energies

Article

Privacy-Functionality Trade-Off: A Privacy-Preserving Multi-Channel Smart Metering System

Xiao-Yu Zhang [1,*], Stefanie Kuenzel [1,*], José-Rodrigo Córdoba-Pachón [2] and Chris Watkins [3]

[1] Department of Electronic Engineering, Royal Holloway, University of London, London TW20 0EX, UK
[2] School of Business and Management, Royal Holloway, University of London, London TW20 0EX, UK; J.R.Cordoba-Pachon@rhul.ac.uk
[3] Department of Computer Science, Royal Holloway, University of London, London TW20 0EX, UK; C.J.Watkins@rhul.ac.uk
* Correspondence: xiaoyu.zhang.2018@live.rhul.ac.uk (X.-Y.Z.); stefanie.kuenzel@rhul.ac.uk (S.K.)

Received: 8 April 2020; Accepted: 18 June 2020; Published: 21 June 2020

Abstract: While smart meters can provide households with more autonomy regarding their energy consumption, they can also be a significant intrusion into the household's privacy. There is abundant research implementing protection methods for different aspects (e.g., noise-adding and data aggregation, data down-sampling); while the private data are protected as sensitive information is hidden, some of the compulsory functions such as Time-of-use (TOU) billing or value-added services are sacrificed. Moreover, some methods, such as rechargeable batteries and homomorphic encryption, require an expensive energy storage system or central processor with high computation ability, which is unrealistic for mass roll-out. In this paper, we propose a privacy-preserving smart metering system which is a combination of existing data aggregation and data down-sampling mechanisms. The system takes an angle based on the ethical concerns about privacy and it implements a hybrid privacy-utility trade-off strategy, without sacrificing functionality. In the proposed system, the smart meter plays the role of assistant processor rather than information sender/receiver, and it enables three communication channels to transmit different temporal resolution data to protect privacy and allow freedom of choice: high frequency feed-level/substation-level data are adopted for grid operation and management purposes, low frequency household-level data are used for billing, and a privacy-preserving valued-add service channel to provide third party (TP) services. In the end of the paper, the privacy performance is evaluated to examine whether the proposed system satisfies the privacy and functionality requirements.

Keywords: smart grids; smart energy system; smart meter; GDPR; data privacy; ethics

1. Introduction

The smart grid is a worldwide modernization of electrical power systems in the 21st century. Two-way communication networks enable smart grids to collect real-time data from both the electricity supply (i.e., power stations) and demand (i.e., households) sides, and further boost the power system's reliability, availability, and efficiency.

As an essential enabler and prerequisite of the smart grid, smart meters are being installed country- and world-wide at single houses to collect real-time data on energy consumption. Smart meters offer an opportunity to consumers to play an active role in household energy consumption management. Based on these advantages, the UK government is working to ensure 80% of households install smart meters by 2020, paving the way for future smart grid construction [1].

However, with the EU's mandate to install smart meters, worries about privacy intrusions caused by smart meters are rising. Researchers point out that private household information can be revealed by smart meters [2–4]. Through continuously monitoring the real-time smart meter data, third parties (TP) could have an inside view of household activities and behaviours (e.g., how many residents live in the house, when people leave the home, what the residents are doing at particular times, such as sleeping, bathing, watching TV, washing clothes, etc.). Although data collection may be justified on ethical grounds of utilitarianism (i.e., ensuring the greater, collective good of energy efficiencies in smart grids), the intrusion into privacy could also have negative ethical social consequences, including the conditional shaping of freedom and behaviour of individuals and households [5,6].

It is urgently expected that a more reliable smart metering system should be proposed to improve privacy and security. To do this, there could be three operational methods to protect households' privacy: (a) user demand shaping, (b) data manipulation, and (c) encryption techniques. User demand shaping approaches modify electricity data using methods such as energy storage systems or rechargeable batteries in households [7]. This requires the installation of extra devices, which is expensive. Data manipulation approaches modify energy data before sending it to TP (i.e., utility companies) by employing strategies like data obfuscation, data aggregation [8], data down-sampling, encryption protocols [3], or data anonymization. However, these methods sacrifice functionalities to protect privacy. Encryption techniques include homomorphic encryption (HE) and multi-party computation (MPC); these techniques encrypt the input data and can still implement essential operations with encrypted data, but techniques such as HE also cause computing overhead, increasing the budget.

At a legal level, the General Data Protection Regulation (GDPR) has been in force since 25 May 2018 [9]. Covering all European countries, the purpose of GDPR is to protect all EU citizens from privacy and data violation, providing more power to individuals to control their personal information. With these operational and legal operational possibilities, it is also important to consider 'soft' ethical strategies that use them to contribute to protect household privacy, potentially enabling households to be more in control of their digital data [10]. One such strategies is that of considering different stakeholders involved or affected by digital data gathering [11].

In this paper, we extend the approach from [8,12,13] to the combined use of existing data aggregation and data down-sampling techniques to design a privacy-preserving smart metering system. The system follows an operational and ethically (consequentialist) driven trade-off strategy and model which could contribute to increase functionalities of current smart metering devices in smart grids whilst ensuring that digital privacy intrusion is minimised and protected if not appropriately governed. In addition, the system provides three different communication channels for data collection to enable diverse data granularity transmission to TP, with each channel also providing required functionalities (time-of-use billing, grid operation and management, and TP services). We present our system and discuss the results of testing it with implications for the future design or management of smart meters by TP and households.

The paper is organized as follows: A presentation of smart grids and smart metering systems with ethical concerns about privacy intrusion is offered in Section 2. A review of current operational strategies to deal with privacy intrusion is presented in Section 3. In Section 4 our main contribution is proposed: a trade -off strategy is discussed with a proposed new smart metering system model to support it. A simulation work to quantify the privacy boundary is given in Section 5. The conclusion, implications, and future work are drawn in the last sections of the paper.

2. Background

2.1. Smart Grids

Smart grids are physical networks that use cutting-edge technologies and equipment, enabling the interconnection of different components through two-way networks that could achieve real-time optimizations to deliver electricity more reliably and efficiently. Smart grids contain not only electricity interfaces, but also communication interfaces. With these, other stakeholders (utility companies) or domains (electricity markets) can be included for analysis and management. Future smart grids can enable better operation and control, better network planning and maintenance, advanced smart metering infrastructure (AMI), and overall energy efficiency for countries [14].

2.2. Advanced Smart (Metering) Infrastructures

Within smart grids, AMI systems are integrations of smart meters, communication networks, and data management systems [14,15]. With the adaptation of narrowband(NB) powerline communication (PLC) technologies (e.g., Powerline Intelligent Metering Evolution (PRIME) and G3-PLC standards adopted in Europe), AMI enable real-time bidirectional communication between the TP (suppliers) and electricity consumers [16–18]. Smart meters are the most vital components within AMI. As smart energy sensors are installed in consumers' residences (households), smart meters can gather and transmit data including power consumption and electricity/gas bills on a real-time basis.

As illustrated in Figure 1, stakeholders of the smart metering system can include the consumers, energy suppliers, network operators, and data and communications companies (DCC) and TP. With smart meters, consumers can obtain near real-time and more accurate power usage data and bills, which helps them manage their energy usage. Energy suppliers (ES) are the utility companies that buy electricity from the wholesale market, then sell it to consumers. For instance, large British ES include British Gas, E-On, and SSE. Network operators (NO) (i.e., transmission system operators or TSOs, distribution system operators, etc.) construct, maintain, and operate the energy network, ensuring normal operation. These latter stakeholders can also benefit from smart meters: firstly, with the near real-time communication networks, utility companies can save money initially used for manual billing; secondly, network operators can implement demand-based management responses, in particular under peak load times; and finally, operators and companies can detect fraud or electricity theft and thus improve their efficiencies.

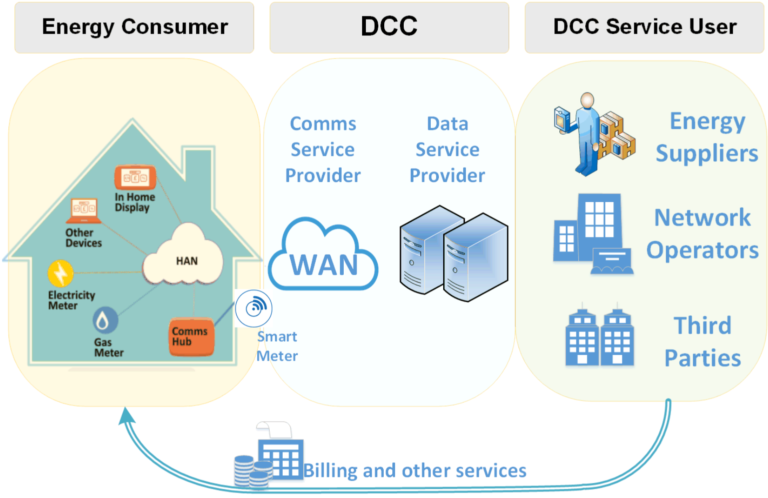

Figure 1. The structure of the current smart metering system.

The DCC collect energy consumers' data through the wide area network (WAN). Processed data are then sent to energy suppliers and network operators. DCC are responsible for ensuring compliance with the GDPR directive [19]. However, there is a lack of clarity about other stakeholders' responsibilities, making smart meters potentially fragile to a few privacy risks and concerns. These need to be identified and further explored if improvements in smart metering systems are to be made by or affecting several or all the stakeholders presented in the above figure. Before doing so, basic functions of smart meters are presented as following subsections.

2.3. Functions of the Smart Metering System

The European Commission identifies the 13 main functions of a smart meter and classifies them into five categories [20]. The most significant functions are listed in [21], which are billing correctness, grid operation and management, and additional consumer services. In addition, an emerging function is that of time-of-use (TOU) tariff.

2.3.1. Billing

The most vital function of the smart meter is providing accurate billing for consumers. Any data protection method which influences the accuracy of billing is useless. The current sample interval of the smart meter is 15 min up to a few seconds; however, consumers do not need such high-frequency billings, weekly or monthly basis billing is enough [21].

2.3.2. Grid Operation and Management

The smart meter contributes to the smart grid by improving the efficiency and stability of the whole power system. The real-time two-way communication networks provided by the smart metering system can measure, analyse, and control the energy consumption data, and further support the smart grid to implement demand side response services and power system estimation. For grid operators, the measurement of every individual household smart meter is not compulsory. Instead, they have more interest in high aggregated level data, such as measurement at feeder level or substation level [22].

2.3.3. Value-Added Services

The consumers can order additional services provided by the utility or TP. The additional consumer services could be awareness, (e.g., sending a warning for exceeding power), or scheduling and control (scheduling for controllable appliances, peak shaving) [23]. Demand-side response and non-intrusive load monitoring (NILM) have received the most attention. Demand-side response [21,24,25] optimizes the strength of the grid and enhances the power quality by utilizing power plants, distributed generators, and loads and energy storages. In demand-side response, consumers can also participate in the response process by accepting the bids provided by grid operators. By turning off appliances such as air conditioners and heaters, the load would be shed during peak time. NILM is a technique to disaggregate consumers' power consumption curve into individual appliance usage. The consumer can have an insight into how electricity is consumed and can better manage their home appliances to save energy and reduce carbon dioxide emissions [26]. Normally, value-added services require consumers to submit their energy data to a server; the server would use a pre-trained model to evaluate the data and send the results back to consumers. The difficulty exists in how to share personal data with TP while guaranteeing privacy at the same time.

In [21], two privacy-preserving value-added schemes are proposed. The naive scheme down-samples the original data into multiple interval resolution data, referring to the requirement of different services. Then the different resolution data are sent to different TPs with a key [13]. The second solution is to enable services at consumers' own devices (personal computer, mobile phone) via a home area network (HAN), however, TPs have the risk of revealing their models/algorithms [21].

2.3.4. Time-of-Use Tariff

The TOU tariff determines the electricity price during different periods. Consumers benefit from the TOU tariff by shifting their electricity usage habits to enjoy a cheaper bill, while the energy suppliers can also reduce the power plant capacity as a result [14], so TOU is becoming the mainstream method for billing in the UK. With the installation of the smart meter, the TOU moves closer to the real-time pricing tariff, allowing it to better represent the true conditions [27]. Although TOU tariff needs high-frequency data, the price volatility is determined by the aggregated power usage of the whole area rather than individuals. So, consumers do not have to send high-frequency data to realize the TOU tariff.

