IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 13, 2021, accepted January 25, 2021, date of publication February 16, 2021, date of current version March 5, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3057525

Avoiding Occupancy Detection From Smart Meter Using Adversarial Machine Learning

IBRAHIM YILMAZ AND AMBAREEN SIRAJ
Department of Computer Science, Tennessee Tech University, Cookeville, TN 38505, USA
Corresponding author: Ibrahim Yilmaz (iyilmaz42@tntech.edu)

This work was supported by the Center for Energy Systems Research (CESR) at Tennessee Technological University with resource support from the Cybersecurity Education Research and Outreach Center (CEROC).

ABSTRACT More and more conventional electromechanical meters are being replaced with smart meters because of their substantial benefits such as providing faster bi-directional communication between utility services and end users, enabling direct load control for demand response, energy saving and so on. However, the fine-grained usage data provided by smart meter brings additional vulnerabilities from users to companies. Occupancy detection is one such example which causes privacy violation of smart meter users. Detecting the occupancy of a home is straightforward with time of use information as there is a strong correlation between occupancy and electricity usage. In this work, our major contributions are twofold. First, we validate the viability of an occupancy detection attack based on a machine learning technique called Long Short Term Memory (LSTM) method and demonstrate improved results. In addition, we introduce an Adversarial Machine Learning Occupancy Detection Avoidance (AMLODA) framework as a counter attack in order to prevent abuse of energy consumption. Essentially, the proposed privacy-preserving framework is designed to mask real-time or near real-time electricity usage information using calculated optimum noise without compromising users' billing systems functionality. The results show that without the use of the proposed AMLODA approach, our occupancy detection attack models using LSTM achieve a high detection rate with Matthews Correlation Coefficient (MCC) value of 0.89 on average for the five different households energy consumption data under investigation captured during the winter and summer seasons. With the proposed AMLODA approach working to protect consumers' privacy, occupancy detection attacks are demonstrated to be mitigated with the MCC values of the attack models converging to zero with no significant change over the actual consumption data and thus protecting needed functionalities of the utility companies.

INDEX TERMS Adversarial machine learning, long short term memory, private information retrieval, privacy, smart meter, smart grid.

I. INTRODUCTION

In modern-day households and businesses, smart meters are being deployed more than traditional meters. For example, approximately 86.9 million smart meters were installed across the United States and nearly 88% of them were deployed into residential buildings in 2018 [1]. This number is expected to increase substantially in the coming years. While old-fashioned analog meters allow company employees to read users' electricity consumption data manually on a monthly basis, fully digitized smart meters can continuously measure and report the energy consumption to the utility providers as needed without direct human intervention. Such detailed and timely energy usage information offers numerous advantages to both grid participants and utility companies. On the utilities side, benefits of smart meters include the elimination of manual meter reading once a month, tracking of the electric system constantly to minimize power outages, energy savings and so on [2]. Furthermore, on the users' sides, benefits of smart meters include monitoring of the users' electricity usage pattern in a timely manner, which allows users to keep track of their energy consumption in real-time or near real-time. This results in robust demand response systems that allow customers to save money by consuming less energy during peak hours and selling excess energy to the grid provider [3]. For these and other benefits,

The associate editor coordinating the review of this manuscript and approving it for publication was Ahmed M. Elmisery.

it is expected that conventional meters will be largely superseded by smart meters globally in the near future.

With all technological advances, there are risks and the same is true for the Smart Grid (SG). The collection of information at a high granularity (e.g., minutes or seconds) inevitably provides utility companies insight into the private lifestyles of its inhabitants. This sensitive information can be sold by utility companies to interested external parties to get market in the industry or for other subsidiary revenue. It can also accidentally or wrongfully fall in the hands of unauthorized individuals through eavesdropping and other adversarial means. Such unintended information extracted from electricity usage profiles can expose the lifestyles and habits of households. This time-of-use information can later be used for a broad range of purposes and nefarious intentions such as advertising or surveillance. For example, it can be used to deduce how often an occupant is on vacation each year and thus, the occupant may be exposed to advertisement bombardments from travel agencies. Or analyzing home power signatures can help companies identify its occupants' meal habits which can, in turn, make the household target for food companies.

Many researches have highlighted this invasion of privacy concerns by demonstrating identification of occupants' activity by analyzing energy consumption data [4]–[9]. Some researchers even identified the appliances being used by employing Non-Intrusive Load Monitoring (NILM) techniques on energy usage data [10]–[13].

Although the aforementioned researches establish security and privacy concerns with the advanced metering infrastructures, existing smart grid regulations are inadequate in protecting customers against misuse of their private data. State legislators and public utility commissions do not have any standard codes of conduct in place to prevent proprietary information collection. In Europe, data privacy is put under protection by the European Union Data Protection Directive, where it is clearly articulated that "*personnel data which is collected for specified purposes can not be further processed for other purposes*" [14]. Any personal data that is collected can only be analyzed with users' explicit given consent. However, users do not have extensive knowledge about for what purposes their information is used and, mostly, they are not well informed about potential privacy consequences. As a result, they are likely to rubber-stamp any such requests from a utility personnel unconsciously. Furthermore, although such legislations might be necessary from a privacy point of view, legally protected data can hinder crucial investigations such as police investigation of a crime or investigation after security incidents [15]. On the other hand, in the United States, privacy regulations with regard to personal data protection vary from state to state. In some states, privacy information is put under protection by law as in Europe, whereas in other states, there is no explicit specific legislation related to this matter [14]. Under some local jurisdictions, such enforcement activities are approved as legal. For instance, law and enforcement agencies taking advantage of monitoring the electricity consumption information on the purpose of catching marijuana or drug manufacturer in Texas since such activities consume remarkable signature electricity [16].

While lawmakers continue to revisit and update regulations regarding the protection of the smart meter consumers' rights, we consider solving this challenge through technological advances by developing a new design with aid of artificial intelligence (AI) that inherently preserves privacy. In this work, we present a privacy preserving AI model that conceals time of use information of consumers without hindering any of its utility. The proposed model tracks electricity usage signal of a user using a machine learning model and identifies the characteristic behavior of flow information from past experience. Actual energy consumption patterns are modified slightly per second through optimized noise, which is obtained from observation, and the process still allows all necessary usage of smart metering data. As a result, the electricity supplier gains no useful knowledge other than the total electricity usage of its customers. As shown in Figure 1, users' private information is masked through designated noise in a way that makes it harder to infer usable information about a household.

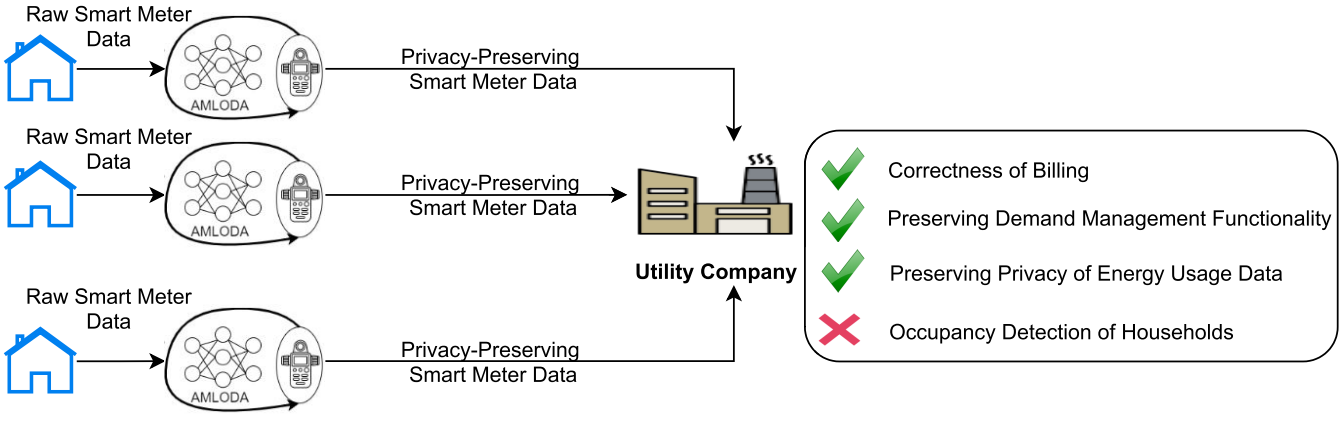


FIGURE 1. Overview of AMLODA model approach for privacy preservation of energy usage data.

It is important to note that machine learning techniques are inherently computationally expensive because of the requirement of training time to build a model [17], [18]. However, in our approach, we pre-train the model offline before we use it with test data in real-time. This allows it to avoid heavy computation in building the model and results in low computational complexity and little or no transmission latency in time-critical traffic. In addition, the new proposed approach allows easy installation and rapid adaptation to existing smart metering infrastructure, taking the SG environment to a higher level of user privacy-preserving.

II. RELATED WORK

Many studies focused on measuring and analyzing the electricity consumption of households over the past years. These investigations addressed various aspects like the estimation of socio-economic characteristics of homeowners [19], whereas some tried to place them in groups by their load data [20], [21]–[23]. De Silva *et al.* looked into smart meter data and came to the conclusion that the energy companies can predict future energy consumption by examining the data that is measured from occupied households [24]. Therefore, there is a high probability for the energy companies to differentiate between houses that are vacant and those that are occupied during different times of the day. These houses that are identified as occupied are good candidates to receive special offers like automatically getting their heater switched off when they are not at home.

Additionally, due to machine learning algorithms demonstrating effectiveness in tackling many complex problems, some of these methods are also used to detect occupancy of a home. Conditional Random Field Model and a Hidden Markov Support Vector Machine (HMSVM) were used by Yang textitet al., for estimating the number of occupants in a three person residence by using smart meter data [25]. There are other studies that employed various metrics to detect occupancy. An important study used sound, temperature, CO2, and PIR motion sensors data with a neural network model and their reported accuracy was as high as 75% [26]. Akbar *et al.* used smart energy meters to calculate electricity consumption in their research center from the devices on employees' work desks [4] and their accuracy was reported around 94%.

Consumers' electricity usage was discussed from a privacy point of view by some other researchers. One group addressed the problem of identifying different types of appliances from their energy usage at a given time. Similar studies do not inherently aim to detect occupancy of a home but their results can be used to help with the detection of occupancy. George Hart proposed the first time Non-Intrusive Load Monitoring (NILM) approach in 1992 [12] and his method differentiated characteristic changes in the consumption of energy. He then went on to compare these changes with previously recorded values stored in a database. His findings showed that time of use smart metering data leak users' sensitive information. Since then, securely handling consumers' information during the smart meter data management process has been attracted by many researchers. We can categorize these solutions into two groups.

The first one is cryptographic-based privacy-preserving solutions, where smart meter data is encrypted and decrypted with users' keys in order to prevent any unauthorized access to sensitive information [27]–[30]. This type of solution provides confidentiality over data-in-use. In other words, it provides a secure communication channel between consumer and providers in order to protect smart meter data transmission from third parties. However, in a real-word scenario, providers or utility companies behave more like *honest-but-curious attackers* [31]–[33]. To put it all in simple terms, electricity suppliers abide by protocol rules but they can leak the private information of users. Therefore, users' sensitive information has to be secured from, not only the external threat actors, but also internal entities in a smart grid environment. For these reasons, a solution based on cryptography is not an effective solution where utility companies are not considered part of the problem. The second category of solutions aims to protect data itself from electricity providers. One such naive solution is the data aggregation method through a third party [34]–[36]. These solutions offer an escrow mechanism for data collection by smart meters and deliver aggregated data to the necessary operational unit at regular intervals. This escrow system makes out an invoice for each customer and keeps their private information confidential. This method assumes that third parties are fully trusted. However, a 'trusted third party' concept solely passes over trust assumption from utility companies to an intermediary. Users' privacy is always subjected to the mercy of the intermediary with this technique. In the absence of trust, this method is impractical. It should be noted that data aggregation service can be performed by an Advanced Metering Infrastructure (AMI) system itself. Since AMI is managed by utility companies, this is still conceptually similar to the *honest and curious attacker* models, therefore, it is not sufficient to provide necessary security safeguard with respect to user privacy.

