by the privacy-preserving system is based on reducing the granularity of the SM data, i.e. down-sampling the data. However, unlike common down-sampling, we propose a more sophisticated non-uniform down-sampling by deciding whether to release the data at each time instant t or not. Specifically, the release mechanism $\mathcal{M}$ is as follows:

$$\mathcal{M}: \; W^t \to Z_t = \begin{cases} Y_t & \text{w.p. } \; q_t(W^t) \\ 0 & \text{w.p. } \; 1 - q_t(W^t) \end{cases} \tag{1}$$

where $t \in \{1, \ldots, T\}$, $q_t(.)$ determines the chance of releasing sample Y_t at time instant t, and W_t is the observed data or input to by privacy-preserving system at time t (which uses both X_t and Y_t, see Algorithm 1 for details). Notice that $\mathcal{M}$ produces a sparse representation of the data, which is stochastic and a function of the input W^T.

Following the study [12], we use the DI $I(X^T \to \hat{X}^T)$ between the private attribute X^T and its estimation by a worst-case adversary $\hat{X}^T$ as the privacy measure. On the other hand, the utility is measured based on the expected distortion between Y^T and its best reconstruction $\hat{Y}^T$ based on Z^T. Therefore, the problem of finding the optimal sparse representation following the mechanism $\mathcal{M}$ in (1), which leaks minimum information about sensitive attribute while keep the utility of the data, can be formulated as follows:

$$\min_{q^T} \frac{1}{T} I\left(X^T \to \hat{X}^T\right) \quad \text{s.t.} \quad \frac{\mathbb{E}\left[\|Y^T - \hat{Y}^T\|_2^2\right]}{T} \leq \varepsilon, \tag{2}$$

where $\|\cdot\|_2$ is the euclidean norm, and $\varepsilon > 0$ is the maximum tolerance on the expected reconstruction error.

III. Privacy-preserving Framework and Implementation

The general framework for designing the privacy-preserving system is shown in Fig. 2. Notice that, in addition to a releaser network, two more networks named as utility and adversary are included. On the one hand, the releaser keeps the reconstruction error minimum by getting feedback from the utility network, which estimates the useful data. On the other hand, the adversary network, which estimates the sensitive attribute from the released data, provides feedback for the releaser network to measure the leakage of information about the sensitive data. This process continues until all networks converge.

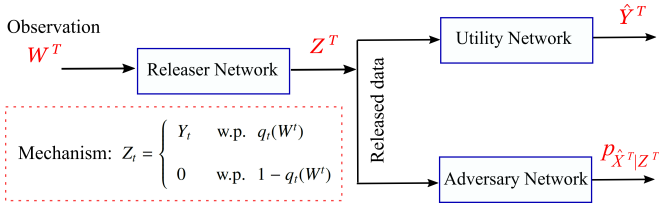

Fig. 2. Privacy-preserving model framework for sharing/releasing the SMs data.

In the following, we describe how to implement the privacy-preserving framework of Fig.2 using deep neural networks. To this end, the sparse representation Z^T is considered as a masked version of the Y^T as $Z^T = Y^T \circ M^T$ where $\circ$ is the Hadamard product (or element-wise product) and M^T is a $0-1$ mask. In the training phase, the releaser network would learn a soft mask with elements q_t where $0 \leq q_t \leq 1$. This can be done using the sigmoid function $\sigma(z) := 1/(1+\exp(-z))$. Fig.3 shows the privacy-preserving framework implemented using RNNs to model the temporal correlation in the data. We now define the loss functions for training each of the networks. On the one hand, since the goal of the utility network is to recover the actual SMs data, we use the expected distortion as its loss function:

$$\mathcal{L}_{\mathcal{U}}(\psi) := \frac{1}{T}\mathbb{E}\left[\|Y^T - \hat{Y}^T\|_2^2\right], \tag{3}$$

where ψ are the parameters of the utility network. Let us assume that X_t is a discrete random variable, so the adversary act as a classifier and we use the cross-entropy as its loss function:

$$\mathcal{L}_{\mathcal{A}}(\phi) := \frac{1}{T}\sum_{t=1}^{T}\mathbb{E}\left[-\log p_{\hat{X}_t|Z^t}(X_t|Z^t)\right], \tag{4}$$