2.4. Privacy Intrusion Issues

Currently, smart metering systems could easily suffer from internal [28] and external attacks [29] and be subject to privacy intrusion [2]. All privacy intrusion issues related to the smart meters fall into two categories:

Category (i) Data sensitivity. Personal energy data that cannot be measured by a conventional electricity meter. While the traditional electricity meter measures the power consumption with a low resolution (e.g., one month) and can only provide the energy consumption information in kWh, the smart meter measures the power consumption with a high frequency (ranging from every second to every half hour, and normally every 15 min [21]), and more parameters are recorded, such as real-time active/reactive power, voltage, current, TOU tariff, etc. The high granularity data provide adversaries enough information to intrude on personal information.

Category (ii) Algorithm sensitivity. Advanced algorithms/mechanisms to intrude on privacy-sensitive features that could not be extracted from raw data using traditional data processing mechanisms. With the implementation of smart meters in smart grids to meet the above functions, and the increasing development of new services and applications by TP based on big data and artificial intelligence (AI) (e.g., Machine Learning (ML), Deep Neural Network (DNN), cloud computing), more and more sophisticated data could become available [30]. New services to better understand and monitor household behaviour include NILM [26], short-term load forecasting (STLF), distributed data mining, and others [14,30]. These advanced techniques are a double-edged sword to the consumers. The benefits espoused to consumers described above (e.g., managing their own energy consumption) and the adoption of a utilitarian ethic (i.e., ensuring the greater, collective good of energy efficiencies in smart grids) need to be weighed against potential privacy intrusion risks. Privacy intrusion would mean that not only individual but also collective freedom is compromised, given that household behaviour would be shaped and constrained by the perceived presence of digital surveillance [10,11,31].

Moreover, referring to the US National Institute of Standards and Technology (NIST) guideline NIST IR 7628v2 [32], the above two categories can be divided into four aspects as follows:

2.4.1. Behaviour Patterns Identification

Behaviour patterns identification belongs to category i; it aims to identify the appliances used. The smart meter and AMI communication network enables the utility and TP to access individual energy data continuously [15]. The high granularity data can reveal information about specific appliances at certain times and locations inside the home. Based on this information, operators can further infer the activities inside the house [32]. Potential usage of the appliance information may include that the retailers would adjust the warranty policy or use the information for advertising and marketing purposes.

2.4.2. Real-Time Surveillance

Real-time surveillance means that by regularly accessing energy data via smart meters, power system operators/TPs can have an overall picture of the activities inside a house, and even the entire life cycles of all residents (waking/sleeping pattern, number of residents, when people leave their home). This privacy concern belongs to category ii; the surveillance relies on advanced techniques such as data mining, machine learning/deep learning algorithms [26,30,32]. This information could be abused by hackers and stolen for criminal purpose [33].

2.4.3. Fraud

Fraud represents the potential risks of personal energy data being modified without authority, either to increase/decrease energy consumption or attribute the energy consumption to another house [32]. This risk belongs to category ii; the AMI enables more opportunities for adversaries to implement fraud than conventional meters since the vulnerabilities of the real-time communication network would be abused.

2.4.4. Non-Grid Commercial Uses of Data

This privacy risk falls into category ii. The smart meter data may be used by TP to make a profit from the data; activities include advertising and insurance that are not welcomed by consumers [32]. Companies would sell their products to residents according to the personal preference information revealed by the energy data. Even sensitive information, such as employment information [30], can be inferred from energy data with machine learning algorithms. This information can be used by adversaries to estimate the income of the target family.

3. Related Work for Privacy Intrusion Protection

The state-of-the-art methods dealing with the above smart meter privacy issues can be divided into two categories: user demand shaping and data manipulation. Both these techniques try to reduce the privacy loss by decreasing the probability to infer individual appliance signatures from the overall power data [34].

3.1. Demand Shaping

User demand shaping uses external energy storage devices (such as a large rechargeable battery (RB) [7,35–42], renewable energy system (RES) [43–46]), or load shifting [47–49] to distort the real power consumption curves. The RB and RES method can be treated as a noise-adding approach at the physical layer, as the original power demand is distorted, the utility cannot infer sensitive information from the smart meter data. An RB system contains a smart meter, a battery, and an energy management unit (EMU), the EMU controls battery to implement optimal energy management policy (EMP), with the injection of power from the RB B_t, the mismatching between the power supplied by the grid Y_t and consumers' power demand X_t provide privacy guarantee to consumers. The works conclude that the larger the battery capacity size, the better privacy can be guaranteed. However, the RB is a finite capacity energy storage device with capacity ranges from 2 kWh to 20 kWh [50], therefore there exists a lower and upper bound ($\hat{P}_c$ and $\hat{P}_d$) to limit the performance of the mechanism. The optimal EMP, such as best-effort (BE) algorithm [7], water -filling algorithm [51], Q -Learning algorithm [1], non-intrusive load-leveling (NILL) algorithm [52] are introduced to optimize the charging/discharging process, these algorithms control the battery either hide, smooth, or obfuscate the load signature [7]. NILL algorithms are designed to blind the NILM [52], instead of only one target load, the NILL has two states, a steady-state and recovery state if the battery capacity cannot enable the load to maintain steady-state, the load is switched to the recovery state. A privacy-versus-cost trade-off strategy considering the TOU tariff is proposed by Giaconi et.al in 2017 [53]. Instead of a constant load target, a piecewise load target referring to the current TOU price is generated, the cost of the electricity is minimized, and the consumers can also sell extra energy to the grid to reduce the cost further.

RES utilizes rooftop PV, small wind turbine, and even Electric Vehicle (EV) [54] to replace the conventional battery. To overcome the difficulty to roll -out expensive RES and RB facilities, Reference [55] proposed a multiuser shared RSE strategy that enables serval users to share one RES and one EMU. The EMU control the RES to allocate the energy from the RES to each user. In this case, the target of the system is to minimize the overall privacy loss of all users rather than an individual user. EV is another scheme to reduce the reliance of the RB [54] since the charging period is almost overlapping with the peak load, it can mask other appliance signatures. However, the EV can only be used when the consumers are at home, the consumers are still under real-time surveillance since the adversary would obtain information when the residents leave their home.

To summarize, in RB/RES methods, researchers view the identification information of the load curve as the variation of the load measurements of two neighboring measure points $Y_t - Y_{t-1}$. The ideal situation for the grid curve is a constant value C_t which will not reveal any sensitive features of the demand, the modified load curve Y_t is then compared to C_t, the more similarities between these two curves, better privacy can be guaranteed. To quantify the privacy loss, Mean Squared-Error (MSE) [53], Mutual Information (MI), Fisher Information (FI) [35], KL divergence [7], Empirical MI [37] are adopted in related works. However, user demand shaping also has drawbacks: Firstly, extra energy storage systems and renewable energy sources are required to implement the demand shaping strategy; these devices are prohibitively expensive and can be difficult to roll-out, the batteries need to be renewed frequently. Secondly, the energy storage system blinds demand response, which is one of the most important functions of the smart grid.

As the drawbacks of RB/RES methods are obvious, another demand shaping method named load shifting is proposed to replace the RB/RES techniques. This method hides sensitive information by shifting the controllable loads [47–49]. The loads can be divided into uncontrollable loads (e.g., lighting, microvan, kettle) and controllable loads (e.g., heating, ventilation, and air conditioning (HVAC) systems, EV, dishwasher, washing machine). The operation time and model of the controllable loads can be scheduled by consumers to prevent occupancy detection. In [49], combined heat and privacy (CHPr) are proposed, thermal energy storage such as electric water heater is adopted to mask occupancy. Compared with the RB approach, CHPr neither requires expensive devices nor increase electricity cost. There are several limitations of the load shifting technique, firstly, some of the controllable loads have limited operation modes and cannot be interrupted; secondly, there are restrictions for the thermal loads to store energy.

3.2. Data Manipulation

Different from the demand shaping approach, data manipulation aims to modify the smart meter data before sending it to the utility. Data aggregation, data obfuscation, data down-sampling, and anonymization all belong to this category.

Data obfuscation, which is also called data distortion, tries to add noise to the original smart meter data to cover the real power consumption [56–60]. Like demand shaping technique, data obfuscation also reduces the privacy loss by distorting the smart meter data, but on the network layer. Noises such as Gaussian noise [56,60], Laplace noise [56], gamma noise [57] are added into the original smart meter data to distort the load curve. These noise-adding mechanisms follow normal distributions with mean μ equals to zero, hence the noise would cancel out if enough readings are added up together, P. Barbosa, et al. [59] conclude that these probability distributions would not influence the relationship between the utility and privacy, so all distributions can achieve similar performance in protecting privacy. Moreover, to guarantee the billing correctness, serval schemes are proposed: Reference [56] proposes a power consumption distribution reconstruction methods by adding another Gaussian distribution into the data, but the method does not quantify how much noise should be added to recover the original curve; Reference [59] sends a filtered profile to the utility rather than masked profile, then result shows that the error of the overall power consumption is reduced in this way. However, they also find that the error during different periods (peak period, off-peak period) is significantly different, which provides new challenge. In summary, although the data distortion scheme shows efficient performance in reducing privacy loss, there are serval problems which should be discussed in future studies: (1) The TOU tariff is unavailable. Although the noise would be zero-mean, but the multiplier for TOU pricing is not. Hence the sum of TOU bills would be influenced. (2) Although from the signal processing and information-theoretic viewpoint that a zero-mean noise would not influence the result, we should notice that the power system is operating on a real-time basis. The power system operator manages the grid with the real-time data sent from the smart meter, even a minor error between the ground truth with the distorted data could result in serious faults, even the collapse of the whole system.

Data aggregation reduces the privacy loss by constructing aggregators to collecting the data from a few smart meters together, so the utility is unable to detect the electricity events in a single house [8,22,60–62]. The data aggregation technique is divided into aggregation with trusted third parties (TTP) [60] and aggregation without TTP [8,22]. J.-M Bohli, et al. [60] propose data aggregation with TTP, the data aggregator (DA) operated by the TTP is responsible for gathering the data from neighbouring smart meters and then sending the aggregated data to ES. At the end of every month, the DA also generates energy consumption of individual consumer for billing purpose. However, there are several concerns about involving TTP. Above all, a TTP could try to infer the personal information, so the TTP itself may bring extra privacy risks to the system. Secondly, with the increasing numbers of smart meters being installed, it is unrealistic for the TTP to build enough DA to satisfy the demand, and the maintenance and development budget would be unaffordable to EP and NO.

References [8,22,61–63] introduces data aggregation mechanisms without TTP. Instead, encryption techniques such as HE, MPC [8,22,62,63] are employed. Both HE and MPC encrypt personal smart meter data before sending it to the utility/TP. However, differently from conventional encryption techniques, HE and MPC enable TPs to manipulate the data without knowing the detail of it. F. Li, et al. [8] and R. Lu, et al. [22] independently proposed an aggregation method with HE separately. By encrypting smart meter data, the DA can implement aggregation without knowing the data details. In this way, there are no concerns that the TTP may infer sensitive information without permission. However, the drawbacks of data aggregation technology are twofold. Firstly, after aggregating, it is impossible for the utility to obtain the power usage information of an individual consumer. Secondly, complex encryption would cause high computational overhead. MPC requires low computing ability but involves several servers to deal with the data [63]. In MPC, each server holds a part of the input data and they cannot infer the whole information. MPC has been successfully adopted in smart metering services such as TOU billing. However, complex value-added services, such as load forecasting and online energy disaggregation, require an advanced cloud server to implement these algorithms. So, the availability of MPC in these services should be discussed. The privacy boundary of aggregation size is also investigated in T.N. Buescher, et al. work [61]. They investigated the aggregation size referring to a privacy metric named 'privacy game'. Referring to the data-driven evaluation, a conclusion is made that even a DA with over 100 houses can still reveal private information. But the privacy measure they adopt is abstract and just simply measures the difference between the individual load curve and the aggregated curve, a more detailed privacy measure should be proposed to reflect whether advanced algorithms (such as NILM) can infer personal information from the aggregated data.

References [56–58] combines data aggregation with noise-adding technique together, to enable differential privacy to the aggregated data. Differential privacy is employed as privacy guarantee, the concept of differential privacy is through adding noise to a largescale dataset, any two neighboring datasets (only one data in these two datasets is different) should be indistinguishable [64]. In other aggregation mechanisms, N smart meters are aggregated at first, then a distributed Laplacian Perturbation Algorithm (DLPA) is applied to the aggregated data. By adjusting the parameters ε and δ, then we can say (ε, δ)-differential privacy is achieved (ε is the parameter to show the strength of privacy guarantee, and the δ is the failure probability, the closer ε and δ to 0, the better privacy can guarantee). The security and privacy performance are analysed in [56], two denoising filter attacks, the linear mean (LM) filter, and the non-local mean (NLM) filter are employed to evaluate the original. The results convince that attackers cannot infer the original load curve from the distorted one.

