Adaptive Energy Theft Detection in Smart Grids using Self-Learning with Dual Neural Network

Ahlam Althobaiti, *Graduate Student Member, IEEE*, Charalampos Rotsos, *Member, IEEE*, and Angelos K. Marnerides, *Member, IEEE*

***Abstract*— Energy theft is an extremely prominent challenge causing significant energy and revenue losses for utility providers worldwide. The introduction of advanced metering infrastructures (AMI) consisting of smart meter (SM) deployments has undeniably extended the attack surface, enabling individual consumers or prosumers to trigger composite energy theft attack vectors. In this work, we introduce an energy theft detection system capable of distinguishing properties of power consumption and generation theft with possible misconfigurations caused by non-malicious intent. The proposed approach is adaptive through a self-learning operation that is updated continuously as new measurements become available. With the synergistic use of measurements collected by real PV installations and openly available weather information, the system achieves high accuracy and precision result in theft identification over streamed data measurements. Thus, it promotes low computational costs and its architecture can be easily integrated within smart grid infrastructures to realize next-generation cross-batch energy theft detection.**

***Index Terms*— Energy theft, smart meters, data-driven detection, smart grid, cybersecurity**

I. Introduction

THE modernisation of traditional power grids into smart grids through the demand response (DR) paradigm alongside the integration of distributed renewable energy sources (DRES) within grid optimisation practices is undoubtedly contributing towards the global net-zero initiative. A core property of modern power grids revolves around the adequate operation and optimisation of AMI as underpinned by networked smart meters (SM). In the UK alone, the number of SM deployed by utility companies reached 28.8 million by the first quarter of 2022, with a full coverage projected by the end of 2025 [1], [2]. Given the diversity of hardware and software technologies entailed within SM integration and the lack of holistic grid-specific cybersecurity practices, we witness an evolving threat landscape in which energy theft activities are further enabled [3].

A. Althobaiti is with the School of Computing & Communications, Lancaster University, Lancaster, UK. (E-mail: a.althobaiti@lancaster.ac.uk), and College of Computers and Information Technology, Taif University, Taif, SA. (E-mail: a.s.althobaiti@tu.edu.sa).

C. Rotsos is with the School of Computing & Communications, Lancaster University, Lancaster, UK. (E-mail: c.rotsos@lancaster.ac.uk).

A. K. Marnerides is with the School of Computing Science, University of Glasgow, Scotland, UK. (E-mail: angelos.marnerides@glasgow.ac.uk).

Energy theft has been a problem since the very early coal-based power grids and its manifestation has changed dramatically with the introduction of networking technologies, as well as, advanced energy trading platforms. Estimates of monetary loss attributed to energy theft in the UK and the US have been put at $170 million and $6 billion, respectively, in the last few years [4]. Evidently, the cybersecurity loopholes inherited by the interface of IoT technologies with AMI and legacy or bespoke industrial control system (ICS) in modern grids constitute the basis for various threat vectors in which consumers or prosumers could exploit primarily for monetary gain [5].

By virtue of the direct relationship and impact of the DR paradigm with energy trading as translated into financial transactions, energy theft has received a considerable level of attention by a number of studies. Nonetheless, the majority of studies was limited in scope due to their explicit focus on particular types of measurements or properties of the overall smart grid ecosystem. Effectively, existing energy theft detection schemes rely on readings related to consumption measurements [4], [6]–[15] or focus on DRES energy generation measurements [3], [16]–[18]. We argue that such monolithic approaches would be ineffective to be deployed and synchronised in practice by providers at different levels of aggregation, since they pose highly demanding computational requirements. Moreover, the algorithmic properties entailed within such approaches have proven to fail to adequately distinguish theft-related activities with anomalous events that could be caused by non-malicious intent (e.g., AMI equipment misconfiguration). Finally, the vast majority of theft detection solutions fail to effectively adapt and re-optimise their detection thresholds as they should by considering the addition of new types of grid components and the adoption of new technologies. Hence, a practical, holistic and adaptive energy theft detection scheme is required, capable to distinguish energy theft from device misconfiguration.

Therefore, in this paper, we aim to tackle some of the above challenges and gaps within the literature and thus present a novel energy theft detection approach that considers both power generation and consumption measurements. The proposed method is capable of distinguishing theft-related events from noisy data generated by misconfigured devices and more importantly, it can self-optimise based on the properties of incoming measurement streams without human intervention. In summary, we contribute by:

1) Formalising a novel and generic adversary model explicit to stealthy energy theft causing benign anomalies in consumption and generation measurements.
2) Introducing a novel energy theft detection system defined by the synergy of an adaptive feature composition scheme and an energy SM classification component resulted by the aggregation of weather condition measurements and misconfiguration events over DRES deployments.
3) Constructing a self-learning process to enable our system to continuously and autonomously retrain based on instantly available measurements.

The rest of this paper is structured as follows; Section II elaborates on previous related work, while Section III presents a generic model for mapping energy theft and misconfiguration events. Section IV describes the methodology underpinning our detection system whereas Section V demonstrates our evaluation methodology. Section VI evaluates the proposed soluton and demonstrates its ability to achieve high precision and accuracy in energy theft detection, whereas Section VII concludes this work.

II. Related Work

In general, energy theft detection can be categorised into two key approaches: (i) theft detection in consumptionmeasurements [4], [6]–[15], and ii) theft detection by profiling DRES generation measurements [3], [16]–[18]. The majority of recent research falls within the former strategy, aiming to detect theft activity in consumption measurements. Wen *et al.* in [4] introduce a novel privacy-preserving energy theft detection framework based on consumption measurements utilising federated learning. Similarly, the studies in Zheng *et al.* [6] and Yao *et al.* in [7] exploit the statistical properties of consumption measurements along with the use of convolutional neural networks (CNN) and the synergy of CNN with the Paillier cryptosystem's address privacy-preserving energy theft detection as a classification problem.

In addition, Zheng *et al.* in [9] employ measurements obtained from a smart observer meter installed to aggregate the sum of consumption measurements of each consumer group in a specific geographical area. The approach proposed in [9] is a composite of two data-driven techniques, namely, the maximum-information coefficient and a clustering technique facilitated by fast search and finding density peaks (CFSFDP). The detector developed by Takiddin *et al.* [10] is based on an adaptation of deep autoencoders with a long short-term memory network (LSTM) based sequence-to-sequence structure, with the synergy of energy consumption measurements. Gu *et al.* in [11] proposed a classification energy theft detection scheme based on a one-dimensional CNN, along with a set of fully-connected networks. Cui et al. in [8] adopt a synergistic approach that comprises a hand-crafted correlation feature extraction scheme and a CNN-based classifier.

In parallel, Gao *et al.* in [12] adapt the synergy of a modified linear regression model to estimate energy consumption measurements and examine regression residuals and thus detect energy theft activities. Similarly, Raggi *et al.* in [13] employ a data analytical detection approach based on a three-phase state estimator. Tariq *et al.* [14] introduce a theft detection system in which they initially construct a probabilistic Petri net model to analyse instances of energy theft attacks. They then employ singular value decomposition to accurately estimate line losses. Based on voltage and current observations, Salinas *et al.* [15] develop a Kalman filter-based state estimation scheme to identify measurement biases that can be used to detect energy theft activities. The scheme proposed in [15] employs a distributed approach to enable privacy-preserving identification of energy theft activities by leveraging communication technologies.

Nonetheless, all the aforementioned studies require large amounts of data that in practical resource-constrained energy systems and AMI deployments would incur high computational costs. In addition, the use of federated learning as in [4] or the employment of a smart observer meter as in [9] requires local detection points. and adding new components or customers to the grid would negatively affect both scalability as well as accuracy performance. Moreover, the effectiveness of the detector proposed in [12]–[15] relies on obtaining voltage data, distribution network topology and parameters. However, these may not be fully accessible to utility providers, thereby limiting the applicability of such detection schemes in practical scenarios.

