Advances in Manufacturing Technology XXXVI
A. Thomas et al. (Eds.)

doi:10.3233/ATDE230930

Local Differential Privacy-Based Data-Sharing Scheme for Smart Utilities

Veniamin BOIARKIN[1]*, Bruno Bogaz ZARPELAO[2], Muttukrishnan RAJARAJAN[1], Rajkumar ROY[1], Katy TAPPER[3]
[1] *School of Science and Technology, City, University of London, United Kingdom*
[2] *Department of Computer Science, State University of Londrina, Brazil*
[3] *Department of Psychology, City, University of London, United Kingdom*

Abstract. The manufacturing sector is a vital component of most economies, which leads to a large number of cyberattacks on organisations, whereas disruption in operation may lead to significant economic consequences. Adversaries aim to disrupt the production processes of manufacturing companies, gain financial advantages, and steal intellectual property by getting unauthorised access to sensitive data. Access to sensitive data helps organisations to enhance the production and management processes. However, majority of the existing data-sharing mechanisms are either susceptible to different cyber-attacks or heavy in terms of computation overhead. In this paper, a privacy-preserving data-sharing scheme for smart utilities is proposed. First, a customer's privacy adjustment mechanism is proposed to make sure that end-users have control over their privacy, which is required by the latest government regulations, such as the General Data Protection Regulation. Secondly, a local differential privacy-based mechanism is proposed to ensure privacy of the end-users by hiding real data based on the end-user preferences. The proposed scheme may be applied for different industrial control systems, whereas in this study, it is validated for energy utility use case consisting of smart intelligent devices. The results show that the proposed scheme may guarantee the required level of privacy with an expected relative error in utility.

Keywords. Data-sharing, Local Differential Privacy, Manufacturing, Privacy-preserving mechanism, Smart Utility.

1. Introduction

The manufacturing sector, which is the backbone of world economies, experiences a large number of cyber-attacks that are performed by attackers to disrupt production processes, compromise, or steal sensitive information, and gain financial advantages. By integrating Information Technology (IT) and Operational Technology (OT) systems, organisations open new avenues for adversaries. Vulnerabilities in the manufacturing sector may be caused by different factors, such as the economic impact of disruption, legacy systems, and the integration of IT and OT systems. The results of cyber-attacks range from financial losses and compromised intellectual property to the disruption of operation processes.

More than 75% of organisations in manufacturing sector unpatched Common Vulnerabilities and Exposures (CVEs), whereas nearly 40% of these organisations

suffered malware infections in 2022 [1]. Cloud adoption within the manufacturing sector has become a solution to support remote workers. Around 38% of respondents experienced an account compromise at least one, whereas the average for all other industries was around 31% [2]. According to the report [3], around 85% of organisations had very little visibility into their OT environments, where 77% of organisations had poor network segmentation, 70% had outside connections to their Industrial Control Systems (ICSs), and 44% of companies shared credentials between IT and OT systems.

In this work, a smart utility environment is considered as a use case of the proposed approach, whereas the proposed model can be applied across all utility infrastructures. Manufacturing companies produce components that are used by smart utility companies, as well as industrial Internet of Things (IoT) devices, such as smart meters that are deployed on the end-users' side. In this specific use case, the end-users' energy usage data that are generated by the smart meters should be protected from any types of cyber-attacks. Although access to utility usage data brings many benefits, there is a number of challenges regarding end-users' privacy. These data are considered as "personal data", which means that the operation of smart meters within the EU must be in line with the General Data Protection Regulation (GDPR) [4]. Currently, security and privacy of the end-users and their data are highly prioritised in many countries including EU [5], UK [6], [7], Australia [8].

Differential Privacy (DP) has become one of the most popular approaches to ensure privacy of end-users' data, and it is widely utilised both in academia and industry. By utilising DP, controllable noise is added to the original data, thus hiding the sensitive data from other parties. Most of the existing DP-based schemes do not allow the end-user to control the level of privacy. To fill this gap, this paper proposes a Local Differential Privacy (LDP)-based data-sharing mechanism that preserves privacy of the end-users, whereas the end-users are able to control the level of privacy. The main contributions of this paper are as follows:

- A mechanism that allows end-users adjust and control the level of privacy (privacy budget) based on their preferences.
- A data-sharing scheme that utilises local differential privacy to ensure privacy of end-users' sensitive data.