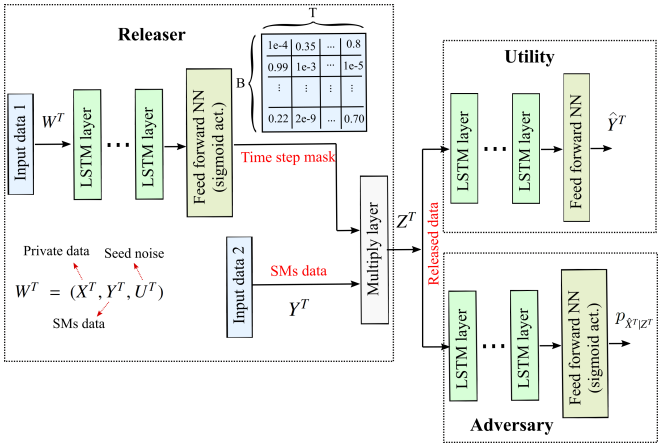

Fig. 3. Privacy-preserving framework implemented based on Long-Short Term Memory (LSTM) layers. The seed noise is generated according to a Uniform distribution, i.e. $U_t \sim U[0,1]$.

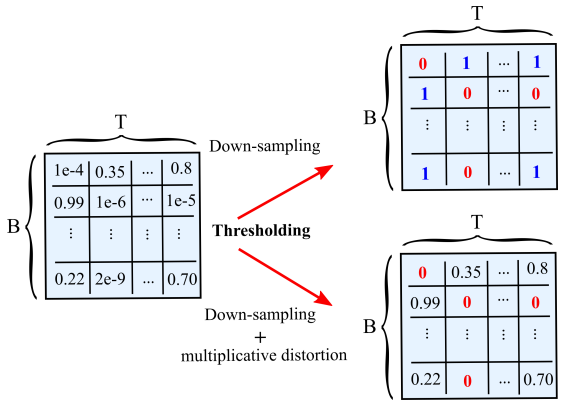

Fig. 4. Soft mask thresholding in the testing phase of the privacy-preserving model. The level of threshold is a hyperparameter.

where ϕ are the parameters of the utility and adversary networks. Finally, the loss functions of the releaser network can be determined based on the optimization problem (2). Since the DI is intractable, we use the following upper bound [12]:

$$I\left(X^T \to \hat{X}^T\right) \leq T \log|\mathcal{X}| - \sum_{t=1}^{T} H(\hat{X}_t|Z^t). \tag{5}$$

Therefore, by substituting this bound as a surrogate of the DI, the following loss function is obtained:

$$\mathcal{L}_{\mathcal{R}}(\theta,\phi,\psi,\lambda) \coloneqq \frac{1}{T}\mathbb{E}\left[\|Y^T - \hat{Y}^T\|_2^2\right] - \frac{\lambda}{T}\sum_{t=1}^{T} H(\hat{X}_t|Z^t), \tag{6}$$

where λ controls the privacy-utility trade-off. The complete training algorithm for this privacy-aware framework is presented in detail in Algorithm 1.

Algorithm 1: Privacy-preserving model based on down-sampling. Batch size B, seed noise dimension m, number of steps to apply to the Adversary k, and ℓ_2 regularization parameter β are hyperparameters.

for number of training iterations **do**
  for k steps **do**
    Sample minibatch of B examples $\{w^{(b)T} = (x^{(b)T}, y^{(b)T}, u^{(b)T})\}_{b=1}^{B}$.
    Generate released data $\{z^{(b)T}\}_{b=1}^{B}$ as the Hadamard product of soft mask $\{M^{(b)T}\}_{b=1}^{B}$ and data $\{y^{(b)T}\}_{b=1}^{B}$.
    Compute the gradient of $\mathcal{L}_{\mathcal{A}}(\phi)$, approximated empirically for minibatch, with respect to ϕ and update ϕ by applying the RMSprop optimizer [31].
  end for
  Sample minibatch of B examples $\{w^{(b)T}\}_{b=1}^{B}$ and generate $\{z^{(b)T}\}_{b=1}^{B}$.
  Compute the gradient of $\mathcal{L}_{\mathcal{U}}(\psi)$, approximated empirically for minibatch, with respect to ψ and update ψ by applying the RMSprop optimizer.
  Compute the gradient of $\mathcal{L}_{\mathcal{R}}(\theta,\phi,\psi,\lambda)$, approximated empirically for minibatch, with respect to θ.
  Use Ridge(L_2) regularization [32] with value β and update θ by applying RMSprop optimizer.
end for