A number of studies have developed energy theft models based on energy generation readings as reported by DRES owners (i.e. prosumers). The work by Ismail *et al.* in [16] considers energy theft as a classification problem through a deep learning-based approach and by integrating diverse DRES-oriented data sources, including weather data, supervisory control and data acquisition (SCADA) measurements. Moreover, Shaaban *et al.* in [3] develop an anomaly detection-based approach entailing a regression tree model and a probability density function. Yuan *et al.* [18] develop a theft detection approach using a synergistic least-squares method and a moving time window. Nevertheless, theft detection in individual DRES is proposed by Krishna *et al.* in [17] by exploiting the synergy of principal component analysis (PCA) with Kullback-Leibler divergence and auto-regressive integrated moving average (ARIMA) regression.

However, the unsupervised nature of such approaches as well as the data imbalance properties within actual test data sets may very possibly mislead the detection process, resulting in any abnormal profiles occurring due to non-malicious activity being detected as malicious behaviour. In addition, SCADA measurements as well as local metering components may not be readily available for detecting stealthy energy theft vectors and in many cases are not available to some utility providers, as also discussed in [19]. Hence, the applicability of the approach in [16], [18] is not generic.

In general, we witness that existing detection strategies lag behind in the following respects: (i) a holistic approach that considers both generation and consumption measurements has not been proposed in the context of energy theft detection, (ii) none of the schemes proposed in previous studies can adapt to varying properties of energy theft attack vectors along with SM misconfigurations, as we investigate in this paper, and (iii)

most of the current solutions fail to re-optimise their detection thresholds; they should be considering how these need to adapt in response to the adoption of new grid components and technologies.

III. Smart Grid & Energy Theft

A. System description

We consider an energy distribution network $G = \{A, N\}$ consisting of a set of consumers A distributed in several geographical regions and a set of low/medium voltage distribution buses N. Bidirectional data communication and power streams are used for energy transmission and distribution through corresponding power systems and networked data management components.

Each consumer u_i in G is equipped with an SM to measure energy consumption. The consumption of a single u_i at a given hour $h \in H$ for a day $d \in D$ and month $m \in M$, is represented by $Ec_i(h, d, m)$. For this representation, $H = 1, 2, ..., 24$, $D = 1, 2, ..., 30$ and $M = 1, 2, ..., 12$ are defined as the set of hours within a day, the set of days in a month and the set of months in a year, respectively. We define a subset $R \subseteq A$ as a group of consumers owning and managing a DRES installation (e.g. domestic solar panels) as well as consuming power (i.e. prosumers). The energy produced by a single prosumer $i \in R$ in a given time period h, d, m is measured by a second SM and mapped as the function $Er_i(h, d, m)$: $Er_i(h, d, m) = 0 \ \ \forall i \notin R$.

In this context, energy theft activities result in energy losses defined as the difference between the energy supplied into a grid and the energy consumed under normal conditions [9]. Thus, the cumulative energy loss over a single time period h, d, m can be expressed as follows:

$$NTL(h,d,m) = \Delta Es(h,d,m) + \sum_{i=1}^{|R|} \Delta Er_i(h,d,m) - \sum_{i=1}^{|A|} \Delta Ec_i(h,d,m) + \sum_{i=1}^{|N|} TL_p(h,d,m) \quad (1)$$

where $Es(h, d, m)$ is the energy supplied by the utility provider to all individuals in A at a time interval h, d, m. Δ is the discrepancy in the SM measurements for the actual and reported readings of a single consumer/prosumer u_i due to the energy theft activities at time h, d, m, and TL is the transmission line losses caused by physical restrictions.

B. Energy theft and SM misconfiguration model

The primary assumption of this work is that prosumers and/or consumers can manipulate their consumption and/or generation measurements to report erroneous energy readings. Thus, in Eq. 1, we rule out discrepancies in the energy supplied by the utility provider having $\Delta Es(h, d, m) = 0$, since this measurement is assumed to be usually secure under a reliable communication link [20]. However, the discrepancy in the SM generation and consumption readings in Eq. 1, Δ, may occur by both a theft-related activity or a non-malicious event, such as a misconfiguration. In general, energy losses defined in Eq. 1 relate to metering conditions that manifest as anomalous behaviour in the measurement of that particular meter. Such occurrences are common in instances of energy theft-related activities as well as SM misconfiguration incidents.

Therefore, to distinguish SM discrepancies, we present in Table I a taxonomy of SM anomaly function definitions, based on energy consumption and generation measurements. All functions mimic pragmatic characteristics of fraudulent or misconfigured SM patterns in terms of erroneously reported measurements. There anomaly functions are based on findings in the literature [9], [16], [20]–[24] and reflect a representative collection of common anomaly operations. According to Table I, misconfiguration and theft activities can partially or completely change the reported energy timeseries signal. Theft activities within consumption measurements target to decrease the monetary value of a consumer and thus they are mapped as a direct decrease in consumed energy. However, SM misconfigurations lead to unexpected increases in consumed energy. Theft functions exploiting DRES generation measurements with a goal for monetary gain feature an increase in the reported generated energy, while the misconfiguration of the DRES's SM is described as the curtailment of DRES energy back to the grid.

IV. Energy Theft Detection

As illustrated in Fig. 1, our system consists of two stages: (i) feature construction and, (ii) SM classification modules.

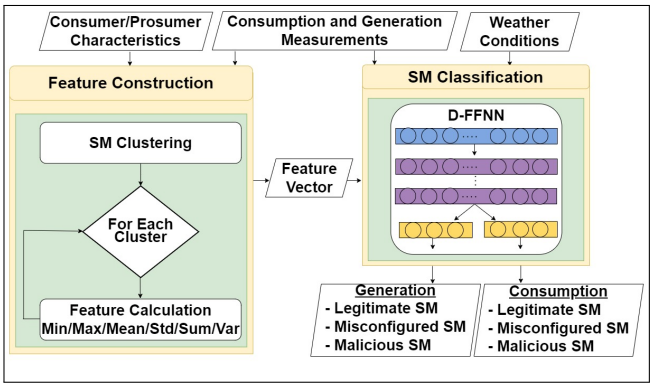

Fig. 1: Data-flow of the proposed system.

A. Feature construction

The feature construction stage processes timeseries data from the infrastructure and builds extended feature sets. This is achieved by composing first order statistics (e.g., min/max, variance) of generation and consumption measurements for each group of consumers and prosumers. We consider correlated spatiotemporal behaviour across timeseries measurements by virtue of behavioral similarities in seasonal consumption and generation patterns.

For example, a peak in consumption pattern caused by air-conditioning demand during a hot wave could be observed across a large number of neighbouring consumers with similar characteristics. Similarly, prosumers managing solar panels can have a correlated generation pattern based on sunlight availability. It is thus feasible to establish a ground truth

TABLE I: Energy theft and SM misconfiguration functions where α, β, $\gamma(.)$, $\zeta(.)$, $\iota(.)$ and $\tau(.)$ are anomaly coefficients.