To mitigate the aforementioned limitation of data aggregation method, some researchers proposed complex load data aggregation schemes utilizing cryptographic methods for protecting users' private information from both the grid operator and the aggregator itself. Borges *et al.* [37] presented a privacy-preserving protocol that offered data aggregation with secure and verifiable billing. To preserve customers' privacy, measured data is encoded with homomorphic encryption or homomorphic commitment. Afterwards, energy consumption data is securely aggregated for protecting individual privacy before it is sent to the utility company. Tonyali *et al.* [38] looked into the feasibility and performance of homomorphic encryption aggregation in AMI networks and showed that homomorphic cryptography is inefficient in terms of delay and bandwidth usage. Therefore, Borges *et al.*'s approach can create a high computational burden on resource-demanding smart meters. Furthermore, the approach was not validated with proof-of-concepts and

experimental simulations, and thus, it is hard to study its benefits properly. Mármol *et al.* [39] presented a privacy enhancing aggregation architecture which allowed the aggregator to successfully receive total consumption of smart meter data in a protected way. In this approach, each smart meter encrypts its own consumption using a key and the electricity consumption of the group of users is aggregated using a ring-based topology ensuring that the aggregator obtains the integrated data in an encrypted form without compromising individual's privacy. Afterwards, the aggregator can decrypt the total meter readings of the all the users with a single static key. This approach creates a high level of complexity because of usage of the homomorphic encryption scheme, which also doesn't provide non-repudiation since asymmetric encryption is involved. Additionally, this architecture has adaptability issues because a reconfiguration is required when a node joins/leaves the network. Another drawback of this scheme is low scalability as a high number of smart meters are linked directly to the latter. This situation imposes high overhead on the utility side because they have to perform a large number of aggregation operations. Erkin *et al.* [40] proposed a modified Paillier (additive) homomorphic aggregation scheme allowing any user to additively aggregate total energy consumption for all users for each agreed time slot. In addition, the method offered random numbers to be added into all individual readings to keep information secure from other users. Decryption can only be possible after the computation of all individual consumption such that any user is not able to decrypt load data for others. However, there are a lot of interactions among smart meters which leads to heavy communication overhead. Also, the proposed protocol assumes that a trusted third party generates all the necessary parameters such as keys and modulii in the set-up phase and requires a secure channel to be established between each pair of smart meters in the initialization phase. Also, the proposed method cannot detect fraudulent individuals from malicious aggregators in the system. A single point of failure during the uploading process of the data makes the scheme impractical. Kursawe *et al.* [41] suggested an innovative scheme for privacy-preserving aggregation using Diffie-Hellman and a Biliniear-map based protocol instead of homomorphic encryption. In this method, each participating set of smart meters conceal their measured consumption from the aggregator by adding random numbers, which cancels out when added together. In this way, aggregator can obtain total consumption of participating smart meters without revealing any additional information about individual smart meter usage. The authors showed that their proposed protocol improved efficiency compared to a homomorphic solution in terms of communication overhead. However, this mechanism requires a complex reinitialization process when a smart meter joins or leaves a group. This can negatively impact the protocol's performance when the public keys of all other smart meters in the group have to be initialized at the same time. Although the authors mention existence of signature keys to provide data origin, there is no detail on how the protocol assures non-repudiation. Knirsch *et al.* [42] presented a masking-based scheme for a privacy-aware data aggregation. This approach employs the notion of homomorphic hashing in order to confirm the correctness of the shared secrets. Nevertheless, this strategy has a few issues. The technique are complicated to implement and the data aggregation approach using hash is vulnerable to collusion attacks. Therefore, an aggregator can collude with a smart meter to figure out consumption data of another smart meter, which is undoubtedly an important privacy concern. While the above mentioned data aggregation models with cryptographic primitives provide strong protection of the privacy of consumers, these privacy models work under the assumption that security models have desired security properties. There are multiple challenges with these security models. First of all, cryptographic keys have to be securely created. Then, keys have to be securely distributed to all parties which is not an easy process. Security models always offer a solution based on the assumption that keys have safe storage and the adversary has limited computational power. Stolen or hacked private keys can lead to a loss of privacy of consumers and billing accuracy of users. Our proposed AMLODA model uses optimum noise added to or subtracted from the meter data such that the adversary receives scrambled data without using any cryptographic keys. To balance between operational efficiency and customer privacy, the AMLODA model provides an alternative solution as a trade-off between the noise and the leakage of privacy. In addition, utility companies may prefer individual load profile of users rather than aggregated one for delivering various beneficial services such as improving detection of energy theft, fair distribution, virtualization of power consumption of users and so on. For example, a smart meter might behave as an attacker by hacking another smart meter by tampering of its reading. Such fraudulent behavior cannot be recognized easily over aggregated data, since no suspicion can arise due to no change in the aggregate mean consumption [43]. The collection of electricity consumption data of grid users on a regular basis can help energy suppliers to detect and identify electricity theft [44]. In addition, high-frequency energy usage measurements of individual users help utility companies to track and manage their energy efficiently. For example, utility companies can identify high rate of consumption approaching by analyzing regular granular load data and alert consumers accordingly -a process known as consolidated consumption [45].

Another approach is anonymizing smart metering data for each individual participant by hiding their real identity against electricity providers [46]–[48]. In the context of anonymity, a user must be undetectable [49]. However, such a technique is still inadequate in hiding grid users' personal information because it still streams significant information to the utility providers [50]. For instance, electricity providers can still access electricity consumption information and infer grid users' identities from this auxiliary information. Additionally, these data aggregation and anonymizing smart metering data techniques benefit from cryptographic primitives in order to establish a secure channel. Therefore,

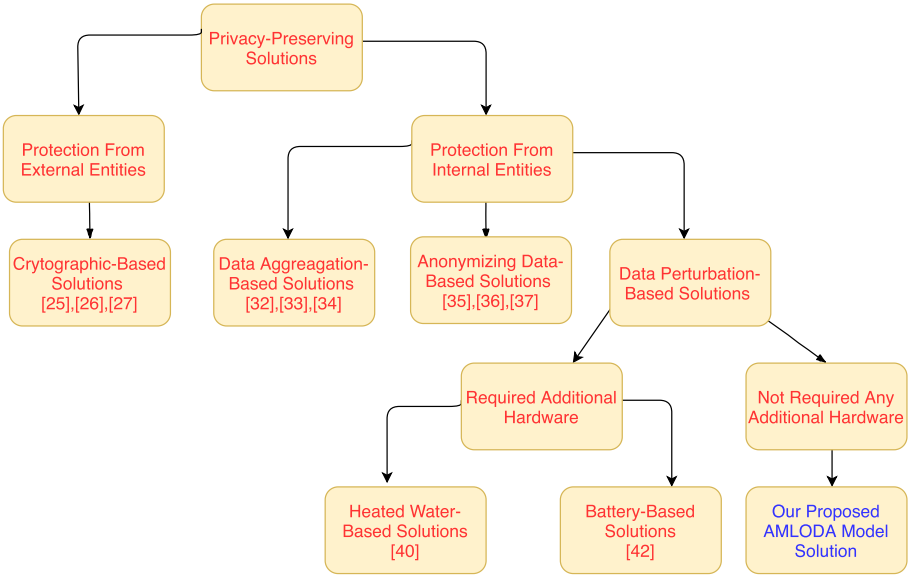


FIGURE 2. A tree diagram of privacy-preserving solutions.

this is the cost of high overhead because of intensive computational power, which poses additional operational challenges on the resource restrained SG environments.

A. CONTRIBUTIONS

Our privacy-preserving solution is obfuscation based and uses data perturbation without data aggregation approach or having to trust any institution. Data perturbation is not a new idea and has already been proposed for ensuring user privacy by a few researchers. Dong *et al.* [51] proposed a heated water-based technique to make users' electrical power routing flat at the highest consumption point by tampering with smart metering data. Flat signals make it look like an occupant is always at home. Implementation of this technique is very challenging with no knowledge of future users' consumption in the absence of sufficient thermal storage, especially when the difference between the highest and the lowest point of the signal is great. In addition, not every household supports electric water heaters. As per a survey, approximately half of the families in the US have natural gas water heater systems at their residences, while 41% have electric water heater systems [52]. The implementation of the electric water heater system is also impractical because converting natural gas heater systems to electric water heater systems is expensive. Man *et al.* [53] proposed a battery-based technique to make the electricity signal flat in a similar way by defining a threshold point while charging or discharging this external battery. However, batteries are costly and they deplete after extended use. Furthermore, defining a threshold value is challenging, especially without knowledge of user electricity consumption patterns. The success of the battery-based solution is highly dependent on storage capacity and sometimes storage capacity may not be enough to implement this algorithm. Another point to consider is that SG environment is designed to generate revenue by scheduling of electricity as per demand response. A significant change with a flat rate will produce a negative impact on the demand response market. Both of the aforementioned solutions do not take into consideration this important fact.

To alleviate these concerns and maintain system reliability with consumer privacy preservation, we propose a novel method that integrates well with current smart metering infrastructure with any changes at the infrastructure level. Our unique privacy framework also does not require any hardware change on the smart meter. The only change it necessitates is a small software change to the program running on the smart meters. The proposed add-on functionality can simply be incorporated as a software update. Figure 2 shows the distribution of schemes along with proposed AMLODA model for privacy-preserving security solutions.

As mentioned before, our proposed method is based on a data perturbation technique by means of noise injection. In order to inject noise in an intelligent way, the model initially aims to learn users' energy consumption profile patterns from their past electricity usage. Then, these usage patterns are used to calculate optimum noises in order to modify the consumers' current usage information in the shortest period of time in a cost-effective manner that preserves overall data integrity. These modifications lead to 'data-obliviousness', a term that is used in the research community [54] to designate no obvious learning of new knowledge from the pattern of the operations. In our case, it means that users' energy consumption is presented in such a way that electricity providers are unable to learn any usable information other than what is needed for billing. Thus, our proposed model preserves information needed for meaningful interactions between consumers and providers that is crucial for SG environment economy. This solution empowers SG users to monitor and control their energy savings by accessing their own data as needed. Most importantly, consumers are able to control a

level of influence over their smart meter data that best meets their privacy-preserving needs. As stated previously, our proposed model reports households' energy consumption in a way that does not affect the correctness of the billing invoice. In addition to properly managing energy usage data with users' privacy preservation, the model also prevents timing analysis for a possible occupancy attack. Thus, the proposed model presents a win-win situation for both utility companies and smart meter users.

To the best of our knowledge, this paper presents the first research that demonstrates an effective and efficient obfuscation-based privacy preserving solution that does not rely on any external devices/entities for maintaining consumers' privacy. Our research has the following contributions:

- Using LSTM, we show the viability of an occupancy detection attack over a massive real-world electricity consumption dataset.
- We propose a non-intrusive automatic method for protecting the privacy of grid customers with the extension of the meter program functionality. Our method works by allowing self-coordination and self-healing through false data injection in smart meter data. Carried out in a trustworthy manner, with rearrangement of users' electricity consumption data over a period, the added noise does not compromise the correctness of users' billing, while preserving privacy.
- We propose a client-driven system that allows them to govern their own data with the aim of fulfilling their privacy needs.

The rest of this paper is organized as follows: the background relevant to occupancy detection attacks is reviewed in Section III. We present the proposed model in Section IV. Section V describes the implementation and the evaluation results of our model. In conclusion, we finalize the paper in section VI.

III. BACKGROUND

In this section, we review background information related to our research.

1) SMART METERING DATA

Utility companies have a need to better understand consumers' usage profiles for operational reasons. More detailed energy usage information supports more efficient energy management services. Therefore, SG technology was designed to collect information more widely and quickly than its predecessors. Such information is vital for operational efficiencies such as automatic billing, load monitoring and dynamic pricing.

Smart meters report information every fifteen minutes as a default [16]. New brand meters are capable of collecting data every minute or second by increasing data storage capacity. Time-of-use tariffs might change from minute to minute. Hence, the more precise data is, the more accurate calculations for customers' billing can be made to assist grid managers. In addition, the fine-grained usage data is useful for monitoring customers' loads in more detail. This helps to forecast future load needs in order to cover all users' demands. However, as stated previously, this time of use data can conflict with security and privacy goals of users. This information can be used malevolently for other purposes than intended. For example, smart meter data at frequent time intervals provides insight into customers' eating habits or sleep/wake circles. Because of this double-edged sword, the expected data frequency of smart metering could not be standardized. Each utility company has slightly different types of the metering system. As a remedy of this problem, we propose to intercept smart meter readings in order to mask critical information without worsening its operational efficiency. As a result of our proposed approach, both grid providers and grid participants can take advantage of smart grid benefits with ease.