Data Anonymization mechanism [12,65,66] reduces privacy loss by replacing the real smart meter identification with pseudonyms. C. Efthymiou and G. Kalogridis proposed a data anonymization method with a TTP escrow in 2010 [12]. They suggested that two IDs are attached to each smart meter, LFID for sending attributable low frequency and HFID for sending anonymous high-frequency data, while the HFIDs are kept by a TTP, making it unknown to the utility. The low-frequency data are used for billing purposes while the high-frequency information is for network management. However, the workload of the TTP is high, and the development costs increase since all anonymous IDs are processed here. Moreover, with the introduction of the TTP escrow, the privacy risks are not eliminated but just shift from the utility to TTP.

The down-sampling method is a naive approach that aims to reduce sensitive information by reducing the interval resolution of the metered data [13,33,66]. However, like other methods, functions such as demand response and TOU billing would be sacrificed. Moreover, value-add services that require high-resolution data are unavailable as well. To quantify the privacy loss with different interval data, G. Eibl and D. Engel adopt NILM as adversary to the extract of personal information. They apply an edge detection NILM to smart meter data and examine the performance of 15 appliances via F-score values and the proportion of appliances. They conclude that 15-min interval data already protect most appliances. We would like to have an in-depth research based on the research by implanting more powerful NILM algorithm (such as deep learning based NILM) since deep learning has shown distinctive ability to extract features than conventional approaches.

To sum up, solutions either require the installation of expensive devices (rechargeable battery or RES) or employ complex and high computing algorithms (data distortion and data aggregation). Moreover, some schemes introduce TTP into the smart metering system, which just moves the privacy risk from one party (ES) to another one (TTP). Most importantly, unlike other communication networks, the physical connections of the electricity grid already aggregate load consumptions at feeder level or substation level without privacy concerns, the construction of the data aggregator is superfluous. And no existing solution emphasizes the availability of value-added services, which is the vital functionality the smart meter brings to consumers. Comparing the two solutions listed above, the proposed scheme is simpler and more efficient: The proposed scheme is based on existing physical facilities (the smart meter, private platform, distribution substation) and does not require any extra RES or high computation encryption. In the proposed scheme, the smart meter only communicates with the private platform (PC or smartphone) inside the house via Home Area Network (HAN). A multi-channel smart metering system enables the private platform to communicate with other stakeholders (e.g., ES, TP) with different data granularity, which takes the advantages of both data aggregation mechanism to enable grid operation and management and data down sampling mechanism to provide accurate TOU bills. Furthermore, a privacy preserving NILM algorithm is designed to enable value-added services.

4. A Proposed Privacy-Functionality Trade-off Strategy and Model

Given the scale of smart meter roll-out processes in countries and worldwide, the above risks and operational strategies could be dismissed or subordinated to utilitarian market logic, with the responsibility for their implementation and subsequent privacy protection of consumers (i.e., households) delegated to third parties, many of whom might not have privacy protection as a priority in their agendas. Moreover, and as stated before, there is a lack of clarity about such responsibilities. Furthermore, whilst smart grids could be conceived as necessary technologies to regulate the conduct of individuals in our societies [67], what could be more concerning is that privacy intrusion could also generate negative social consequences [31]. Consumers can be left powerless or socially isolated to devise their own strategies to counteract intrusion to their privacy, becoming mere means rather than ends [5].

It might be possible, however, for stakeholders to exert their creativity even in the face of privacy intrusion and existing regulations (i.e., GDPR directive) [5,10,68]. This would help households comply with the functionalities that digital technologies establish for them [68] whilst socially protecting or enhancing their sense of authentic household 'hood' [6].

To meet this, we thus propose a trade-off strategy that attends to both the operational and ethical concerns for smart meters and smart grids raised in this paper. The strategy adopts these principles:

I. Ensuring the compulsory functions of smart meters as previously described and complemented.
II. Data minimization.
III. Protection from inner or outer attacks (to be explained in Section 5).

The operation of the strategy is shown in the proposed model, Figure 2, as follows. The model components are consumers, DCC, energy supplier (ES), a network operator (NO), third parties (TP), and the distribution-level substations (Sub) which supply electricity to households.

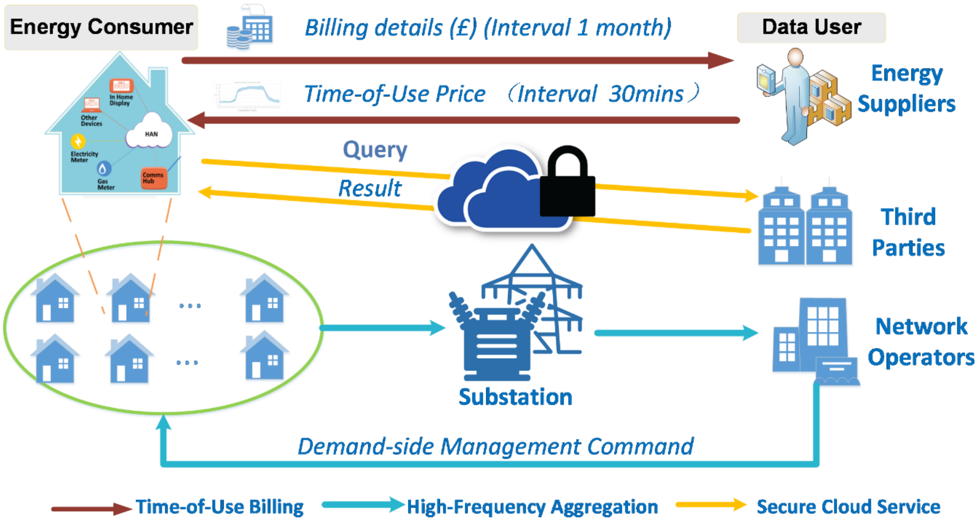

Figure 2. Proposed smart metering system.

4.1. Compulsory Functions

The interval resolution and categories of data of compulsory functions are listed in Table 1 below. For billing purposes, the frequent transmission of the power consumption data would put consumers under the monitoring of the utility. For grid operation and management, although the utility requires high interval resolution data (seconds to 100 Hz), it is unnecessary to access every individual's power consumption; aggregated data of a defined area is more desirable. Most additional services provided by TP only require a specific part of the power consumption data (a certain period, a specific appliance power consumption, etc.), so, all TPs are to obey the data minimization principle (explained below), and only collect the minimum data required to complete the service.

Table 1. Summary of data granularity of different functionalities.

Functionalities	Sample Frequency Required	Data Required
Billing	Low (weekly or monthly)	Usage of every single household smart meter
Grid Operation and Management	Very High (sometimes more than 50 Hz)	Active/Reactive power, voltage of selected area
Value-added Services	Depending on specific services	Depending on specific services
TOU tariff	High (15 min–1 h)	The TOU price from the electricity market

In the proposed strategy and model, it is not considered appropriate to authorize TTP (described earlier) to be responsible for data aggregation, since as a potential inner adversary TTP can still acquire valuable information during the aggregating process. Rather, substations could be a better choice for data aggregation. In countries such as the US and China, there is already an installation of substation-level supervisory control and data acquisition (SCADA) systems [69]. This provides evidence that substation-level smart metering or intelligent substation data would be a trend of the future smart grid system.

Moreover, in contrast to conventional smart metering systems that can only transmit a single temporal resolution trace, this novel scheme contains three communication channels to support multi-temporal resolutions data. These three channels are a high-frequency aggregated data channel, to transmit 100 Hz aggregated data measured at the distribution level substation; a TOU billing channel, to send dynamic TOU price information to smart meters and send bills to the ES monthly; and an additional service channel, to transmit selected data to support additional services. The smart meter in the scheme plays the role of the assistant processor rather than the information sender and receiver; it has basic computation ability to calculate billing inside the house rather than sending individual power consumption near real-time.

4.2. Data Minimisation and Protection

As one of the most vital principles of data protection, data minimization is mentioned in five separate sections in GDPR (Article 5 (Chapter II), Article 25 (Chapter IV), Article 47 (Chapter V), Article 89 (Chapter IX)) [9]. It highlights that limitations should be set on the measurement of personal data implemented by organizations; only the minimized information necessary to complete specific required purposes can be collected. More specifically, the data minimization principle for the smart grid is recommended in the US National Institute of Standards and Technology (NIST) Guidelines [32]. To deal with privacy risks caused by smart meters, strict limitations need to be set; only the data which are essential for smart grid operation should be collected (e.g., billing, demand-side management, grid planning). Data minimization is strongly related to protection from inner and outer attacks, as will be presented in the following section of the paper.

4.3. Mathematical Model

4.3.1. The Smart Meter

The smart meter in the proposed system does not communicate with the energy supplier directly, the measurements of the smart meter will be uploaded to a private platform (PC or smartphone) via HAN. The private platform has basic storage and computation ability to save power consumption and calculate the bills. Assume the area involves a smart meter group SM $= \{sm_1, \ldots sm_i, \ldots sm_N\}(i \in [1, N])$. The smart meter can measure power consumption with interval T (normally 15 min), marked as $P_{T,i}$. The smart meter data are encrypted to prevent consumers from modifying the power consumption data. There is no backdoor when the smart meter is manufactured, so manufacturers or energy suppliers cannot illegally access the smart meter data, and all data transmission between consumers and the utility is monitored by the DCC. In the proposed system, the smart meter reports the monthly energy consumption E_{month} and monthly bills B_{month}.

4.3.2. Protection from Inner and Outer Attacks—Adversary Element

Using a consequentialist perspective to ensure that stakeholders are held to identification and account [11], in our model all stakeholders could adopt an "honest-but-curious" ethic [21]. They follow functional protocols properly and provide expected services to consumers ("honest"), but at the same time, they keep inferring sensitive information from the consumers ("curious"). In the proposed system, household adversaries could access aggregated power consumption P_{AGG} (kW) and monthly energy consumption of smart meter i E_{month} (kW·h). Their purpose would be to obtain data. They could have a high computational ability to disaggregate the obtained data into individual appliance power consumption data by applying methods like the NILM algorithm, leading them to potentially use data for unethical or illegal purposes.

4.4. High-Frequency Aggregated Data Channel

The high-frequency aggregated data channel transmits the aggregated power consumption data to the DCC. We install a substation-level smart meter inside the distribution-level substation. The substation contains all consumers' power consumption in the local area without requiring every individual smart meter to send data to it, so it plays the role of an "aggregator," but without collecting the power consumption data from every single house. The measurement frequency of substations in our research is selected as $f_{hf} = 100$ Hz, which is twice the British power system frequency. The high interval resolution data is used for grid operation and management since near real-time data is vital for demand-side management to deal with unexpected incidents such as a blackout.

The reason that the distribution-level substation can play the role of "aggregator" is twofold. Firstly, substations already exist. No extra facilities like data aggregators need to be constructed, so the development investment can be saved. Secondly, no TTP or homomorphic encryption is involved in this scheme, so the concerns of inner attacks from TTP and computation overhead raised by complex encryption are eliminated. Table 2 shows three typical feeder models summarized by GridLAB-D's feeder taxonomy [70], these three models represents feeders at light rural area, heavy suburban, and moderate urban respectively. The house units under each feeder can be estimated by adding up household-level data to match the feeder model [71]. From the table, the light rural area consists around 408 houses. In Section 5, an evaluation is implemented whether feeder/substation level measurement at light rural area satisfies the privacy requirement.

Table 2. House units under different feeder models [70,71].

Feeder Model	Active Power/kW	Description	Units under the Feeder
R4-25.00-1	948	Light rural	408
R1-12.47-4	5334	Heavy suburban	2299
R2-25.00-1	17,021	Moderate urban	7336

4.5. Time-of-Use Billing Channel

The TOU channel enables the dynamic TOU tariff, see Figure 3. In the conventional smart metering system, the smart meter should report the energy consumption at each charging point to obtain TOU bills. The more charging points the utility sets, the more detailed information about an individual is obtained by the utility, and the more it is possible that privacy is breached.

In our TOU billing channel, the direction of information transmission is the opposite. The algorithm of calculating the TOU billing is shown in Algorithm 1.