Type	Measurement	Function
Curtailment misconfiguration	Generation	$\Delta Er_i(h,d,m) = \alpha Er_i(h,d,m) \quad \forall\, Er_i(h,d,m) > 0$, where $\{\ \alpha \in \mathbb{R} \mid 0 \leq \alpha < 1\}$
Amplification misconfiguration	Consumption	$\Delta Ec_i(h,d,m) = \beta Ec_i(h,d,m) \quad \forall\, Ec_i(h,d,m) > 0$, where $\{\beta \in \mathbb{R} \mid \beta > 1\}$
Disconnect misconfiguration	Generation	$\Delta Er_i(h,d,m) = \text{NaN}$
	Consumption	$\Delta Ec_i(h,d,m) = \text{NaN}$
Total scaling theft	Generation	$\Delta Er_i(h,d,m) = \gamma(h,d,m) Er_i(h,d,m) \quad \forall\, Er_i(h,d,m) > 0$, where $\{\gamma(h,d,m) \in \mathbb{R} \mid \gamma > 1\}$
	Consumption	$\Delta Ec_i(h,d,m) = \zeta(h,d,m) Er_i(h,d,m) \quad \forall\, Ec_i(h,d,m) > 0$, where $\{\ \zeta(h,d,m) \in \mathbb{R} \mid 0 \leq \zeta(h,d,m) < 1\}$
Partial scaling theft	Generation	$\Delta Er_i(h,d,m) = \begin{cases} Er_i(h,d,m), & Er_i(h,d,m) \geq \iota \\ \iota, & Er_i(h,d,m) < \iota \end{cases}$ where $\{\iota > \in \mathbb{R} \mid \iota > \text{Min}\big(Er_i(1,d,m), Er_i(2,d,m), ..., Er_i(24,d,m)\big)\}$
	Consumption	$\Delta Ec_i(h,d,m) = \begin{cases} Ec_i(h,d,m), & Ec_i(h,d,m) \leq \tau \\ \tau, & Ec_i(h,d,m) > \tau \end{cases}$ where $\{\tau \in \mathbb{R} \mid \tau < \text{Max}\big(Ec_i(1,d,m), Ec_i(2,d,m), ..., Ec_i(24,d,m)\big)\}$
Off-peak theft	Generation	$\Delta E_r(h,d,m) = \begin{cases} \gamma(h,d,m) Er_i(h,d,m), & hs \leq h \leq he \mid Er_i(h,d,m) > 0 \\ Er_i(h,d,m), & otherwise \end{cases}$ where hs and he is the off-peak operating weather conditions for DRES.
On-peak theft	Consumption	$\Delta E_c(h,d,m) = \begin{cases} \zeta(h,d,m) Ec_i(h,d,m), & hb \leq h \leq hc \mid Ec_i(h,d,m) > 0 \\ Ec_i(h,d,m), & otherwise \end{cases}$ where hb and hc is the on-peak load hours.
Reply theft	Generation	$\Delta Er_i(h,d,m) = \text{Max}\big(Er_i(h-1,d,m), Er_i(h,d,m)\big)$
	Consumption	$\Delta Ec_i(h,d,m) = \text{Min}\big(Ec_i(h-1,d,m), Ec_i(h,d,m)\big)$
Stability theft	Generation	$\Delta Er_i(h,d,m) = \text{Max}\big(Er_i(1,d,m), Er_i(2,d,m), ..., Er_i(24,d,m)\big)$
	Consumption	$\Delta Er_i(h,d,m) = \text{Min}\big(Ec_i(1,d,m), Ec_i(2,d,m), ..., Ec_i(24,d,m)\big)$

with respect to normal generation or consumption profiles. In particular, the feature construction module stage clusters SM using an incremental K-means algorithm, which partitions SMs into k clusters based on a set of consumer/prosumer characteristics. In this work, these characteristics include geographical location, DRES physical characteristics (i.e. solar panel capacity), and tariff agreement type. Clustering SMs based on common characteristics allows the classification stage to extract common energy generation and consumption patterns emerging between consumers/prosumers within the same cluster [25], [26].

Let an initial set of K-means $\left[\xi_1^{[1]}, \xi_2^{[1]}, ..., \xi_K^{[1]}\right]$, each consumer/prosumer $u_i \in G$ would group into a cluster whose mean is the shortest squared Euclidean distance as:

$$s_q^{[r]} = \left\{ u_i \ :|| \ u_i - \xi_q^{[r]} \ ||^2 \leq || \ u_i - \xi_j^{[r]} \ ||^2 \ \forall \ j \in [1,k] \right\} \tag{2}$$

In each iteration, the mean of the clusters can be updated as follows:

$$\xi_q^{[r+1]} = \frac{1}{\mid s_q^{[r]} \mid} \sum_{u_j \in s_q^{[r]}} u_j \tag{3}$$

Formally, the objective here is to minimise intra-cluster variance as:

$$\arg\min_{s} \sum_{q=1}^{k} \sum_{u \in s_q} || \ u - \xi_q \ ||^2 \tag{4}$$

where ξ_q is the mean of consumers and prosumers in s_q. The output of this process is a list of clusters $S = \left[s_1, s_2, ..., s_K\right]$ determining which cluster each individual $u_i \in G$ is grouped into and a list of the mean of each cluster $\Xi = \left[\xi_1, \xi_1, ..., \xi_K, \right]$ determining the mean of the individuals in each cluster. Once consumers and prosumers with correlated consumption and generation measurements are grouped, we calculate a set of variables representing regular consumption and generation patterns for the individuals within each cluster.

Hence, for each cluster, we calculate the minimum (min), maximum (max), (var) variance, standard deviation (std), sum and mean of the generation and consumption measurements of a set of completely legitimate consumers/prosumers in that cluster. These variables provide different perspectives on the generated and consumed energy within that cluster, and overall they reflect the regular consumption and generation patterns for customers within that group. Thus, these features are preserved to serve as the ground truth of the regular generation and consumption patterns to support the detection process within each cluster.

B. SM classification

Due to its ability to address multiple tasks simultaneously, this module adopts a dual deep feed forward neural network (D-FFNN) to determine whether each consumption and generation measurement is malicious, misconfigured or legitimate. This ability of the proposed D-FFNN offers several advantages over conventional feed-forward neural networks (FFNN), which adapt two isolated networks for each classification process. Hence, our D-FFNN is able to learn information shared between the classification processes of consumption and generation measurements in order to boost the performance of both. In addition, the inherent layer-sharing of our D-FFNN reduces the memory demands of both classification processes. Similarly, the proposed D-FFNN avoids repeatedly calculating the features in shared layers, which substantially increases the inference speeds of both classification processes.

The structure of the proposed D-FFNN is illustrated in Fig. 2. It comprises of an input layer with v neurons followed by l fully-connected hidden layers, each with ne neurons, and finally, dual output layers, each with 3 neurons as per the category each sample is stratified (i.e. malicious, misconfigured, legitimate). The input layer sends the input data $X = \{x^{[1]}, x^{[2]}, ..., x^{[|X|]}\}$ to the hidden layers to extract features and understand patterns to facilitate producing a given category by each output layer. Each $x^{[i]} \in X$ is an instance in the $\mathrm{v}-$dimensional feature space, i.e. $x^{[i]} = [x_1, x_2, ..., x_v]$.

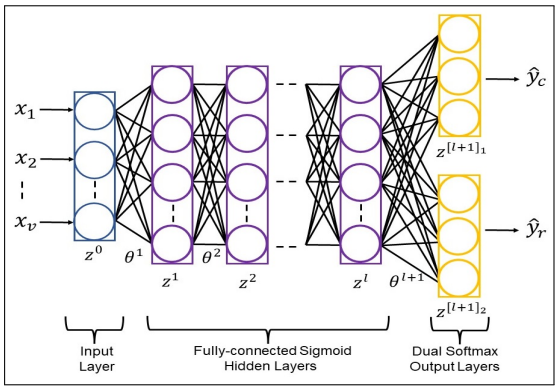

Fig. 2: The basic architecture of the D-FFNN.