2) DEMAND RESPONSE MANAGEMENT

Demand Response Management (DRM) is a key component to improve the efficiency of energy consumption of grid users economically in an automated manner. DRM records a large range of information such as the real-time price of electricity and net demand. This helps to properly optimize customers' demand by shifting demand to off-peak hours considering dynamic pricing with customers permission. For example, the temperature at the thermostat can be controlled by the utility server and set automatically to a lower temperature setting during the period of high prices.

Any significant changes to data that DRM uses can cause operational inefficiency. Accordingly, we follow a reasonable strategy by manipulating smart meter data to safeguard consumer privacy in a way that is compatible with the metering price and demand prediction policies.

3) GRADIENT DESCENT ALGORITHM

The gradient descent algorithm, which is widely used by various machine learning models, is a first-order iterative optimization technique. It is used to find an optimal point of a given function that helps to minimize error rates. This algorithm modifies all parameters to find the most appropriate way to minimize errors. The parameters are randomly initialized at the beginning of the process. Then the cost function is calculated based on these parameters. During the backpropagation phase, the parameters self-update until the lost function converges to the minimum point.

The perturbed version of the time series energy data produced by the exploiting and modifying the gradient descent algorithms behavior can help to prevent unauthorized disclosure of private information. Section IV will explain how we used this algorithm to control the privacy of users in their energy usage data.

4) LONG SHORT-TERM MEMORY (LSTM) MODEL

The Recurrent Neural Network (RNN) is a neural sequence model successfully used for the processing of sequential

data such as handwriting recognition, speech recognition, language modeling, machine translation, among others [55]–[59]. The architecture of RNNs consists of internal state (memory) to store historical data. The model considers this past contextual information along with current input to make a better decision for further timestep predictions. The learning process is carried out based on computing the gradient of a loss function in terms of the weights of the model during backpropagation. However, the model has access to limited contextual information because of its limited storage capacity, a phenomenon known as the vanishing gradient problem [60].

In order to mitigate the vanishing gradient problem, an elegant RNN, known as LSTM was designed [61]. LSTM relies on gating mechanisms that regulate the flow of information. These gates are able to learn which data in a sequence deserves to be kept or discarded, based on its importance. By doing that, LSTM allows remembering information for an extended number of timesteps (up to 1000). Due to its learning capacity of long term dependencies present in long sequences, LSTM has received a great deal of attention in the research community for its solution of time series prediction problems.

IV. AVOIDING OCCUPANCY DETECTION

In the following subsections, we first describe the proposed scheme. We then present another straightforward solution based on Gaussian noise perturbation as a benchmark to compare with the proposed model.

A. AMLODA MODEL

As outlined earlier, we assume a scenario where the utility companies behave like *honest-but-curious attacker* models, meaning that they follow the protocol rules but compromise user privacy. To prevent such a scenario, we propose the Adversarial Machine Learning for Occupancy Detection Avoidance (AMLODA) model inspired by [62]. The AMLODA model learns by capturing the most prominent features of occupancy detection from historical usage data. For example, a significant change in the power consumption is a good indicator of the interaction of an occupant. Such special movement patterns are automatically acquired by the system. Our proposed scheme then generates indiscernibly small carefully crafted perturbations to hide the electricity consumption patterns. Therefore, manipulated smart meters' data reveals less useful information and occupancy detection attack classifiers would likely work less accurately when predicting sensitive user behavior patterns.

Typically machine learning algorithms use cost functions by model parameters in order to penalize any predictions that are far from the correct label. The models are trained using the gradient descent algorithm to find the model's optimum parameters by minimizing the cost function. The idea behind the proposed novel framework is to find adversarial directions that can lead to misclassifications [63], [64]. Adding or subtracting subtle computed noises in the same direction of the gradient descent of the cost function of the pre-trained model based on LSTM, allows it to maximize the cost function, instead of minimizing it. By doing this, we are able to assign modified electricity consumption data with minimal changes to the incorrect labels with high confidence from the machine learning models. The reason to exploit the gradient descent to generate oblivious samples is that without a good gradient, the loss function cannot be successfully optimized. Mathematically speaking, we wish to solve the following optimization problem:

$$objective\ max\ c(M, \hat{x}, y) \tag{1}$$

$$y \neq \hat{y} \tag{2}$$

$$subjectto\hat{x} = x \pm \delta_x \tag{3}$$

$$\delta_x \leq \gamma.|x| \tag{4}$$

In the above equations, let M be our pretrained model, x represents electricity usage of users for a given time interval and y represents the corresponding ground-truth output label (occupied or unoccupied) of each x value. $C(M,\hat{x},y)$ is the cost function used to train occupancy attack models and γ is the level of perturbation. $\hat{x}$ is the manipulated smart meter data which is crafted by our proposed AMLODA model at the given time and $\hat{y}$ is the prediction of the model given $\hat{x}$.

The aim is to maximize error in (1) and if our proposed solution succeeds, the equation in (2) must be true. In addition δx in (3) denotes perturbation added or subtracted to the original power consumption data. The magnitude of this perturbation should be equal or less than γ as constrained in (4). δx is computed as follows:

$$\delta_x = \epsilon\ sign(\nabla_x c(M, x, y)) \tag{5}$$

where ∇_x c(M,x,y)) is the gradient descent of the cost function. We compute the gradient of all smart meter data at each time slot for the finding calculated perturbation. The ∇ operator is a derivative of a function according to its parameters and ϵ is the penetration coefficient. $Sign(\nabla_x c(M,x,y))$ is the direction of minimizing of the cost function of the pretrained model and ϵ controls the penetration magnitude.

To visualize, we draw a scenario in Figure 3, with squares representing occupancy of a home and circles representing the vacancy of a home at a certain time interval. An occupancy attack model plots the data in feature space for class prediction. For data that is close to the boundary, the decision is predicted correctly by the attack model as unoccupied. After adding subtle perturbation by gradient descent, the same model predicts the same data incorrectly as occupied.

It should be noted that a large perturbation to the data could lead to substantial changes in load patterns and hence it can have a detrimental impact on DRM's performance. Hence, finding the optimum minor perturbation is of vital importance to carry out privacy-preservation of users' information without compromising the operations of the utility. Therefore, we set the epsilon to very small numbers. As it can be seen from Figure 4, when we set the epsilon value to 0.0001,

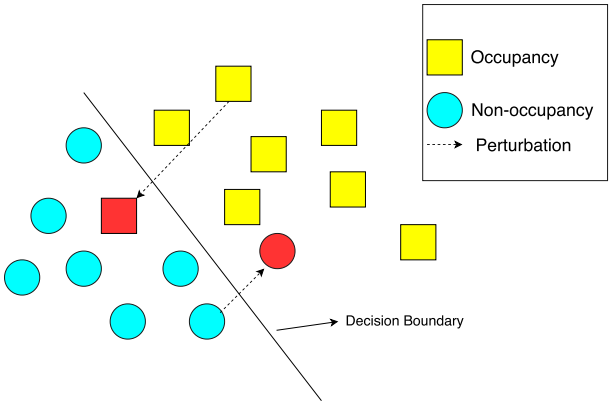


FIGURE 3. AMLODA counter attack scenario.

Time Interval	Original Electricity Consumption	Perturbed Electricity Consumption
'02:21:00'	6.578530	6.331495
'02:21:01'	110.676003	110.923035
'02:21:02'	4.440550	4.193515
'02:21:03'	31.981501	32.228535
'02:21:04'	4.332490	4.085455
'02:21:05'	0.000000	0.247035
.	.	.
.	.	.
.	.	.

FIGURE 4. Energy usage of a house for secondly time interval with epsilon value 0.0001.

the original data is corrupted slightly, which is statistically insignificant. Therefore, with its negligible impact, DRM services are not disrupted. It should also be pointed out that the AMLODA model will not work for a home, that is not being used for a long time such as a vacation home.

Note: Before the proposed AMLODA modeling algorithm runs, a pre-trained model needs to be built with historical consumption metering data and we can assume that a trusted third party will be responsible for this task. This third party will be no longer needed after the model is implemented.

In order to develop the pre-train model, the trusted third party will need to have the consumption data and ground-truth information of some users for several days. For this, the trusted third party can select a set of customers with different load profiles based on incentivized voluntary agreements. Each individual profile can be categorized based on energy consumption and used to create a diverse set of systematic load profiles.

To collect ground-truth occupancy information of participants, the trusted third party can install additional devices [65] at the participants' households with their permission. This will help to build realistic generic profile of customers of different behavioral patterns. However, due to the additional costs and efforts of planting these additional devices in residential homes, unsupervised learning approaches can be used as well to label the dataset as occupied or unoccupied at each time interval [66]. Using consumption data and ground-truth information of the participants, pre-train models can be tailored to any related load profile groups and provided to the utility companies. When a new user signs up to use the AMLODA model for privacy preservation, the utility company matches the user to a specific profile and pre-train model based on their responses to a set of screening questions and then, the proposed algorithm retrieves the pre-train model of this profile for this user. Once the AMLODA model is in use, the system can adapt more closely to the specific usage pattern of the particular user. This process is shown step by step in Figure 5.

The trusted third party can introduce the AMLODA model as new business model and provide the service to the utility companies for commercial purposes. Also, our privacy-friendly solution is both realistic logistically and economically feasible and therefore smart metering manufacturers can consider it as an investment tool to strengthen consumer privacy and trust.

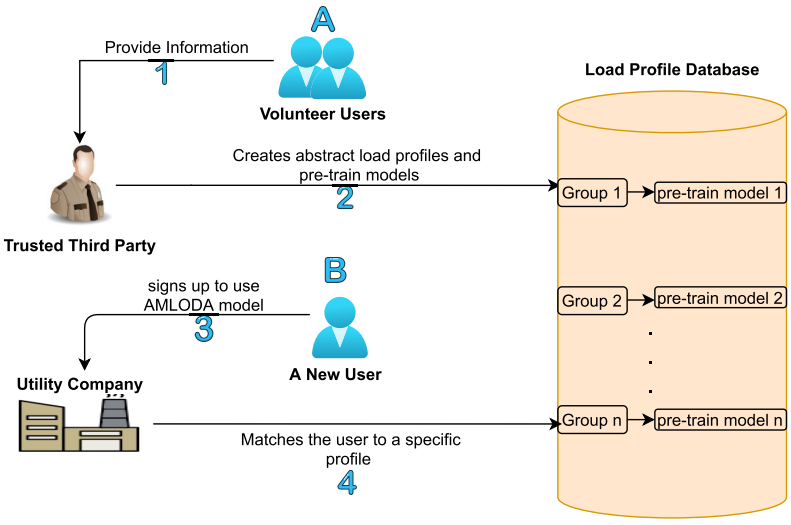


FIGURE 5. Collecting ground-truth occupancy information and developing pre-train models scenario.

Note: For the sake of simplicity, we use publicly available dataset which contains both residential electricity usage and ground truth occupancy information. The detail information regarding the dataset is provided in Section V-A.

The AMLODA model is designed in a way that conceals instantaneous energy usage, not a long term period. Due to this property of the system, it does not interfere with the utilization of the original characteristic patterns found in the consumers' power usage for various beneficial purposes. For example, electricity theft can be detected by identifying abnormal changes in the long-term consumption of electricity.

It is important to note that this attack scenario using a machine learning model can be regarded as a black-box in real-world settings. In this black-box scenario, we have zero knowledge about a target model's internal workings. However, for the sake of simplicity, we implement our proposed technique under the white-box assumption, where we obtain optimum perturbation by accessing the target model in order to compute gradients. Although the black-box assumptions can be perceived as more realistic for this work, it should not be forgotten that previous works proved that adversarial samples have *transferability property* [67]–[69]. This means that an adversarial example generated for one occupancy detection model is more likely to be misclassified by another machine learning model as well, because when different machine learning models are trained with the same data distribution dataset, they learn similar decision boundaries. Therefore, in this research study, we have shown a successful generation of less privacy-related samples using data perturbation techniques under the white-box assumption. We leave testing adversarial examples under the black-box settings for future work. We hope that our method establishes a strong baseline for further research.

