energies

MDPI

Review

Data Privacy Preservation and Security in Smart Metering Systems

Mohamed S. Abdalzaher [1,*], Mostafa M. Fouda [2] and Mohamed I. Ibrahem [3,4]

[1] Department of Seismology, National Research Institute of Astronomy and Geophysics, Cairo 11421, Egypt
[2] Department of Electrical and Computer Engineering, College of Science and Engineering, Idaho State University, Pocatello, ID 83209, USA
[3] Department of Cyber Security Engineering, George Mason University, Fairfax, VA 22030, USA
[4] Department of Electrical Engineering, Faculty of Engineering at Shoubra, Benha University, Cairo 11672, Egypt
* Correspondence: msabdalzaher@nriag.sci.eg

Abstract: Smart meters (SMs) can play a key role in monitoring vital aspects of different applications such as smart grids (SG), alternative currents (AC) optimal power flows, adversarial training, time series data, etc. Several practical privacy implementations of SM have been made in the literature, but more studies and testing may be able to further improve efficiency and lower implementation costs. The major objectives of cyberattacks are the loss of data privacy on SM-based SG/power grid (PG) networks and threatening human life. As a result, losing data privacy is very expensive and gradually hurts the national economy. Consequently, employing an efficient trust model against cyberattacks is strictly desired. This paper presents a research pivot for researchers who are interested in security and privacy and shade light on the importance of the SM. We highlight the involved SMs' features in several applications. Afterward, we focus on the SMs' vulnerabilities. Then, we consider eleven trust models employed for SM security, which are among the common methodologies utilized for attaining and preserving the data privacy of the data observed by the SMs. Following that, we propose a comparison of the existing solutions for SMs' data privacy. In addition, valuable recommendations are introduced for the interested scholars, taking into consideration the vital effect of SM protection on disaster management, whether on the level of human lives or the infrastructure level.

Keywords: smart meters; smart grid; privacy-preserving mechanisms; differential privacy; game theory; machine learning; disaster management

Citation: Abdalzaher, M.S.; Fouda, M.F.; Ibrahem, M.I. Data Privacy Preservation and Security in Smart Metering Systems. *Energies* **2022**, *15*, 7419. https://doi.org/10.3390/en15197419

Academic Editor: Abu-Siada Ahmed

Received: 17 September 2022
Accepted: 7 October 2022
Published: 10 October 2022

1. Introduction

Implementing smart meters (SMs) for the observation of different metrics has become inevitable. Power grids (PG) are among the most vulnerable applications that need to be accurately monitored. The PG provides many benefits for both consumers and power utility providers. In this regard, SMs can reduce electricity costs, create a more reliable flow of power, and provide efficient viewing of information based on power consumption levels [1–8]. Additionally, SMs promote renewable energy and dynamic pricing for consumers [9–15]. Despite the logistical advantages, the increased flow of sensitive information for SMs comes with a higher opportunity for the loss of privacy for users and power providers. The undesired loss of data from a breach in SMs can prove to be catastrophic not only to power supply companies but also to individual households [16–18]. Accordingly, engineers are constantly looking for finding methods to increase scalable privacy in SMs without sacrificing the efficiency and cost of implementation [19–24].

In [25,26], the authors presented possible solutions to implementing privacy in SMs in a smart grid (SG) environment. Those efforts focused on the use of differential privacy (DP) as a means of introducing privacy into SMs. DP essentially compares information in two different datasets with groups rather than individuals. This allows individuals to not need

to share their private information over a wide area while still giving enough information to power producers to make SG technology work smoothly. The motivation behind this is that this method has the potential to keep information flow fast and efficient while keeping additional costs at a minimum level. In [26], the proposed model examined a technique called data distortion, in which companies can use algorithms to distort individual SM data while finding correct cumulative results when combined with other SM data. In [25], the authors interpreted that privacy in SMs requires significant research and mitigation because the concern over privacy remains a leading factor in the reluctance to implement SMs into the PG. Many believe that methods for ensuring privacy would either be too costly, too weak, or would make information exchange too inefficient.

The SG can assist utilities in reducing expenses, improving dependability and transparency, and streamlining procedures. However, as SM-based electric power systems are used more often, cyber security risks are growing, which raises the need for security methods. In other words, SMs can be the key player in the SG and PG networks, in which the SMs' sensitivity to the power metrics (voltage and current) is reflected by stepping up or stepping down of these metrics. For example, in such networks, SMs represent control and protection devices. Based on their measures, an action is taken to reduce or increase the electric current level to preserve the power network against destructive failures, such as in electricity production, transfer, distribution, and street lighting systems. This process is conducted to mitigate normal power consumption or as a defense model against cyberattacks. Therefore, for SG security, SM protection is crucial. It supports any security architecture and technology created and used in the SG, as well as enhances the system's reliability and resilience to cyberattacks. There are several methods to protect the privacy of SM data in the SG environment, such as DP, machine learning (ML), Kullback–Leibler (KL) divergence, game theory, generative adversarial privacy, data aggregation, pseudonyms, clustering, entropy, fuzzy, and Bayesian models. However, they have their drawbacks, such as limiting the usefulness of the data or proving computationally taxing.

In addition, one method that was used was the down-sampling of the electric usage data that are being taken in from the SM and sent to the third-party service provider [27–32]. However, the problem that is faced with this method of preservation of privacy is that down-sampling the data might incur time delays to detect critical events, which will negatively affect other processes [33–35].

ML has proved beneficial for different research directions in several research trends, including the security front and preserving human lives [36–44]. More particularly, ML has also played a key role in mitigating the SMs' security issues. The flexibility of the proposed model in [45] is to adapt univariate and multivariate situations, conduct the selection of features, and contain static or dynamic impacts. In addition, it contains an intrinsic application for measurement and fulfillment, solving numerous basic shortcomings. Deep learning (DL) found its way in this regard. To address the drawbacks of existing methods, the authors in [46] introduced a novel class-balancing mechanism using the oversampling of the interquartile minority methodology and an integrated electrical theft detection (ETD) model. Long short-term memory (LSTM), UNet, and adaptive boosting (Adaboost) make up the combined ETD model, also known as LSTM-UNet-Adaboost. In this way, LSTM-UNet-Adaboost combines the benefits of ensemble learning (Adaboost) and deep learning (LSTM-UNet) for ETD. Additionally, the State Grid Corporation of China provided real-time SM information, which was used to simulate and assess the efficiency of the proposed method.

Another method focuses on the approach of using physical resources, in this case being Rechargeable Batteries and Renewable Energy Sources, i.e., a solar panel using the sun for its power source [47–51]. This method was used because it did not need to distort the SM data, which means there will not be any time delays such as in the down-sampling method. However, the problem with this solution was that the incorporation of these physical resources would make the problem of privacy more complex and limited in scope

while also generating massive costs as you would quickly need to replace the resources due to the wear and tear caused by the increased charging and discharging rate.

It is noted from the literature that there are many practical implementations of privacy in SMs, but further research and experimentation can potentially further increase efficiency and decrease the cost of implementation. By comparing and contrasting strengths and weaknesses within the presented models in the literature, this paper builds on this information to provide more robust ideas for privacy implementation in SMs and highlight any shortcomings. In addition, this survey examines the limitations of the exerted research works and solutions to their limitations. Table 1 lists the abbreviations utilized in the manuscript. It is worth mentioning that effective mitigation of the attack manipulations affecting SMs using modern technologies can alleviate the catastrophic consequences, whether on the level of human lives or on the infrastructure level [37,52–56].

Table 1. List of abbreviations.

Abbreviation	Description
SMs	Smart Meters
PG	Power Grid
KL	Kullback–Leibler
ANN	Artificial Neural Network
RNN	Recurrent Neural Network
LSTM	Long Short-Term Memory
DNN	Deep Neural Network
ML	Machine Learning
DL	Deep Learning
DP	Differential Privacy
ETD	Electrical Theft Detection
Adaboost	Adaptive Boost
AC	Alternative Current
PGN	Power Grid Network
HPPs	High-Priority Packets
HPT	High-Priority Data Trustworthiness
GAP	Generative Adversarial Privacy
NE	Nash Equilibrium
HC	Hierarchical Clustering
KM	K-Medoids
FPGA	Field Programmable Gate Array
VHDL	VHSIC Hardware Description Language
DPMDs	Distribution-level Phasor Measurement Devices
MAC	Medium Access Control
BDST	Dempster–Shafer theory

The major contributions of this paper are listed as follows:

- Establishing a pivot for the interested researchers of the importance of SMs;
- Quantifying the existing problems regarding operation stability;
- Addressing the common defense mechanisms employed for protecting SMs' data privacy;

- Proposing a comprehensive comparison of the involved trust models for SMs' data privacy;
- Highlighting the role of SMs' security for disaster management;
- Recommending the future directions of the SM privacy for the interested scholars.

The rest of the paper is organized as follows. Section 2 discusses the common existing problems facing the SMs' operation stability. Section 3 addresses the defense mechanisms of SMs. Then, a comparison of the existing solutions to SM problems is presented in Section 4. Afterward, significant recommendations for future directions to the interested scholars are provided in Section 5. Finally, the paper is concluded in Section 6.