After training the privacy-preserving framework in Fig.3 using Algorithm 1, in the testing phase, the soft mask can be treated in two ways by changing the thresholding operation: considering a 0−1 mask or a zero and non-zero mask (see Fig.4). In the former case, privacy is provided just using the down-sampling mechanism, i.e., removing some time instances for hiding sensitive information, while in the later case both down-sampling and multiplicative distortion mechanisms are used.

IV. Results and Discussion

In this study, the performance of the proposed model is assessed based on the Electricity Consumption & Occupancy (ECO) dataset. The ECO dataset collected and proposed by [33] includes 1 Hz power consumption of five houses in Switzerland labeled with the occupancy status of the dwellings. These occupancy labels are considered as a private attribute. Therefore, the goal of the releaser network is to generate a sparse representation from which an adversary cannot infer the occupancy labels while the utility network can use the released data to recover the actual power consumption. In this setting, the releaser and utility are regression networks while the adversary is a binary classifier. To make the proposed model comparable with the state-of-the-art method such as the one proposed in [12], the dataset is re-sampled every one hour and daily samples (with length $T = 24$) are considered. The total 11225 sample sequences are split into train and test dataset with the ratio 85 : 15, and 10% of the training dataset is used as the validation dataset to tune the hyperparameters of the model. The proposed smart down-sampling method (with and without multiplicative distortion) is compared with uniform down-sampling, random (non-uniform) down-sampling, and the additive distortion approach proposed in [12]. The architectures of the networks used for each method are presented in Table I. Notice that, unlike the smart down-sampling, for the uniform down-sampling and random down-sampling, since there are no parameters to be learned, the sparse representation is generated independently of the utility network. It should be noted that the releaser for the random method would be a non-uniform down-sampling of the SMs data where the decimated time instances are selected randomly.

As the first comparison, the privacy-utility of the models (on the test dataset) are assessed based on the performance of an attacker which is trained (by having access to the (Z^T, X^T) training dataset, i.e., in a supervised manner) to infer the private

TABLE I

NETWORKS ARCHITECTURES AND HYPERPARAMETERS VALUES FOR THE PRIVACY-AWARE MODELS.

	Releaser 4 LSTM layers each with 64 cells and $\beta = 1.5$	**Adversary** 2 LSTM layers each with 32 cells	**Utility** 3 LSTM layers each with 48 cells	**Attacker** 3 LSTM layers each with 32 cells	B 128	k 4	m 8
Smart Down-Sampling	✓	✓	✓	✓	✓	✓	✓
Smart Down-Sampling and Multiplicative Distortion	✓	✓	✓	✓	✓	✓	✓
Uniform Down-Sampling*	—	—	✓	✓	—	—	—
Random Down-Sampling	—	—	✓	✓	—	—	—
Additive Distortion [12]	✓	✓	—	✓	✓	✓	✓

* To generate the released data, the *resample* function of Matlab is used where a FIR Antialiasing Lowpass Filter is applied to the data.

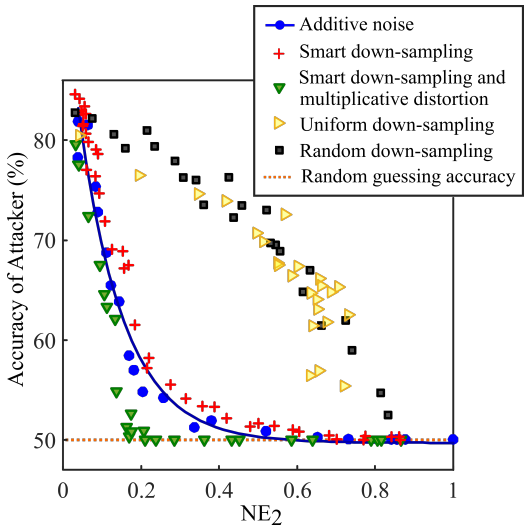

Fig. 5. Privacy-utility trade-off of the proposed model compare with the uniform down-sampling, random (non-uniform) method, and additive noise approach [12]. The result of the random method are averaged over five times random testing.