Preserving of total energy consumption of users: When it comes to not compromising users' billing systems' functionality, we use the calculated noise to raise and lower the consumption energy identically every two seconds so that the positive and negative manipulation cancels each other out. Thus, there is no net change in users' power consumption for the two second period. Also, since in reality energy consumption of a household cannot be negative, when we implement the model, we take this into consideration. This strategy is implemented in the following manner:

$$\hat{P}_t : \begin{cases} = P_t - n_t, & \text{if } P_t \geq n_t \\ = P_t, & otherwise; \end{cases}$$

$$\hat{P}_{t+1} : \begin{cases} = P_{t+1} + n_t, & \text{if } P_t \geq n_t \\ = P_{t+1}, & otherwise; \end{cases}$$

In the above equation, let P_t, $\hat{P}_t$ denote actual and perturbed power consumption data of a user respectively at any time slot t. 'n_t' represents calculated noise at time t. Calculated noise are estimated every other time. If actual consumption value is higher than the calculated noise at time t, consumption value is subtracted from the calculated noise, otherwise, no change takes place. The same perturbation value is added to the next consumption value at t+1. This process is repeated every two seconds. Therefore, the proposed scheme always guarantees that the total energy usage that the utility companies receive for the their customers will be equivalent to the actual usage by customers. In Figure 6, we can see that the total energy consumption remains unchanged for a one day period with our proposed scheme.

Algorithm 1: Pseudocode of Our Proposed Approach in Order to Produce Oblivious Data

```
Input:
- Train data pair {x_i, y_i} where x_i = Smart meter data
  at each time slot and Y_i = Corresponding
  ground-truth label
- Training iteration number N_itr, Number of
  manipulated examples N_adv, Number of training
  samples N_train
- Test data pair {x_j, y_j}
Function generate oblivious data
    for iteration = 0, ..., N_itr
        Update all parameters based on gradient
         descent algorithm
    end
    for iteration = 0, ..., N_adv
        for iteration = 0, ..., N_train
            δ_xi = ϵ × sign(∇_xi l(M, x_i, y_i))
            # Calculate penetration for each time slot
            if x_i > δ_xi
                x̂_i = x_i − δ_xi;
                x̂_i+1 = x_i+1 + δ_xi;
            else
                continue;
            end
            # Generating oblivious samples to avoid
             detection
        end
    end
    Output: X̂    # Generating oblivious samples for
     each time slot to avoid detection
end
```

For convenience, the outline of the this algorithm is given in Algorithm 1.

Design of a Privacy-Preserving Billing Policy: Energy companies apply various tariff policies for their customer service such as time-of-use pricing, variable peak pricing, peak-load pricing and so on. Our propose algorithm supports different smart metering tariffs while providing maximum privacy. In this study, we investigate how the proposed scheme meets the requirements of time-of-use (TOU) and the peak-load pricing (PLP) tariff structures which are two most commonly used tariff plans by service providers.

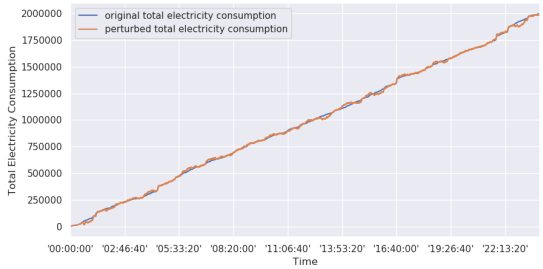


FIGURE 6. Comparison between original total energy consumption with perturbed one from our dataset with epsilon value 0.1.

1-) *TOU Pricing Tariff:* This electricity consumption rate plan allows energy providers to charge their customers for amount of energy based upon time of energy usage. In this policy, time is split into the frames and each frame has different price rate. The customer's electricity cost is calculated with TOU as follows:

Assume that the day is divided into the n different rates, denoted by a vector form of T. Then $\vec{T} = (t_1, t_2, \ldots, t_n)$. $\vec{M}$ represents the actual total consumption measurement at each time frame, where $\vec{M} = (m_1, m_2, \ldots, m_n)$. With knowledge of T and M, the utility company can calculate the result of the price function as:

$$P(\vec{M}, \vec{T}) = \sum_{i=1}^{n} t_i * m_i$$

With AMLODA model, let $\vec{\hat{M}}$ be the perturbed version of the electricity consumption that is generated by our proposed algorithm, where $\vec{\hat{M}} = (\hat{m}_1, \hat{m}_2, \ldots, \hat{m}_n)$.

$$\text{if} \quad T = 2\,i \quad \textit{then} \quad P(\vec{M}, \vec{T}) = \hat{P}(\vec{\hat{M}}, \vec{T})$$
$$\text{because} \quad \vec{M} = \vec{\hat{M}} \quad \forall i$$

In the above equation, i is an arbitrary number. If service provider selects time intervals for the pricing rate as a multiple of two seconds, the proposed model does not compromise the correctness of users' billing as shown mathematically by the above equation.

2-) *PLP Tariff:* According to this tariff, price mechanism is arranged based on either the time of the day or customers' electricity consumptions. PLP tariff based on the time of the day is calculated the same way as TOU tariff cost estimation explained above. In this case, customers pay more for electricity consumed during peak times compared to off-peak times. As is proven above, our proposed method supports a time-based tariff. On the other hand, PLP tariff can be implemented based on consumers' energy usage. In such cases, the consumption usages are split into certain intervals with price differentiations. Electricity usage during high load can be penalized more than electricity consumption at low load. Therefore, this tariff is used with the aim of protecting peak demand. Price function at time slot t is calculated in the following equation.

$$p(m,t) = \begin{cases} m * p_1(t) & \text{if } m < k_1 \\ m * p_2(t) & \text{if } k_1 \le m < k_2 \\ . \quad . \quad . & \\ . \quad . \quad . & \\ m * p_n(t) & \text{if } k_n \le m \end{cases}$$

where k_1, k_2,.. k_n are different threshold values that is defined by utilities whereas p_1, p_2, .. p_n are different price rates of the interval the consumption falls into. The total cost for the consumer is calculated for the billing period as follows:

$$P(\vec{M}, \vec{T}) = \sum_{i=1}^{n} p_i(m_i, t_i)$$
$$\text{if} \quad T = 2i \quad \text{then} \quad P(\vec{M}, \vec{T}) = \hat{P}(\vec{\hat{M}}, \vec{T})$$
$$\text{because} \quad p_i(m_i, t_i) = p_i(\hat{m}_i, t_i) \quad \forall i$$

As a consequence, we verify that the sum of electricity cost of the consumer with actual consumption is equal to total cost for the consumer with perturbed consumption generated using AMLODA model based on TOU and PLP tariff designs. However, substantial changes in load patterns can cause a negative effect on demand management system such as adjusting demand of users' consumption by reducing their demands during peak hour times. The main goal of this research is to propose a mechanism to minimize this trade-off between privacy protection and data-utility. While our novel framework provides an efficient level of privacy with infinitesimal perturbation amount, a more sophisticated analysis is needed for the evaluation and optimization load control and perturbation amount. It remains an important topic for future work.

B. GAUSSIAN NOISE PERTURBATION

To prevent inadvertent disclosure of users' private information, the smart meter readings have also been modified based on Gaussian noise perturbation and we evaluate its performance with the proposed AMLODA model's. The majority of datasets, including electricity consumption data, have Gaussian distribution by nature. For example, an electricity load profile's curves, peak points, and the position of the center peak can be calculated with a small error margin using Gaussian function [70]. Therefore, the goal of such noise interference on the individual metering data is to obfuscate the power consumption patterns in order to avoid information leakages. The Gaussian function has the following expression:

$$f(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$$

where σ^2 is the variance of the data distribution and μ is the mean of the data distribution. We set a mean of zero in our implementation so that the total load remains unchanged. Therefore, new perturbed samples are calculated as follows:

$$\hat{x} = x + \Delta x \tag{6}$$

$$\Delta x \sim N(0, \sigma^2) \tag{7}$$

In the above equations, x represents actual electricity consumption for a given time interval and Δx represents the magnitude of perturbation under the $N(0, \sigma^2)$ data distribution.

Technically speaking, the goal of this approach is to enforce the posterior distribution p(y|x) in order to pursue $N(\hat{x}, \sigma^2)$ instead of $N(x, \sigma^2)$. The assessment of privacy loss details based on different variance values is presented in the following section.

V. EVALUATION

A. DATASET

ETH Zurich provides Electricity Consumption and Occupancy (ECO) dataset to the general community in an effort to encourage researchers to contribute in improvement of grid participants' information security [71]. The dataset contains both residential electricity usage and ground truth occupancy information. Data was collected from June 2012 to January 2013 over a period of more than 6 months by observation of five distinct homes in Switzerland.

Data is sampled every second within a day from 00:00:00 to 23:59:59 using off-the-shelf digital electricity meters deployed in the individual houses. This dataset contains 5 different files and each file holds the average power consumption (in watts). This smart metering data is divided into two periods which are summer (July to September 12) and winter (November 2012 to January 2013).

B. MODEL IMPLEMENTATION

To verify the effectiveness of an occupancy detection attack, we implement a machine learning model based on LSTM in Python programming language using Pytorch library. For the implementation of the model, we split the dataset into two parts as training and test. We use 80% of the dataset to train the model and the remaining is reserved for evaluation of the model's performance. Figure 7 shows the fine-tuned system parameters for the experiment.

System Parameters	Value
Hidden Layer Size	2
Each Hidden Layer's Node Count	150
Learning Rate	0.001
Epoch Number	200
Loss Function	Cross Entropy
Optimizer	Adam Optimizer

FIGURE 7. Experimental parameters for occupancy detection attacks.

Briefly speaking, the LSTM model consists of two hidden layers. After each hidden layer, Rectier Liner Unit (ReLU) functions are applied whereas, after the output layer, the sigmoid function is applied to ensure the non-linearity of the model which is required to solve complex problems.

It is important to note that the dataset includes some missing values. Therefore, in order to eliminate the negative impact of the missing values on the smart metering time-series data, we remove them in the pre-processing phase. In addition, in our implementation, only power consumption data is considered as a feature and this feature is normalized between 0 and 1 during the pre-processing phase in order to have all features at the same scale. In this way, none of the electricity patterns becomes dominant.

C. OCCUPANCY DETECTION ATTACK EVALUATION

To show privacy concerns with highly granular smart meter data and to quantify the amount of information leaked, we utilize machine learning techniques. A massive energy profile data collected from real homes are analyzed to evaluate the viability of an occupancy detection attack by implementing an LSTM model. We evaluate the performance of the LSTM model by considering the following metrics:

Accuracy: The number of correct predictions over the total predictions of the model [72].

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{8}$$

Precision: The number of true predictions of positive samples over the total number of positive samples. [73].

$$Precision = \frac{TP}{TP + FP} \tag{9}$$

Recall: The proportion that is correctly predicted as positive samples within all positive samples [74].

$$Recall = \frac{TP}{TP + FN} \tag{10}$$

F1 score: The harmonic mean of precision and recall [73].

$$F1\ score = \frac{2 * Precision * Recall}{Precision + Recall} \tag{11}$$

False Positive Rate (FPR): The ratio of the number of negative labeled samples incorrectly predicted as positive [75].

$$FPR = \frac{FP}{FP + TN} \tag{12}$$

False Negative Rate (FNR): The proportion of positive samples incorrectly predicted as negative [76].

$$FNR = \frac{FN}{FN + TP} \tag{13}$$

Table 1 demonstrates how different households are prone to privacy threats. The occupancy of five homes is detected with high accuracy using the LSTM attack model. According to our findings, home-4 and home-5 are the most vulnerable because of the availability of detailed smart metering data. On the other hand, home-1's energy consumption profile is more resilient on revealing the behavior of its occupants but still vulnerable to the extraction of private information with 92% accuracy during the winter period and 93% during the summer period.

In addition, as it can be seen in Table 1, the value of FPR is generally higher than the value of FNR. This is because the ground truth label data collected for these houses are imbalanced and as a result, the occupancy attack model's prediction is biased to the majority class presented by the

TABLE 1. Performance of the occupancy detection attack.