2. Existing Problems of Smart Meters

In this section, we discuss the problems affecting SMs concerning several applications. Figure 1 shows some of the prominent applications supported by SMs. In this regard, SMs are prone to different attacks that falsify the reports delivered to decision makers. It can lead to catastrophic situations on both the level of human lives and utilities [57]. Hereafter, we discuss the common vulnerabilities that SMs suffer from.

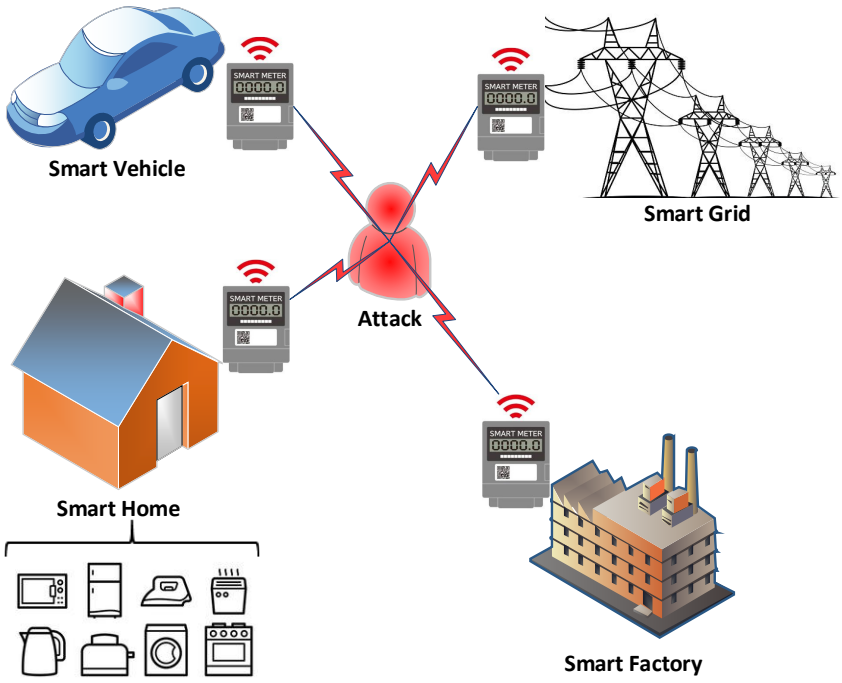

Figure 1. Framework of smart meter applications with attack existence.

2.1. Optimal Power Flow

The objective of the optimum power flow model is to provide the optimum power output to meet consumer demand at the lowest possible cost of operation for the utility provider. This model can be used to determine locational marginal prices. Locational marginal prices show the generator costs, line costs, and the costs of specific nodes at specific times. Therefore, using the optimum power flow model, utility providers can calculate the exact cost of the noise that is being added to a particular regional area. In [58], the authors presented a mixed integer programming model to optimize the packet size and the inter-node distance in SG. The model presented the optimal distance that can be used between the communicating nodes to prolong the wireless-nodes-based SG lifetime.

2.2. Privacy Problems

Privacy issues are and have been one of the main problems of SMs [59–63]. These SM devices send power consumption data back and forth from your home to the electricity company thousands of times per day, enabling real-time applications and analysis of data,

e.g., energy theft prevention, monitoring of power quality, timely detection of faults, and demand response. This level of power consumption monitoring has an alarming concern for consumers, despite being a considerable benefit to the power companies in terms of the usability and reliability of SMs. It is not surprising that people may be concerned about privacy with these SMs around their homes and monitoring their daily activities.

To make sure the data from a consumer's SM is secure, the innovative DP-compliant algorithm was developed. In this privacy-preserving method, the consumer is guaranteed that by choosing between including or excluding their SM data from a data set, their chances of suffering negative impacts will not be disproportionately increased. How is this achieved? Differentially private systems are characterized by the fact that a query from one data set should never differ from the result of a query from a neighboring data set. Therefore, the consumer should be indifferent about whether their data are included in the database or not.

3. Defense Mechanisms of Smart Meters

This section addresses the proposed defense mechanisms of the SMs' security issues along with their limitations. The frequently used notations are summarized in Table 2.

Table 2. The Frequently Used Notations.

Notation	Description
L_{releaser}	Releaser loss function
L_{attacker}	Attacker loss function
α	The releaser parameter
β	The attacker parameter
γ	A parameter that controls the privacy-utility trade-off
R^T	The released data
U^T	The useful data
D^T	The private data
$\mathbf{C}_t$	Cell state
$\mathbf{h}_t$	Hidden state
$\mathbf{f}_t$	Forget gate
$\mathbf{g}_t$ and $\mathbf{i}_t$	Input gates
$\mathbf{O}_t$	Output gate
b	The biases
K	Input weights
V	Recurrent weights
T	Total period
u_i	The utility of the ith player
A_i	The action of the ith player
A	The actions of all players
N	The number of players
a^*	The optimal action
a_{-i}	The strategies of all players except i

3.1. Differential Privacy

Energy retailers need to collect data about users' energy consumption to accurately meet load demand while minimizing costs. The problem is that energy consumption is

highly personal and can be used to infer a lot of private information about a consumer. DP is a method of adding noise to individual consumers' load profiles to protect their privacy. Here is how it works: In a large data set containing many users' load profiles, noise is added to every consumer's load profile based on the largest change that they could have on the result of a given query. The noise level to add to the consumer's load is calculated by first recording the result of a query to a data set that includes the consumer's information. Then, the same query is made to the same data set, except this time, the consumer's load is not included. Finally, the results of these two queries are compared to determine how much of an impact the consumer's data had on the aggregated result of the query. Noise is then added to the consumer's load profile based on its impact. This means that the same query for two separate data sets, one with the specified user's data and one without the user's data, should have the same result. Therefore, even if an adversary knew that a specific consumer's data was included in a data set, they would be unable to determine the user's consumption. Alternatively, given a data set and a user's load profile, an adversary would not be able to determine if that user was included in the data set. DP ensures privacy in that data sets can only be used to infer information about a group at large, but they cannot be used to infer information about any one individual. Therefore, consumers should theoretically be indifferent about volunteering their personal information.

That said, DP does not ensure complete privacy, it only guarantees that there is a max amount of privacy loss that an individual can suffer. Generalizations of the whole data set can still be used by an adversary to make statistical inferences about the user's consumption. However, the more users that are added to a data set, the less of an impact that any one individual can have on the data set. Therefore, statistical inferences about a user are harder to make on larger data sets. In addition, large data sets mean that less noise is required to anonymize an individual consumer's load profile.

When it comes to the DP algorithm, it should be assessed on its impacts in the four system operations it goes through: no privacy, low privacy, medium privacy, and high privacy. On the consumer end, an individual that would opt-in to the algorithm would then select one of the categories previously mentioned and from there be charged accordingly. In this case, the lower the epsilon value, the higher the security; therefore, the options increment to a lower epsilon, and the lower the epsilon, the more complex the calculation, requiring more computational power and creating a higher price baseline to equalize profit margins. The Laplacian noise, which aggregates in the load profile, fluctuates the profile significantly. When isolated, the fluctuations are very obvious and telling; however, when a composite of buses or consumers are added to the load profiles, it creates a smoothing effect on the data without losing any security. In some cases, smoothing functions may be applied due to the fact that the load profile with DP is immune to post-processing [64]. The smoothing functions are applied to a time series to remove the fine-grained variations between time steps. Once and if a smoothing effect is applied, the noise sum is periodically stored in its respective server, either by a third party or directly to the retailer. As the raw SM data are sent out at whatever the tick rate that is seen best by the retailer, the noise signal is added to the raw data, which then becomes the secure SM reading. That secure reading and the database of noise for the individual consumers is then sent to the retailer, by whom the calculation of additional cost using the database of the recorded noise is stored. From there, the allocation of extra costs to the various consumers is processed and carried out by the retailer.

3.2. Machine Learning

In [65], the proposed model is concentrated on the short-term forecasting of residential buildings' air conditioning usage utilizing information from a traditional SM. Through energy disaggregation methods, the air conditioning load is isolated from the SMs' aggregate consumption at each time step. The calculated air conditioning demand and the associated historical weather information are then used as input characteristics for the forecast process. Different ML methods, such as ANNs, Support Vector Machines, and Random Forests,

are employed in the prediction stage to make hourly and daily forecasts. In [25], the researchers went to the solution of the SM privacy problem by modeling the releaser (entity) of releasing data and the attacker as Recurrent Neural Networks (RNNs). It is appropriate for the time series of the SMs data, as depicted by Figure 2. RNN is a branch of neural networks that is capable of threading sequential data through the modeling of temporal correlation data. As such, an output of RNN at a time affects the output at a given time. More concretely, the authors exploited DNNs to adopt a DL model to take inputs to process into another layer of nodes. These nodes communicate their results with each other to form new layers until a final output is reached. In other words, the privacy-preserving model utilizes an RNN and Long Short-Term Memory. The algorithm is performed generally by a gradient descent utilizing the backpropagation algorithm. One issue with RNN is that learning conditional long-term time series data can lead to a lot of problems; hence, the LSTM cell was added. An LSTM cell creates four gating units to control and limit the flow of information, which all subsequently have sigmoid activation [66,67].