This feature space includes the reported consumed energy $Ec_i(h, d, m)$ and generated energy $Er_i(h, d, m)$ together with the features constructed in Section (IV-A) and the weather conditions of i's geographical region for each $i \in G$ over the time slot h, d, m. The first output layer projects the category of the consumer's i consumption measurement $\hat{y}_c^{[i]}$ whereas the second output layer projects the category of the generation reading $\hat{y}_r^{[i]}$ at the time h, d, m. These two decisions indicate whether each SM of each consumer or prosumer is legitimate, malicious, or misconfigured.

To train the D-FFNN, the input instances in X are mapped through the hidden layers from the input layer to the dual output layers as follows:

$$z^{[n]} = \sigma\left(\theta^{[n]} \cdot z^{[n-1]} + b^{[n]}\right) \quad \forall\, n \in [1, l+1] \tag{5}$$

where:

$$\begin{cases} z^{[0]} = x^{[i]} = [x_1, x_2, ..., x_v] \\ z^{[l+1]_1} = \hat{y}_c^{[i]} \\ z^{[l+1]_2} = \hat{y}_r^{[i]} \end{cases}$$

Here b represents a bias vector, θ is the connection weight, and $\sigma(\cdot)$ is a sigmoid function for the hidden layer and a softmax function for the dual output layers. The objective of the training process of our D-FFNN is to use a standard back-propagation to find b and θ. The training process here is achieved by minimizing the dual objective function:

$$\arg\min_{\theta,b} J = \frac{1}{|X|} \sum_{i=1}^{|X|} \left(L\left(\hat{y}_c^{[i]}, y_c^{[i]}\right) + L\left(\hat{y}_r^{[i]}, y_r^{[i]}\right) \right) \tag{6}$$

where $y_c^{[i]}$ and $y_r^{[i]}$ represent the actual category corresponding to a sample $x^{[i]} \in X$ and $L(\cdot)$ is a three-class cross entropy function formulated as:

$$L(\hat{y}, y) = -\sum_{i=1}^{3} \eta_i \, y_i \log(\hat{y}_i) \tag{7}$$

where η represents an adjustment weight map for each category to force the detector to focus on the category where a larger learning loss occurs, resulting from an imbalance issue, to improve its performance.

Algorithm 1 outlines the workflow for the entire training process. Within this algorithm, $\odot$ represents element-wise multiplication, ρ is a predefined learning rate, T is transpose operation, $\sigma'(\cdot)$ is the derivative of an activation function $\sigma(\cdot)$, ∇_z is the gradient of the loss function J with respect to z, and $\delta^{[n]}$ is the error in the layer n. As illustrated in this algorithm, each training sample $x^{[i]} \in X$ undergoes forward processing in our D-FFNN to determine the output vectors of each layer $n \in [1, l+1]$. This process yields the final dual classification outputs, denoted as $\hat{y}_c^{[i]}$ and $\hat{y}_r^{[i]}$. The gradient of the three-class cross-entropy function (Equation (6)) with respect to the output of the last layer, $l+1$, is then computed by utilizing an error term $\delta^{[l+1]}$. Subsequently, the gradient is backpropagated through the D-FFNN to obtain gradients with respect to the inputs and weights of the previous layers. The weights θ and bias b values for each layer of the D-FFNN are then adjusted utilizing the gradient descent method.

Algorithm 1 D-FFNN training.

Initialise $\theta^{[n]}$ and $b^{[n]}$ randomly $\forall\, n \in [1, l+1]$
for each training sample $x^{[i]} \in X$ **do**
  for each layer $n \in [1, l+1]$ **do**
    Calculate $z^{[n]}(x^{[i]})$ using Equation 5
  end for
  Calculate

$$\delta^{[l+1]}(x^{[i]}) = \nabla_z J(x^{[i]}) \odot \sigma'\left(\theta^{[l+1]} \cdot z^{[l]}(x^{[i]}) + b^{[l+1]}\right)$$

  Calculate $\theta^{[l+1]} = \theta^{[l+1]} - \rho\, \delta^{[l+1]}(x^{[i]})\left(z^{[l]}(x^{[i]})\right)^T$
  Calculate $b^{[l+1]} = b^{[l+1]} - \rho\, \delta^{[l+1]}(x^{[i]})$
  for each hidden layer $n \in [1, l]$ **do**
    Calculate

$$\delta^{[n]}(x^{[i]}) = \left((\theta^{[n+1]})^T \delta^{[n+1]}(x^{[i]})\right) \odot \sigma'\left(\theta^{[n]} \cdot z^{[n-1]} + b^{[n]}\right)$$

    Calculate $\theta^{[n]} = \theta^{[n]} - \rho\, \delta^{[n]}(x^{[i]})\left(z^{[n-1]}(x^{[i]})\right)^T$
    Calculate $b^{[n]} = b^{[n]} - \rho\, \delta^{[n]}(x^{[i]})$
  end for

end for

Finally, the initial D-FFNN defined by its trained parameters, i.e. θ and b, is preserved to save the knowledge acquired during the learning process from the input data X. Thus, it can be used for detecting further measurements where each SM is listed in one of three groups – legitimate, malicious, or misconfigured – based on the results of the classification process.

C. Self-learning operation

The self-learning operation of our detection system starts once a new batch of SM measurements is available. In this

regard, new consumption and generation measurements are collected from the grid's consumers and prosumers, whose measurements may have been collected in the first data batch, or from new individuals who were connected recently to the power system. In order to accommodate new individuals within a new batch of SM measurements without rerunning the clustering process on old individuals within old batches, our self-learning operation builds on top of the incremental clustering strategy proposed by Chakraborty and Nagwani in their work [27].

A generalised workflow of the self-learning operation is described in Algorithm 2. As illustrated in this algorithm, the system initially assigns each individual in the new batch to a corresponding cluster defined in the saved list of clusters S in Section IV-A. However, if the new batch contains measurements from new consumers/prosumers, the squared Euclidean distance between these new individuals and the K-means in Ξ is measured. Subsequently, each new consumer/prosumer is assigned to the nearest cluster whose mean is the shortest distance, if this distance is smaller than a predefined threshold T_k. Otherwise, the system creates a new cluster for this new individual and updates the cluster set S and means set Ξ by adding the means of the recently created cluster. We set the threshold T_k by referencing the longest distance between each individual and its cluster mean in the initial measurement batch. Once consumers and prosumers are clustered, the system calculates the set of features proposed in Section IV-A from the newly available measurements to create the new input batch X' along with the weather data.

Algorithm 2 Self-learning operation.

```
Recall S and Ξ
Assign each consumer/prosumer u_i to its cluster s_q
for each new u_i do
    Find ξ_q ∈ Ξ : || u_i − ξ_q ||^2 is the smallest
    if || u_i − ξ_q ||^2 < T_k then
        s_q = s_q ∪ u_i
        Updated Ξ
    else
        Updated S
        Updated Ξ
    end if
end for
Construct features from each cluster
Collect weather condition measurements
Merge all measurements to create input data X'
Load D-FFNN
for each x^[i] ∈ X' do
    ŷ_r^[i] and ŷ_c^[i] ← D-FFNN(θ, b, x^[i])
end for
Calculate AC_c and AC_r using Equation (8)
if AC_c ≤ T_c OR AC_r ≤ T_r then
Retrain D-FFNN with X' using Equation (5) to minimise the objective function in Equation (6)
end if
Save D-FFNN
```

Following the update of the new features based on newly available measurements, the previous version of the D-FFDD detection module is loaded such as to predict the consumption categories $\hat{y}_c$ and generation categories $\hat{y}_r$ in X'. The accuracy of this detection process is measured as follows:

$$AC = \frac{1}{3}\sum_{c=1}^{3}\frac{TP_c + TN_c}{TP_c + FN_c + FP_c + TN_c} \tag{8}$$

where TP are true positives, TN are true negatives, FN are false negatives, and FP are false positives.