The rest of this paper is organised as follows. Section II summarises the related works. The system model of a smart utility environment is presented in Section III. The proposed data-sharing scheme is presented in Section IV. Simulation results are presented in Section V. Finally, the conclusion is given in Section VI.

2. Related Work

DP has become a very popular technique to ensure data privacy by controlling the amount of noise added to the data. To reduce the risk of privacy leakage, Zhao et al. [9] proposed a strategy using differential privacy, which can protect end-users' data from being stolen by other parties in the process of data exchange. Lako et al. [10] proposed differentially private algorithms based on the discrete Fourier transform and the discrete wavelet transform, whereas the noise is added on the aggregator's side. To preserve an individual end-user's privacy, Gai et al. [11] proposed a privacy-preserving data aggregation scheme that satisfies LDP based on randomised responses, where sensitive data are perturbed by randomised response on the end-user's side. Although these schemes ensure end-users' privacy, there is no option for the end-user to control the level

of privacy, which is required by the regulations, such as [4]. In addition, there are only a few data-sharing schemes that propose to add noise on the end-user's side.

Another popular approach to ensure end-users privacy during the data exchange is to utilise cryptographic techniques, such as Homomorphic Encryption (HE). To address the issues regarding privacy and security in a fog-based environment, Zhao et al. [12] proposed a privacy-preserving data aggregation scheme using Somewhat Homomorphic Encryption (SHE), which requires a trusted authority that is responsible for the registration of different parties. To provide flexible and efficient data aggregation, while maintaining data integrity and data privacy, Qian et al. [13] proposed a lightweight data aggregation scheme using HE. Zhang et al. [14] proposed a lightweight and fault-tolerant data aggregation scheme using modified version of the symmetric HE, random masking techniques, and Shamir secret-sharing mechanism. To reduce the complexity of certificate management, as well as to enhance security and privacy of end-users' data, a certificate-based data aggregation scheme is proposed in [15], which utilises homomorphic encryption. Although encryption-based data aggregation schemes ensure end-users' data privacy, a trusted authority is required for registration purposes or distribution of secret materials. In addition, encryption-based schemes add additional computation overhead compared to the DP-based models.

3. System Model

Fig. 1 shows the structure of a smart utility environment consisting of N end-users, a Data Communications Company (DCC) gateway, and grid operators including Electricity System Operator (ESO), Energy Suppliers (ESs), and Authorized Third Parties (ATPs). A Smart Meter (SM), which is deployed at the end-user's side, measures the electricity consumption of the end-user, and submits the data to the Communications Hub (CH). End-users' data are encrypted and sent to the grid operators through the DCC infrastructure. DCC has no access to end-users' data because the data are encrypted using grid operators' keys. ESs, ESO, and ATPs decrypt end-users' data using their private keys to perform their tasks and manage the electricity grid. In case of a key leakage attack, or an insider attack on the operators' side, privacy of the end-user might be disclosed, namely conclusions about the end-user's behaviour might be drawn by accessing sensitive data [16]. To address this issue, this work allows end-users to set the required level of privacy, based on which a controllable noise is added to the original data before encryption.

Let $N = \{1, 2, 3, ..., N\}$ denote the set of the end-users, where n is the index of the end-user and $n \in N$, whereas the total number of end-users is given by $N \triangleq |N|$. A smart meter that is deployed on the end-user's side measures the electricity consumption in real-time and stores measurements in memory. The interval at which a smart meter records and stores measurements may vary depending on the smart meter model. In this work, a smart meter stores electricity measurements at the end of each time slot, where each time slot is of 30 minutes. This reflects the minimum time interval, at which a grid operator may access end-users' data. Let $T = \{1, 2, 3, ..., T\}$ denote the set of all time slots when electricity measurements are stored in a smart meter's memory, where t is the time slot index and $t \in T$, whereas the total number of time slots is given by $T = 48$.