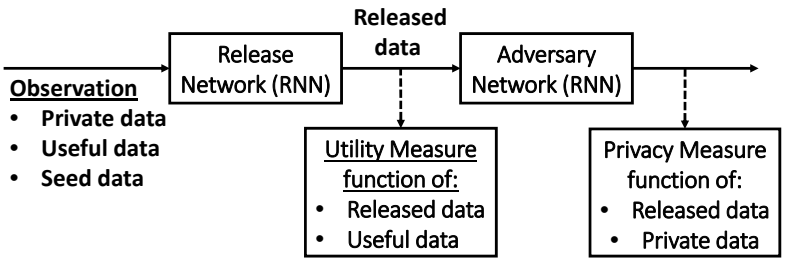

Figure 2. Diagram of privacy preservation.

Furthermore, the attacker is used to train the releaser mechanism while deploying two loss functions, one for each RNN, which are defined as:

$$L_{\text{releaser}}(\alpha, \beta, \gamma) := f\left(R^T, U^T\right) - \frac{\gamma}{T} \sum_{t=1}^{T} f\left(\hat{D}_t \mid R^t\right) \tag{1}$$

where $\gamma \geq 0$, which controls the privacy–utility trade-off. α is the parameter of the "releaser" and β for the "attacker" parameter.

There are some special cases this formula can run into, such as lambda being 0. However, the system still stands as estimated for an attacker to fail in concluding to address random estimation performance. For the adversary, the loss function would be defined as:

$$L_{\text{attacker}}(\beta) := \frac{1}{T} \sum_{t=1}^{T} \mathbb{E}\left[-\log p_{\hat{D}_t|R^t}\left(D_t \mid R^t\right)\right] \tag{2}$$

In the given model the expectation is with respect to $D_t R^t$. It is important to note that the previous loss function is approximated by evaluating the expectation empirically. Here, the loss function of the releaser and attacker is approximated as follows:

$$\begin{aligned} L_{\text{releaser}}(\alpha, \beta, \gamma) \approx & \frac{1}{IT} \sum_{i=1}^{I} f\left(z^{(i)T}, y^{(i)T}\right) \\ & + \frac{\lambda}{IT} \sum_{i=1}^{I} \sum_{\hat{d}_t^{(i)} \in \mathcal{D}} p_{\hat{D}_t|R^t}\left(\hat{d}_t^{(i)} \mid r^{(i)t}\right) \\ & \times \log p_{\hat{D}_t|R^t}\left(\hat{d}_t^{(i)} \mid r^{(i)t}\right), \\ L_{\text{attacker}}(\beta) \approx & -\frac{1}{IT} \sum_{t=1}^{T} \sum_{i=1}^{I} \log p_{\hat{D}_t|R^t}\left(d_t^{(i)} \mid r^{(i)t}\right). \end{aligned} \tag{3}$$

Since RNNs are usually executed by gradient descent relying on the backpropagation algorithm [68], it can result in an event called gradient vanishing/exploding problems that cause the training to be unsuccessful [69]. The resolution of this problem is the use of an LSTM cell that includes four gating units to supervise the information flow. The parameter b is for biases, K is for input weights, and V is for recurrent weights, as depicted in Figure 3 [66,67].

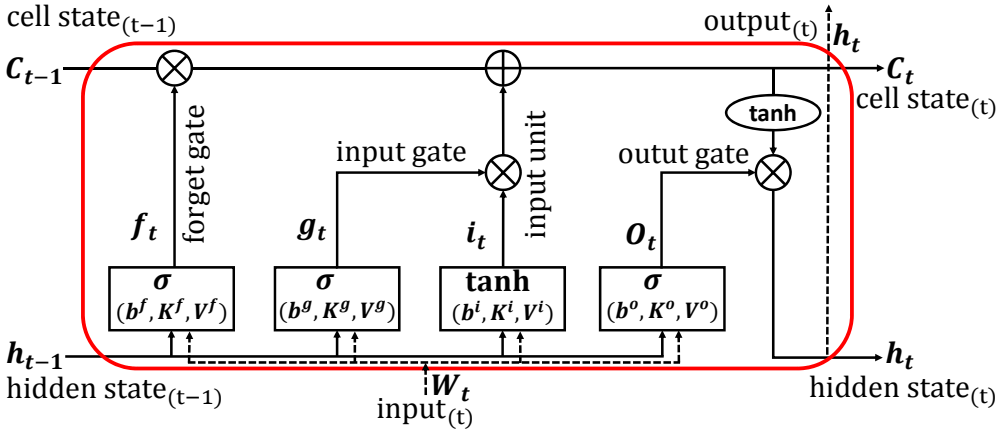

Figure 3. LSTM diagram at a time t.

This lets the user train models using sequences with several hundreds of time steps, which RNN struggles to do [70]. In that model, an adversarial modeling framework is then created that consists of the two previously mentioned RNNs, to which a random variable will be appended to the observed signal Wt that randomizes the released data. For both networks, an LSTM architecture is selected; then, the training begins using the proposed algorithm to take the data, and the attacker will try to obtain the data to be tested for accuracy of 80%, almost no privacy, and 50% privacy.

These data will then be used for the addition of distortion to the released data based on the demand load and sensitive information because of the learned noise distribution to fit specific data based on the framework. This is a much better way than what is usually performed, which is to use a fixed noise distribution for all the SMs data. In the context of SMs, an adversary with access to distorted SM data as an input can utilize DNNs to accurately guess a homeowner's non-distorted SM readings.

In [71], measurements were categorized as secure or under attack using ML techniques. To overcome limitations brought on by the problem's sparse nature and to make use of any prior information about the system that may be accessible, an attack detection framework was offered in the suggested method. To represent the attack detection issue, well-known batch and online learning methods (supervised and semi-supervised) were combined with decision- and feature-level fusion. For meter data encryption, the authors in [72] suggested a localization-based key management system. Data were encrypted using a random key index and the key assigned to the meter's location. A dependable third party was in charge of maintaining and distributing the encryption keys. A technique based on received signal intensity and the highest likelihood estimator was suggested for the localization of the meter. At the control center, the packets were decrypted using a key that was mapped to the key index and meter coordinates. A demand-side management engine that was in charge of maintaining the effective use of energy based on priorities has been presented in [73]. The control of intrusions in the SG was suggested using a unique resilient paradigm. Using the ML classifier, the resilient agent predicts dishonest entities. The ML has also proved beneficial in the detection of SG data falsification due to the attack injection, as presented in [74].

3.3. Kullback–Leibler Divergence

Kullback–Leibler (KL) divergence is used to interpret the information loss between expected and ground truth distribution. On the other hand, by the KL divergence, some samples produced by the model may not fit the data distribution. The attacker's aim is to reduce the KL divergence between the related predictors. In [25], the goal is to use DNNs to minimize the accuracy of the attacker's potential inferences while also minimizing the distortion rate between the released data (R^T) and the useful data (U^T). The attacker's goal is to most accurately infer the private data (D^T) with the following equation:

$$\underset{\hat{d}_t \in \mathcal{D}}{argmax}\ p_{\hat{D}_t|R^t}(\hat{d}_t|r^t), t \in \{1, 2, \cdots, T\} \tag{4}$$

In that work, Shateri et al. developed a sample output for each SM reading parameter before simulating an attacker's guessed DNN output, $P_{D_T|R_T}$. After this, the goal is to determine the level of distortion needed and to utilize KL distance to measure the attacker's accuracy. The KL distance is a mathematical formula employed to calculate the gap between two distributions using the following formula:

$$\inf_{p_{\hat{D}_t|R^t}} KL(p_{D^tR^t}||p_{\hat{D}^t|R^t}) = \inf_{p_{\hat{D}_t|R^t}} \mathbb{E}\left[\log \frac{p_{D^tR^t}(D^t|R^t)}{p_{\hat{D}^t|R^t}(D^t|R^t)}\right] \tag{5}$$

It is noted that the closer the output of this equation is to 0, the less privacy the DNN offers.

3.4. Game Theory

Game theory can be used to incentivize cooperation between parties to determine a fair cost allocation for the noise that is added to a system. Game theory is thus a sophisticated subset of intelligent optimization. The game theory model depicts a contest between groups of players who might choose to work cooperatively or antagonistically to advance their outcomes/payoffs via the employed strategy or strategies carried out by the progressive player actions. The essential game parameters definitions, as in [75,76], can be summed up as follows:

- The strategic interaction between competing or cooperative interests when the limitations and compensation for actions are taken into account is referred to as a game.
- A player is a fundamental component of a game. Each player in the game, given by the number i, is responsible for acting rationally, as shown by the symbol A_i. In a game, a player may take the place of a human, a machine, or a team of players N.
- The Utility/Payoff is expressed by the reward or punishment to a player based on a given action throughout the game given by $u_i : A \to \mathbb{R}$, which calculates the output for the ith player, and pinpointed by the participating players actions $A = \times_{i \in N} A_i$, where the symbol $\times$ represents a Cartesian product.
- A strategy is defined by an action plan throughout the game in which a player can adopt a strategic game $\langle N, (A), (u_i) \rangle$.