	Winter						Summer					
	Accuracy	Precision	Recall	F1 Score	FPR	FNR	Accuracy	Precision	Recall	F1 Score	FPR	FNR
Home1	92.42	93.04	97.15	95.05	21.73	2.85	93.41	94.16	98.13	96.10	29.45	1.87
Home2	94.01	92.92	94.50	96.91	11.98	0.65	98.79	99.61	98.64	99.12	0.87	1.36
Home3	96.11	96.98	98.53	97.75	18.19	1.47	N/A	N/A	N/A	N/A	N/A	N/A
Home4	99.64	99.90	99.71	99.81	1.41	0.29	98.97	99.15	99.73	99.44	9.67	0.27
Home5	97.59	98.51	99.15	98.62	12.49	0.85	99.69	99.80	99.87	99.84	2.84	0.13

TABLE 2. Comparison the performance of the occupancy detection attacks based on different machine learning models.

	Winter					Summer				
	[5]				Our Results	[5]				Our Results
Home	SVM	KNN	GMM	HMM	LSTM	SVM	KNN	GMM	HMM	LSTM
1	84	81	79	87	**92**	83	80	78	83	**93**
2	**94**	91	88	92	**94**	92	89	76	90	**98**
3	78	76	59	71	**96**	83	79	70	82	N/A
4	92	90	70	84	**99**	91	88	70	87	**98**
5	85	79	63	74	**97**	90	84	59	79	**99**

data. It should be pointed out that house-3 data for the summer period is not made publicly available. Therefore, we could not analyze the data for house-3 during that time interval.

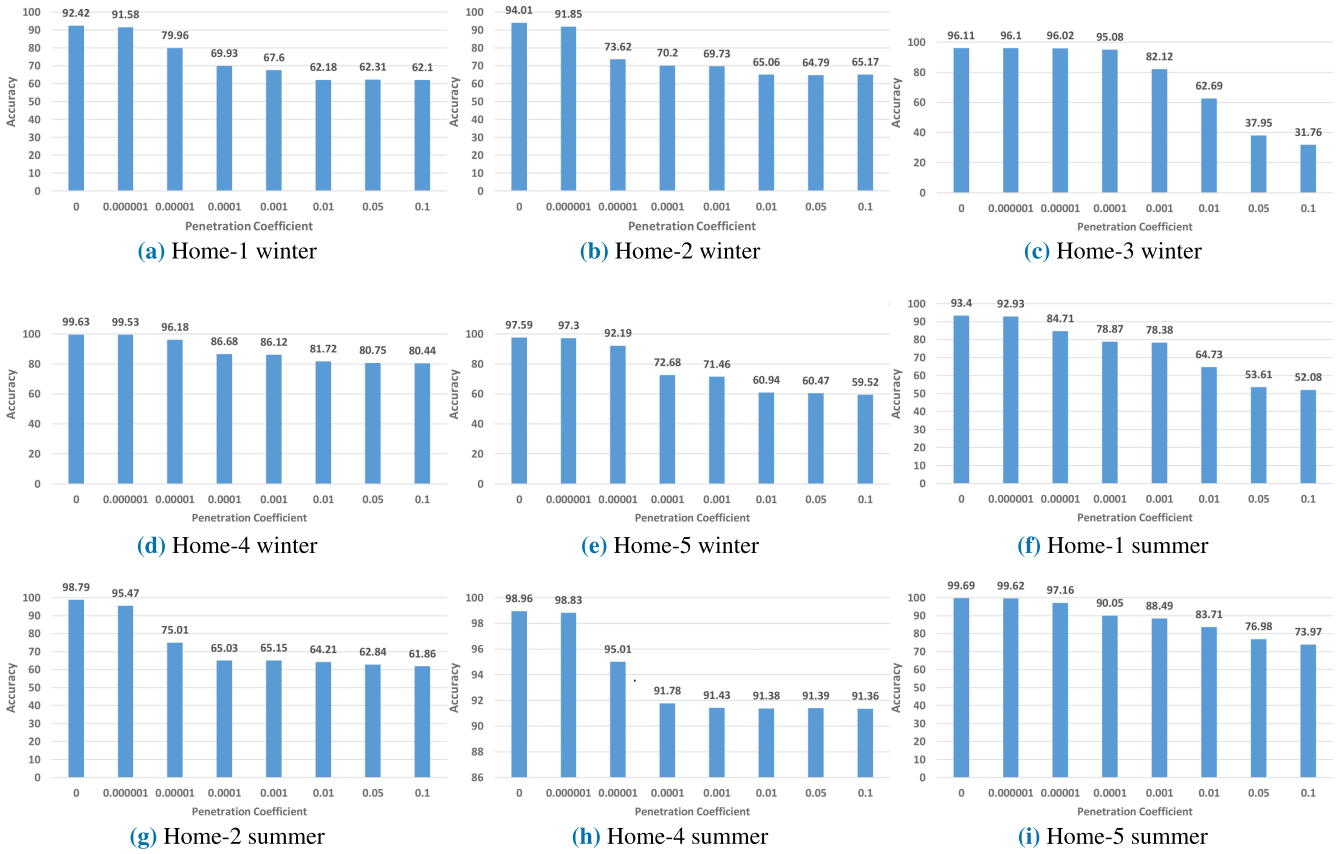
We also compare our model's effectiveness with another research that used the same dataset. Kleiminger *et al.* [5] used the ECO dataset to addres privacy issues by carrying out privacy threat analysis using machine learning models based on a Support Vector Machine (SVM) classifier, a K-Nearest Neighbor (KNN) classifier, a Gaussian Mixture Model (GMM) and a Hidden Markov Model (HMM). Table 2 shows that in comparison with their models, the occupancy detection attack is more successful with our proposed LSTM model. The main reason for this is that the LSTM model is better at adapting to the non-linear surface of the feature space and therefore, it can capture more meaningful information regarding the relationship between high granularity smart metering data and occupancy.

The drawbacks of the other models are explained as follows. With SVM, each time stamp is considered as an individual optimization problem. However, time-series smart metering data has a long dependency, which cannot be recognized well by SVM. The KNN gives a good result with a basic recognition problem but does not work well with complicated large datasets and is not robust to noise. Especially, KNN cannot capture sudden changes in electric power supply well, which is a good indicator of occupancy detection. GMM is more like a probability distribution function than a model. It can predict the occupancy of a house based on the prior distribution of electricity consumption. The main disadvantage of GMM is that it cannot consider the prior distribution's dependency. Although HMM can consider historical data relying on some strong assumptions, making external assumptions are not trivial, especially over a large and complex dataset. On the other hand, LSTM can acquire automatically usable information efficiently for occupancy detection. Based on the discussion above, it is safe to conclude that our approach is superior for occupancy attacks where users' private information can be inferred. To address the challenge of hiding privacy revealed by granular smart metering data, we present the AMLODA model. The model's performance presents in the next subsection.

D. AMLODA COUNTER ATTACK MODEL PERFORMANCE

As previously noted, the AMLODA model is designed to deliberately change meter readings in a way that preserves billing integrity but at the same time provides assurance that users' data is protected against occupancy type of privacy attacks. In order to evaluate the effectiveness of our proposed model in protecting against the occupancy attack, we initially observe the impact of various noise coefficients.

As noted in Figure 8, we first set the epsilon value to zero. It represents the original data without noise and associated manipulation. Then, we perturb the data with small distinct epsilon values and monitor the extent to which the crafted samples impair the performance of the occupancy attack for five house during summer and winter periods. As the epsilon value is increased, the accuracy of the LSTM model used in the occupancy attack degrades until it stabilizes at an



(a) Home-1 winter (b) Home-2 winter (c) Home-3 winter

(d) Home-4 winter (e) Home-5 winter (f) Home-1 summer

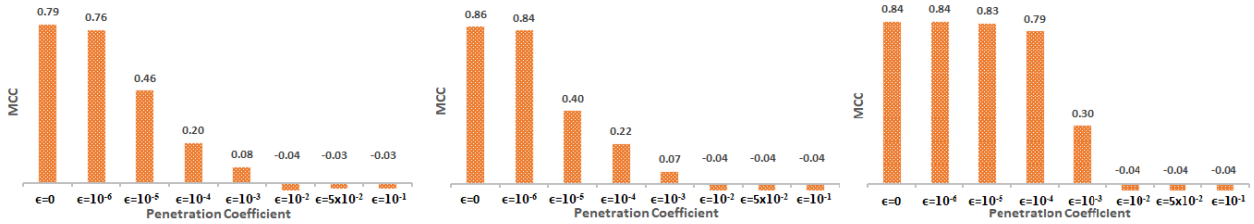
(g) Home-2 summer (h) Home-4 summer (i) Home-5 summer

FIGURE 8. Accuracy vs. penetration coefficient for five houses during winter and summer periods.

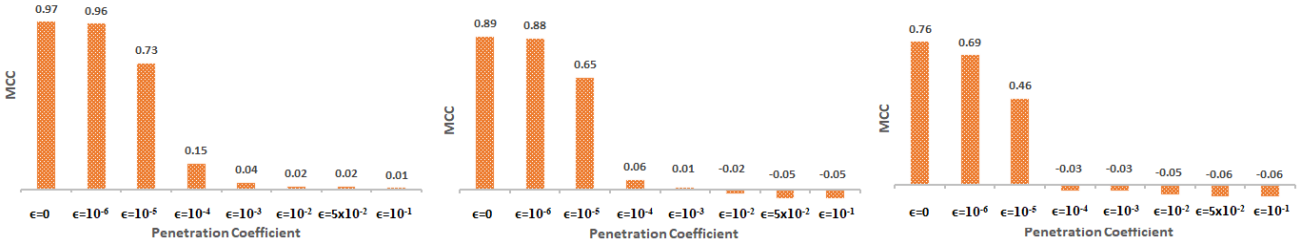
equilibrium. This is due to the model undergoing training to the extent that it can recognize the occupancy detection patterns. As it is seen in Figure 8, once the equilibrium point is reached, increasing the epsilon value might cause arbitrary fluctuations on the accuracy. [77].

However, the real electricity consumption dataset we use is highly imbalanced. Even though, the most widely used model evaluation metric is accuracy, this metric can be misleading when working with an imbalanced dataset [75]. In such cases, alternative evaluation metrics should be taken into account along with accuracy. Therefore, we have added alternative evaluation metrics, which are Matthews Correlation Coefficient (MCC) and area under the receiver operating characteristic (ROC) curve (AUC), for assessing the effectiveness of the proposed AMLODA model. These metrics are reliable and robust parameters in the presence of class imbalance so that they are commonly used for evaluating the classification of a highly imbalanced datasets [78]. MCC is used as the measure of the binary classifier's performance, in the range between -1 to 1 [79]. 1 represents perfect prediction while -1 indicates totally wrong prediction and 0 means random prediction. MCC values that converge to 0 are better for masking users' private information because that is no better than random prediction. On the other hand, ROC curve is a performance metric for binary classification problems at different threshold values [80]. The AUC value lies between 0 to 1, similar to MCC, where 0 indicates the absolutely worst prediction, the mid point 0.5 denotes random prediction and the highest value 1 signifies perfect prediction. As seen in Figure 9, the AMLODA model successfully manages to mask users' privacy most of the time with epsilon set to 0.0001, which is an insignificant change over actual consumption pattern. However, this number fails to protect users' information adequately for Home-3 during the winter period. If we increase the epsilon value up to 0.01, the MCC value converges to zero indicating that the occupancy attack performs similarly to random guessing. In addition, we measure AUC values of houses during the summer and winter periods based on different epsilon values in Table 3 and in Table 4. The result of AUC values confirms that our proposed method leads the occupancy attack model to be close to a random guess model most of the time, with epsilon value set to 0.0001.