As a result, we obtain two values AC_c and AC_r indicating the average number of correct predictions of $\hat{y}_c$ and $\hat{y}_r$, respectively, for all observations in X'. If one of the calculated values is less than the predetermined thresholds T_c and T_r, the batch is considered challenging, and the preserved D-FFDD is retrained automatically, using Equation (5), with the goal of minimizing the objective function in Equation (6). We set these thresholds by referencing arbitrary values around the accuracy of the training step of the system in the initial measurement batch. Similarly with the rest of the parameters, the weights for the preserved D-FFNN will also be incrementally updated with the back-propagation as the new batch X' pass. This step is required such as the proposed classification module will adapt to observe the newly arrived generation and consumption measurements and self-optimise its own parameters.

V. Datasets and Evaluation Methodology

A. Datasets description

To validate our work, we utilise energy consumption and generation datasets collected in the power network of Australia's largest electricity provider, Ausgrid [1]. The dataset represents the generation and consumption measurements captured at a real installation of 300 different consumers and prosumers with rooftop solar panels from 1 July 2010 to 30 June 2013. However, in this work, we use only 139 individuals whose measurements were valid for the entire period. In addition to the consumption and generation SM measurements, the dataset includes information with respect to consumer/prosumer geolocation (e.g., postal codes) and solar panel capabilities (e.g., capacity).

As already mentioned, our system depends solely on weather conditions. For this purpose, the available weather measurements were extracted from the World Weather Online API [2] and predictions of worldwide energy resources (POWER) project API [3] over the same observational period as that of the measurements obtained for Asugrid individuals.

B. Evaluation methodology

To demonstrate the effectiveness of our system, we conduct a performance comparison across four clustering algorithms named the density-based spatial clustering of applications with noise (DBSCAN), agglomerative nesting (AGNES), affinity propagation (AP), and fuzzy C-means clustering (FCM). We measure the **silhouette coefficient (SC)** score to evaluate whether individuals are clustered in well-defined groups. The SC is defined as:

$$SC = \frac{1}{\mid A \mid}\sum_{e=1}^{|A|}\frac{c(e) - o(e)}{\mathrm{Max}\big(c(e), o(e)\big)} \tag{9}$$

[1]Explore – Ausgrid Solar Home Electricity Data, Available:https://www.ausgrid.com.au/Industry/Our-Research/Data-to-share/Solar-home-electricity-data

[2]Explore – Weather API, Available:https://www.worldweatheronline.com/developer/api/

[3]Explore – Power Hourly API, Available:https://power.larc.nasa.gov/api/pages/

where $\mid A \mid$ is the total number of individuals in the grid, $c(.)$ is the average distance between a consumer/prosumer and other individuals in the same cluster, and $o(.)$ is the minimum average distance between that individual and all individuals belonging to other clusters.

Furthermore, we conduct a performance evaluation of various classification algorithms including both classic techniques (such as conventional FFNN, decision tree (DT), support vector (SVM) and K-nearest neighbours (K-NN)) and advanced methods (such as extreme gradient boosting (Xgboost)). This evaluation excludes advanced deep learning models such as LSTM because they require a two-dimensional feature vector, whereas our data is only one-dimensional. For this comparison, we utilise the following performance metrics:

1) **Precision (PR)** defined as:

$$PR = \frac{1}{3}\sum_{c=1}^{3}\frac{TP_c}{TP_c + TF_c} \tag{10}$$

2) **Recall (RE)** defined as:

$$RE = \frac{1}{3}\sum_{c=1}^{3}\frac{TP_c}{TP_c + FN_c} \tag{11}$$

3) **F1 Score (F1)** defined as:

$$F1 = 2 \times \frac{RE \times PR}{RE + PR} \tag{12}$$

4) **Area Under the Curve (AUC)** defined as:

$$AUC = \frac{1}{3}\sum_{i=1}^{3}\sum_{j>i}^{3}\Big(\mathrm{BAUC}(i,j) + \mathrm{BAUC}(j,i)\Big) \tag{13}$$

where

$$BAUC(x,y) = \frac{\mathrm{Ranks} - \frac{AP}{2} \times (1 + AP)}{AP \times AN} \tag{14}$$

Here Ranks represents the sum of the ranks from class x, AP is the number of samples in class x and AN represents the number of samples in class y. The samples are arranged in ascending order based on the prediction of class i for ranking [6].

5) **Computational complexity:** to measure the inference time required to obtain classification decisions on test data.

It is worth mentioning that the computational complexity excludes the grid search process utilised to train and fine-tune hyper-parameters. It transforms a hyper-parameter domain into a grid and then traverses each point on the grid to obtain the optimal classifier parameters. Utilising such a search strategy is straightforward, and the optimal search speed is quite reasonable. In addition, the optimal hyper-parameters are determined independently, enabling simultaneous optimization. Table II illustrates the results of the grid-search process for each classification algorithms.

In addition, the **RE**, **PR**, **F1** and **AUC** are utilised to conduct a performance evaluation of the self-learning operation employed within the cross-batch theft detection process. The cross-batch theft detection process is described as the classifier trained on the initial batch training data is used to directly identify thefts and misconfigurations for the test set across other batches.

TABLE II: Optimal hyper-parameters of the classification algorithms.

Algorithm	Measurement	Hyper-parameters
D-FFNN	Dual (Generation, Consumption)	l=8, ne in hidden layer 1=70, ne in hidden layer 2=70, ne in hidden layer 3=60, ne in hidden layer 4=50, ne in hidden layer 5=30, ne in hidden layer 6=40, ne in hidden layer 7=20, ne in hidden layer l=4, Batch size=32, Optimizer=adam, Learn rate=0.001
FFNN	Generation	Number of hidden layers= 5, Number of neurons in each hidden layer=$[20, 20, 10, 5, 5]$, Batch size=32, Optimizer=adam, Learn rate=0.01
	Consumption	Number of hidden layers= 7, Number of neurons in each hidden layer=$[50, 40, 30, 20, 10, 10, 6]$, Batch size=32, Optimizer=adam, Learn rate=0.0001
SVM	Generation	Kernel= radial basis function, C=1, Gamma=$0, 2$
	Consumption	Kernel= radial basis function, C=10, Gamma=$0, 1$
DT	Generation	Maximum depth=12, Minimum samples split=2, Minimum samples leaf=2
	Consumption	Maximum depth=15, Minimum samples split=4, Minimum samples leaf=2
K-NN	Generation	Number of neighbors=15
	Consumption	Number of neighbors=20
Xgboost	Generation	Number of estimators=7, Maximum depth=10
	Consumption	Number of estimators=10, Maximum depth=15

During our evaluation, we synthetically inject anomalous patterns within Ausgrid's dataset using the functions in Table I to emulate fraudulent and misconfigured samples. In order to avoid a data imbalance issue resulting from this procedure, a higher weight to the loss encountered by the samples associated with minor categories in Equation 7 is assigned. To note that we filter out instances of disconnect misconfgurations during the pre-processing stage. Evidently, such events demonstrate extremely large numbers of missing values in both generation and consumption measurements and they were affecting significantly the training phase. We also adjust the value of the solar panel SM to zero for a randomly chosen third of individuals to simulate simple consumers (i.e. not owning/managing a DRES).