Game theory may be utilized in the security area to identify rogue nodes, mitigate the impact of foreign intrusions, and uncover nodes which act egotistically and overload the entire network. Nash equilibrium (NE), in general, is an intelligent approach to social issues that has emerged as a viable idea for wireless networks, and more particularly for wireless node security [75–80].

- NE is defined as the profile of the optimal action, $a^* \in A$, as a player $i \in N$ is not able to gain from unilaterally changing its course and opting for a different course of action [77,80]. This process is reflected by the utility function as $u_i(a_i^*, a_{-i}^*) \geq u_i(a_i, a_{-i}^*)$ for all $a_i \in A$, where a_i is the player strategy i and a_{-i} represents the strategies of all players except i [75].

In [26], the authors assumed that consumers all have different privacy preferences and different values for how much they are willing to pay for their privacy. Researchers tested three different game theory functions to fairly allocate costs. The cost that must be distributed amongst a group is determined by the optimum power flow model, which can determine the overall energy consumption for a given region. Therefore, the groups that will split the costs are formed around their locational proximity to one another. A consumer may be responsible for more of the shared cost of noise depending on their chosen class of privacy. The first cost-allocating function tested is the Shapely value. The marginal cost is determined by calculating the additional cost incurred to a system by a consumer at the time that they join a given group. This cost is different depending on the consumer's entrance order to the group, so the cost the consumer pays is the average of all costs from all entrance orders. The second cost allocating function is the Vickery–Clark–Groves mechanism. This model incentivizes consumers to truthfully report their SM consumption after it has already been processed by the DP masking algorithm. Consumers are allocated costs based on their marginal contribution of noise to the system. The third cost allocation function is the nucleolus mechanism. This model finds the degree to which a group is dissatisfied with a given price allocation, and then attempts to minimize the dissatisfaction. The algorithm first calculates the most inequitable price allocation and then attempts to minimize the overall consumer dissatisfaction with it. Then, the next most inequitable price allocation is subsequently minimized. This process continues until a suitable vector is created, which can minimize consumer dissatisfaction with overall price allocations.

In [81], the authors studied how to use game theory models for protecting wireless nodes from selfish nodes or malicious nodes. In this study, we surveyed the different game-theoretic defense strategies for wireless nodes and presented a classification of the game theory approaches using the attack nature. Then, a trust model using game theory for decision making was presented, in which the significant role of evolutionary games for wireless nodes' security confronting intelligent attacks was identified. Finally, several prospective game theories were proposed to promote the data trustworthiness and cooperation of different wireless nodes. To prevent interrupting the reported data in clustered sensor networks, a Stackelberg game was created to counteract external assault manipulations using the energy defensive budget versus the corresponding attack budget, as proposed in [82]. In [83], the proposed work can effectively resolve the hardware problem that occurs in the presence of the attack impact in sensor-network-based cognitive radio. In addition, the consumed energy is well managed using the proposed model. In this regard, refs. [84] presented a Stackelberg game in order to implement a security model for sensor-network-based cognitive radio to confront the data falsification attack. This approach was developed for two different attack–defense scenarios. Two scenarios were presented relying on the threshold level of determining the interference power. In [85], an effective Stackelberg game was proposed in order to achieve data trustworthiness in PGN. This attack scenario regularly manipulates sets of the deployed nodes in the PGN, which cannot be managed using the previously provided technique. The proposed model was offered to combat the attack scenario, which is more serious than that taken into account in prior work. In [86], a game-theoretic protection approach was proposed for clustered wireless sensor networks based on a repeated game. The suggested approach was created to find rogue nodes that drop high-priority packets (HPPs) to increase the reliability of high-priority data (HPT). The findings of this study show that the suggested protection model's HPT is enhanced over a non-cooperative defensive mechanism, achieving the Pareto optimum HPT. In [87], a game-theoretic approach based on a non-zero-sum game is developed to build a robust trust model against intelligent attacks facing the IoT applications. The obtained results show enhanced performance in detecting the malicious nodes and to model low complexity.

3.5. Generative Adversarial Privacy

Shateri et al. suggest that SM data releasers can implement DNNs to combat this in a "minimax" game. This is a reference to a game theory concept in statistics in which one bases their own moves or decisions based on an opponent's possible decisions with the goal of minimizing the opponent's worst possible loss. Using DNNs to implement this minimax game is called generative adversarial privacy (GAP). In the case of SM privacy, a data releaser would use GAP to strategically add noise wherever necessary to give an adversary using DNNs to ensure an attacker's least accurate inference of the non-distorted SM data. The data releaser must decide where to add noise in an SM data set, and the extent of noise to add while also minimizing the loss of privacy and utility (privacy/utility tradeoff). This can be difficult without the use of DNNs due to the fact that adding noise to a data set sacrifices utility, yet adding too little compromises its privacy for an attacker. With the addition of DNNs and GAP, however, one can use as little noise addition as possible and still ensure adequate privacy [25]. This study assumed that an attacker can eavesdrop on signals sent from a homeowner to a utility company to obtain released data and that the utility company knows what SM data need to be kept private to a consumer. The releaser refers to the actor that is authorized to read SM data, and an attacker refers to an eavesdropping adversary who attempts to infer the useful data based on the released signal.

3.6. Data Aggregation

Data aggregation, which takes multiple data from multiple SMs and organizes it into one big comprehensive medium, is another solution to the privacy problem. The limitation of this solution is that as more data are aggregated, the data become less accurate, thus degrading the positioning of the power measurements. Through the implementation of data aggregation, an additional privacy issue comes to the surface: each participating SM sees intermediate plain-text aggregation results routed through itself. This is because the intermediate SMs are authorized to achieve collected data decryption, adopt mathematical operations for aggregation tasks that are not capable to be executed over encryption. Data aggregation can resolve this issue by employing homomorphic encryption to enable secure in-network encryption and privacy protection. The electricity usage data from child SMs are encrypted with a semantically secure encryption methodology [88]. At the same time, to enable aggregation functions, the algebraic operations of the plaintext are permitted to be carried out on the cipher domain. The main limitation this data aggregation method brings is a reasonable computation overhead [27]. In [89], the authors used a linear integer program to represent the data aggregation scheduling problem. The problem was split into two different variations. The first model presupposed that the routing tree was established, for instance, through a network layer protocol, and that node broadcasts should be timed to minimize latency. The second variation required combined optimization of the node scheduling and routing topology creation.

3.7. Pseudonyms

Additional existing solutions include the use of pseudonyms rather than the real names of homeowners [90], standard encryption methods [91], the user of Deep Neural Networks (without the use of GAP as proposed by Shatiri et al.) [92], and random noise addition [93]. Pseudonyms in smart meter data do not require substantial computational overhead, but many consider it a weak form of privacy due to attackers' abilities to link identities to their pseudonyms [90]. Standard encryption methods have similar issues to data aggregation. The computational overhead of implementing strong encryption sacrifices utility [91]. The use of DNNs requires low overhead and provides adequate privacy to homeowners, but Shatiri et al. attempt to build on this because privacy may be compromised if an attacker also uses DNNs [92]. With random noise addition, a data releaser may add noise to SM readings in order to make these readings unintelligible to an attacker. A utility company can receive these readings and remove the randomly added

noise to view a homeowner's raw SM data. This, however, introduces the dilemma of adding either too much noise and sacrificing utility or too little—sacrificing privacy [93].

3.8. Clustering

This technique adopts a hierarchical paradigm to confront the attack manipulations. In [94], SM data were disaggregated and utilized to understand patterns of energy usage using clustering techniques such as Fuzzy C-Means. In [95,96], the authors used a cluster ensemble of various clustering techniques to create an automated system for phishing detection. The hierarchical clustering (HC) Algorithm, which employed cosine similarity (using the TF-IDF metric for assessing the similarity between two points), and K-Medoids (KM) Clustering method were used as feature selection algorithms for extracting different phishing email attributes. To mitigate intrusions in wireless nodes, a hybrid method was put out. To specifically reduce the amount of information to analyze and the energy needed, a clustering approach is used [97].

3.9. Entropy

To determine the weight value, the information entropy theory, an objective weighing approach, examines the information order of each evaluation index. Entropy theory has been widely used in many fields, which has steadily raised the issue of adding entropy to the power system. The research done in [98], is intended to investigate information entropy data mining-based smart terminal security technology of the PG perception layer. This article examined similar techniques and creates a smart PG terminal. A safety strategy was created and a platform for data analysis was constructed on this foundation. In contrast to several different energy demand time series, the authors in [99,100] showed how to use a multidimensional anomaly detection technique for the early identification of manipulated electricity meters. The technique can improve and supplement current monitoring systems, which typically only assess one-time series. Since DET was the goal, there are obvious outliers as a result. To emphasize the requirements and fine-tuning procedures for the aggregation and comparison of various data sources, the model offered three data prepossessing techniques to generate outliers in the event of energy theft.