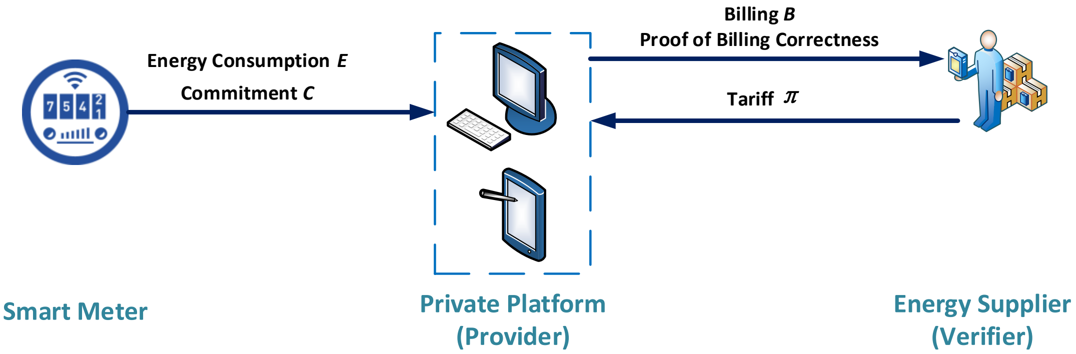
Billing *B*
Proof of Billing Correctness
Energy Consumption *E*
Commitment *C*
Tariff π
7 5 4 2
Smart Meter
Private Platform (Provider)
Energy Supplier (Verifier)

Figure 3. Time-of-use billing channel and billing correctness verification.

Algorithm 1 Dynamic TOU billing program.

```
Input: Half-Hourly Energy Consumption $E_{d,t}$, Half-Hourly TOU tariff $\pi_{d,t}$;
For d = 1; d ≤ 30 (d is the day of month) do
  for t = 1; t ≤ 48 (t is the time of the day) do
    Record and storage $E_{d,t}$ and $\pi_t$ during t.
  End
End
While d ≥ 30 do:
      Calculate $E_{month} = \sum_{d=1}^{30} \sum_{t=1}^{48} E_{d,t}$.
      Calculate $\mathrm{B}_{month} = \sum_{d=1}^{30} \sum_{t=1}^{48} \pi_{d,t} E_{d,t}$.
End
Return $E_{month}$, $\mathrm{B}_{month}$.

Output: Monthly Energy Consumption $E_{month}$, Monthly Bills $B_{month}$.
```

- Step 1: Data storage. The ES sends the TOU price π to the smart meter every 30 min. The smart meter stores the energy consumption of the past half-hour with the current TOU price in pairs
- Step 2: Bills calculation. The total TOU bills in £ are calculated at the end of each month, then sends the bill data to the ES, the ES then assigns a bill to the consumers.
- Step 3. Billing correctness verification. A zero-knowledge proof [72] is utilized to verify the billing correctness. A detailed description is shown in Appendix A.

4.6. Additional Service Channel

The additional service channel is designed for TP to provide additional services to the consumers. The "third party" refers to non-licensed energy service companies. They bring profits and innovation to the smart grid industry. The consumers have the freedom of choice to select wanted services. Currently, services include a warning for exceeding power thresholds, monitoring for seniors/children, monitoring the operating condition of selected appliances. From the consultation documents of Department of Energy & Climate Change (DECC) [19], there are strict limitations on TPs' access to data, an agreement is required among TP, DCC, and consumers, and the TP can only access the consumers' smart meter data when they have consumer consent.

Referring to the privacy-functionality trade-off strategy mentioned in Section 4, the value-added service channel follows a data minimization principle, preventing personal data "leaving" consumer's house. Rather than sending personal data to the server of TPs, TPs send algorithms and models to consumers' private platforms, including their personal computers and mobile phone, then the consumer can use the model to obtain the result on these platforms. However, there are two concerns related to this method referring to [21]:

- By sending algorithms/model parameters to consumers, the model's parameters and training dataset would be stolen by users, while these models and datasets are confidential.
- It is difficult to implement a privacy-preserving algorithm to complex models such as machine learning/deep learning-based services.

To settle the above two concerns, particularly relevant to our work [73], a value-added service channel utilizing a privacy-preserving deep learning algorithm is proposed. The algorithm adds noise into gradient descents of deep neural network parameters to reduce the sensitivity of single training data, and further preserve the privacy of both neural network model and training dataset [74]. The privacy-preserving deep learning combines two advanced techniques, differential privacy, and deep learning together.

As shown in Figure 4, the process of the value-added service channel consists of the following steps, and all steps can be divided into two categories depending on the network (WAN or HAN):

Operations via WAN:

- Step 1: the model owner trains the service model with a private database using a noisy algorithm.
- Step 2: the trained model is sent to consumers' private platform (personal computer, mobile phone).

Operations via HAN:

- Step 3: the smart meter uploads the measurements to the private platforms.
- Step 4: the consumer starts a query to the platform; then the platform returns a result to the consumer.

The data flow in Figure 4 shows that the consumer's energy data are shared inside HAN and are never sent to the utility, but the services are enabled. The enabled services include NILM, STLF, and demand response. The detail of the privacy-preserving deep learning NILM algorithm is shown in our paper [73].

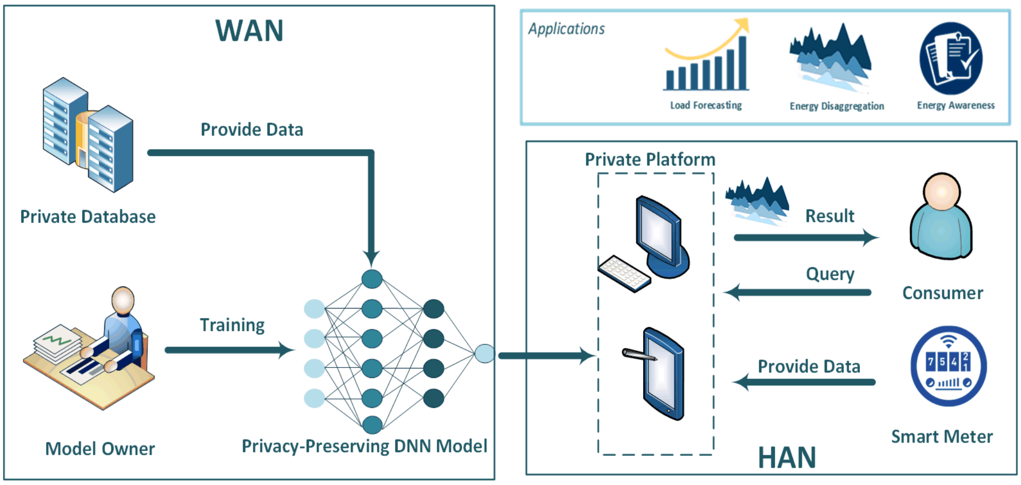

Figure 4. Privacy-preserving valued-added services.

5. Evaluation

In this section, an evaluation is implemented to discuss whether the proposed scheme satisfies the requirements in Section 2 considering both functionality and privacy.

5.1. Privacy Measure

The privacy measures are adopted to the smart meter data shared with stakeholders (high-frequency aggregated data and down-sampled individual data). Referring to privacy intrusion categories highlighted in Section 2.4, all privacy intrusion issues belong to two categories: data sensitivity and algorithm sensitivity. In many previous works, researchers view the sensitive information from the smart meter as the variation of the power consumption curve, a constantly changing curve would reveal more private information than a flattening curve. While the advanced NILM algorithms are used to infer individual appliance signatures, state-of-the-art algorithms such as DNN, ML, Hidden Markov Model (HMM) are proposed.

Hence, in this paper, both above two privacy intrusion issues are studied, Mutual Information and Mean Squared Error (MSE) is utilized to quantify the sensitivity of the data, and a NILM adversary, named NILMTK, is adopted to examine whether the proposed scheme can blind the algorithms.

Moreover, since a noise-adding deep learning approach is applied to the value-added services, privacy performance is evaluated to determine whether the system can provide differential privacy guarantees.

5.1.1. Mean Square Error (MSE) as a Privacy Measure

Mean squared error (MSE) is a naïve metric to evaluate the error between two groups of data. In this paper, MSE is adopted to quantify the difference between original consumption data and the modified data:

$$\text{MSE} = \frac{\sum_{i=1}^{N}(\hat{y}-y)^2}{N} \tag{1}$$

5.1.2. Mutual Information (MI) as a Privacy Measure

Mutual information (MI) is employed as a privacy measure to quantify privacy loss in [44,46,51,53,75]. MI $I(X^n;Y^n)$ measures the dependence between two random variable sequences X^n and Y^n [76]. In other word, MI can explain the reduction of the original load sequence X^n given knowledge of the modified sequence Y^n:

$$\begin{aligned} I(X^n;Y^n) &= H(X^n) - H(X^n|Y^n) \\ &= H(X^n) + H(Y^n) - H(X^n,Y^n) \\ &\approx -\tfrac{1}{n}logp(Y^n) - \tfrac{1}{n}logp(X^n) + \tfrac{1}{n}logp(X^n,Y^n) \end{aligned} \tag{2}$$

where $H(X^n)$ and $H(Y^n)$ are the marginal entropies, which measures the uncertainty about the random variable; $H(X^n|Y^n)$ is the conditional entropies, and (X^n, Y^n) is the joint entropy of $H(X^n)$ and $H(Y^n)$. In this paper, a variant MI named Normalized Mutual Information (NMI) is adopted to show the normalized results between 0 and 1 (0 represents no mutual information, 1 represents perfect correlation).

5.1.3. NILM Performance as a Privacy Measure

NILM is used as a privacy measure in previous works [33,35,56,61], the NILM plays the role of a powerful adversary to evaluate the privacy loss of the smart metering system. The adversary can adopt a state of the art NILM algorithms to obtains individual appliance signatures from the measured demand, hence the NILM is a desirable privacy measure to quantify the privacy loss. In this paper, the NILMTK toolbox [77] in Python is used to implement the NILM algorithm, we utilize the deep neural network model proposed in [78]. Five appliances, Air conditioner (Air), EV, refrigerator, stove, and dryer are investigated in this paper. Confusion matrix and F-score are used to evaluate the performance of the adversary, see Table 3.

$$F - measure = \frac{1}{1 + (\text{FN} + \text{FP})/(2\text{TP})} \tag{3}$$

Table 3. Confusion matrix.

	Actual Positive	**Actual Negative**
Predicted Positive	True Positive (TP)	False Positive (FP)
Predicted Negative	False Negative (FN)	True Negative (TN)

5.1.4. Differential Privacy as Privacy Guarantee

As a state of the art notion of privacy, differential privacy is proposed by Dwork in 2006 [64], the adversary cannot distinguish two neighboring datasets with only one pair of data that are different. Normally, differential privacy is achieved by adding noise into the data (e.g., Laplacian noise [64], Gaussian noise [79], exponential noise). A (ε, δ) differential privacy is obtained, while ε denotes the amount of noise added to the data, and δ represents the threshold to break the privacy.

Definition 1. *(ε-Differential Privacy) A randomized function $\mathfrak{R}$ satisfies (ε, δ) privacy $\mathbb{P}_{\mathbb{R}}$ for any two neighboring datasets β and β'*

$$\mathbb{P}_{\mathbb{R}}[\mathfrak{R}(\beta) \in \xi] \leq e^{\varepsilon}\mathbb{P}_{\mathbb{R}}[\mathfrak{R}(\beta') \in \xi] + \delta \tag{4}$$

where ξ denotes all possible outcomes in range R, and δ is the possibility that the differential privacy is broken, in this paper, we select 10^{-5} *as* δ*.*

Definition 2. *(Global Sensitivity) For a random function f,* the global sensitivity, S_f, *is the maximum difference between the outputs of two neighboring datasets β and β'. S_f also determines the overall noise to be added into the DP mechanism:*

$$\Delta f = \max_{d(\beta,\beta')=1} \| f(\beta) - f(\beta') \| \tag{5}$$

5.2. *Dataset Description and Data Preprocessing*

We adopted the Dataport [80] as the dataset. As the world's largest residential electricity consumption dataset, the dataset contains electricity data from 722 houses in the US. The interval resolution of the data is 1 min. We delete the data from 11 pm to 6 am since fewer electricity activities occur during this period.

5.3. *The High-Frequency Aggregated Channel Satisfies Privacy Requirement*

In this case study, the privacy performance of the high-frequency aggregated data is evaluated. As shown in Figure 5, with the increasing aggregation level, the curve of power consumption becomes smoother, and the details of individual appliance signature become difficult to extract. The dataset used for simulation is the Dataport [80] during 2018, the dataset contains both total power consumption as well as the details of each appliance. Different aggregation sizes are investigated (1 house, 2 houses, 5 houses, 10 houses, and 50 houses, respectively). The following will evaluate the privacy loss from both data sensitivity and algorithm sensitivity aspects.

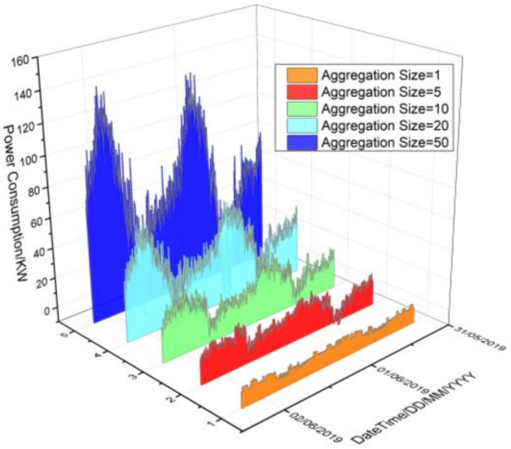

Figure 5. Single house power consumption versus different aggregation sizes of power consumption.