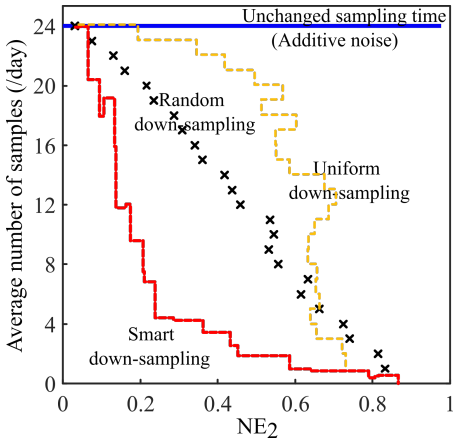

Fig. 6. Averaged number of samples released daily versus the utility for the proposed models.

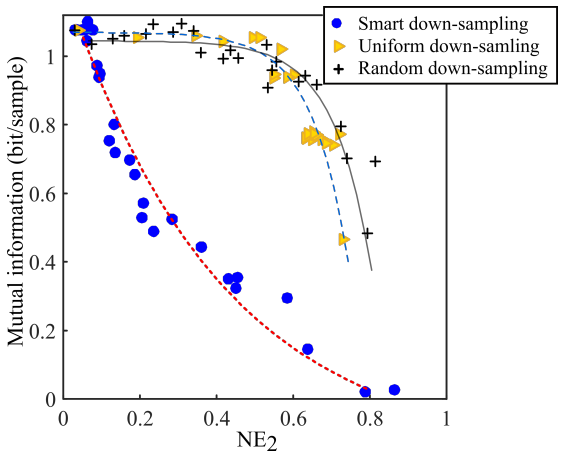

Fig. 7. Information leakage about the users' private attribute (occupancy labels) from the shared data based on the KSG approximation of mutual information.

attributes. It should be noted that since the attacker is a classifier, the performance of the attacker is evaluated using balanced accuracy, defined as follows [34]:

$$\text{Balanced Accuracy} := \frac{1}{2}\left(\frac{c_{11}}{c_{11}+c_{12}} + \frac{c_{22}}{c_{22}+c_{21}}\right), \tag{7}$$

where c_{ij} is the fraction of samples of class i classified as class j. The utility on the other hand, is measured based on the normalized square error, defined as follows:

$$\text{NE}_2 := \frac{\mathbb{E}\left[\|Y^T - \hat{Y}^T\|_2\right]}{\mathbb{E}\left[\|Y^T\|_2\right]}. \tag{8}$$

The privacy-utility trade-off for the different methods is shown in Fig. 5. As expected, the smart down-sampling greatly outperforms both the uniform and the random down-sampling methods. In addition, the performance of the smart down-sampling is closely comparable with the additive noise approach, and smart down-sampling with multiplicative distortion approach actually outperforms the state-of-the-art.

As another comparison, we evaluate the average number of samples released daily (non-zero samples in down-sampling methods) by each scheme. Results are presented in Fig. 6. Interestingly, looking at this figure and Fig. 5, we can see that, for a fixed level of distortion, the smart down-sampling method outperforms the other methods in terms of privacy while also reducing the sample data rate.

The general leakage of information about the users' private attribute (occupancy labels for this study) from the shared data is estimated by considering the mutual information between the

occupancy labels X^T and the shared data Z^T as a function of the distortion (see Fig. 7). In this figure, the mutual information is approximated based on the Kraskov–Stögbauer–Grassberger (KSG) method (with parameter 4). For more information about the KSG method, the reader is referred to [35]. Fig.7 clearly shows that for the same level of distortion, the smart down-sampling method would leak less information about the users' power consumption compared with other methods.