3.10. Fuzzy

To demonstrate the benefits of the fuzzy logic trust model, it was compared against an existing model in this research to identify untrusted nodes in SG networks. The routing effectiveness and detection rate for all classes of activities regarded as malicious can be increased using the suggested approach [101]. To manage the power converter DC bus voltage, a fuzzy logic controller is used. The information gathered in [102] was cross-disciplinary, and none of the methodologies used have ever been offered in their entirety. To increase efficiency and take advantage of parallelism and high speed, all control functions were incorporated into a FPGA device using VHDL. The capability of the control functions was first demonstrated using an FPGA-in-the-loop simulation approach, and then experimental assessments were carried out to demonstrate equipment dependability and operation.

3.11. Bayesian

Utilizing two different types of readings from SMs and distribution-level phasor measurement devices (DPMDs), the authors in [103] created a method for harmonic state estimate DPMDs. Regression analysis was used to calculate the power flow, recurrent neural networks were used to anticipate demand, and sparse Bayesian learning was used to estimate the state. The suggested method was more compatible with current distribution grids since it needed fewer DPMDs than nodes. The efficiency of the suggested estimator was demonstrated by in-depth numerical simulations on an IEEE test feeder. To address the metrics of the physical layer (node transmission rate) and MAC layer (node buffering capacity) and determine trust at the node level for packet delivery, the Bayesian theory and Dempster–Shafer theory (BDST) were merged in [104]. To manage metrics of the MAC layer

(link capacity) and Network layer (distance and link quality) for computing confidence at the link level for protected routing, the fuzzy theory was also integrated with BDST.

4. Existing Solutions Comparison

When it comes to DP, its main benefits are its cost and benefit analysis, sequential composition, accurate billing, and easy implementation, really showing its strength and viability in a real-world application. Due to the fact that the consumer can choose a plan of privacy such as the four aforementioned (None, Low, Medium, High), a consumer can decide how much they are willing to pay for privacy and how important privacy is to the particular individual. Secondly, the sequential composition is used, but DP puts it ahead of neural networking in terms of speed due to the fact that sequential composition can consult the data more than once and run parallel composition in a broken down piece for higher security without losing out on speed of processing. Due to the fact that the processing is sent out periodically when the DP is reversed, the retailer and consumer can expect very accurate billing rather than a monthly or annual lump sum billing that is estimated. In addition, the consumer could accurately see what is running up their bill, so they can then effectively balance their lifestyles to effects billing expenses. Lastly, it is very easy to implement this system into modern-day homes, offices, etc. To integrate such an algorithm, all that is needed is communication and trust between the retailer and consumer keeping the business side of things simple and it is cheaper to implement and compute than neural networking.

While DP has its pros, it also carries its share of cons, the first being that it has no protection against inference privacy. Based on the data seen, even with noise an attacker could infer what could be running or not in one's household. Due to the algorithm allowing lower epsilon, higher security levels can create errors and uncertainties that could effectively cause more computation errors, throwing your billing prices off slightly or even creating an opening for an attacker to take advantage of your security due to an error. Lastly, as everything is now running through the DP algorithm or, in some cases, a third-party station, a greater energy loss is unavoidable.

When it comes to ANNs, the main benefits are its high precision with the amount of data that is returned while being very good at protecting against inference privacy as the data that can be seen by potential attackers are less than 50 percent, which guarantees privacy. The issue with this approach is that the training of this recurrent neural network can be very slow and complex. This problem becomes even worse as the use of long short-term memory requires more memory to train, which makes an already slow training process even slower. This also makes the training of the neural network more expensive, as the longer it takes, the more money it eats up, especially with all of the different technical parameters that are in this solution. Table 3 lists a comparison of the eleven considered defense strategies examined in the literature.

Table 3. Security Models' Comparison.

Security Model	Advantages	Disadvantages	Recommendation
Game theory	The utility of the nodes is calculated when the association between nodes is analyzed as a cooperative and non-cooperative game. The game model addresses the logical issue involving the rational participants.	Complexity of implementation.	Medium
Clustering	The cluster's node rearrangement and network scalability. Easy to put into action.	Very significant overheads for control. Certain protocols have a long transmission latency. Sophisticated algorithms.	Low
Bayesian	The degree of confidence is taken into account while making decisions.	Scalable network design cannot be taken into account since assessment is solely focused on the node's QoS.	High

Table 3. *Cont.*

Security Model	Advantages	Disadvantages	Recommendation
Entropy	Inspired by the theory of thermodynamics that deals with the degree of uncertainty in a signal or random occurrence, employed for ad hoc.	Handles attacks individually.	Low
Fuzzy	To address a control issue, it inserts a number of if–then rules.	Memory overflow results from adding more if–else statements.	Medium
Differential privacy	Can interactively support machine learning models.	Expensive computation, does not support sufficient performance with high complexity problems.	High
Machine learning	Easy to pinpoint patterns, supports full automation, supports several applications.	Long training time, high probability of error, big datasets are needed.	High
Kullback-Leibler Divergence	It depicts the information loss between expected and ground truth distribution.	Some samples produced by the model may not fit the data distribution.	Meduim
Generative Adversarial Privacy	Easy to combine with machine learning, easy to interpret its generated data.	Oscillation of model's parameters leads to non-convergence, the generator can collapse.	Low
Data Aggregation	Data aggregation aids in condensing information from various, dissimilar, and many sources.	If data are not gathered and organized meaningfully, they are difficult to identify and analyze.	Low
Pseudonyms	Anonymity.	Twice the identities.	Low

5. Recommendations for Future Directions

Real-Time Data Release for SMs with privacy protection for different SG environments has become an inevitable concern that still needs a more reliable and adaptive solution. Accordingly, more extensive efforts are still desired that open the door for new intelligent solutions. Hereafter, we propose some recommendations for the interested scholars in this regard as follows:

- Analyzing the impact an attacker could have on the data release framework if they have prior knowledge about their victim that was obtained without using smart meter data;
- Combining their algorithm with physical distortion methods, such as renewable energy or batteries, could further increase a consumer's privacy by shaping their demand profile;
- Observing the privacy impact of the DP algorithms when the resolution of the model, or the data collection interval, is over a specific time threshold;
- Investigating the effects of privacy preservation against non-intrusive load monitoring techniques;
- Providing more inference privacy techniques;
- Considering the modern technologies and adaptive protocols of the Internet of Things to attain acceptable disaster management and risk mitigation.

6. Conclusions

Time series data, adversarial training, SG, air conditioning, and other applications can all benefit from the monitoring that SMs can provide. There have been several real-world SM privacy implementations in the literature, but further research and testing may be needed to increase effectiveness and decrease implementation costs. It is significant to mention that modern technology may effectively mitigate attack manipulations that affect SMs to lessen the devastating impacts on both infrastructure and human life. This article sheds light on the significance of the SM and offers academics interested in security and

privacy a research pivot. We draw attention to the relevant SM characteristics in many applications. Electricity service interruptions are quite expensive: for example, the annual cost of the harm done to the U.S. economy by these interruptions is estimated to be between USD 104 billion and USD 164 billion. In addition, the data privacy loss of SM-based SG/PG networks is among the main targets of cyberattacks, leading to the deterioration of the networks. Accordingly, losing data privacy is significantly costly and rapidly degrading the national economy. Therefore, we concentrate on the SMs' weaknesses. Then, we take a look at eleven trust models used for SM security, which are among the widely used techniques for safeguarding the data privacy of the SMs' observed data in SG and PG networks. Then, we compare the current methods for protecting the data privacy of SMs. In addition, insightful suggestions are made for the interested researchers, taking into account the critical role that SM protection plays in catastrophe management, whether on the level of infrastructure or human life.