5.3.1. Influence of Aggregation Size on Data Sensitivity

The data sensitivity of the aggregated smart meter is evaluated in this subsection. In this scenario, we wanted to find out whether the adversary can still infer the individual's power usage data P_{real} from the high-frequency aggregated data P_{AGG}. Figure 6 shows the value of MI and MSE with different aggregation sizes. A reduction of the MI value is observed, from 1 at a single house to 0 at 10 houses, and the MI value would remain 0. The MSE value increases from 0 to 10^4 kW^2 when the aggregation size changes from a single house to 100 houses. The result shows that when aggregation size AGG is larger than 10 houses, P_{real} and P_{AGG} are totally independent, and no knowledge about the P_{real} would be revealed from P_{AGG}.

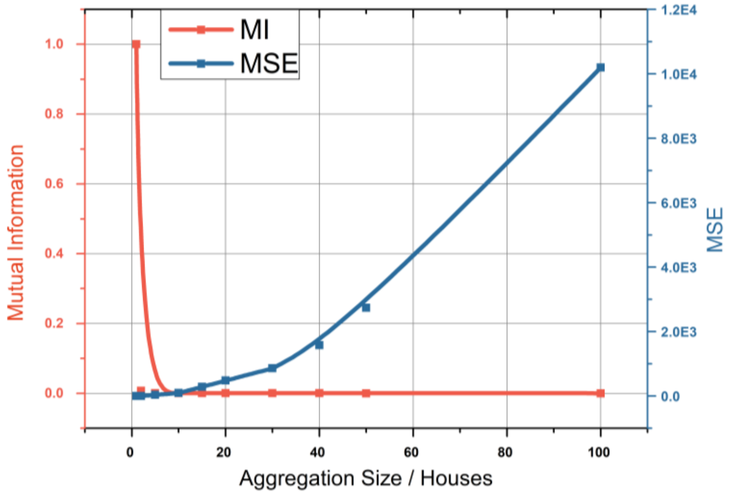

Figure 6. Mutual information and MSE of different aggregation sizes.

5.3.2. Influence of Aggregation Size on Algorithm Sensitivity

The algorithm sensitivity of the aggregated data P_{AGG} is evaluated via NILMTK tool, the target of the algorithm is inferring the appliance signature inside house i given aggregated load P_{AGG}. From Figure 7, when implementing NILMTK to a single house, the adversary can infer the appliance signatures with F-score between 80–100%, presenting that the NILMTK has perfect performance. When the aggregation size AGG reaches 2, the performance of NILMTK on most appliances such as EV, fridge, stove, and dryer has been influenced greatly, especially the F-score of EV reduces from 100% to 0. By continuously increasing AGG to 50 houses, the F-score of all appliances decreases to zero. From the result, it is concluded that at least 50 houses need to be aggregated to blind the NILM adversary.

To summarize, when AGG is larger than 50, both privacy intrusion issues can be prevented.

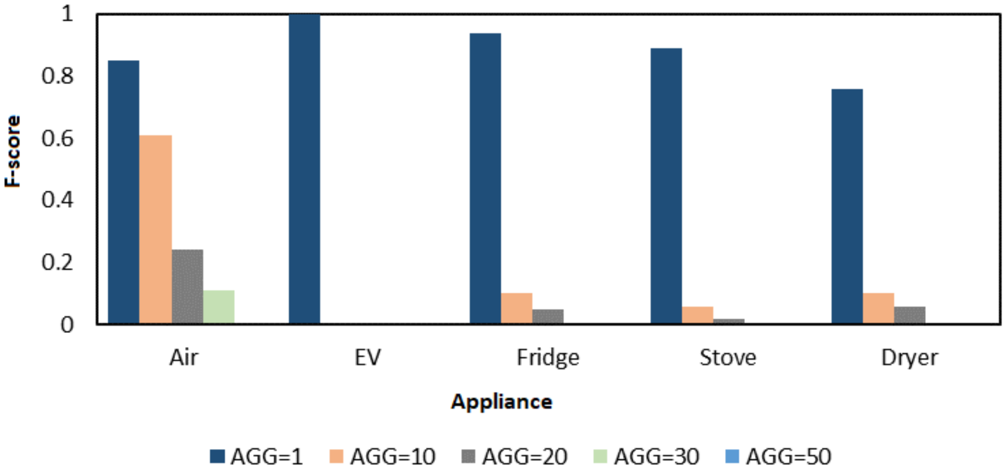

Figure 7. F-score of the NILMTK performance on appliances from different aggregation sizes.

5.4. The TOU Tariff Channel Satisfies Privacy Requirement

The temporal resolution level is another vital parameter that influences the privacy loss. In this case study, we take the data with 1 min interval as the P_{real}, and then downsample P_{real} to the lower interval T by taking the average values of all sampling points of P_{real} duration interval T (in this study, T ranges from 5 min to 1 month).

5.4.1. Privacy Measure of Data Sensitivity

This scenario tries to find out whether the adversary can still infer the individual's power usage data P_{real} from the downsampled data, P_T. Figure 8 shows the value of MI and MSE with the increase of interval resolution T. A dramatic reduction in MI is observed when T increases from 1 min to 180 min (3 h), the reduction of MI then becomes gentle when T continuously increases. The F-score drops to 0 when T reaches 1440 min (24 h) when only one data is recorded each day under this interval resolution. In contrast to MI, the value of MSE increases from 0 to 12.8, showing that the increase of T would reduce the knowledge of the original load curve.

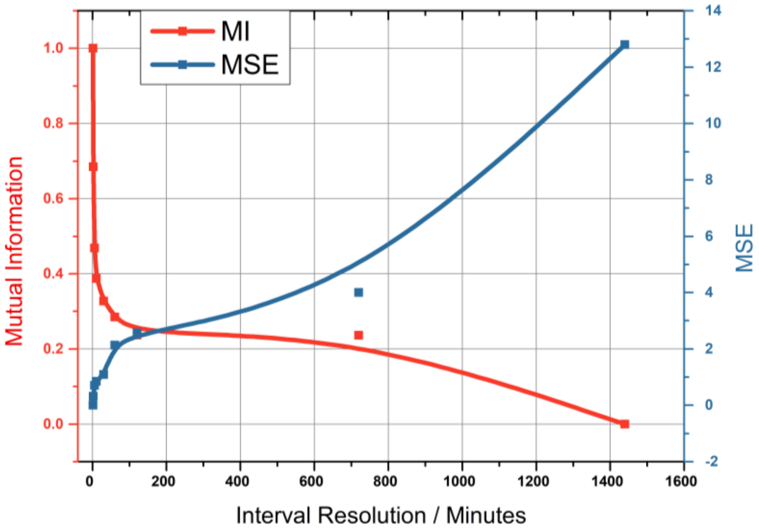

Figure 8. F-score of the NILMTK performance on appliances from different interval resolution.

5.4.2. Privacy Measure of Algorithm Sensitivity

The algorithm sensitivity on smart meter data different interval resolution is evaluated in this subsection, as shown in Figure 9. The F-score shows how the NILMTK adversary infers appliance information from the overall power consumption. While the NILMTK has a good performance with 1-min interval resolution data (achieving an F-score of 80–100%), the F-score drops gradually when the interval resolution increases. Taking air conditioner as an example, the NILMTK adversary achieves an F-score with 83%, representing that most of the operation duration of the air conditioner is detected. When interval resolution T increases to 1 h, the F-score drops to 42%. Furthermore, the F-score decreases to 0 when T equals to 24 h, meaning that the NILMTK is blinded totally. Most importantly, it is observed that even with 6-h interval resolution, the NILMTK achieves an estimation with 36%, 21%, and 20% F-score in EV, fridge, and dryer respectively, showing that a large interval (such as 6 h) still cannot guarantee the privacy.

Based on the above two discussions, to completely reduce the privacy loss, a 24 h smart meter data is required.

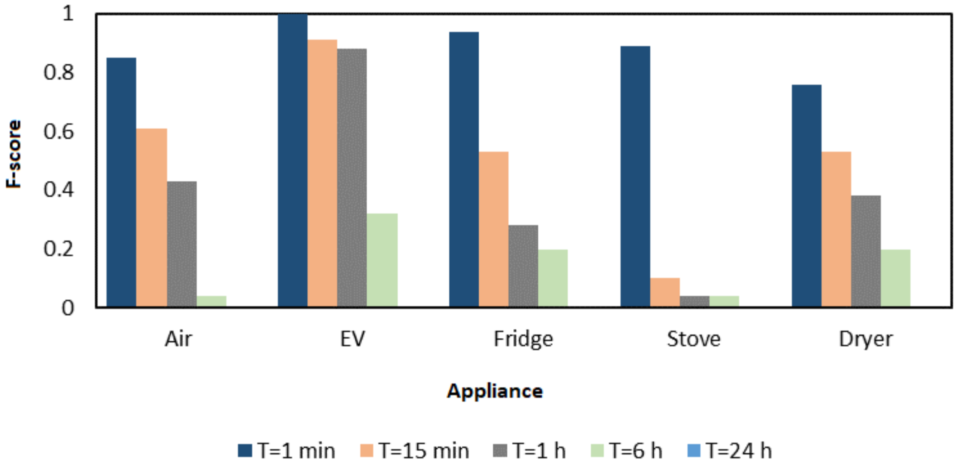

Figure 9. F-score of the NILMTK performance on appliances from different interval resolution.

5.4.3. ES Can Verify Billing Correctness

A detailed proof is given in Appendix A. The private platform generates a bill to ES monthly according to the stored TOU tariff and energy consumption, then the private platform sends a series of commitments to ES. Given TOU record and bill, ES can open commitments and verify if the commitments match the received bill.

5.5. Value-Added Service Channel Satsifies Privacy Requirements and Provides Differential Privacy to ES

Referring to the Demonstration in Appendix B, the value-added service channel provides a $(2\frac{L}{N}\varepsilon\sqrt{T}, \delta)$-differential privacy guarantee to ES, hence the model parameters and training dataset for the service is protected. As for consumer, since the service is implemented inside HAN and completed by private platform, the private information never be shared with other parties.

5.6. Comparison of the Proposed System with Related Schemes

In this Subsection, a comprehensive comparison is made between the proposed smart metering system and other related operational strategies (e.g., rechargeable battery, data aggregation, data down-sampling) from the aspects of both functionalities and privacy protection. Referring to Sections 2.3 and 2.4, the four compulsory functionalities: billings, TOU tariff, grid management and operation, and value-added services. While the four privacy intrusion risks cover data sensitivity and algorithm sensitivity, and can be further divided into fraud, real-time surveillance, behaviour patterns identification, non-grid commercial uses of data four categories. These strategies cover the private information by modifying the load curves or encrypting the consumer's energy data. And privacy evaluations employed in these would either assess the performance of data sensitivity (MI, FI, KL-Divergence, etc.) or the performance of algorithm sensitivity (NILM as adversary). As shown in Table 4, it is observed that most strategies settle both privacy intrusion problems, but some strategies sacrifice conclusory functionalities: data distortion adds noise to the original data making the modified data different from the real energy consumption, as a consequence the TOU billing is unavailable; the data aggregation method adds dozens of smart meters' data together and then sends it to the utility, which also prevents the utility from obtaining individual bills' information; and the data down-sampling technique reduces the sampling interval of the smart meter, which would influence grid management and value-added services. Moreover, HE and rechargeable battery approaches require either extra expensive energy storage systems or extremely high computation ability, which is unrealistic to roll-out. The proposed system enables different granularity data to be transmitted between the smart meter and the utility/TP, depending on the required functionalities. What the adversaries can obtain is high-frequency but aggregated data (substation/feeder level) and household-level but down-sampled data, both these two information streams would not reveal useful personal information (see Section 6 for demonstration). In addition, instead of adopting a TTP, the proposed method installs smart meter besides feeders or substations directly, so the worries about the privacy risks brought by TTP are solved.