V. Concluding Remarks

In this study, we presented a privacy-preserving method for electricity consumption data, recorded by SMs, based on down-sampling or reducing the data rate of SMs data. The problem was first formulated as learning a sparse representation of the SMs time series signal which leaks minimum information about private data while keeping the reconstruction error of the original data minimum. This was implemented by simultaneously training three deep recurrent neural networks: a releaser network (providing the representation of the data to be shared), a utility network (which estimates the power consumption from the representation) and an adversary network (which attempts to infer the sensitive attribute from the representation). The performance of the proposed technique was tested based on actual SMs data and compared with a state-of-the-art algorithm, uniform down-sampling, and random down-sampling methods. The empirical results showed that this simple technique is as good as the state-of-the-art in terms of the privacy-utility trade-off, while reducing the data rate tremendously. This reduction in the temporal data resolution is of interest for smart grids since it reduces the stress on the data communication channel and relaxes the storage requirements.

Acknowledgment

This work was supported by Hydro-Quebec, the Natural Sciences and Engineering Research Council of Canada, and McGill University in the framework of the NSERC/Hydro-Quebec Industrial Research Chair in Interactive Information Infrastructure for the Power Grid (IRCPJ406021-14).

References

[1] E. Kabalci and Y. Kabalci, "Introduction to smart grid architecture," in *Smart grids and their communication systems*, pp. 3–45, Springer, 2019.

[2] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," *IEEE Security Privacy*, vol. 8, no. 1, pp. 81–85, 2010.

[3] G. Giaconi, D. Gunduz, and H. V. Poor, "Privacy-aware smart metering: Progress and challenges," *IEEE Signal Processing Magazine*, vol. 35, no. 6, pp. 59–78, 2018.

[4] G. Kalogridis, R. Cepeda, S. Z. Denic, T. Lewis, and C. Efthymiou, "Elecprivacy: Evaluating the privacy protection of electricity management algorithms," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 750–758, 2011.

[5] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *2010 First IEEE International Conference on Smart Grid Communications*, pp. 238–243, IEEE, 2010.

[6] L. Sankar, S. R. Rajagopalan, S. Mohajer, and H. V. Poor, "Smart meter privacy: A theoretical framework," *IEEE Transactions on Smart Grid*, vol. 4, pp. 837–846, June 2013.

[7] H. Yang, L. Cheng, and M. C. Chuah, "Evaluation of utility-privacy trade-offs of data manipulation techniques for smart metering," in *2016 IEEE Conference on Communications and Network Security (CNS)*, pp. 396–400, IEEE, 2016.

[8] M. Shateri and F. Labeau, "Privacy-preserving adversarial network (PPAN) for continuous non-gaussian attributes," *arXiv preprint arXiv:2003.05362*, 2020.

[9] P. Barbosa, A. Brito, and H. Almeida, "A technique to provide differential privacy for appliance usage in smart metering," *Information Sciences*, vol. 370-371, pp. 355 – 367, 2016.

[10] A. Tripathy, Y. Wang, and P. Ishwar, "Privacy-preserving adversarial networks," in *2019 57th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pp. 495–505, IEEE, 2019.

[11] M. Shateri, F. Messina, P. Piantanida, and F. Labeau, "Deep directed information-based learning for privacy-preserving smart meter data release," in *2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, pp. 1–7, 2019.

[12] M. Shateri, F. Messina, P. Piantanida, and F. Labeau, "Real-time privacy-preserving data release for smart meters," *IEEE Transactions on Smart Grid*, vol. 11, no. 6, pp. 5174–5183, 2020.

[13] M. Shateri, F. Messina, P. Piantanida, and F. Labeau, "On the impact of side information on smart meter privacy-preserving methods," in *2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, pp. 1–6, 2020.

[14] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, and R. Cepeda, "Privacy for smart meters: Towards undetectable appliance load signatures," in *2010 First IEEE International Conference on Smart Grid Communications*, pp. 232–237, IEEE, 2010.

[15] J. Yao and P. Venkitasubramaniam, "On the privacy-cost tradeoff of an in-home power storage mechanism," in *2013 51st Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pp. 115–122, IEEE, 2013.