Author Contributions: Conceptualization, M.S.A., M.I.I. and M.M.F.; methodology, M.S.A., M.I.I. and M.M.F.; investigation, M.S.A., M.I.I. and M.M.F.; writing—original draft preparation, M.I.I. and M.M.F.; writing—review and editing, M.S.A.; supervision, M.I.I.; resources, M.S.A., M.I.I. and M.M.F.; data curation, M.S.A., M.I.I. and M.M.F.; visualization, M.S.A. and M.I.I. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

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

References

1. Alsharif, A.; Nabil, M.; Mahmoud, M.M.; Abdallah, M. EPDA: Efficient and privacy-preserving data collection and access control scheme for multi-recipient AMI networks. *IEEE Access* **2019**, *7*, 27829–27845. [CrossRef]
2. Alsharif, A.; Nabil, M.; Tonyali, S.; Mohammed, H.; Mahmoud, M.; Akkaya, K. EPIC: Efficient privacy-preserving scheme with EtoE data integrity and authenticity for AMI networks. *IEEE Internet Things J.* **2018**, *6*, 3309–3321. [CrossRef]
3. Fadlullah, Z.M.; Fouda, M.M.; Kato, N.; Takeuchi, A.; Iwasaki, N.; Nozaki, Y. Toward intelligent machine-to-machine communications in smart grid. *IEEE Commun. Mag.* **2011**, *49*, 60–65. [CrossRef]
4. Fouda, M.M.; Fadlullah, Z.M.; Kato, N.; Lu, R.; Shen, X.S. A Lightweight Message Authentication Scheme for Smart Grid Communications. *IEEE Trans. Smart Grid* **2011**, *2*, 675–685. [CrossRef]
5. Fadlullah, Z.M.; Fouda, M.M.; Kato, N.; Shen, X.; Nozaki, Y. An early warning system against malicious activities for smart grid communications. *IEEE Netw.* **2011**, *25*, 50–55. [CrossRef]
6. Abdulaal, M.J.; Ibrahem, M.I.; Mahmoud, M.M.E.A.; Khalid, J.; Aljohani, A.J.; Milyani, A.H.; Abusorrah, A.M. Real-Time Detection of False Readings in Smart Grid AMI Using Deep and Ensemble Learning. *IEEE Access* **2022**, *10*, 47541–47556. [CrossRef]
7. Ali, S.S.; Choi, B.J. State-of-the-art artificial intelligence techniques for distributed smart grids: A review. *Electronics* **2020**, *9*, 1030. [CrossRef]
8. Saxena, N.; Choi, B.J. State of the art authentication, access control, and secure integration in smart grid. *Energies* **2015**, *8*, 11883–11915. [CrossRef]
9. Alsharif, A.; Nabil, M.; Mahmoud, M.; Abdallah, M. Privacy-preserving collection of power consumption data for enhanced AMI networks. In Proceedings of the 2018 25th International Conference on Telecommunications (ICT), Saint-Malo, France, 26–28 June 2018; pp. 196–201.
10. Sherifl, A.; Alsharif, A.; Mahmoud, M.; Abdallah, M.; Song, M. Efficient privacy-preserving aggregation scheme for data sets. In Proceedings of the 2018 25th International Conference on Telecommunications (ICT), Saint-Malo, France, 26–28 June2018; pp. 191–195.
11. Aladdin, S.; El-Tantawy, S.; Fouda, M.M.; Tag Eldien, A.S. MARLA-SG: Multi-Agent Reinforcement Learning Algorithm for Efficient Demand Response in Smart Grid. *IEEE Access* **2020**, *8*, 210626–210639. [CrossRef]
12. Fouda, M.M.; Fadlullah, Z.M.; Kato, N.; Takeuchi, A.; Nozaki, Y. A novel demand control policy for improving quality of power usage in smart grid. In Proceedings of the 2012 IEEE Global Communications Conference (GLOBECOM), Anaheim, CA, USA, 3–7 December 2012; pp. 5154–5159. [CrossRef]
13. Badr, M.M.; Ibrahem, M.I.; Baza, M.; Mahmoud, M.; Alasmary, W. Detecting Electricity Fraud in the Net-Metering System Using Deep Learning. In Proceedings of the 2021 International Symposium on Networks, Computers and Communications (ISNCC), Dubai, United Arab Emirates, 31 October–2 November 2021; pp. 1–6. [CrossRef]

14. Ilo, A. Design of the smart grid architecture according to fractal principles and the basics of corresponding market structure. *Energies* **2019**, *12*, 4153. [CrossRef]
15. Junior, J.M.; da Costa, J.P.C.; Garcez, C.C.; de Oliveira Albuquerque, R.; Arancibia, A.; Weichenberger, L.; de Mendonça, F.L.L.; Galdo, G.D.; de Sousa, R.T., Jr. Data security and trading framework for smart grids in neighborhood area networks. *Sensors* **2020**, *20*, 1337. [CrossRef] [PubMed]
16. Alsharif, A.; Nabil, M.; Sherif, A.; Mahmoud, M.; Song, M. MDMS: Efficient and privacy-preserving multidimension and multisubset data collection for AMI networks. *IEEE Internet Things J.* **2019**, *6*, 10363–10374. [CrossRef]
17. Alsharif, A.; Tonyali, S.; Mahmoud, M.; Akkaya, K.; Ismail, M.; Serpedin, E. Performance analysis of certificate renewal scheme for ami networks. In Proceedings of the 7th International Workshop on Computer Science and Engineering, Beijing, China, 25–27 June 2017; pp. 25–27.
18. Ibrahem, M.I.; Nabil, M.; Fouda, M.M.; Mahmoud, M.M.E.A.; Alasmary, W.; Alsolami, F. Efficient Privacy-Preserving Electricity Theft Detection With Dynamic Billing and Load Monitoring for AMI Networks. *IEEE Internet Things J.* **2021**, *8*, 1243–1258. [CrossRef]
19. Alsharif, A.; Shafee, A.; Nabil, M.; Mahmoud, M.; Alasmary, W. A multi-authority attribute-based signcryption scheme with efficient revocation for smart grid downlink communication. In Proceedings of the 2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Atlanta, GA, USA, 14–17 July 2019; pp. 1025–1032.
20. Ibrahem, M.I.; Mahmoud, M.; Fouda, M.M.; Alsolami, F.; Alasmary, W.; Shen, X. Privacy Preserving and Efficient Data Collection Scheme for AMI Networks Using Deep Learning. *IEEE Internet Things J.* **2021**, *8*, 17131–17146. [CrossRef]
21. Badr, M.M.; Ibrahem, M.I.; Mahmoud, M.; Fouda, M.M.; Alsolami, F.; Alasmary, W. Detection of False-Reading Attacks in Smart Grid Net-Metering System. *IEEE Internet Things J.* **2022**, *9*, 1386–1401. [CrossRef]
22. Ibrahem, M.I.; Badr, M.M.; Fouda, M.M.; Mahmoud, M.; Alasmary, W.; Fadlullah, Z.M. PMBFE: Efficient and Privacy-Preserving Monitoring and Billing Using Functional Encryption for AMI Networks. In Proceedings of the 2020 International Symposium on Networks, Computers and Communications (ISNCC), Montreal, QC, Canada, 16–18 June 2020; pp. 1–7. [CrossRef]
23. Ibrahem, M.I.; Badr, M.M.; Mahmoud, M.; Fouda, M.M.; Alasmary, W. Countering Presence Privacy Attack in Efficient AMI Networks Using Interactive Deep-Learning. In Proceedings of the 2021 International Symposium on Networks, Computers and Communications (ISNCC), Dubai, United Arab Emirates, 31 October–2 November 2021; pp. 1–7. [CrossRef]
24. Badr, M.M.; Ibrahem, M.I.; Mahmoud, M.; Alasmary, W.; Fouda, M.M.; Almotairi, K.H.; Fadlullah, Z.M. Privacy-Preserving Federated-Learning-Based Net-Energy Forecasting. In Proceedings of the SoutheastCon 2022, Mobile, AL, USA, 26 March–3 April 2022; pp. 133–139. [CrossRef]
25. Shateri, M.; Messina, F.; Piantanida, P.; Labeau, F. Real-time privacy-preserving data release for smart meters. *IEEE Trans. Smart Grid* **2020**, *11*, 5174–5183. [CrossRef]
26. Gough, M.B.; Santos, S.F.; AlSkaif, T.; Javadi, M.S.; Castro, R.; Catalão, J.P. Preserving privacy of smart meter data in a smart grid environment. *IEEE Trans. Ind. Inform.* **2021**, *18*, 707–718. [CrossRef]
27. Mashima, D. Authenticated down-sampling for privacy-preserving energy usage data sharing. In Proceedings of the 2015 IEEE International Conference on Smart Grid Communications (SmartGridComm), Miami, FL, USA, 2–5 November 2015; pp. 605–610.
28. Azizi, E.; Shotorbani, A.M.; Hamidi-Beheshti, M.T.; Mohammadi-Ivatloo, B.; Bolouki, S. Residential household non-intrusive load monitoring via smart event-based optimization. *IEEE Trans. Consum. Electron.* **2020**, *66*, 233–241. [CrossRef]
29. Shateri, M.; Messina, F.; Piantanida, P.; Labeau, F. Learning Sparse Privacy-Preserving Representations for Smart Meters Data. In Proceedings of the 2021 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Aachen, Germany, 25–28 October 2021; pp. 333–338.
30. Reinhardt, A.; Pereira, L. Energy Data Analytics for Smart Meter Data. *Energies* **2021**, *14*, 5376. [CrossRef]
31. Stadler, M.; Pecenak, Z.; Mathiesen, P.; Fahy, K.; Kleissl, J. Performance comparison between two established microgrid planning MILP methodologies tested on 13 microgrid projects. *Energies* **2020**, *13*, 4460. [CrossRef]
32. Athanasiadis, C.; Doukas, D.; Papadopoulos, T.; Chrysopoulos, A. A scalable real-time non-intrusive load monitoring system for the estimation of household appliance power consumption. *Energies* **2021**, *14*, 767. [CrossRef]
33. Farokhi, F. Review of results on smart-meter privacy by data manipulation, demand shaping, and load scheduling. *IET Smart Grid* **2020**, *3*, 605–613. [CrossRef]
34. Zhang, X.Y.; Kuenzel, S.; Córdoba-Pachón, J.R.; Watkins, C. Privacy-Functionality Trade-Off: A privacy-preserving multi-channel smart metering system. *Energies* **2020**, *13*, 3221. [CrossRef]
35. Abdalzaher, M.S.; Muta, O. A Game-Theoretic Approach for Enhancing Security and Data Trustworthiness in IoT Applications. *IEEE Internet Things J.* **2020**, *7*, 11250–11261. [CrossRef]
36. Hamdy, O.; Gaber, H.; Abdalzaher, M.S.; Elhadidy, M. Identifying Exposure of Urban Area to Certain Seismic Hazard Using Machine Learning and GIS: A Case Study of Greater Cairo. *Sustainability* **2022**, *14*, 10722. [CrossRef]
37. Abdalzaher, M.S.; Soliman, M.S.; El-Hady, S.M.; Benslimane, A.; Elwekeil, M. A deep learning model for earthquake parameters observation in IoT system-based earthquake early warning. *IEEE Internet Things J.* **2021**, *9*, 8412–8424. [CrossRef]
38. Abdalzaher, M.S.; Elwekeil, M.; Wang, T.; Zhang, S. A deep autoencoder trust model for mitigating jamming attack in IoT assisted by cognitive radio. *IEEE Syst. J.* **2021**, *16*, 3635–3645. [CrossRef]