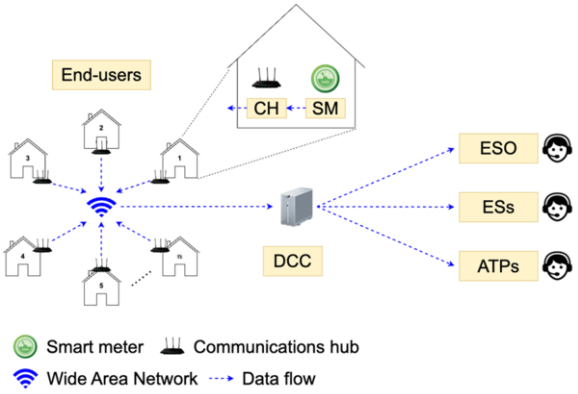

Figure 1 System Model

Let QD_n denote the electricity consumption profile for the end-user n for one day, and it is defined as follows:

$$QD_n = \{QD_{n1}, QD_{n2}, ..., QD_{nT}\}, \quad n \in \mathrm{N} \tag{1}$$

where QD_{nt} is the level of electricity consumption for the end-user n in a time slot t and $QD_{nt} \in QD_n$.

4. Proposed Scheme

In this section, a privacy-preserving data-sharing scheme for smart utility environment using local differential privacy is presented. A smart meter measures electricity consumption of the end-user and stores these measurements (QD_{nt}) in memory. End-users have control over the level of privacy that affects the amount of noise added to the original data. After the noise is added, data are encrypted and sent to the grid operators. Thus, a smart meter stores the level of privacy set by user and utilises ϵ-differentially private algorithm to modify electricity measurements before reporting them.

Definition 1 (ϵ-local differential privacy). A randomised algorithm M: $D \rightarrow S$ satisfies ϵ-local differential privacy iff for any output $s \in S$, and two neighbouring datasets $d, d' \in D$:

$$\frac{Pr[\mathcal{M}(d) = s]}{Pr[\mathcal{M}(d') = s]} \leq e^{\epsilon} \tag{2}$$

where $Pr[\mathrm{M}(d) = s]$ is the probability of the mechanism M outputting the result s given the input d, S is the set of all possible outputs that an algorithm M can produce, and ϵ is the privacy budget that bounds the probability of M outputting the same result for any pair of values d, d' [17]. A smaller value of ϵ provides stronger privacy guarantee, and larger ϵ provides weaker privacy guarantee. Two datasets (d, d') are called neighbouring datasets, iff d' can be produced by adding, removing, or modifying exactly one element from d. Let f: $D \rightarrow \mathrm{R}$ denote the function that maps datasets (D) to real numbers. In this work, f outputs the mean of electricity consumption readings (QD_n) of the end-user n for one day, which is expressed as follows:

$$f(QD_n) = \frac{1}{T}\sum_{t=1}^{T} QD_{n_t} \tag{3}$$

To introduce required noise to the result of a query (f) on individual dataset d, Laplace mechanism that relies on the sensitivity (L_1-sensitivity) of f is used.

Definition 2 (L_1-sensitivity). Given a query function $f(\cdot)$, its L_1-sensitivity Δf is the maximum L_1 distance between the results of f over any pair of neighbouring datasets d and d', which can be expressed as follows:

$$\Delta f = \max_{d,d'} ||f(d) - f(d')|| \tag{4}$$

The Laplace distribution is one of the most popular mechanisms to introduce noise to the result of a query function f. The probability density function of the Laplace distribution centered around 0 with the scale factor $b = \Delta f/\epsilon$ is defined as follows:

$$Lap(x|b) = \frac{1}{2b}\, exp\, (-\frac{|x|}{b}) \tag{5}$$

The LDP mechanism (M) using the Laplace distribution generates and injects the random noise drawn from the Laplace distribution to query function f, whereas the scale of the noise is calibrated due to the sensitivity of f. The Laplace mechanism preserves ϵ-local differential privacy, and is defined as follows:

$$\mathcal{M}_L(x, f(\cdot), \epsilon) = f(x) + Lap(b) \tag{6}$$

Let Δf_n^{max} denote the maximum historical sensitivity for the end-user n, which is stored in a smart meter's memory. At the end of the day, a smart meter calculates the sensitivity of f based on the measurements of electricity consumption (QD_n) recorded during the day. First, all the possible modifications of a dataset d ($d = QD_n$) are generated by removing entries one-by-one from d. Let $D' = \{D'_1, D'_2, \ldots, D'_K\}$ denote the set of all possible modifications of an original dataset d, where k is the index of a modification and $k \in K$, whereas the total number of modifications is given by $K \triangleq |D'| = T(T-1)$.