Moreover, we group the Ausgrid dataset by year to simulate a scenario in which SM measurements were presented continuously over time. Nevertheless, to simulate a scenario in which new individuals join the grid, we removed the measurements of ten arbitrarily chosen individuals from the first batch, and reintroduce them incrementally across batches. Each batch is split into training and testing sets, with a ratio of $70 : 30$ respectively. Overall, the training data size for all batches is set to $32,824,584$ samples, while the testing data size is $14,336,712$ samples. In order to reliably evaluate the performance of our classifiers, we utilise the 10-fold cross-validation technique on the training data. This enables us to

fine-tune the hyper-parameters, while the test data is employed for the final evaluation. We then normalise the training and test data incrementally to transform all the features' values into a single scale with unit variance and mean of zero and for categorical time series, we encode them using a binary encoder [28].

As part of our evaluation, we analyse the sensitivity of the proposed approach in order to reflect its robustness to emerging energy-theft behaviours. We introduce three cases of training data for this evaluation. In the first case, we inject malicious samples based on two arbitrarily selected theft functions from Table I into the training data of the 2010 batch, while retaining all legitimate and misconfigured samples. Malicious samples gradually increase as we inject one more theft function across the other two training-data cases. Test data were maintained across all three cases to include all seven functions of theft. Hence, in this scenario, our detection approach is evaluated against theft-attack functions that were not included in the training data sets.

VI. Results

Following the evaluation methodology presented earlier, the produced outputs in Fig. 3 indicate that the K-means formulation achieved the highest SC score (i.e. SC=0.44), with 5 clusters generated during the training phase of our system. Thus, we utilize its capabilities for the proposed detection system. Note that DBSCAN and AP algorithms, unlike K-means, AGNES, and FCM, do not require a prior determination or estimation of the number of clusters. Instead, they infer the number of clusters from the number of individuals in the training dataset. In Fig. 3, the SC scores of these algorithms are plotted solely with respect to their calculated cluster number (i.e. 5 clusters for the AP algorithm and 4 clusters for DBSCAN).

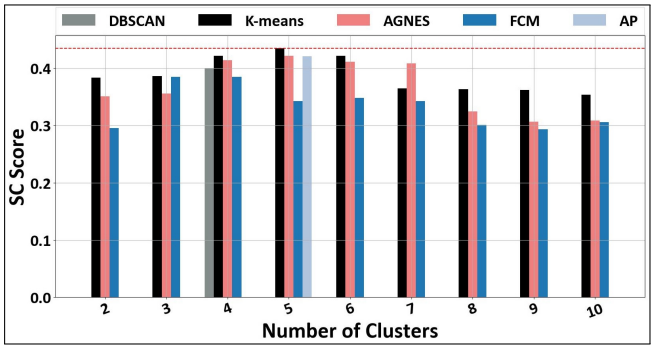

Fig. 3: SC score of different clustering algorithms.

In addition, the D-FFNN, formulation performed better than all classification algorithms in detecting malicious and misconfigured meters as demonstrated in Table III. With respect to generation measurements, the D-FFNN scheme recorded a precision of 0.92, 0.90, 0.85, 0.84 and 0.91 higher than that of the conventional FFNN, DT, SVM, K-NN and Xgboost respectively. This was similar to the consumption measurements, where the D-FFNN outperformed the other classifiers, as it recorded a 72% precision accuracy, while the conventional FFNN, DT, SVM, K-NN and Xgboost achieved 0.69, 0.68, 0.71, 0.59 and 0.68 respectively.

TABLE III: Detection performance of the SM classification module using different algorithms.

Algorithm	Performance Parameter							
	Consumption				Generation			
	PR	RE	F1	AUC	PR	RE	F1	AUC
D-FFNN	0.72	0.69	0.70	0.73	0.92	0.92	0.92	0.91
FFNN	0.69	0.67	0.67	0.68	0.89	0.88	0.88	0.89
DT	0.68	0.61	0.64	0.68	0.90	0.89	0.89	0.88
SVM	0.71	0.69	0.69	0.69	0.85	0.85	0.85	0.84
K-NN	0.59	0.49	0.53	0.60	0.84	0.84	0.84	0.83
Xgboost	0.68	0.65	0.66	0.67	0.91	0.90	0.90	0.89

Evidently, the D-FFNN superiority over the conventional FFNN, DT, SVM, K-NN and Xgboost in generation and consumption measurements were uniform, even when RE, F1 and AUC scores were measured. We argue, that the D-FFNN formulation is superior due to its ability to capture hidden patterns in the weather condition data as well as the constructed features in Section IV-A. Moreover, compared to the conventional FFNN, our proposed D-FFNN scheme is superior because of its ability to handle multiple tasks simultaneously. It can fully utilize shared information in the classification processes of consumption and generation SMs to improve the performance of both.

Superior detection performance in terms of RE, PR, F1, and AUC was observed, particularly for generation measurements, as depicted in Table III. This better performance can be attributed to the feature construction module discussed in Section IV-A, which effectively enhances the performance of our classifier for generation SMs. The aim of this module is to build a set of variables that profile normal energy behaviours in order to boost the classification process of generation and consumption SMs, i.e. whether each one is malicious, misconfigured or legitimate. However, Ausgrid's data set does include some consumer/prosumer characteristics. The characteristics included in Ausgrid's data set are geographical location, DRES physical characteristics (i.e. panel capacity) and tariff agreement type. In the case of generation measurements, the variables distilled by the original solar-panel capacity feature, which are available in Ausgrid's data set, were instrumental in profiling prosumer normal behaviour with respect to generation. Hence, the objective of the module to construct valuable features was achieved, and classification performance was boosted. Nonetheless, Ausgrid's data set lacks consumer characteristics (e.g. number of rooms, appliances) that can contribute to better profiling of consumers with similar consumption patterns. Accordingly, the objective of the feature construction module was not met, and the classification performance of consumption measurements was not improved as required.

In this scenario, it is necessary to use extra features in the SM clustering procedure in order to improve the performance of the classification process in consumption measurements. However, a trade-off should be made between the efficiency benefit and the issue of over-fitting. Hence, the addition of features can lead to a detection strategy that is specifically

tailored to suit particular data conditions and settings, limiting its generalisability. Overall, these findings indicate that our feature construction module plays a significant role in boosting up the detection performance; however, it should be trained with consumer/prosumer characteristics that effectively reflect behavioral similarities in consumption and generation patterns.

Apart from high precision accuracy, the D-FFNN formulation also operates with relatively lower computational time compared to other schemes including the conventional FFNN as depicted in Fig.4[4]. Arguably, this outcome revolves around the fact that the rest of the formulations required independently trained models explicit to either generation or consumption measurements incurring extensive computational overheads. In addition, compared to the conventional FFNN, the proposed D-FFNN avoids repeatedly calculating the features in shared layers, which significantly increases the inference speeds of energy theft classifications. This demonstrates the efficacy of using a dual, deep learning technique instead of conventional techniques in our detection system, as we need to train one model with two outputs to address both tasks simultaneously.

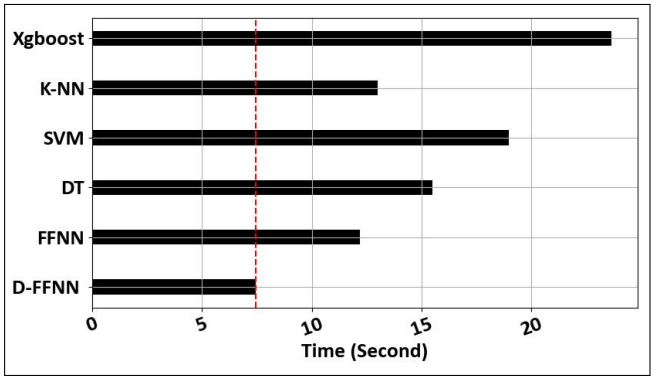

Fig. 4: The computational complexity time of different classification algorithms.