39. Abdalzaher, M.S.; Moustafa, S.S.; Abd-Elnaby, M.; Elwekeil, M. Comparative performance assessments of machine-learning methods for artificial seismic sources discrimination. *IEEE Access* **2021**, *9*, 65524–65535. [CrossRef]
40. Moustafa, S.S.; Abdalzaher, M.S.; Yassien, M.H.; Wang, T.; Elwekeil, M.; Hafiez, H.E.A. Development of an optimized regression model to predict blast-driven ground vibrations. *IEEE Access* **2021**, *9*, 31826–31841. [CrossRef]
41. Ibrahem, M.I.; Mahmoud, M.; Alsolami, F.; Alasmary, W.; AL-Ghamdi, A.; Shen, X. Electricity Theft Detection for Change-and-Transmit Advanced Metering Infrastructure. *IEEE Internet Things J.* **2022**. [CrossRef]
42. Abdulaal, M.J.; Ibrahem, M.I.; Mahmoud, M.; Bello, S.A.; Aljohani, A.J.; Milyani, A.H.; Abusorrah, A.M. DRFD: Deep Learning-Based Real-time and Fast Detection of False Readings in AMI. In Proceedings of the SoutheastCon 2022, Mobile, AL, USA, 26 March–3 April 2022; pp. 682–689. [CrossRef]
43. Ibrahem, M.I.; Abdelfattah, S.; Mahmoud, M.; Alasmary, W. Detecting Electricity Theft Cyber-attacks in CAT AMI System Using Machine Learning. In Proceedings of the 2021 International Symposium on Networks, Computers and Communications (ISNCC), Dubai, United Arab Emirates, 31 October–2 November 2021; pp. 1–6. [CrossRef]
44. Abdalzaher, M.S.; Moustafa, S.S.; Abdelhafiez, H.; Farid, W. An Optimized Learning Model Augment Analyst Decisions for Seismic Source Discrimination. *IEEE Trans. Geosci. Remote Sens.* **2022**, *60*. [CrossRef]
45. Roth, J.; Chadalawada, J.; Jain, R.K.; Miller, C. Uncertainty matters: Bayesian probabilistic forecasting for residential smart meter prediction, segmentation, and behavioral measurement and verification. *Energies* **2021**, *14*, 1481. [CrossRef]
46. Aslam, Z.; Javaid, N.; Ahmad, A.; Ahmed, A.; Gulfam, S.M. A combined deep learning and ensemble learning methodology to avoid electricity theft in smart grids. *Energies* **2020**, *13*, 5599. [CrossRef]
47. Qiu, Y.L.; Wang, Y.D.; Xing, B. Grid impact of non-residential distributed solar energy and reduced air emissions: empirical evidence from individual-consumer-level smart meter data. *Appl. Energy* **2021**, *290*, 116804. [CrossRef]
48. Brown, J.; Abate, A.; Rogers, A. Disaggregation of household solar energy generation using censored smart meter data. *Energy Build.* **2021**, *231*, 110617. [CrossRef]
49. Hussain, S.S.; Tak, A.; Ustun, T.S.; Ali, I. Communication modeling of solar home system and smart meter in smart grids. *IEEE Access* **2018**, *6*, 16985–16996. [CrossRef]
50. Donaldson, D.L.; Jayaweera, D. Effective solar prosumer identification using net smart meter data. *Int. J. Electr. Power Energy Syst.* **2020**, *118*, 105823. [CrossRef]
51. Chatterji, E.; Bazilian, M.D. Smart meter data to optimize combined roof-top solar and battery systems using a stochastic mixed integer programming model. *IEEE Access* **2020**, *8*, 133843–133853. [CrossRef]
52. Abdalzaher, M.S.; Elsayed, H.A. Employing data communication networks for managing safer evacuation during earthquake disaster. *Simul. Model. Pract. Theory* **2019**, *94*, 379–394. [CrossRef]
53. Ghamry, E.; Mohamed, E.K.; Abdalzaher, M.S.; Elwekeil, M.; Marchetti, D.; De Santis, A.; Hegy, M.; Yoshikawa, A.; Fathy, A. Integrating pre-earthquake signatures from different precursor tools. *IEEE Access* **2021**, *9*, 33268–33283. [CrossRef]
54. Moustafa, S.S.; Abdalzaher, M.S.; Khan, F.; Metwaly, M.; Elawadi, E.A.; Al-Arifi, N.S. A Quantitative Site-Specific Classification Approach Based on Affinity Propagation Clustering. *IEEE Access* **2021**, *9*, 155297–155313. [CrossRef]
55. Elhadidy, M.; Abdalzaher, M.S.; Gaber, H. Up-to-date PSHA along the Gulf of Aqaba-Dead Sea transform fault. *Soil Dyn. Earthq. Eng.* **2021**, *148*, 106835. [CrossRef]
56. Abdalzaher, M.S.; El-Hadidy, M.; Gaber, H.; Badawy, A. Seismic hazard maps of Egypt based on spatially smoothed seismicity model and recent seismotectonic models. *J. Afr. Earth Sci.* **2020**, *170*, 103894. [CrossRef]
57. Hegazy, H.I.; Tag Eldien, A.S.; Tantawy, M.M.; Fouda, M.M.; TagElDien, H.A. Real-Time Locational Detection of Stealthy False Data Injection Attack in Smart Grid: Using Multivariate-Based Multi-Label Classification Approach. *Energies* **2022**, *15*, 5312. [CrossRef]
58. Elwekeil, M.; Abdalzaher, M.S.; Seddik, K. Prolonging smart grid network lifetime through optimising number of sensor nodes and packet length. *IET Commun.* **2019**, *13*, 2478–2484. [CrossRef]
59. Vallent, T.F.; Hanyurwimfura, D.; Mikeka, C. Efficient certificate-less aggregate signature scheme with conditional privacy-preservation for vehicular ad hoc networks enhanced smart grid system. *Sensors* **2021**, *21*, 2900. [CrossRef]
60. Farao, A.; Veroni, E.; Ntantogian, C.; Xenakis, C. P4G2Go: A Privacy-Preserving Scheme for Roaming Energy Consumers of the Smart Grid-to-Go. *Sensors* **2021**, *21*, 2686. [CrossRef]
61. Llaria, A.; Dos Santos, J.; Terrasson, G.; Boussaada, Z.; Merlo, C.; Curea, O. Intelligent Buildings in Smart Grids: A Survey on Security and Privacy Issues Related to Energy Management. *Energies* **2021**, *14*, 2733. [CrossRef]
62. Son, Y.B.; Im, J.H.; Kwon, H.Y.; Jeon, S.Y.; Lee, M.K. Privacy-preserving peer-to-peer energy trading in blockchain-enabled smart grids using functional encryption. *Energies* **2020**, *13*, 1321. [CrossRef]
63. Syed, D.; Refaat, S.S.; Bouhali, O. Privacy preservation of data-driven models in smart grids using homomorphic encryption. *Information* **2020**, *11*, 357. [CrossRef]
64. Dwork, C.; Roth, A. The algorithmic foundations of differential privacy. *Found. Trends® Theor. Comput. Sci.* **2014**, *9*, 211–407. [CrossRef]
65. Manivannan, M.; Najafi, B.; Rinaldi, F. Machine learning-based short-term prediction of air-conditioning load through smart meter analytics. *Energies* **2017**, *10*, 1905. [CrossRef]
66. Hochreiter, S.; Schmidhuber, J. Long Short-Term Memory. *Neural Comput.* **1997**, *9*, 1735–1780. [CrossRef] [PubMed]