[16] O. Tan, D. Gunduz, and H. V. Poor, "Increasing smart meter privacy through energy harvesting and storage devices," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, pp. 1331–1341, 2013.

[17] J. Gomez-Vilardebo and D. Gündüz, "Smart meter privacy for multiple users in the presence of an alternative energy source," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 1, pp. 132–141, 2014.

[18] Z. Zhang, Z. Qin, L. Zhu, J. Weng, and K. Ren, "Cost-friendly differential privacy for smart meters: Exploiting the dual roles of the noise," *IEEE Transactions on Smart Grid*, vol. 8, no. 2, pp. 619–626, 2016.

[19] G. Giaconi, D. Gündüz, and H. V. Poor, "Smart meter privacy with renewable energy and an energy storage device," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 1, pp. 129–142, 2017.

[20] S. Li, A. Khisti, and A. Mahajan, "Information-theoretic privacy for smart metering systems with a rechargeable battery," *IEEE Transactions on Information Theory*, vol. 64, no. 5, pp. 3679–3695, 2018.

[21] E. Erdemir, P. L. Dragotti, and D. Gündüz, "Privacy-cost trade-off in a smart meter system with a renewable energy source and a rechargeable battery," in *ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, IEEE, 2019.

[22] G. Giaconi, D. Gündüz, and H. V. Poor, "Optimal demand-side management for joint privacy-cost optimization with energy storage," in *2017 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 265–270, IEEE, 2017.

[23] Y. Sun, L. Lampe, and V. W. Wong, "Smart meter privacy: Exploiting the potential of household energy storage units," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 69–78, 2017.

[24] M. Shateri, F. Messina, P. Piantanida, and F. Labeau, "Privacy-cost management in smart meters using deep reinforcement learning," in *2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*, pp. 929–933, 2020.

[25] M. Shateri, F. Messina, P. Piantanida, and F. Labeau, "Privacy-cost management in smart meters: An information-theoretic deep reinforcement learning approach," *arXiv preprint arXiv:2006.06106*, 2020.

[26] J. Huchtkoetter and A. Reinhardt, "On the impact of temporal data resolution on the accuracy of non-intrusive load monitoring," in *Proceedings of the 7th ACM International Conference on Systems for Energy-Efficient Buildings, Cities, and Transportation*, pp. 270–273, 2020.

[27] A. Cárdenas, S. Amin, and G. Schwartz, "Privacy-aware sampling for residential demand response programs," in *Proc. 1st International ACM Conf. High Confidence Netw. Syst.(HiCoNS)*, 2012.

[28] D. Mashima, "Authenticated down-sampling for privacy-preserving energy usage data sharing," in *2015 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 605–610, IEEE, 2015.

[29] G. Eibl and D. Engel, "Influence of data granularity on smart meter privacy," *IEEE Transactions on Smart Grid*, vol. 6, pp. 930–939, March 2015.

[30] X.-Y. Zhang, S. Kuenzel, J.-R. Córdoba-Pachón, and C. Watkins, "Privacy-functionality trade-off: A privacy-preserving multi-channel smart metering system," *Energies*, vol. 13, no. 12, p. 3221, 2020.

[31] G. Hinton, N. Srivastava, and K. Swersky, "Neural networks for machine learning lecture 6a overview of mini-batch gradient descent," *Cited on*, vol. 14, p. 8, 2012.
[32] T. Hastie, R. Tibshirani, J. Friedman, and J. Franklin, "The elements of statistical learning: data mining, inference and prediction," *The Mathematical Intelligencer*, vol. 27, no. 2, pp. 83–85, 2005.
[33] C. Beckel, W. Kleiminger, R. Cicchetti, T. Staake, and S. Santini, "The eco data set and the performance of non-intrusive load monitoring algorithms," in *Proceedings of the 1st ACM Conference on Embedded Systems for Energy-Efficient Buildings*, pp. 80–89, ACM, 2014.
[34] L. Mosley, *A balanced approach to the multi-class imbalance problem*. PhD thesis, Iowa State University, 2013.
[35] A. Kraskov, H. Stögbauer, and P. Grassberger, "Estimating mutual information," *Physical review E*, vol. 69, no. 6, p. 066138, 2004.