By iterating over D' and calculating the sensitivity for all possible pairs of neighbouring datasets, a new sensitivity Δf_n^{new} is obtained and stored in a smart meter's memory if $\Delta f_n^{new} > \Delta f_n^{max}$. It should be noted that to reduce the memory usage, a smart meter may generate the modifications of the original dataset d one-by-one.

Each end-user has control over the required level of privacy. In other words, the end-user may adjust the privacy budget parameter ϵ based on his preferences. If the end-user decides to set ϵ to be a small value, it will provide strong privacy guarantee, which affects the quality of the services provided by grid operator, such as an electricity bill that is provided by ES. Otherwise, if ϵ is set to be a large value, it will provide weak privacy guarantee, while the quality of the services provided by the grid operators will be better. Thus, the end-user may decide on privacy versus utility by tuning the privacy budget ϵ. Let ϵ_n denote the privacy budget determined by the end-user n. Each end-user may set different privacy budgets for each day of a week or set one privacy budget for a workweek and another for a weekend depending on circumstances. By combining the end-user's privacy budget ϵ_n, the sensitivity Δf_n^{max}, the proposed local differential private mechanism may be defined as follows:

$$\mathcal{M}_L(x, f(\cdot), \epsilon_n) = f(x) + Lap(\frac{\Delta f_n^{max}}{\epsilon_n}) \tag{7}$$

where x is the electricity consumption profile for the end-user n for one day. Since a query function f produces the mean of electricity consumption readings, a grid operator needs to multiply the mean value by T to get the total electricity consumption for the end-user n in a particular day. Let C_n denote the total energy consumption for the end-user n for one day, which a grid operator (ES) receives. Let P_n denote the energy usage cost for the end-user n for one day, which can be calculated as follows:

$$Pn = C_n * \lambda_{buy} \tag{8}$$

where λ_{buy} is the buying price of energy from the utility grid in a particular day. It has to be noted that in this work, a simple energy usage cost calculation is used to show how the privacy budget set by the end-user affects the quality of the services provided by a grid operator (energy supplier).

5. Results

This section presents the simulation results to evaluate the proposed LDP-based data-sharing scheme for a smart utility environment, which consists of 50 end-users ($N = 50$) using real electricity consumption data from [18]. Fig. 2 (a) shows the electricity consumption for two randomly chosen end-users for one day. An increase in electricity consumption for the User 2 can be observed at 10 a.m. and at 4 p.m., which means that the User 2 is highly likely at home and uses some appliances. Conversely, the electricity consumption for the User 1 does not change significantly during the day. Based on the electricity consumption data for the User 1, someone could conclude that nobody is at home turning appliances on and off, which discloses the User 1 privacy. Thus, User 1 may decide to increase the level of privacy by adjusting the privacy budget ϵ_n.

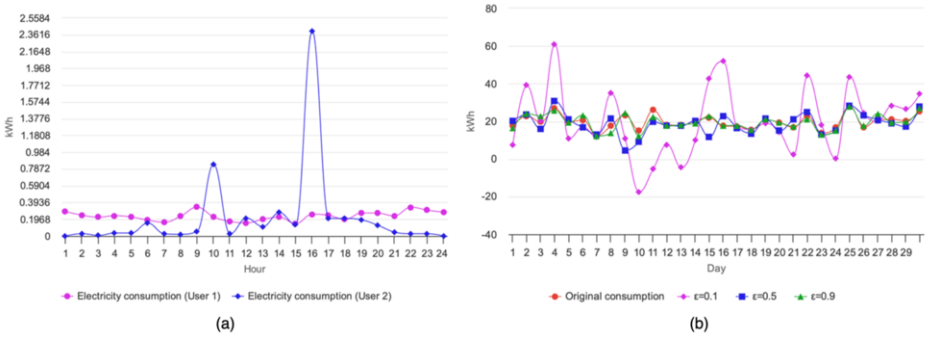

Figure 2 (a) Electricity consumption for two randomly chosen end-users for one day **(b)** Dependency of the change in electricity consumption on the privacy budget (ϵ_n) for a randomly chosen end-user for a period of 30 days