Especially, a Distribution Network Operator (DNO) would benefit from the proposed smart metering system from both economic and technical aspects. As for economic benefits, the proposed smart metering system provides a more cost-effective network for DNO. By monitoring the real-time substation/feeder level demand, DNO has an insight view about the operation condition of the distributed network. The improvement of the visibility help DNO implements better and prioritized management to feeder voltage, and the energy loss is reduced as a result. Moreover, substation/feeder level smart meters help DNO understand peak demand patterns of the local area, the DNO takes advantages of these patterns when designing and planning networks. In this case, DNO can save the unnecessary cost of networks and enable the network to operate just above the maximum peak load. As for the technical aspect, the proposed smart metering system provide high-resolution electricity data to DNO, DNO can utilize the collected data for following technical tasks: (1) Load forecasting and feeder-level energy disaggregation. With feeder/substation level historical and real-time smart meter data, DNO can forecast the variation of load demand accurately, and the load components under the substation can be evaluated via ML or DNN algorithms, paving way for demand-side management; (2) Batter manage distributed generation. The continuously increasing of the distributed generation (such as solar panel and wind turbine) bring high reserve power flow to the low-voltage (LV) network, which causes stability issues such as voltage spikes. The proposed smart metering system help DNO identify the reserve power flow, and DNO can employ operation to maintain the stability of the power system.

As for the cost of the proposed system, the system is mostly constructed based on existing smart metering infrastructure, except for the installation of feeder/substation-level smart meters and utilization of the private platform to store the historic energy data. The rechargeable battery/energy storage system method requires each house to install a mini energy storage system or EV to flatten the power consumption curve [7] and that they should change the battery frequently, while the cost of each battery can reach thousands of pounds [81]. When we are comparing the cost at substation scale (each substation contains hundreds of houses), the cost of rechargeable batteries is much higher than the proposed system. As for encryption techniques, traditional encryption techniques such as symmetric encryption can only guarantee the security of data transmission from the consumer side to energy suppliers/third parties' side. However, energy suppliers and third parties are potential adversaries as well, the privacy of consumer's data cannot be ensured. As for encryption methods such as HE, they enable TP to process/manipulate data without knowing the detail of the data. However, the disadvantages of HE is also obvious, HE requires extremely high computation ability to encrypt/decrypt the data. Considering memory usage, 1 Mb of data results in more than 10 Gb of encrypted data [82]. As far as computation, multiplication takes over 5 s per multiplication. The above is just the cost of one smart meter when we move to the whole smart metering system it contains millions of smart meters, the cost would be an astronomical figure.

Table 4. Comparison of the performance between proposed method and related operational strategies.

Operational Strategies		Functionalities of the Smart Metering System				Privacy Intrusion Issues Protection		Comments
		Billing	TOU	Grid Management	Value-Added Service	Data Sensitivity	Algorithm Sensitivity	
Proposed method		✓	✓	✓	✓	✓	✓	
Demand Shaping	Rechargeable battery [7,35–42]	✓	✓	✓	×	✓	✓	Battery is expensive
	Load shifting [47–49]	✓	✓	✓	×	✓	Unknown	
	Energy Storage System [43–46]	✓	✓	✓	×	✓	✓	Device is expensive
Data Manipulation	Data obfuscation [56–60]	✓	×	×	×	✓	✓	Data is useless to grid
	Data aggregation with TTP [60]	×	×	✓	×	✓	✓	TTP brings new privacy issues
	Data aggregation without TTP [8,22,61–63]	×	×	✓	×	✓	✓	Computation overhead
	Data aggregation with noise-adding [56–58]	×	×	✓	×	✓	✓	
	Data down-sampling [13,33,66]	✓	×	×	Unknown	✓	✓	
	Data anonymization [12,65,66]	✓	×	✓	Unknown	✓	✓	

6. Conclusions and Future Work

6.1. Conclusions

In this paper, we have presented a smart metering scheme (strategy and model) to prevent privacy risks (operational and ethical) raised by the smart meter. The proposed scheme has three communication channels to enables power system management and operation, TOU billing, and value-added services three functionalities. The different channel transmits different interval resolution data. As for privacy aspects, we divide all privacy issues related to the smart meter into two categories, data sensitivity, and algorithm sensitivity.

There are two main contributions of this paper to existing operational methods to deal with privacy intrusion. Firstly, in the high-frequency aggregation channel, we adopt the distribution-level substation as "aggregator", the substation supplies power to over 400 houses in a light rural area and over 7000 houses in a moderate urban area. In this way, we eliminate the risk of an inner attack from the TTP. Secondly, we use the private platform as a data processor, only reporting billing details monthly without frequently sending individual energy consumption data to the utility. Thirdly, privacy preserving NILM algorithm is employed to the value-added services to protect both consumers and ES's privacy. Finally, an evaluation is implemented to the system which demonstrates the proposed system satisfies all privacy requirements. From the evaluation, the conclusion is made a dataset with aggregation size over 50, and interval resolution larger than 24 h can overcome both data sensitivity and algorithm sensitivity.

6.2. Implications for Policy

Current smart metering systems always share the real-time household-level smart meter data with the utility. Smart metering system policymakers (e.g., the Department for Business, Energy & Industrial Strategy (BEIS) in the UK) should be aware of the trade-off between functionalities and privacy when operating the system and should have a clear idea about the data granularity required by different stakeholders. [83] suggests that the policymaker should classify the smart meter data into different openness categories, ranging from open data (the data can be totally open to the public) to closed data (private data that is confidential). In this case, the operators can maximize the value of data and minimize the privacy and security issues. Different stakeholders (e.g., NO, ES, TP) should access different granularity of smart meter data, while the granularity of the data includes the interval resolution, the aggregation size, etc.

Policymakers could also find it difficult to sacrifice functionalities to protect individual consumers' (i.e., households') privacy. The importance of the smart metering system is to provide accurate real-time reading and further reduce energy costs. Policymakers could carefully implement methods such as noise-adding or load curve distortion. Although these methods would reduce the sensitivity of personal information and thus risks of privacy intrusion, the usability and the value of the data would decrease as well, potentially undermining the achievement of benefits for stakeholders. The proposed strategy and model suggest that it might be possible to balance demands and benefits without compromising household privacy; rather other opportunities could emerge if policy considers freedom from digital surveillance and analysis as a creative situation. In this regard, and through the inclusion of adversaries and aggregators as potentially valuable 'stakeholders' of smart meters, it might be possible to help households comply with societal functionalities whilst retaining their sense of freedom and using it creatively for other purposes than energy efficiencies.

6.3. Future Work

In this paper, only the overall smart metering system is proposed. However, the efficient of the proposed smart metering system should be evaluated in practice, a pilot network with small groups of residence to be built to validation the availability of proposed system. Secondly, the functionality for grid management and operation in the proposed system should be verified via simulation. Thirdly, since we adopt multi-frequency communication channels in the proposed system, the noise would be generated in data transmission; we would propose a further study to investigate the influence on the quality of data. Finally, we could also devise participative methods to continue exploring the ethical consequences of smart meters for different (digital and non-digital) stakeholders.

Author Contributions: X.-Y.Z. and S.K. did the methodology, simulation, and validation. X.-Y.Z. did the analysis and wrote the paper. Writing-Original Draft Preparation, X.-Y.Z. and S.K.; Writing-Review Editing, X.-Y.Z., S.K., J.-R.C.-P., and C.W.; Supervision, S.K., J.-R.C.-P., and C.W. All authors have read and agreed to the published version of the manuscript.

Funding: This research is funded by The Leverhulme Trust. This research is a part of the project "Ethics and Laws of Algorithms" funded by Royal Holloway, University of London.

Acknowledgments: The author acknowledges the support of the Department of Electronic Engineering, Department of Computer Science, School of Business and Management, Royal Holloway, University of London. Thanks to the anonymous peer-reviewers and editors whose comments helped to improve and clarify this manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations and Notations

The following abbreviations are used in this manuscript:

TOU	Time-of-use
HE	Homomorphic Encryption
TP	Third party
MPC	Multi-party computation
GDPR	General Data Protection Regulation
PRIME	Powerline Intelligent Metering Evolution
PLC	Powerline communication
NILM	Non-intrusive Load Monitoring
ES	Energy suppliers
NO	Network operators
DCC	Data and communications companies
DNN	Deep Neural Network
MI	Mutual Information
SCADA	Supervisory control and data acquisition
HAN	Home Area Network
WAN	Wide Area Network
TTP	Trusted third parties
P_{real}	Active power of individual house
P_{AGG}	High frequency aggregated active power
P_T	Down sampled power consumption data
E_{month}	Monthly energy consumption of smart meter
B_{month}	Monthly bills
$E_{d,t}$	Half-Hourly Energy Consumption
$\pi_{d,t}$	Half-Hourly TOU tariff

Appendix A. Billing Verification with Zero-Knowledge Proof

After the bill is generated by the private platform, the ES should verify the correctness of the bill. Zero-knowledge proof (ZKP) is a proof approach that can verify the correctness of the provided information without revealing the details of the information [72,84]. ZKP protocol involves two parties, provider (P) and verifier (V), P interacts with V to convince that a secret is true, but V has no knowledge about the secret P wants to prove. Pedersen Commitment is employed in this verification process [85]. A commitment with secret x is generated as $c = Commit(x, r)$, and x is difficult to infer from c, the commitment can be opened with c, x, r, marked as $Open(c, x, y)$. The $Open(c, x, y)$ would return True if c is the commitment of secret x, otherwise False is returned. They have homomorphic features of commitments are important to verify the billing correctness:

$$Commit(x, y) \times Commit(m, n) = Commit(x + m, y + n) \tag{A1}$$

$$Commit(x, y)^{n} = Commit(x \times n, y \times n) \tag{A2}$$

In the proposed TOU billing channel, the private platform is P, and the ES is V, Public Key Infrastructure (PKI) assigns a series of commitments ***COM*** with the power consumption sequence $\boldsymbol{E} = E_{1,1,}\ E_{1,2,}\ \ldots E_{d,t} \ldots E_{30,48,}$ and random value sequences $\boldsymbol{R} = r_{1,1,}\ r_{1,2} \ldots r_{d,t} \ldots E_{30,48}$ to the private platform:

$$Commit_{d,t} = Commit\Big(E_{d,t}, r_{d,t}\Big) \tag{A3}$$

$$\boldsymbol{COM} = \Big(Commit_{1,1}, Commit_{1,2} \ldots Commit_{d,t} \ldots Commit_{30,48}\Big) \tag{A4}$$

The private platform will receive the commitment c and energy consumption sequence E from the smart meter, and the TOU tariff sequence $\boldsymbol{TARIFF} = \pi_{1,1}, \pi_{1,2} \ldots \pi_{d,t} \ldots \pi_{30,48}$ from the ES. So, the private platform can calculate monthly price:

$$\mathrm{B}_{month} = \sum_{d=1}^{30} \sum_{t=1}^{48} \pi_{d,t} E_{d,\mathrm{t}} \tag{A5}$$

referring to (A1) and (A2), the ES multiplies ***COM*** with ***TARIFF*** to obtain the commitment of monthly bill:

$$Commit_{Bill} = \prod_{d=1,t=1}^{30\times 48} Commit\Big(E_{d,t}, r_{d,t}\Big)^{\pi_{d,t}} \tag{A6}$$

By opening the commitment of monthly bill, ES can verify the correctness of the bill:

$$Open_{Bill} = (Commit_{Bill},\ \mathrm{B}_{month}, r_{Bill}) \tag{A7}$$

If $Commit_{Bill}$ is really the commitment of B_{month}, ES accepts the generated bill, otherwise, ES reject the bill.

Appendix B. Privacy-Preserving Deep Learning-Based NILM Algorithm

Deep learning is an important branch of machine learning, it is based on an artificial neural network (ANN) with multi-layers (normally one input layer, one output layer, and several hidden layers between the input and output), each layer contains a number of neurons. A neuron is a mathematic function that computes the sum of weighted input and obtain nonlinear output via an activation function (e.g., ReLU, Sigmoid, Tanh). Compared with a shallow ANN, a deep neural network (DNN) contains several hidden layers, which enables much more complex computation tasks. The expression for a typical N-layer DNN with input x is shown in (A8):

$$a_N(x;\ \theta_{1,\ldots,N}) = f_N(f_{N-1}(\ldots f_1(x, \theta_1), \theta_{N-1}), \theta_N) \tag{A8}$$

where f_i is the activation function of ith layer, and θ_i is the weight of ith layer.

A loss function $\mathcal{L}$ is adopted to calculate the mismatch between ground truth y and a_N. The purpose of the DNN is to find the optimal parameters of the model θ^* that minimize the $\mathcal{L}$ throughout the whole training process:

$$\mathcal{L}(\theta) = \frac{1}{N} \sum_{(x,y)\in(X,Y)} \mathcal{L}(y, a_N(x; \theta_{1,\ldots,N})) \tag{A9}$$

$$\theta^* \leftarrow argmin_{\theta}\mathcal{L}(\theta) \tag{A10}$$

Differential privacy-stochastic gradient descent (DP-SGD) provides ε-differential privacy to the DNN model by adding noise to the SGD [74]. The hyperparameters of the model are shown in Table A1. Different from conventional SGD, at each time to calculate the gradient, the gradient is clipped and then a random Gaussian noise is added to the gradient. By adding the noise, *a* (ε, δ)-differential privacy is enabled each step. Since the number of training steps are large (range from hundreds to thousands), referring to the Composition Theorem stated as follow, the overall privacy guarantee is extremely large.