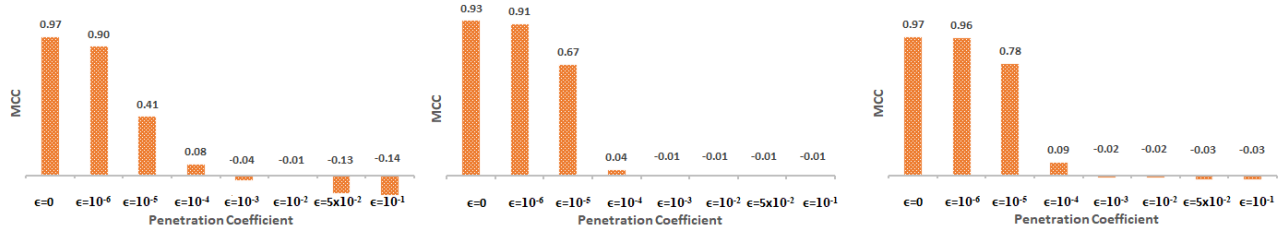
As seen in Figure 10, infinitesimally small epsilon values, like 0.0001, in Figure (10a) slightly perturb the original data. This difference is not even visible on the figure due to the very negligible change. Such subtle changes do not affect the demand response efforts for real-time optimization,



(a) Home-1 winter, Home-2 winter, Home-3 winter (from left to right)

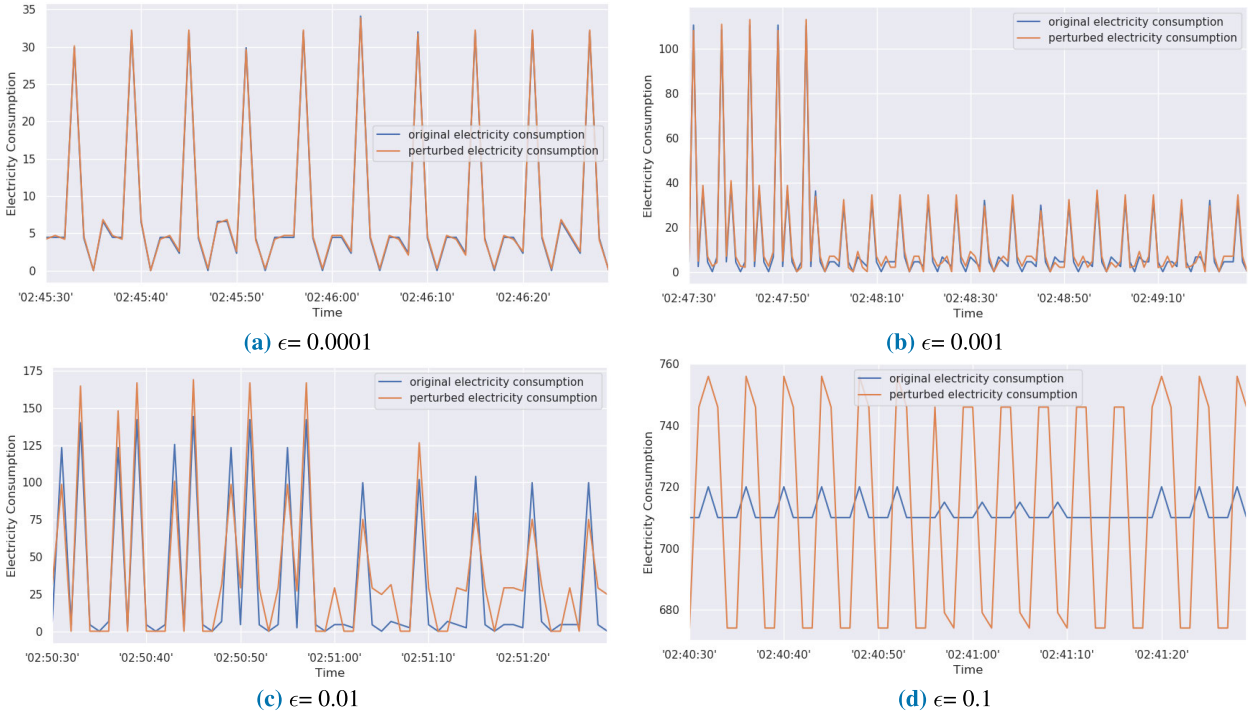


(b) Home-4 winter, Home-5 winter, Home-1 summer (from left to right)



(c) Home-2 summer, Home-4 summer, Home-5 summer (from left to right)

FIGURE 9. Matthews correlation coefficient vs. penetration coefficient for five houses during winter and summer periods.



(a) $\epsilon = 0.0001$ (b) $\epsilon = 0.001$

(c) $\epsilon = 0.01$ (d) $\epsilon = 0.1$

FIGURE 10. Different options for masking occupancy under the AMLODA technique.

which tend to present the best profitable service. When we set the epsilon value to 0.001 in Figure (10b), the difference is more prominent. Also, when we set the epsilon to a relatively high value to observe its' affect, we noticed, as seen in the Figure (10d), the noise changes the actual energy consumption data to a great extent. This can lead

TABLE 3. Area under the curve vs. penetration coefficient for five houses during summer periods.

	AUC			
Epsilon	Home1	Home2	Home4	Home5
0	0.84	0.99	0.95	0.99
0.000001	0.84	0.96	0.94	0.98
0.00001	0.73	0.71	0.85	0.91
0.0001	0.48	0.54	0.51	0.57
0.001	0.47	0.48	0.5	0.49
0.01	0.47	0.45	0.5	0.48
0.05	0.46	0.45	0.5	0.47
0.1	0.46	0.46	0.5	0.48

TABLE 4. Area under the curve vs. penetration coefficient for five houses during winter periods.

	AUC				
Epsilon	Home1	Home2	Home3	Home4	Home5
0	0.88	0.91	0.90	0.99	0.93
0.000001	0.87	0.90	0.90	0.99	0.93
0.00001	0.73	0.69	0.90	0.92	0.80
0.0001	0.61	0.60	0.85	0.59	0.54
0.001	0.54	0.52	0.68	0.52	0.50
0.01	0.48	0.49	0.47	0.51	0.48
0.05	0.48	0.49	0.47	0.51	0.46
0.1	0.48	0.49	0.47	0.50	0.46

to a compromise of the operational efficiency of the smart grid environment. In this experiment, we sometimes set epsilon values high intentionally to demonstrate maximum damage to occupancy detection attack model. There is a trade-off between efficiency and privacy. Some users may deem privacy more important than energy efficiency and vice versa.

To provide the control at the users' hands, the level of noise or influence on the perturbation can be regulated by the customers. To accomplish this, the customer needs to visit the service provider with a valid identification. To be truly secure, the customer and the utility company's first interaction needs to happen out-of-band with a face-to face meeting. After identity authentication, the customer needs to fill out an application form to request use of our proposed model for privacy protection and selects the amount of privacy level. Whenever the users need to update this preference, they will need to contact the utility company in the same way. This can be added to the customer's contract terms and the service provider must follow these rules. Public Utility Commissions (PUCs) can protect consumers from unethical behavior of utility companies if consumers file a complaint regarding any abuse. PUC has already similar responsibilities for protection of users' rights [81].

E. COMPARISON OF AMLODA MODEL's PERFORMANCE WITH GAUSSIAN PERTURBATION

To analyze AMLODA model's performance, we carry out the same experimental approach under the Gaussian noise assumption and compare the experimental results. Home-4 and home-5 are the most vulnerable against occupancy detection attack based on our findings in Table 1. For this reason, we select home-4 and home-5 as case studies for comparison analysis of both perturbation techniques.

Table 5, Table 6, Table 7 and Table 8 show this comparison in terms of accuracy, MCC and AUC. We see that both techniques aid in protecting users' privacy to some extent with a small change in power consumption data, however, larger perturbation is required to significantly compromise the performance of the attack models until an equilibrium

TABLE 5. Comparison of performances between AMLODA and Gaussian techniques with different level of perturbations on home-4 during summer period.

Home4							
Gaussian Technique				AMLODA Model			
Variance	Accuracy	MCC	AUC	Epsilon	Accuracy	MCC	AUC
0.0	98.96	0.93	0.95	0	98.96	0.93	0.95
0.1	97.53	0.87	0.93	10^{-6}	98.83	0.91	0.94
0.2	97.64	0.82	0.91	10^{-5}	95.01	0.67	0.85
0.3	91.45	0.80	0.90	10^{-4}	91.78	0.04	0.51
0.5	91.42	0.75	0.88	10^{-3}	91.43	-0.01	0.5
1.0	91.38	0.67	0.85	10^{-2}	91.38	-0.01	0.5
5.0	91.38	0.67	0.85	$5x10^{-2}$	91.39	-0.01	0.5
7.5	91.39	0.67	0.85	10^{-1}	91.36	-0.01	0.5

TABLE 6. Comparison of performances between AMLODA and Gaussian techniques with different level of perturbations on home-4 during winter period.

Home4							
Gaussian Technique				AMLODA Model			
Variance	Accuracy	MCC	AUC	Epsilon	Accuracy	MCC	AUC
0.0	99.63	0.97	0.99	0	99.63	0.97	0.99
0.1	98.48	0.92	0.96	10^{-6}	99.53	0.96	0.99
0.2	96.15	0.88	0.92	10^{-5}	96.18	0.73	0.92
0.3	92.34	0.85	0.90	10^{-4}	86.68	0.15	0.59
0.5	92.31	0.79	0.87	10^{-3}	86.12	0.04	0.52
1.0	92.34	0.76	0.85	10^{-2}	81.72	0.02	0.51
5.0	92.33	0.65	0.80	$5x10^{-2}$	80.75	0.02	0.51
7.5	92.35	0.65	0.80	10^{-1}	80.44	0.01	0.50

point can be reached. We also notice that the occupancy of the households is harder to detect with AMLODA model compared to the Gaussian model evident by more significant MCC and AUC value deteriorations. This experiment shows that even though the real data can be manipulated with large Gaussian noise, this solution fails to protect users privacy effectively for home-4 during summer and winter and home-5 during summer. We still observe occupancy prediction of the attack model that it has AUC of 85% and 8O% for home-4 during summer and winter periods respectively and it has AUC of 76% for home-5 during summer period. On the other hand, AMLODA model effectively conceals users' private information in such a way that an attacker cannot obtain any meaningful information from this perturbed data. As shown in Tables 5 through 8, AUC values of the attack model are close to 5O%, which means that the model is close to random guessing, with the small perturbation amount for home-4 and home-5 during all season.

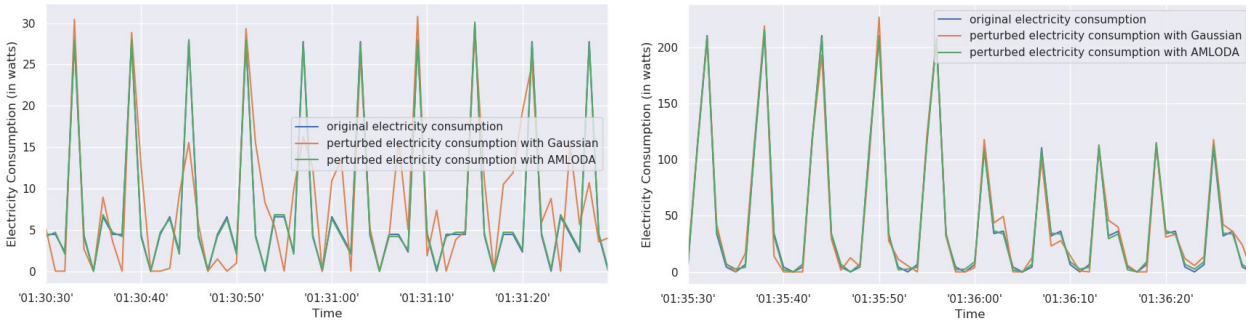
In Table 5, Table 6, Table 7 and Table 8, it is important to note the differences in the used noises and their impact on the attack's model performance in terms of accuracy, MCC and AUC. In order to analyze the impact of noise better, we plot Figure (11a). In Figure (11a), the green line corresponds to the perturbed electricity consumption under the AMLODA model with 0.0001 epsilon value for noise while the orange line corresponds to perturbed electricity consumption under the Gaussian noise with 7.5 variance value. The reason we selected such value pair is because they have similar success rate for home-5 over the winter period as observed in Table 8. Although same results are achieved with both approaches, the electricity changes are more negligible in AMLODA

TABLE 7. Comparison of performances between AMLODA and Gaussian techniques with different level of perturbations on home-5 during summer period.