Fig. 2 (b) shows the dependency of change in electricity consumption on different privacy budgets (ϵ_n) for a randomly chosen end-user for a period of 30 days. It can be seen that the lower the privacy budget ϵ_n, the more change in electricity consumption may be observed. For example, when the privacy budget ϵ_n is set to 0.9, the electricity consumption pattern is almost the same as original with tiny deviations. Changes in electricity consumption may be clearly observed when the privacy budget ϵ_n is set 0.5,

namely on day 9 and 15. The largest fluctuations in electricity consumption may be observed when the privacy budget ϵ_n=0.1.

With the increasing scale factor b of Laplace distribution, the amount of noise increases. Taking into account that the sensitivity Δf_n^{max} changes dynamically depending on the measurements of electricity consumption, the ratio $\Delta f_n^{max}/\epsilon_n$ may lead to a variable scale factor b, which is used in the Laplace mechanism to generate noise. Thus, if the end-users do not adjust the privacy budget ϵ_n, it may lead to an unexpected energy usage cost because of unexpected b. Let P_n' denote the energy usage cost for the end-user n for a particular day, which is calculated based on the noisy consumption data as follows:

$$P_n' = C_n' * \lambda_{buy} \tag{9}$$

where C_n' is the noisy consumption data for the end-user n for one day, which is calculated by injecting noise to the original data C_n. Let RE denote the relative error that reflects the difference between the original energy usage cost P_n and the energy usage cost P_n', which is calculated based on the noisy consumption data. RE is calculated as follows:

$$RE = \frac{P_n' - P_n}{P_n} * 100\% \tag{10}$$

Fig. 3 (a) shows the dependency of the relative error RE in the energy usage cost on the scale factor b for 5 randomly chosen end-users for one day. RE is calculated 10 times for each end-user and for each scale factor b, whereas the final RE is the maximum RE observed during 10 iterations. It can be seen that when the scale factor b is lower than 0.008, the RE is lower than 10%, whereas the first time $RE \geq 10\%$ is observed at b=0.008 (RE = 16.5%). The first occurrence of the $RE \geq 60\%$ is observed when the scale factor b is equal to 0.032 (RE = 65.09%). Finally, RE = 155.5% is observed when b=0.05. In other words, Fig. 3 (a) suggests possible scale factors b that can be used in the Laplace distribution to get expected level of noise. For example, if the end-user agrees to pay up to 10% more for the energy, the privacy budget ϵ_n needs to be adjusted in a way, so that $\Delta f_n^{max}/\epsilon_n < 0.008$.

In this work, three levels of privacy are selected based on the results in Fig. 3 (a), namely Low Privacy (b = 0.008) with the $RE \leq 10\%$, Medium Privacy (b = 0.032) with the $RE \leq 60\%$, and High Privacy (b = 0.05) with the $RE \leq 100\%$. Thus, if the end-user selects the Medium Privacy level, an expected RE should not exceed 60%.

Fig. 3 (b) shows the dependency of the absolute relative error in the energy usage cost on the level of privacy for a randomly chosen end-user for a period of 30 days. It can be seen that for the Low Privacy level, the amount of noise added is small, and RE does not exceed 10%. If the end-user selects the Medium Privacy level, the RE in the energy usage cost increases compared to the Low Privacy level, while it does not exceed 60%. Finally, if the end-user needs the High Privacy level, the fluctuations in the energy usage cost are larger compared to the Medium and Low Privacy levels, whereas RE does not exceed 100%. Let us take as an example, the sensitivity Δf_n^{max} = 0.0055 on day 4. For the Low Privacy level, the privacy budget ϵ_n should be equal to 0.6875, so that $\Delta f_n^{max}/\epsilon_n = b$ = 0.008, with a resulting RE = 0.23%. Similarly, for the High Privacy level, ϵ_n is equal to 0.07 because the sensitivity Δf_n^{max} = 0.0035 on day 9. Thus, a large increase in the energy usage cost may be observed on day 9 for High Privacy level, whereas RE = 99.36%.