67. Gers, F.; Schmidhuber, J.; Cummins, F. Learning to forget: continual prediction with LSTM. In Proceedings of the 1999 Ninth International Conference on Artificial Neural Networks ICANN 99, (Conf. Publ. No. 470), Bristol, UK, 6–9 September 1999; Volume 2, pp. 850–855. [CrossRef]
68. Werbos, P.J. Backpropagation through time: what it does and how to do it. *Proc. IEEE* **1990**, *78*, 1550–1560. [CrossRef]
69. Bengio, Y.; Simard, P.; Frasconi, P. Learning long-term dependencies with gradient descent is difficult. *IEEE Trans. Neural Netw.* **1994**, *5*, 157–166. [CrossRef]
70. Gers, F.A.; Schmidhuber, J.; Cummins, F. Learning to forget: Continual prediction with LSTM. *Neural Comput.* **2000**, *12*, 2451–2471. [CrossRef]
71. Ozay, M.; Esnaola, I.; Yarman Vural, F.T.; Kulkarni, S.R.; Poor, H.V. Machine Learning Methods for Attack Detection in the Smart Grid. *IEEE Trans. Neural Netw. Learn. Syst.* **2016**, *27*, 1773–1786. [CrossRef]
72. Parvez, I.; Sarwat, A.I.; Wei, L.; Sundararajan, A. Securing metering infrastructure of smart grid: A machine learning and localization based key management approach. *Energies* **2016**, *9*, 691. [CrossRef]
73. Babar, M.; Tariq, M.U.; Jan, M.A. Secure and resilient demand side management engine using machine learning for IoT-enabled smart grid. *Sustain. Cities Soc.* **2020**, *62*, 102370. [CrossRef]
74. Esmalifalak, M.; Liu, L.; Nguyen, N.; Zheng, R.; Han, Z. Detecting stealthy false data injection using machine learning in smart grid. *IEEE Syst. J.* **2014**, *11*, 1644–1652. [CrossRef]
75. Wang, B.; Wu, Y.; Liu, K.R. Game theory for cognitive radio networks: An overview. *Comput. Netw.* **2010**, *54*, 2537–2561. [CrossRef]
76. Roy, S.; Ellis, C.; Shiva, S.; Dasgupta, D.; Shandilya, V.; Wu, Q. A survey of game theory as applied to network security. In Proceedings of the System Sciences (HICSS), 2010 43rd Hawaii International Conference, Honolulu, HI, USA, 5–8 January 2010; pp. 1–10.
77. Han, Z. *Game Theory in Wireless and Communication Networks: Theory, Models, and Applications*; Cambridge University Press: Cambridge, UK, 2012.
78. Shi, H.Y.; Wang, W.L.; Kwok, N.M.; Chen, S.Y. Game theory for wireless sensor networks: A survey. *Sensors* **2012**, *12*, 9055–9097. [CrossRef] [PubMed]
79. Zhang, Y.; Guizani, M. *Game Theory for Wireless Communications and Networking*; CRC Press: Boca Raton, FL, USA, 2011.
80. Yang, F.; Zhou, X.; Jia, G.; Zhang, Q. A Non-cooperative Game Approach for Intrusion Detection in Smartphone Systems. In Proceedings of the Communication Networks and Services Research Conference (CNSR), 2010 Eighth Annual, Montreal, QC, Canad, 11–14 May 2010; pp. 146–151.
81. Abdalzaher, M.S.; Seddik, K.; Elsabrouty, M.; Muta, O.; Furukawa, H.; Abdel-Rahman, A. Game theory meets wireless sensor networks security requirements and threats mitigation: A survey. *Sensors* **2016**, *16*, 1003. [CrossRef] [PubMed]
82. Abdalzaher, M.S.; Muta, O.; Seddik, K.; Abdel-Rahman, A.; Furukawa, H. B-18-40 A Simplified Stackelberg Game Approach for Securing Data Trustworthiness in Wireless Sensor Networks. In Proceedings of the 2016 IEICE General Conference (IEICE), Fukuoka, Japan, 17 March 2016; p. 538.
83. Abdalzaher, M.S.; Muta, O. Employing game theory and TDMA protocol to enhance security and manage power consumption in WSNs-based cognitive radio. *IEEE Access* **2019**, *7*, 132923–132936. [CrossRef]
84. Abdalzaher, M.S.; Seddik, K.; Muta, O. Using Stackelberg game to enhance cognitive radio sensor networks security. *IET Commun.* **2017**, *11*, 1503–1511. [CrossRef]
85. Abdalzaher, M.S.; Seddik, K.; Muta, O. An effective Stackelberg game for high-assurance of data trustworthiness in WSNs. In Proceedings of the 2017 IEEE Symposium on Computers and Communications (ISCC), Heraklion, Greece, 3–6 July 2017; pp. 1257–1262.
86. Abdalzaher, M.S.; Seddik, K.; Muta, O. Using repeated game for maximizing high priority data trustworthiness in wireless sensor networks. In Proceedings of the 2017 IEEE Symposium on Computers and Communications (ISCC), Heraklion, Greece, 3–6 July 2017; pp. 552–557.
87. Abdalzaher, M.S.; Samy, L.; Muta, O. Non-zero-sum game-based trust model to enhance wireless sensor networks security for IoT applications. *IET Wirel. Sens. Syst.* **2019**, *9*, 218–226. [CrossRef]
88. 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, 4–6 October 2010; pp. 327–332.
89. Bagaa, M.; Younis, M.; Balasingham, I. Optimal strategies for data aggregation scheduling in wireless sensor networks. In Proceedings of the 2015 IEEE Global Communications Conference (GLOBECOM), San Diego, CA, USA, 6–10 December 2015; pp. 1–6.
90. 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, 4–6 October 2010; pp. 238–243.
91. Rottondi, C.; Verticale, G.; Krauss, C. Distributed privacy-preserving aggregation of metering data in smart grids. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 1342–1354. [CrossRef]
92. Wang, Y.; Raval, N.; Ishwar, P.; Hattori, M.; Hirano, T.; Matsuda, N.; Shimizu, R. On methods for privacy-preserving energy disaggregation. In Proceedings of the 2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), New Orleans, LA, USA, 5–9 March 2017; pp. 6404–6408.

93. Barbosa, P.; Brito, A.; Almeida, H. A technique to provide differential privacy for appliance usage in smart metering. *Inf. Sci.* **2016**, *370*, 355–367. [CrossRef]
94. Ford, V.; Siraj, A. Clustering of smart meter data for disaggregation. In Proceedings of the 2013 IEEE Global Conference on Signal and Information Processing, Austin, TX, USA, 3–5 December 2013; pp. 507–510.
95. Ford, V.; Siraj, A. Applications of machine learning in cyber security. In Proceedings of the 27th International Conference on Computer Applications in Industry and Engineering, Kota Kinabalu, Malaysia, 28 September–1 October 2014; Volume 118.
96. Zhuang, W.; Ye, Y.; Chen, Y.; Li, T. Ensemble clustering for internet security applications. *IEEE Trans. Syst. Man Cybern. Part C (Appl. Rev.)* **2012**, *42*, 1784–1796. [CrossRef]
97. Sedjelmaci, H.; Feham, M. Novel hybrid intrusion detection system for clustered wireless sensor network. *arXiv* **2011**, arXiv:1108.2656.
98. Ren, S.; Chen, D.; Tao, Y.; Xu, S.; Wang, G.; Yang, Z. Intelligent terminal security technology of power grid sensing layer based upon information entropy data mining. *J. Intell. Syst.* **2022**, *31*, 817–834. [CrossRef]
99. Hock, D.; Kappes, M.; Ghita, B. Using multiple data sources to detect manipulated electricity meter by an entropy-inspired metric. *Sustain. Energy Grids Netw.* **2020**, *21*, 100290. [CrossRef]
100. Singh, S.K.; Bose, R.; Joshi, A. Entropy-based electricity theft detection in AMI network. *IET Cyber-Phys. Syst. Theory Appl.* **2018**, *3*, 99–105. [CrossRef]
101. Alnasser, A.; Sun, H. A fuzzy logic trust model for secure routing in smart grid networks. *IEEE Access* **2017**, *5*, 17896–17903. [CrossRef]
102. Batista, E.A.; de Brito, M.A.; Siqueira, J.C.; Dias, J.C.; Gomez, R.C.; Catharino, M.F.; Gomes, M.B. A Multifunctional Smart Meter Using ANN-PSO Flux Estimation and Harmonic Active Compensation with Fuzzy Voltage Regulation. *Sensors* **2021**, *21*, 4154. [CrossRef]
103. Zhou, W.; Ardakanian, O.; Zhang, H.T.; Yuan, Y. Bayesian learning-based harmonic state estimation in distribution systems with smart meter and DPMU data. *IEEE Trans. Smart Grid* **2019**, *11*, 832–845. [CrossRef]
104. Velusamy, D.; Pugalendhi, G.K. Fuzzy integrated Bayesian Dempster–Shafer theory to defend cross-layer heterogeneity attacks in communication network of Smart Grid. *Inf. Sci.* **2019**, *479*, 542–566. [CrossRef]