Home5							
Gaussian Technique				AMLODA Model			
Variance	Accuracy	MCC	AUC	Epsilon	Accuracy	MCC	AUC
0.0	99.69	0.97	0.99	0	99.69	0.97	0.99
0.1	99.20	0.95	0.98	10^{-6}	99.62	0.96	0.98
0.2	97.60	0.92	0.96	10^{-5}	97.16	0.78	0.91
0.3	88.53	0.80	0.88	10^{-4}	90.05	0.09	0.57
0.5	87.96	0.74	0.84	10^{-3}	88.49	-0.02	0.49
1.0	87.75	0.67	0.80	10^{-2}	83.71	-0.02	0.48
5.0	87.77	0.61	0.75	$5x10^{-2}$	76.98	-0.03	0.47
7.5	87.93	0.61	0.76	10^{-1}	73.97	-0.03	0.48

TABLE 8. Comparison of performances between AMLODA and Gaussian techniques with different level of perturbations on home-5 during winter period.

Home5							
Gaussian Technique				AMLODA Model			
Variance	Accuracy	MCC	AUC	Epsilon	Accuracy	MCC	AUC
0.0	97.59	0.89	0.93	0	97.59	0.89	0.93
0.1	96.20	0.83	0.90	10^{-6}	97.30	0.88	0.93
0.2	93.16	0.76	0.86	10^{-5}	92.19	0.65	0.80
0.3	90.27	0.69	0.82	10^{-4}	72.68	0.06	0.54
0.5	85.57	0.52	0.76	10^{-3}	71.46	0.01	0.50
1.0	81.08	0.32	0.67	10^{-2}	60.94	-0.02	0.48
5.0	73.29	0.08	0.58	$5x10^{-2}$	60.47	-0.05	0.46
7.5	72.89	0.06	0.54	10^{-1}	59.52	-0.05	0.46



(a) Data perturbations by the AMLODA with ϵ= 0.0001 and by the Gaussian noise with variance = 7.5 over home-5 (winter).

(b) Data perturbations by the AMLODA with ϵ= 0.001 and by the Gaussian noise with variance = 7.5 over home-5 (winter).

FIGURE 11. Different false data injections by the AMLODA model and the Gaussian noise technique.

model. As it is seen on the figure (11a), with AMLODA model, the original electricity consumption and perturbed electricity consumption plot lines fall on top of each other because of similarity. However, the Gaussian perturbation's effects on the actual consumption is more apparent than AMLODA. In addition, we plot Figure 12 that demonstrates perturbed energy consumption of home-5 (winter) for secondly time interval by AMLODA and Gaussian techniques

Time Interval	Original Electricity Consumption	Perturbed Electricity Consumption with AMLODA	Perturbed Electricity Consumption with Gaussian
'01:30:55'	110.676003	110.42897	100.785126
'01:30:56'	31.981501	32.228535	25.752052
'01:30:57'	6.578530	6.331495	0.000000
'01:30:58'	112.800003	113.047035	105.987869
'01:30:59'	4.443320	4.196285	1.470129
'01:31:00'	110.676003	110.923035	120.042328
.	.	.	.
.	.	.	.
.	.	.	.

FIGURE 12. Comparison of perturbed energy consumptions of home-5 (winter) for secondly time interval with epsilon value 0.0001 and variance value 7.5.

with abovementioned noise injections in order to show these differences.

Also, Figure (11b) demonstrates that increased perturbation level with AMLODA model resulted in lower model evaluation metrics for the occupancy attack model, thus boosting privacy protection capabilities further. Even though it has higher success in privacy preservation, AMLODA has closer proximity to the actual data. Thus, this experiment demonstrates that the proposed AMLODA model achieve higher success with varying degrees of masking high frequency metering data without jeopardizing workings of the demand response systems in the smart grid environment. In addition, we can consider the AMLODA model as a one-way function to produce calculated noise. Therefore, attacker cannot feasibly recover actual consumption of users from perturbed consumption. On the other hand, if the supplier knows the distribution of actual consumption of a user, (s)he can compute the noise distribution and eventually actual measurements because Gaussian based noise data is correlated to the actual data.

VI. CONCLUSION

Commentators have defined privacy in different ways. Some of these definitions are '*Essential to democratic government*', '*Heart of our liberty*', '*The beginning of all freedom*' [82]. Although privacy has vital importance for freedom and democracy, promising and futuristic new technologies like SG suffer from privacy leakage. Therefore, this paper presents a valid countermeasure named AMLODA model to accomplish the enhancement of user's privacy. The proposed model's aim is to maximize the privacy protection by finding the optimum rescheduling of smart metering consumption data. In addition, we offer different required levels of privacy by customizing users' preferences. When households enjoy a very high degree of privacy with the proposed customer-oriented model, the system maintains the correctness of payments. Since the involvement of any trusted third party or any additional hardware devices is not required, it makes the adaption of the proposed model practical.

Furthermore, we analyze the impact of the noise coefficient found from both AMLODA model and a Gaussian model. We demonstrated with empirical experiments that our novel framework protects users' privacy more efficiently without reducing the performance of SG operations and satisfy existing privacy-related challenges. Consequently, the essential security requirements of dwellers are fulfilled.

REFERENCES

[1] *How Many Smart Meters are Installed in the United States, and Who Has Them*. [Online]. Available: https://www.eia.gov/
[2] M. I. Ibrahem, M. Nabil, M. M. Fouda, M. M. E. A. Mahmoud, W. Alasmary, and F. Alsolami, "Efficient privacy-preserving electricity theft detection with dynamic billing and load monitoring for AMI networks," *IEEE Internet Things J.*, vol. 8, no. 2, pp. 1243–1258, Jan. 2021.
[3] M. R. Asghar, G. Dan, D. Miorandi, and I. Chlamtac, "Smart meter data privacy: A survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2820–2835, 4th Quart., 2017.
[4] A. Akbar, M. Nati, F. Carrez, and K. Moessner, "Contextual occupancy detection for smart office by pattern recognition of electricity consumption data," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2015, pp. 561–566.
[5] W. Kleiminger, C. Beckel, and S. Santini, "Household occupancy monitoring using electricity meters," in *Proc. ACM Int. Joint Conf. Pervas. Ubiquitous Comput. UbiComp*, 2015, pp. 975–986.
[6] M. M. Badr, W. A. Amiri, M. M. Fouda, M. M. E. A. Mahmoud, A. J. Aljohani, and W. Alasmary, "Smart parking system with privacy preservation and reputation management using blockchain," *IEEE Access*, vol. 8, pp. 150823–150843, 2020.
[7] C. Rottondi, M. Savi, D. Polenghi, G. Verticale, and C. Krauss, "A decisional attack to privacy-friendly data aggregation in smart grids," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2013, pp. 2616–2621.
[8] M. I. Ibrahem, M. M. Badr, M. M. Fouda, M. Mahmoud, W. Alasmary, and Z. M. Fadlullah, "PMBFE: Efficient and privacy-preserving monitoring and billing using functional encryption for AMI networks," in *Proc. Int. Symp. Netw., Comput. Commun. (ISNCC)*, Oct. 2020, pp. 1–7.
[9] O. Tan, D. Gunduz, and H. V. Poor, "Increasing smart meter privacy through energy harvesting and storage devices," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, pp. 1331–1341, Jul. 2013.
[10] S. McLaughlin, P. McDaniel, and W. Aiello, "Protecting consumer privacy from electric load monitoring," in *Proc. 18th ACM Conf. Comput. Commun. Secur. CCS*, 2011, pp. 87–98.
[11] H. Lam, G. Fung, and W. Lee, "A novel method to construct taxonomy electrical appliances based on load signaturesof," *IEEE Trans. Consum. Electron.*, vol. 53, no. 2, pp. 653–660, Jul. 2007.
[12] G. W. Hart, "Nonintrusive appliance load monitoring," *Proc. IEEE*, vol. 80, no. 12, pp. 1870–1891, Dec. 1992.
[13] G. Kalogridis, R. Cepeda, S. Z. Denic, T. Lewis, and C. Efthymiou, "ElecPrivacy: Evaluating the privacy protection of electricity management algorithms," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 750–758, Dec. 2011.
[14] P. M. Schwartz, "European data protection law and restrictions on international data flows," *Iowa L. Rev.*, vol. 80, p. 471, 1994.
[15] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, and R. Cepeda, "Privacy for smart meters: Towards undetectable appliance load signatures," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, Oct. 2010, pp. 232–237.
[16] E. L. Quinn, "Privacy and the new energy infrastructure," *Available at SSRN*, to be published.
[17] R. Amer, H. ElSawy, J. Kibilda, M. M. Butt, and N. Marchetti, "Cooperative transmission and probabilistic caching for clustered D2D networks," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2019, pp. 1–6.
[18] M. Baza, A. Salazar, M. Mahmoud, M. Abdallah, and K. Akkaya, "On sharing models instead of data using mimic learning for smart health applications," in *Proc. IEEE Int. Conf. Informat., IoT, Enabling Technol. (ICIoT)*, Feb. 2020, pp. 231–236.
[19] C. Beckel, L. Sadamori, and S. Santini, "Automatic socio-economic classification of households using electricity consumption data," in *Proc. 4th Int. Conf. Future energy Syst. e-Energy*, 2013, pp. 75–86.
[20] I. B. Sanchez, I. D. Espinos, L. M. Sarrion, A. Q. Lopez, and I. N. Burgos, "Clients segmentation according to their domestic energy consumption by the use of self-organizing maps," in *Proc. 6th Int. Conf. Eur. Energy Market*, May 2009, pp. 1–6.

[21] J. Scott, A. J. Bernheim Brush, J. Krumm, B. Meyers, M. Hazas, S. Hodges, and N. Villar, "PreHeat: Controlling home heating using occupancy prediction," in *Proc. 13th Int. Conf. Ubiquitous Comput. UbiComp*, 2011, pp. 281–290.

[22] J. Taneja, A. Krioukov, S. Dawson-Haggerty, and D. Culler, "Enabling advanced environmental conditioning with a building application stack," in *Proc. Int. Green Comput. Conf.*, Jun. 2013, pp. 1–10.

[23] B. V. Meerssche, G. Van Ham, G. Deconinck, J. Reynders, M. Spelier, and N. Maes, "Practical use of energy management systems," in *Proc. 10th Int. Symp. Ambient Intell. Embedded Syst.*, Chania, Crete, Greece, Sep. 2011, pp. 1–6.

[24] D. De Silva, X. Yu, D. Alahakoon, and G. Holmes, "A data mining framework for electricity consumption analysis from meter data," *IEEE Trans. Ind. Informat.*, vol. 7, no. 3, pp. 399–407, Aug. 2011.

[25] L. Yang, K. Ting, and M. B. Srivastava, "Inferring occupancy from opportunistically available sensor data," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. (PerCom)*, Mar. 2014, pp. 60–68.

[26] T. Ekwevugbe, N. Brown, V. Pakka, and D. Fan, "Real-time building occupancy sensing using neural-network based sensor network," in *Proc. 7th IEEE Int. Conf. Digit. Ecosyst. Technol. (DEST)*, Jul. 2013, pp. 114–119.

[27] J. Kamto, L. Qian, J. Fuller, and J. Attia, "Light-weight key distribution and management for advanced metering infrastructure," in *Proc. IEEE GLOBECOM Workshops (GC Wkshps)*, Dec. 2011, pp. 1216–1220.

[28] T. Baumeister, "Literature review on smart grid cyber security," Collaborative Softw. Develop. Lab. Univ. Hawaii, Honolulu, HI, USA, Tech. Rep., 2010.

[29] F. Aloul, A. R. Al-Ali, R. Al-Dalky, M. Al-Mardini, and W. El-Hajj, "Smart grid security: Threats, vulnerabilities and solutions," *Int. J. Smart Grid Clean Energy*, vol. 1, no. 1, pp. 1–6, 2012.

[30] S. Shapsough, F. Qatan, R. Aburukba, F. Aloul, and A. R. Al Ali, "Smart grid cyber security: Challenges and solutions," in *Proc. Int. Conf. Smart Grid Clean Energy Technol. (ICSGCE)*, Oct. 2015, pp. 170–175.

[31] H. Bao and R. Lu, "A new differentially private data aggregation with fault tolerance for smart grid communications," *IEEE Internet Things J.*, vol. 2, no. 3, pp. 248–258, Jun. 2015.

[32] A. Paverd, A. Martin, and I. Brown, "Security and privacy in smart grid demand response systems," in *Proc. Int. Workshop Smart Grid Secur.*, Springer, 2014, pp. 1–15.