Theorem A1. *(Composition Theorem) If f is $(\varepsilon_1, \delta_1)$-differential privacy and g is $(\varepsilon_2, \delta_2)$-differential privacy, then*

$$f(D), g(D)\ is\ (\varepsilon_1 + \varepsilon_2, \delta_1 + \delta_2) - Differential\ Privacy \tag{A11}$$

To minimize the value of $\varepsilon_{total} = T\varepsilon, \delta_{total} = T\delta$ (T is the total training steps), a Moments Accountant Theorem is proposed by M. Abadi, et al. [74]:

Theorem A2. *The privacy preserving NILM algorithm provides a $(2\frac{L}{N}\varepsilon\sqrt{T}, \delta)$-differential privacy guarantee to ES.*

Proof of Theorem 1. A detailed proof is given in [74]. □

Algorithm A1. Privacy-preserving Deep Neural Network Algorithm

```
Input: Model input $X = \{x_1 x_2 \ldots x_N\}$.
  Initialisation of weights $\theta_0$;
For training time step t ≤ total training time T:
  Computing Loss function $\mathcal{L}(\theta) = \frac{1}{N}\sum_{(x,y)\in(X,Y)} \mathcal{L}\big(y, a_N\big(x; \theta_{1,\ldots,N}\big)\big)$
  Calculating Gradient $g_B = \frac{1}{B}\sum_{x\in B} \nabla_\theta \mathcal{L}(\theta, x)$;
  Clipping Gradient $\overline{g}(x_i) = \frac{g(x_i)}{\max(1, \|g(x_i)\|_2 / C)}$;
  Adding Random Noise to the Gradient $\widetilde{g}(x_i) = \frac{1}{L}\left(\sum_{x\in L} \overline{g}(x_i) + \mathcal{N}\big(0,\ \Delta f^2\sigma^2\big)\right)$;
  Update Parameters after each training step t $\theta_{t+1} = \theta_t - \alpha\widetilde{g_t}(x_i)$.
End
Output: Output Result Model weights $\theta$ and privacy cost $(\varepsilon, \delta)$.
```

As shown in Figure A1, the target of the NILM services is to evaluate the individual appliance consumption (output) from overall power consumption measured by the smart meter (input). Three hidden layers are linked between input layer and output layer to extract features. DP-SGD algorithm is applied in the neural network to calculate the gradient of each training step.

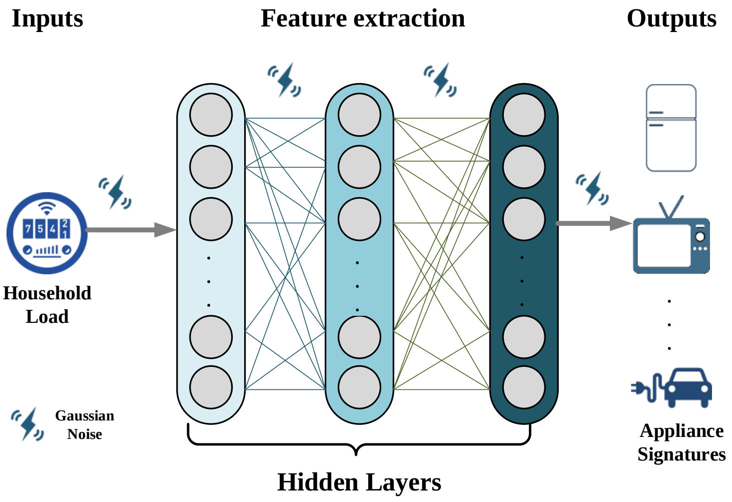

Figure A1. Privacy-preserving deep learning NILM model.

Figure A2 shows the relation between the performance of NILM algorithm and privacy level ε [73], the smaller the value ε, the better privacy it provides. It is found that without using DP-SGD, the accuracy of NILM is near 90%. By increasing the noise scale σ (a decrease of ε), and the accuracy of the algorithm decreases. So, the TPs should carful choose a noise scale that follows privacy-utility trade-off to settle both services and privacy.

Table A1. Hyperparameters of the Model [74,86].

Hyperparameters	Value	Description
Learning rate α	0.05–0.3	The steps to adjust θ according to errors.
Hidden layers number	3	The total number of hidden layers.
Lot size L	$\sqrt{N}$	The group size for computing gradient.
Batch size B	$\ll L$	The number of training examples utilized in one iteration.
Activation function f	ReLU	$f_{ReLU} = \max[0,\ z]$.
Gradient clipping norm C	1–10	Control the range of each gradient value, ensure that no gradient is much different with others.
Noise Scale σ	$\frac{\sqrt{2log1/\delta}}{\varepsilon}$	The amount of noise added.

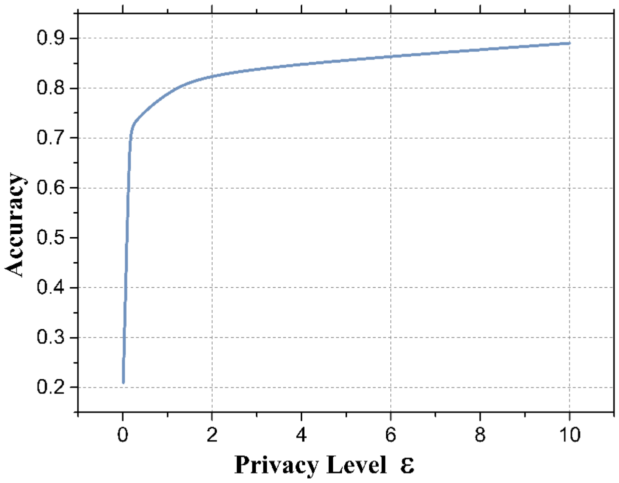

Figure A2. Privacy–accuracy curve of privacy-preserving NILM (Data from [73]).

References

1. *Smart Meters: A Guide*; Department for Business (EIS): London, UK, 2018.
2. King, N.J.; Jessen, P.W. Smart metering systems and data sharing: Why getting a smart meter should also mean getting strong information privacy controls to manage data sharing. *Int. J. Law Inf. Technol.* **2014**, *22*, 215–253. [CrossRef]
3. Molina–Markham, A.; Shenoy, P.; Fu, K.; Cecchet, E.; Irwin, D. Private memoirs of a smart meter. In Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building, New York, NY, USA, 2 October 2010; pp. 61–66.
4. Quinn, E.L. Smart Metering and Privacy: Existing Laws and Competing Policies. *SSRN Electron. J.* **2009**. [CrossRef]
5. Autili, M.; Di Ruscio, D.; Inverardi, P.; Pelliccione, P.; Tivoli, M. A software exoskeleton to protect and support citizen's ethics and privacy in the digital world. *IEEE Access* **2019**, *7*, 62011–62021. [CrossRef]
6. Taylor, C. *The Ethics of Authenticity*; Harvard University Press: Cambridge, MA, USA, 1992.

7. Kalogridis, G.; Efthymiou, C.; Denic, S.Z.; Lewis, T.A.; Cepeda, R. Privacy for smart meters: Towards undetectable appliance load signatures. In Proceedings of the 2010 First IEEE International Conference on Smart Grid Communications, Gaithersburg, MD, USA, 11–13 October 2010; pp. 232–237.
8. Li, F.; Luo, B.; Liu, P. Secure Information aggregation for smart grids using homomorphic encryption. In Proceedings of the 2010 First IEEE International Conference on Smart Grid Communications, Gaithersburg, MD, USA, 11–13 October 2010; pp. 327–332.
9. Voigt, P.; Bussche, A.V.D. *The EU General Data Protection Regulation (GDPR)*; Springer Science and Business Media LLC: Berlin, Germany, 2017.
10. Floridi, L. Soft ethics and the governance of the digital. *Philos. Technol.* **2018**, *31*, 1–8. [CrossRef]
11. Introna, L.D.; Pouloudi, A. Privacy in the information age: Stakeholders, interest and values. *J. Bus. Ethic* **1999**, *22*, 27–38. [CrossRef] [PubMed]
12. Efthymiou, C.; Kalogridis, G. Smart Grid Privacy via Anonymization of Smart Metering Data. In Proceedings of the 2010 First IEEE International Conference on Smart Grid Communications, Gaithersburg, MD, USA, 11–13 October 2010; pp. 238–243.
13. Knirsch, F.; Eibl, G.; Engel, D. Multi-resolution privacy-enhancing technologies for smart metering. *EURASIP J. Inf. Secur.* **2017**, *2017*, 807. [CrossRef]
14. Hernández-Callejo, L.; Callejo, H.-A. Comprehensive review of operation and control, maintenance and lifespan management, grid planning and design, and metering in smart Grids. *Energies* **2019**, *12*, 1630. [CrossRef]
15. Kochański, M.; Korczak, K.; Skoczkowski, T. Technology innovation system analysis of electricity smart metering in the European Union. *Energies* **2020**, *13*, 916. [CrossRef]
16. Fahim, M.; Sillitti, A. Analyzing load profiles of energy consumption to infer household characteristics using smart meters. *Energies* **2019**, *12*, 773. [CrossRef]
17. Llano, A.; Angulo, I.; De La Vega, D.; Marron, L. Virtual PLC lab enabled physical layer improvement proposals for PRIME and G3-PLC standards. *Appl. Sci.* **2020**, *10*, 1777. [CrossRef]
18. Uribe-Pérez, N.; Angulo, I.; Hernández-Callejo, L.; Arzuaga, T.; De La Vega, D.; Arrinda, A. Study of unwanted emissions in the CENELEC-A band generated by distributed energy resources and their influence over narrow band power line communications. *Energies* **2016**, *9*, 1007. [CrossRef]
19. *The Smart Metering System Leaflet*; Department of Energy & Climate Change: London, UK, 2014.
20. *A Joint Contribution of DG ENER and DG INFSO towards the Digital Agenda, Action 73: Set of Common Functional Requirements of the SMART METER*; European Commission: Brussels, Belgium, 2011.
21. Asghar, M.R.; Dán, G.; Miorandi, D.; Chlamtac, I. Smart Meter Data Privacy: A Survey. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 2820–2835. [CrossRef]
22. Lu, R.; Liang, X.; Li, X.; Lin, X.; Shen, X. EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications. *IEEE Trans. Parallel Distrib. Syst.* **2012**, *23*, 1621–1631. [CrossRef]
23. Pitì, A.; Verticale, G.; Rottondi, C.; Capone, A.; Schiavo, L.L. The role of smart meters in enabling real-time energy services for households: The Italian case. *Energies* **2017**, *10*, 199. [CrossRef]
24. Torriti, J. *Peak Energy Demand and Demand Side Response*; Informa UK Limited: London, UK, 2015.
25. Qadrdan, M.; Cheng, M.; Wu, J.; Jenkins, N. Benefits of Demand-Side response in combined gas and electricity networks. *Appl. Energy* **2017**, *192*, 360–369. [CrossRef]
26. Ruano, A.; Hernández, Á.; Ureña, J.; Ruano, M.; Domínguez, J.J.G. NILM techniques for intelligent home energy management and ambient assisted living: A review. *Energies* **2019**, *12*, 2203. [CrossRef]
27. Hogan, W.W. Fairness and dynamic pricing: Comments. *Electr. J.* **2010**, *23*, 28–35. [CrossRef]
28. Parks, R.C. *Advanced Metering Infrastructure Security Considerations*; Sandia Report; Sandia National Laboratories: Albuquerque, New Mexico, 2007.
29. McCullough, J. AMI Security Considerations. Elster. 2010. Available online: https://silo.tips/download/ami-security-considerations (accessed on 30 April 2020).
30. Montanez, C.A.C.; Hurst, W. A machine learning approach for detecting unemployment using the smart metering infrastructure. *IEEE Access* **2020**, *8*, 22525–22536. [CrossRef]
31. Rachels, J. Why privacy is important. In *Privacy*; Informa UK Limited: London, UK, 2017; pp. 11–21.
32. Chan, A.C.; Zhou, J. On smart grid cybersecurity standardization: Issues of designing with NISTIR 7628. *IEEE Commun. Mag.* **2013**, *51*, 58–65. [CrossRef]