Deteriorated performance over time was observed in the cross-batch detection process, where the 2010 training data is used to detect thefts and misconfigurations across 2011, 2012 and 2013 as depicted in Fig. 5. The impact on accuracy performance is a result of the change in data distribution properties across the batches. Consequently, such change misleads the detection system over the years and results in further detection errors.

The main cause for such a change is attributed via including entirely new individuals whose measurement patterns vary from the patterns included in the first batch's training data. Therefore, the detection system fails to identify the measurements of consumers/prosumers who have recently connected to the network and decide whether they are legitimate, malicious, or misconfigured. Even in cases where no new individuals are linked with the grid, the generation and consumption measurements of the same individuals usually have non-stationary properties, so the distribution of the data also varies across batches. The non-stationary properties in the consumption

[4]On 64-bit Windows operating system with an Intel Core i7 ($7th$ Gen) CPU with a 2.80 GHz clock cycle and 32 GB of RAM.

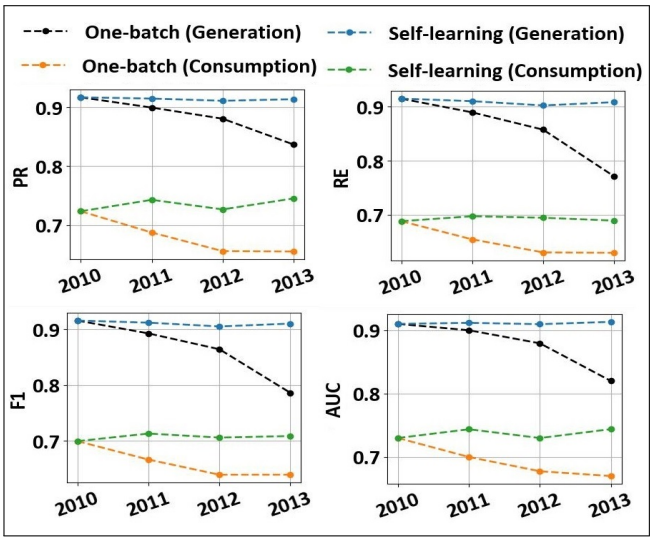

Fig. 5: Cross-batch detection performance.

TABLE IV: Accuracy of the SM classification module in the cross-batch detection process.

Batch	Consumption	Generation	Consumption Threshold	Generation Threshold
2010	0.72	0.92	0.71	0.91
2011	0.67	0.90	0.71	0.91
2012	0.67	0.87	0.71	0.91
2013	0.70	0.90	0.71	0.91

measurements are caused by changes in consumption habits, for example, installing eco-friendly equipment that reduces energy consumption [29], while the non-stationary nature of the generation measurements is usually caused by changes in the weather conditions over many years [30].

However, as depicted in Table. IV, whilst the detection accuracy of the consumption and generation measurements are less than the predefined thresholds in the 2011 data batch, the system considers the batch challenging and self-optimises by retraining on that batch. As a result, the performance of the proposed system is improving based on the test data of the 2011 batch (see Fig. 5). The same process was also carried out for the years 2012 and 2013 to ensure validation.

The sensitivity analysis of our detection approach is depicted in Table V. The D-FFNN formulation maintains superior detection performance even when testing with emergent theft behaviours, demonstrating the robustness of the proposed detection approach. In the first case, the D-FFNN formulation achieved PR, RE, F1, and AUC of 0.68, 0.66, 0.66 and 0.67 in consumption meters, and PR, RE, F1, and AUC of 0.87, 0.88, 0.87, and 0.88 in generation meters. In addition, the performance of the D-FFNN gradually improved as the number of malicious samples increased, and a further theft function was provided in the remaining two cases. These observations are due to the capacity of the DFFNN to generalise pattern-learning knowledge. The DFFNN was effectively able to generalise its knowledge of the most distinguishing characteristics of observed meter patterns, and their relationship to weather condition data and constructed feature in Section IV-A.

TABLE V: The sensitivity analysis of the detection approach.

Case	Performance Parameter							
	Consumption				Generation			
	PR	RE	F1	AUC	PR	RE	F1	AUC
1	0.71	0.60	0.64	0.71	0.88	0.86	0.87	0.89
2	0.73	0.63	0.66	0.72	0.89	0.87	0.88	0.89
3	0.72	0.66	0.68	0.72	0.90	0.89	0.89	0.89

VII. Conclusion

Modern energy theft techniques exploit the highly distributed nature of the modern smart grid and cause significant financial loss to energy providers. Hence, tracking such events is critical but also challenging due to the diversity of the composite attack vectors triggering them where faults promote the same properties as theft. In this paper, we propose a self-learning system that can distinguish energy theft from faults with the joint use of consumption and generation measurements as well as openly available weather information. The outcomes of an extensive and comparative evaluation over real measurements reveal that the introduced scheme can reach over 90% of accuracy under the D-FFNN formulation and with relatively low computational overheads. Its joint use with other ML techniques under the proposed methodology that can provide for the analysis of cross-batch measurement streams can adequately adapt over varying properties of theft or misconfiguration scenarios. It can thus benefit the design of next-generation energy theft detection systems.

As future work, we are currently exploring the use of quantum machine learning strategies in our proposed detection system. Unlike traditional computers that rely on the physical implementation of the 0 and 1 states, quantum computers use qubits that can simultaneously represent both $|0\rangle$ and $|1\rangle$ states, allowing for the execution of multiple computational processes concurrently [31]. We anticipate that using quantum machine learning will improve the learning efficiency of our D-FFNN, potentially enabling us to achieve the same detection performance with fewer training data or simpler architectures. Additionally, the use of quantum machine learning techniques may also reduce computational complexity and speed up the theft classification process for scalable energy systems.

Acknowledgment

This work sponsored by Taif University and the Saudi Arabia Cultural Bureau in London. The authors gratefully acknowledge the support of the Next Generation Converged Digital Infrastructure (NG-CDI) Prosperity Partnership project funded by UK's EPSRC and British Telecom plc.

References

[1] GovUK, "Smart meter statistics in great britain: Quarterly report to end march 2022," 2022, accessed: 2022-01-22. [Online]. Available: https://www.gov.uk/government/statistics/smart-meters-in-great-britain-quarterly-update-march-2022

[2] Ofgem, "Smart meter transition and the data communications company (dcc)," 2022, accessed: 2022-01-22. [Online]. Available: https://www.ofgem.gov.uk/energy-policy-and-regulation/policy-and-regulatory-programmes/smart-meter-transition-and-data-communications-company-dcc

[3] M. Shaaban, U. Tariq, M. Ismail, N. A. Almadani, and M. Mokhtar, "Data-driven detection of electricity theft cyberattacks in pv generation," *IEEE Systems Journal*, 2021.

[4] M. Wen, R. Xie, K. Lu, L. Wang, and K. Zhang, "Feddetect: A novel privacy-preserving federated learning framework for energy theft detection in smart grid," *IEEE Internet of Things Journal*, 2021.

[5] A. Althobaiti, A. Jindal, A. K. Marnerides, and U. Roedig, "Energy theft in smart grids: A survey on data-driven attack strategies and detection methods," *IEEE Access*, vol. 9, pp. 159 291–159 312, 2021.

[6] 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 Transactions on Industrial Informatics*, vol. 14, no. 4, pp. 1606–1615, 2018.

[7] D. Yao, M. Wen, X. Liang, Z. Fu, K. Zhang, and B. Yang, "Energy theft detection with energy privacy preservation in the smart grid," *IEEE Internet of Things Journal*, 2019.

[8] L. Cui, L. Guo, L. Gao, B. Cai, Y. Qu, Y. Zhou, and S. Yu, "A covert electricity-theft cyberattack against machine learning-based detection models," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 11, pp. 7824–7833, 2021.