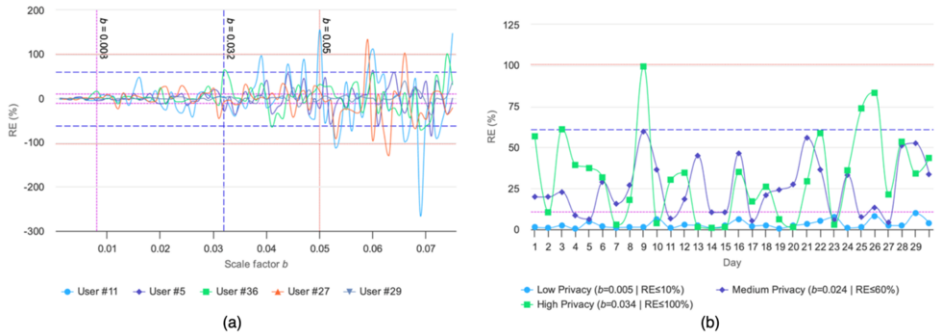

Figure 3 (a) Dependency of the relative error *RE* in the energy usage cost on the scale factor *b* for 5 randomly chosen end-users for one day **(b)** Dependency of the relative error *RE* in the energy usage cost on the level of privacy for a randomly chosen end-user for a period of 30 days

The results show in more detail how the different variables (sensitivity, epsilon, and scale factor b) in the proposed privacy preserving scheme affect each other and the final energy cost for a user. Overall, the proposed scheme allows the user to opt out of sharing fine grained data about energy consumption with the provider in exchange for a higher energy cost. More importantly, the user can manage the level of privacy and the resulting cost increase. It is possible since the noise is added to the original end-user's electricity consumption data based on the sensitivity Δf_n^{max} of a query function *f* and the privacy budget ϵ_n, which is controlled by the end-user. The ratio $\Delta f_n^{max}/\epsilon_n$ determines the scale factor *b* that is used in the Laplace mechanism to generate controllable noise. The greater the scale factor *b*, the greater the noise is injected to the original data. Since the sensitivity Δf_n^{max} depends on the end-user's electricity consumption data, the privacy budget needs to be adjusted in a way, so that the ratio $\Delta f_n^{max}/\epsilon_n$leads to an accurate scale factor *b*, based on which the noise is generated. If the end-user does not adjust the privacy budget ϵ_n, it may lead to unexpected results in terms of the amount of noise added, as well as the energy usage cost.

6. Conclusion

In this paper, a LDP-based data-sharing scheme for a smart utility environment is proposed. To ensure end-users' privacy, a local deferentially private mechanism is proposed that takes into account end-users' preferences regarding the level of privacy. End-users may adjust the required level of privacy (privacy budget) on daily, weekly, or monthly basis, thus controlling the trade-off between privacy and utility. The simulation results show that the proposed scheme may guarantee the required level of privacy with an expected error in the utility (energy usage cost). To ensure the required level of privacy, as well as to make sure that relative error in the energy usage cost does not exceed an expected level, the privacy budget needs to be tuned regularly and carefully.

One of the possible directions for the future work is to design a mechanism that will automatically adjust the privacy budget based on the dynamically changing sensitivity, according to the end-user's preferred level of privacy (low, medium, or high).

Acknowledgement

This work is supported by UKRI funded project on digital technologies in manufacturing called INTERACT.

References

[1] Informa UK Limited, *Critical Manufacturing Sector in the Bull's-eye*, 2023 (accessed Aug 15, 2023). https://www.darkreading.com/ics-ot/ critical-manufacturing-sector-in-the-bulls-eye.