33. Eibl, G.; Engel, D. Influence of Data Granularity on Smart Meter Privacy. *IEEE Trans. Smart Grid* **2014**, *6*, 930–939. [CrossRef]
34. Sultan, S. Privacy-preserving metering in smart grid for billing, operational metering, and incentive-based schemes: A survey. *Comput. Secur.* **2019**, *84*, 148–165. [CrossRef]
35. Farokhi, F.; Sandberg, H. Fisher information as a measure of privacy: Preserving privacy of households with smart meters using batteries. *IEEE Trans. Smart Grid* **2018**, *9*, 4726–4734. [CrossRef]
36. Li, S.; Khisti, A.; Mahajan, A. Privacy-optimal strategies for smart metering systems with a rechargeable battery. In Proceedings of the 2016 American Control Conference (ACC), Boston, MA, USA, 6–8 July 2016; pp. 2080–2085.
37. Varodayan, D.; Khisti, A. Smart meter privacy using a rechargeable battery: Minimizing the rate of information leakage. In Proceedings of the 2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Prague, Czech, 22–27 May 2011; pp. 1932–1935.
38. Zhang, Z.; Qin, Z.; Zhu, L.; Weng, J.; Ren, K. Cost-friendly Differential Privacy for Smart Meters: Exploiting the Dual Roles of the Noise. *IEEE Trans. Smart Grid* **2016**, *8*, 619–626. [CrossRef]
39. Yang, L.; Chen, X.; Zhang, J.; Poor, H.V. Cost-Effective and Privacy-Preserving energy management for smart meters. *IEEE Trans. Smart Grid* **2014**, *6*, 486–495. [CrossRef]
40. Rajagopalan, S.R.; Sankar, L.; Mohajer, S.; Poor, H.V. Smart meter privacy: A utility-privacy framework. In Proceedings of the 2011 IEEE International Conference on Smart Grid Communications (SmartGridComm), Prague, Czech, 22–27 May 2011; pp. 190–195.
41. Zhu, L.; Zhang, Z.; Qin, Z.; Weng, J.; Ren, K. Privacy Protection Using a Rechargeable Battery for Energy Consumption in Smart Grids. *IEEE Netw.* **2017**, *31*, 59–63. [CrossRef]
42. Backes, M.; Meiser, S. Differentially private smart metering with battery recharging. In *Data Privacy Management and Autonomous Spontaneous Security*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 194–212.
43. Tan, O.; Gunduz, D.; Poor, H.V. Increasing smart meter privacy through energy harvesting and storage devices. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 1331–1341. [CrossRef]
44. Giaconi, G.; Gunduz, D.; Poor, H.V. Smart meter privacy with renewable energy and an energy storage device. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 129–142. [CrossRef]
45. Sun, Y.; Lampe, L.; Wong, V.W. Smart meter privacy: Exploiting the potential of household energy storage units. *IEEE Internet Things J.* **2017**, *5*, 69–78. [CrossRef]
46. Gunduz, D.; Vilardebò, J.G. Smart meter privacy in the presence of an alternative energy source. In Proceedings of the 2013 IEEE International Conference on Communications (ICC), Beijing, China, 9–13 June 2013; pp. 2027–2031.
47. Egarter, D.; Prokop, C.; Elmenreich, W. Load hiding of household's power demand. In Proceedings of the 2014 IEEE International Conference on Smart Grid Communications (SmartGridComm), Venice, Italy, 3–6 November 2014; pp. 854–859.
48. Chen, D.; Irwin, D.; Shenoy, P.; Albrecht, J.; Albrecht, J. Combined heat and privacy: Preventing occupancy detection from smart meters. In Proceedings of the 2014 IEEE International Conference on Pervasive Computing and Communications (PerCom), Budapest, Hungary, 24–28 March 2014; pp. 208–215.
49. Chen, D.; Kalra, S.; Irwin, D.; Shenoy, P.; Albrecht, J. Preventing Occupancy Detection from Smart Meters. *IEEE Trans. Smart Grid* **2015**, *6*, 2426–2434. [CrossRef]
50. Giaconi, G.; Gunduz, D.; Poor, H.V. Privacy-Aware smart metering: Progress and challenges. *IEEE Signal Process. Mag.* **2018**, *35*, 59–78. [CrossRef]
51. Tan, O.; Vilardebò, J.G.; Gunduz, D. Privacy-Cost Trade-offs in Demand-Side management with storage. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 1458–1469. [CrossRef]
52. McLaughlin, S.; McDaniel, P.; Aiello, W. Protecting consumer privacy from electric load monitoring. In Proceedings of the 18th ACM Conference on Computer and Communications Security, Chicago, IL, USA, 17–21 October 2011; pp. 87–98.
53. Giaconi, G.; Gunduz, D.; Poor, H.V. Optimal demand-side management for joint privacy-cost optimization with energy storage. In Proceedings of the 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm), Dresden, Germany, 23–27 October 2017; pp. 265–270.
54. Sun, Y.; Lampe, L.; Wong, V.W.S. Combining electric vehicle and rechargeable battery for household load hiding. In Proceedings of the 2015 IEEE International Conference on Smart Grid Communications (SmartGridComm), Miami, FL, USA, 2–5 November 2015; pp. 611–616.

55. Gomez-Vilardebo, J.; Gunduz, D. Smart meter privacy for multiple users in the presence of an alternative energy source. *IEEE Trans. Inf. Forensics Secur.* **2014**, *10*, 132–141. [CrossRef]
56. He, X.; Zhang, X.; Kuo, C.-C.J. A Distortion-Based Approach to Privacy-Preserving metering in smart grids. *IEEE Access* **2013**, *1*, 67–78. [CrossRef]
57. Eibl, G.; Engel, D. Differential privacy for real smart metering data. *Comput. Sci. Res. Dev.* **2016**, *32*, 173–182. [CrossRef]
58. ÁCS, G.; Castelluccia, C. I have a dream!(differentially private smart metering). In *International Workshop on Information Hiding*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 118–132.
59. Barbosa, P.; Brito, A.; Almeida, H.; Clauß, S. Lightweight privacy for smart metering data by adding noise. In Proceedings of the 29th Annual ACM Symposium on Applied Computing, Gyeongju, Korea, 24–28 March 2014; pp. 531–538. [CrossRef]
60. Bohli, J.-M.; Sorge, C.; Ugus, O. A privacy model for smart metering. In Proceedings of the 2010 IEEE International Conference on Communications Workshops, Gaithersburg, MD, USA, 11–13 October 2010; pp. 1–5.
61. Büscher, N.; Boukoros, S.; Bauregger, S.; Katzenbeisser, S. Two is not enough: Privacy assessment of aggregation schemes in smart metering. In Proceedings of the Privacy Enhancing Technologies, Minneapolis, MN, USA, 18–21 July 2017; Volume 2017, pp. 198–214.
62. Kursawe, K.; Danezis, G.; Kohlweiss, M. Privacy-friendly aggregation for the smart-grid. In Proceedings of the International Symposium on Privacy Enhancing Technologies Symposium, Waterloo, ON, Canada, 27–29 July 2011; pp. 175–191.
63. Thoma, C.; Cui, T.; Franchetti, F. Secure multiparty computation based privacy preserving smart metering system. In Proceedings of the 2012 North American Power Symposium (NAPS), Champaign, IL, USA, 9–11 September 2012; pp. 1–6. [CrossRef]
64. Dwork, C. Differential privacy: A survey of results. In Proceedings of the International Conference on Theory and Applications of Models of Computation, Xi'an, China, 25–29 April 2008; pp. 1–19.
65. Martínez, S.; Sebé, F.; Sorge, C. Measuring privacy in smart metering anonymized data. *arXiv Preprint* **2020**, arXiv:04863 2020.
66. Cardenas, A.; Amin, S.; Schwartz, G.A. Privacy-Aware Sampling for Residential Demand Response Programs. Available online: http://www.eecs.berkeley.edu/schwartz/HiCons2012ASG.pdf (accessed on 30 April 2020).
67. Foucault, M. *The Foucault Effect: Studies in Governmentality*; University of Chicago Press: Chicago, IL, USA, 1991.
68. Córdoba-Pachón, J.-R. *Managing Creativity: A Systems Thinking Journey*; Routledge: Abingdon, IK, USA, 2018.
69. Antonijevic, M.; Sučić, S.; Keserica, H. Augmented reality applications for substation management by utilizing standards-compliant scada communication. *Energies* **2018**, *11*, 599. [CrossRef]
70. Schneider, K.P.; Chen, Y.; Chassin, D.P.; Pratt, R.G.; Engel, D.W.; Thompson, S.E. *Modern Grid Initiative Distribution Taxonomy Final Report*; Pacific Northwest National Lab (PNNL): Richland, WA, USA, 2008.
71. Ledva, G.S.; Balzano, L.; Mathieu, J.L. Real-time energy disaggregation of a distribution feeder's demand using online learning. *IEEE Trans. Power Syst.* **2018**, *33*, 4730–4740. [CrossRef]
72. Jawurek, M.; Johns, M.; Kerschbaum, F. Plug-In privacy for smart metering billing. In *Intelligent Tutoring Systems*; Springer Science and Business Media LLC: Berlin, Germany, 2011; Volume 6794, pp. 192–210.
73. Zhang, X.-Y.; Kuenzel, S. Differential Privacy for Deep Learning-based Online Energy Disaggregation System. In Proceedings of the 2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe), The Hague, Netherlands, 25 October 2020.
74. Abadi, M.; Chu, A.; Goodfellow, I.; Mcmahan, H.B.; Mironov, I.; Talwar, K.; Zhang, L. Deep Learning with Differential Privacy. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 308–318.
75. Zhao, J.; Jung, T.; Wang, Y.; Li, X. Achieving differential privacy of data disclosure in the smart grid. In Proceedings of the IEEE INFOCOM 2014-IEEE Conference on Computer Communications, Toronto, ON, Canada, 27 April–2 May 2014; pp. 504–512.
76. Cover, T.M.; Thomas, J.A. *Elements of Information Theory*; John Wiley & Sons: Hoboken, NJ, USA, 2012.
77. Batra, N.; Kelly, J.; Parson, O.; Dutta, H.; Knottenbelt, W.; Rogers, A.; Singh, A.; Srivastava, M. NILMTK: An open source toolkit for non-intrusive load monitoring. In Proceedings of the 5th International Conference on Future Energy Systems, New York, NY, USA, 11 June 2014; pp. 265–276.

78. Kelly, J.; Knottenbelt, W. Neural nilm: Deep neural networks applied to energy disaggregation. In Proceedings of the 2nd ACM International Conference on Embedded Systems for Energy-Efficient Built Environments, Seoul, Korea, 4–5 November 2014; pp. 55–64.
79. Mironov, I. Rényi Differential Privacy. In Proceedings of the 2017 IEEE 30th Computer Security Foundations Symposium (CSF), Santa Barbara, CA, USA, 21–25 August 2017; pp. 263–275.
80. Parson, O.; Fisher, G.; Hersey, A.; Batra, N.; Kelly, J.; Singh, A.; Knottenbelt, W.; Rogers, A. Dataport and NILMTK: A building data set designed for non-intrusive load monitoring. In Proceedings of the 2015 IEEE Global Conference on Signal and Information Processing (GlobalSIP), Orlando, FL, USA, 14–16 December 2015; pp. 210–214.
81. Bmz Gmbh li-io Ess 3.0 Lithium-Ionen-Energy Storage System 3.0 for Sma. Available online: https://www.off-grid-europe.com/bmz-gmbh-li-io-ess-3-0-lithium-ionen-energy-storage-system-3-0-for-sma?gclid=CjwKCAjwv41BRAhEiwAtMDLsuqBrUnfvzcJRUb7lOyCkaH1XWJZAQY7XuNHR5qNVUYk5S9grA7aHxoC1qYQAvD_BwE (accessed on 30 April 2020).
82. Chillotti, I.; Gama, N.; Georgieva, M.; Izabachène, M. TFHE: Fast fully homomorphic encryption over the torus. *J. Cryptol.* **2019**, *33*, 34–91. [CrossRef]
83. Sandys, L. Energy Data Taskforce Report: A Strategy for a Modern Digitalised Energy System. 2019. Available online: https://es.catapult.org.uk/wp-content/uploads/2019/06/Catapult-Energy-Data-Taskforce-Report-A4-v4AW-Digital.pdf (accessed on 30 April 2020).
84. Blum, M.; Calif, U.O.; Feldman, P.; Micali, S. Mit Non-interactive zero-knowledge and its applications. In *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*; Association for Computing Machinery (ACM): New York, NY, USA, 2019; pp. 329–349.
85. Pedersen, T.; Petersen, B. Explaining gradually increasing resource commitment to a foreign market. *Int. Bus. Rev.* **1998**, *7*, 483–501. [CrossRef]
86. Schmidhuber, J. Deep learning in neural networks: An overview. *Neural. Netw.* **2015**, *61*, 85–117. [CrossRef]