[33] F. Li, B. Luo, and P. Liu, "Secure information aggregation for smart grids using homomorphic encryption," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, Oct. 2010, pp. 327–332.

[34] Z. Erkin, J. R. Troncoso-pastoriza, R. L. Lagendijk, and F. Perez-Gonzalez, "Privacy-preserving data aggregation in smart metering systems: An overview," *IEEE Signal Process. Mag.*, vol. 30, no. 2, pp. 75–86, Mar. 2013.

[35] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, Oct. 2010, pp. 238–243.

[36] V. Ford, A. Siraj, and M. A. Rahman, "Secure and efficient protection of consumer privacy in advanced metering infrastructure supporting fine-grained data analysis," *J. Comput. Syst. Sci.*, vol. 83, no. 1, pp. 84–100, Feb. 2017.

[37] F. Borges, D. Demirel, L. Bock, J. Buchmann, and M. Muhlhauser, "A privacy-enhancing protocol that provides in-network data aggregation and verifiable smart meter billing," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jun. 2014, pp. 1–6.

[38] S. Tonyali, K. Akkaya, N. Saputro, and A. S. Uluagac, "A reliable data aggregation mechanism with homomorphic encryption in smart grid AMI networks," in *Proc. 13th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2016, pp. 550–555.

[39] F. G. Mármol, C. Sorge, R. Petrlic, O. Ugus, D. Westhoff, and G. M. Pérez, "Privacy-enhanced architecture for smart metering," *Int. J. Inf. Secur.*, vol. 12, no. 2, pp. 67–82, Apr. 2013.

[40] Z. Erkin and G. Tsudik, "Private computation of spatial and temporal power consumption with smart meters," in *Proc. Int. Conf. Appl. Cryptogr. Netw. Secur.*, Springer, 2012, pp. 561–577.

[41] K. Kursawe, G. Danezis, and M. Kohlweiss, "Privacy-friendly aggregation for the smart-grid," in *Proc. Int. Symp. Privacy Enhancing Technol. Symp.*, Springer, 2011, pp. 175–191.

[42] F. Knirsch, G. Eibl, and D. Engel, "Error-resilient masking approaches for privacy preserving data aggregation," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 3351–3361, Jul. 2018.

[43] S. Bhattacharjee and S. K. Das, "Detection and forensics against stealthy data falsification in smart metering infrastructure," *IEEE Trans. Depend. Sec. Comput.*, vol. 18, no. 1, pp. 356–371, Jan. 2021.

[44] Z. Zheng, Y. Yang, X. Niu, H.-N. Dai, and Y. Zhou, "Wide and deep convolutional neural networks for electricity-theft detection to secure smart grids," *IEEE Trans. Ind. Informat.*, vol. 14, no. 4, pp. 1606–1615, Apr. 2018.

[45] F. B. de Oliveira, *On Privacy-Preserving Protocols for Smart Metering Systems: Security and Privacy in Smart*. Springer, 2016.

[46] F. Mármol, C. Sorge, O. Ugus, and G. Pérez, "Do not snoop my habits: Preserving privacy in the smart grid," *IEEE Commun. Mag.*, vol. 50, no. 5, pp. 166–172, May 2012.

[47] F. Diao, F. Zhang, and X. Cheng, "A privacy-preserving smart metering scheme using linkable anonymous credential," *IEEE Trans. Smart Grid*, vol. 6, no. 1, pp. 461–467, Jan. 2015.

[48] C.-K. Chu, J. K. Liu, J. W. Wong, Y. Zhao, and J. Zhou, "Privacy-preserving smart metering with regional statistics and personal enquiry services," in *Proc. 8th ACM SIGSAC Symp. Inf., Comput. Commun. Secur. - ASIA CCS*, 2013, pp. 369–380.

[49] *Anonymity*. [Online]. Available: https://en.wikipedia.org/wiki/Anonymity

[50] A. Narayanan and V. Shmatikov, *Robust de-Anonymization of Large Datasets (How to Break Anonymity of the Netflix Prize Dataset)*. Austin, TX, USA: Univ. Texas at Austin, 2008.

[51] D. Chen, S. Kalra, D. Irwin, P. Shenoy, and J. Albrecht, "Preventing occupancy detection from smart meters," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2426–2434, Sep. 2015.

[52] *Water Heaters Get an Efficiency Makeover Courtesy of the Department of Energy*. [Online]. Available: http://aceee.org/blog/2015/02/water-heaters-get-efficiency-makeover

[53] D. Man, W. Yang, S. Xuan, and X. Du, "Thwarting nonintrusive occupancy detection attacks from smart meters," *Secur. Commun. Netw.*, vol. 2017, pp. 1–9, Jan. 2017.

[54] D. Micciancio, "Oblivious data structures: Applications to cryptography," in *Proc. 29th Annu. ACM Symp. Theory Comput. STOC*, 1997, pp. 456–464.

[55] W. Zaremba, I. Sutskever, and O. Vinyals, "Recurrent neural network regularization," 2014, *arXiv:1409.2329*. [Online]. Available: http://arxiv.org/abs/1409.2329

[56] K. Greff, R. K. Srivastava, J. Koutnik, B. R. Steunebrink, and J. Schmidhuber, "LSTM: A search space odyssey," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 28, no. 10, pp. 2222–2232, Oct. 2017.

[57] H. Sak, A. Senior, and F. Beaufays, "Long short-term memory based recurrent neural network architectures for large vocabulary speech recognition," 2014, *arXiv:1402.1128*. [Online]. Available: http://arxiv.org/abs/1402.1128

[58] R. Amer, W. Saad, H. ElSawy, M. M. Butt, and N. Marchetti, "Caching to the sky: Performance analysis of cache-assisted CoMP for cellular-connected UAVs," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2019, pp. 1–6.

[59] I. Yilmaz, A. Siraj, and D. Ulybyshev, "Improving DGA-based malicious domain classifiers for malware defense with adversarial machine learning," in *Proc. IEEE 4th Conf. Inf. Commun. Technol. (CICT)*, Dec. 2020, pp. 1–6.

[60] S. Hochreiter, "The vanishing gradient problem during learning recurrent neural nets and problem solutions," *Int. J. Uncertainty, Fuzziness Knowl.-Based Syst.*, vol. 06, no. 02, pp. 107–116, Apr. 1998.

[61] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Comput.*, vol. 9, no. 8, pp. 1735–1780, 1997.

[62] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and harnessing adversarial examples," 2014, *arXiv:1412.6572*. [Online]. Available: http://arxiv.org/abs/1412.6572

[63] I. Yilmaz, "Practical fast gradient sign attack against mammographic image classifier," 2020, *arXiv:2001.09610*. [Online]. Available: http://arxiv.org/abs/2001.09610

[64] I. Yilmaz, R. Masum, and A. Siraj, "Addressing imbalanced data problem with generative adversarial network for intrusion detection," in *Proc. IEEE 21st Int. Conf. Inf. Reuse Integr. Data Sci. (IRI)*, Aug. 2020, pp. 25–30.

[65] Y. Gao, A. Schay, and D. Hou, "Occupancy detection in smart housing using both aggregated and appliance-specific power consumption data," in *Proc. 17th IEEE Int. Conf. Mach. Learn. Appl. (ICMLA)*, Dec. 2018, pp. 1296–1303.

[66] V. Becker and W. Kleiminger, "Exploring zero-training algorithms for occupancy detection based on smart meter measurements," *Comput. Sci. Res. Develop.*, vol. 33, nos. 1–2, pp. 25–36, Feb. 2018.

[67] N. Papernot, P. McDaniel, and I. Goodfellow, "Transferability in machine learning: From phenomena to black-box attacks using adversarial samples," 2016, *arXiv:1605.07277*. [Online]. Available: http://arxiv.org/abs/1605.07277
[68] Y. Dong, F. Liao, T. Pang, H. Su, J. Zhu, X. Hu, and J. Li, "Boosting adversarial attacks with momentum," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit.*, Jun. 2018, pp. 9185–9193.
[69] Y. Liu, X. Chen, C. Liu, and D. Song, "Delving into transferable adversarial examples and black-box attacks," 2016, *arXiv:1611.02770*. [Online]. Available: http://arxiv.org/abs/1611.02770
[70] Y. Ge, J. Dai, K. Qian, D. Hepburn, and C. Zhou, "Simulation of domestic electricity load profile by multiple Gaussian distribution," in *Proc. 23rd Int. Conf. Electr. Distrib.*, 2015, pp. 1–5.
[71] *ECO Dataset (Electricity Consumption and Occupancy*. [Online]. Available: http://vs.inf.ethz.ch/res/show.html?what=eco-data
[72] M. Story and R. G. Congalton, "Accuracy assessment: A user's perspective," *Photogramm. Eng. Remote Sens.*, vol. 52, no. 3, pp. 397–399, 1986.
[73] C. Goutte and E. Gaussier, "A probabilistic interpretation of precision, recall and f-score, with implication for evaluation," in *Proc. Eur. Conf. Inf. Retr.*, Springer, 2005, pp. 345–359.
[74] J. Davis and M. Goadrich, "The relationship between precision-recall and ROC curves," in *Proc. 23rd Int. Conf. Mach. Learn. ICML*, 2006, pp. 233–240.
[75] I. Yilmaz and R. Masum, "Expansion of cyber attack data from unbalanced datasets using generative techniques," 2019, *arXiv:1912.04549*. [Online]. Available: http://arxiv.org/abs/1912.04549
[76] J. A. Royle and W. A. Link, "Generalized site occupancy models allowing for false positive and false negative errors," *Ecology*, vol. 87, no. 4, pp. 835–841, Apr. 2006.
[77] O. Bousquet and A. Elisseeff, "Stability and generalization," *J. Mach. Learn. Res.*, vol. 2, pp. 499–526, Mar. 2002.
[78] S. Boughorbel, F. Jarray, and M. El-Anbari, "Optimal classifier for imbalanced data using matthews correlation coefficient metric," *PLoS ONE*, vol. 12, no. 6, Jun. 2017, Art. no. e0177678.
[79] K. A. Kantardjieff and B. Rupp, "Matthews coefficient probabilities: Improved estimates for unit cell contents of proteins, DNA, and protein-nucleic acid complex crystals," *Protein Sci.*, vol. 12, no. 9, pp. 1865–1871, Sep. 2003.
[80] J. A. Hanley and B. J. McNeil, "The meaning and use of the area under a receiver operating characteristic (ROC) curve," *Radiology*, vol. 143, no. 1, pp. 29–36, 1982.
[81] *Public Utility Commissions (PUCs)*. [Online]. Available: https://www.electricchoice.com/public-utility-commissions/
[82] N. J. Hirschmann, *Revisioning Political: Feminist Reconstructions Traditional Concepts Western Political Theory*. Evanston, IL, USA: Routledge, 2018.

IBRAHIM YILMAZ received the B.S. degree in computer engineering from Gaziantep Zirve University, Gaziantep, Turkey, in 2009 and 2014, respectively. He is currently pursuing the Ph.D. degree with the Department of Computer Science, Tennessee Tech University, Cookeville, TN, USA. He is currently a Graduate Research Assistant with the Department of Computer Science, Tennessee Tech. University. His research interests include cyber-physical systems, machine learning, network security, the Internet of Things, and smart grids.

AMBAREEN SIRAJ is currently a Professor of Computer Science and the Founding Director of Tennessee Tech's Cybersecurity Education, Research and Outreach Center (CEROC). She has served as the leader on several NSF and NSA education, and workforce development grants. She is also the Founder of the Women in CyberSecurity (WiCyS) organization, an initiative to recruit, retain, and advance women in cybersecurity. Her efforts to educate students and enhance the cybersecurity field of study goes beyond classes, research, outreach projects, workshops, and conferences. Her research focus is on security in cyber-physical systems, the Internet of Things, situation assessment in network security, security education, and workforce development. She has authored/coauthored more than 50 publications. She is a frequent speaker in various cybersecurity conferences on topics ranging from education, curriculum, workforce development, outreach, security issues & solutions for cyberphysical systems to diversity and inclusion in cybersecurity. She is a recipient of the Colloquium for Information Systems Security Education Exceptional Leadership in Education Award in 2018 and the ABET Claire L. Felbinger Award for Diversity and Inclusion in 2020.