[2] Informa UK Limited, *Manufacturing Sector in 2022 Is More Vulnerable to Account Compromise and Supply Chain Attacks in the Cloud than Other Verticals*, 2022 (accessed Aug 15, 2023). https://www.darkreading.com/cloud/manufacturing-sector-in-2022-ismore-vulnerable-to-account-compromise-and-supply-chain-attacks-inthe-cloud-than-other-verticals.

[3] DRAGOS, INC., *2021 ICS CYBERSECURITY YEAR IN REVIEW*, 2021 (accessed Aug 15, 2023). https://hub.dragos.com/2021-year-in-review.

[4] Department for Energy Security & Net Zero (DESNZ), *Smart Metering Implementation Programme: review of the Data Access and Privacy Framework*, 2018 (accessed Aug 10, 2023). https://www.gov.uk/government/publications/smart-metering-implementation-programmereview-of-the-data-access-and-privacy-framework.

[5] Official Journal of the European Union, *DIRECTIVE (EU) 2019/944 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on common rules for the internal market for electricity and amending Directive 2012/27/EU*, 2019 (accessed Aug 09, 2023). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri= CELEX:32019L0944&from=EN#d1e2607-125-1.

[6] Department for Energy Security & Net Zero (DESNZ), Energy white paper: Powering our net zero future, 2020 (accessed Aug 3, 2023). https://www.gov.uk/government/publications/energy-whitepaper-powering-our-net-zero-future.

[7] The National Cyber Security Centre (NCSC), The smart security behind the GB Smart Metering System, 2016 (accessed Aug 3, 2023). https://www.ncsc.gov.uk/information/the-smart-securitybehind-the-gb-smart-metering-system.

[8] Australian Competition and Consumer Commission (ACCC), *The Consumer Data Right*, 2023 (accessed Aug 11, 2023). https://www.accc.gov.au/by-industry/banking-and-finance/theconsumer-data-right.

[9] D. Zhao, C. Zhang, X. Cao, C. Peng, B. Sun, K. Li, and Y. Li, "Differential privacy energy management for islanded microgrids with distributed consensus-based admm algorithm," *IEEE Transactions on Control Systems Technology*, vol. 31, no. 3, pp. 1018–1031, 2023.

[10] F. Leukam Lako, P. Lajoie-Mazenc, M. Laurent, and C. Vorakulpipat, "Privacy-preserving publication of time-series data in smart grid," *Sec. and Commun. Netw.*, vol. 2021, jan 2021.

[11] N. Gai, K. Xue, B. Zhu, J. Yang, J. Liu, and D. He, "An efficient data aggregation scheme with local differential privacy in smart grid," *Digital Communications and Networks*, vol. 8, no. 3, pp. 333–342, 2022.

[12] S. Zhao, F. Li, H. Li, R. Lu, S. Ren, H. Bao, J.-H. Lin, and S. Han, "Smart and practical privacy-preserving data aggregation for fog-based smart grids," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 521–536, 2021.

[13] J. Qian, Z. Cao, X. Dong, J. Shen, Z. Liu, and Y. Ye, "Two secure and efficient lightweight data aggregation schemes for smart grid," *IEEE Transactions on Smart Grid*, vol. 12, no. 3, pp. 2625–2637, 2021.

[14] X. Zhang, W. Tang, D. Gu, Y. Zhang, J. Xue, and X. Wang, "Lightweight multidimensional encrypted data aggregation scheme with fault tolerance for fog-assisted smart grids," *IEEE Systems Journal*, vol. 16, no. 4, pp. 6647–6657, 2022.

[15] G. K. Verma, P. Gope, N. Saxena, and N. Kumar, "Cb-da: Lightweight and escrow-free certificate-based data aggregation for smart grid," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 3, pp. 2011–2024, 2023.

[16] European Data Protection Supervisor (EDPS), *TechDispatch #2: Smart Meters in Smart Homes*, 2019 (accessed Aug 9, 2023). https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-2-smart-meters-smart-homes en.

[17] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," *Journal of Privacy and Confidentiality*, vol. 7, p. 17–51, May 2017.

[18] U. P. Networks, *SmartMeter Energy Consumption Data in London Households*, 2022 (accessed Aug 8, 2023). https://data.london.gov.uk/ dataset/smartmeter-energy-use-data-in-london-households.