[9] K. Zheng, Q. Chen, Y. Wang, C. Kang, and Q. Xia, "A novel combined data-driven approach for electricity theft detection," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 3, pp. 1809–1819, 2018.

[10] A. Takiddin, M. Ismail, U. Zafar, and E. Serpedin, "Deep autoencoder-based anomaly detection of electricity theft cyberattacks in smart grids," *IEEE Systems Journal*, 2022.

[11] D. Gu, Y. Gao, K. Chen, J. Shi, Y. Li, and Y. Cao, "Electricity theft detection in ami with low false positive rate based on deep learning and evolutionary algorithm," *IEEE Transactions on Power Systems*, vol. 37, no. 6, pp. 4568–4578, 2022.

[12] Y. Gao, B. Foggo, and N. Yu, "A physically inspired data-driven model for electricity theft detection with smart meter data," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 9, pp. 5076–5088, 2019.

[13] L. M. Raggi, F. C. Trindade, V. C. Cunha, and W. Freitas, "Non-technical loss identification by using data analytics and customer smart meters," *IEEE Transactions on Power Delivery*, vol. 35, no. 6, pp. 2700–2710, 2020.

[14] M. Tariq and H. V. Poor, "Electricity theft detection and localization in grid-tied microgrids," *IEEE Transactions on Smart Grid*, vol. 9, no. 3, pp. 1920–1929, 2016.

[15] S. A. Salinas and P. Li, "Privacy-preserving energy theft detection in microgrids: A state estimation approach," *IEEE Transactions on Power Systems*, vol. 31, no. 2, pp. 883–894, 2015.

[16] M. Ismail, M. F. Shaaban, M. Naidu, and E. Serpedin, "Deep learning detection of electricity theft cyber-attacks in renewable distributed generation," *IEEE Transactions on Smart Grid*, vol. 11, no. 4, pp. 3428–3437, 2020.

[17] V. B. Krishna, C. A. Gunter, and W. H. Sanders, "Evaluating detectors on optimal attack vectors that enable electricity theft and der fraud," *IEEE Journal of Selected Topics in Signal Processing*, vol. 12, no. 4, pp. 790–805, 2018.

[18] X. Yuan, M.-g. Shi, and Z. Sun, "Research of electricity stealing identification method for distributed pv based on the least squares approach," in *2015 5th International Conference on Electric Utility Deregulation and Restructuring and Power Technologies (DRPT)*. IEEE, 2015, pp. 2471–2474.

[19] A. Althobaiti, A. Jindal, and A. K. Marnerides, "Scada-agnostic power modelling for distributed renewable energy sources," in *2020 IEEE 21st International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)*. IEEE, 2020, pp. 379–384.

[20] S.-C. Yip, K. Wong, W.-P. Hew, M.-T. Gan, R. C.-W. Phan, and S.-W. Tan, "Detection of energy theft and defective smart meters in smart grids using linear regression," *International Journal of Electrical Power & Energy Systems*, vol. 91, pp. 230–240, 2017.

[21] M. Liu, D. Liu, G. Sun, Y. Zhao, D. Wang, F. Liu, X. Fang, Q. He, and D. Xu, "Deep learning detection of inaccurate smart electricity meters: a case study," *IEEE Industrial Electronics Magazine*, vol. 14, no. 4, pp. 79–90, 2020.

[22] L. David, "Solar panels underperforming? here's how to fix common issues," 2021, accessed: 2022-01-22. [Online]. Available: https://www.ecowatch.com/solving-solar-panel-output-issues-2655223014.html

[23] J. Peppanen, M. J. Reno, M. Thakkar, S. Grijalva, and R. G. Harley, "Leveraging ami data for distribution system model calibration and situational awareness," *IEEE Transactions on Smart Grid*, vol. 6, no. 4, pp. 2050–2059, 2015.

[24] Y. Dai, Z. Chen, X. Zheng, Y. Du, X. Liu *et al.*, "Smart electricity meter reliability analysis based on in-service data," in *2021 4th International*

Conference on Energy, Electrical and Power Engineering (CEEPE). IEEE, 2021, pp. 143–147.
[25] E. W. S. Angelos, O. R. Saavedra, O. A. C. Cortés, and A. N. De Souza, "Detection and identification of abnormalities in customer consumptions in power distribution systems," *IEEE Transactions on Power Delivery*, vol. 26, no. 4, pp. 2436–2442, 2011.
[26] D. Chen and D. Irwin, "Sundance: Black-box behind-the-meter solar disaggregation," in *Proceedings of the eighth international conference on future energy systems*, 2017, pp. 45–55.
[27] S. Chakraborty and N. Nagwani, "Analysis and study of incremental k-means clustering algorithm," in *International Conference on High Performance Architecture and Grid Computing*. Springer, 2011, pp. 338–341.
[28] A. Althobaiti, A. Jindal, and A. K. Marnerides, "Data-driven energy theft detection in modern power grids," in *Proceedings of the Twelfth ACM International Conference on Future Energy Systems*, 2021, pp. 39–48.
[29] M. N. Fekri, H. Patel, K. Grolinger, and V. Sharma, "Deep learning for load forecasting with smart meter data: Online adaptive recurrent neural network," *Applied Energy*, vol. 282, p. 116177, 2021.
[30] I. Staffell and S. Pfenninger, "The increasing impact of weather on electricity supply and demand," *Energy*, vol. 145, pp. 65–78, 2018.
[31] M. Schuld, I. Sinayskiy, and F. Petruccione, "An introduction to quantum machine learning," *Contemporary Physics*, vol. 56, no. 2, pp. 172–185, 2015.

Ahlam Althobaiti (Graduate Student Member, IEEE) received a master's degree in Computer Science from the Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia in 2016. She is currently pursuing a PhD degree at the School of Computing and Communications (SCC), Lancaster University, Lancaster, UK. She holds the post of lecturer in the Computer Science Department, College of Computers and Information Technology, Taif University, Saudi Arabia. Her research interests include data analytics, artificial intelligence, cyber-physical systems and industrial system cybersecurity with special focuses on anomaly detection for smart energy systems, cybersecurity for Distributed Renewable Energy Sources (DRES) and energy theft in modern power grids. She has peer-reviewed published articles on network protocol design and energy modelling and the security of DRES. She received a First-Class Honours Award from Taif University in 2010 and a scholarship for a PhD degree.

Charalampos Rotsos (Member, IEEE) is a Senior Lecturer in Computer Networks and Networked Systems at Lancaster University. He holds a Ph.D. from the Computer Laboratory, Cambridge University. His research focus is in network service management and orchestration, network programmability and monitoring and cloud operating systems.He has received funding from national (EPSRC, DSIT), and European (H2020) research projects and published more than 50 papers in peer-reviewed international journals and conferences.

Angelos K. Marnerides (Member, IEEE) is Senior Lecturer (eq. tenured Associate Professor) of Computer Science in the School of Computing Science at the University of Glasgow, UK and leads the Glasgow Cyber Defence Group (GCDG). His research revolves around applied and data-driven security and resilience for Internet-enabled cyber physical systems, the Internet at scale and programmable networks. His research has received significant funding from industry (e.g. Fujitsu, BAE, Raytheon) and governmental bodies (e.g. EU, IUK, EPSRC) and he has been invited to serve as a grant reviewer for national (e.g., EPSRC) and international bodies (e.g., EU, Israeli Innovation Authority). He has been a member of the IEEE and the ACM since 2007 and served as a Technical Programme Committee (TPC) member, TPC track and workshop co-chair and organiser for several top-tier IEEE conferences (e.g. IEEE ICC, IEEE GLOBECOM) leading to receiving IEEE ComSoc contribution awards in 2016 and 2018. He obtained his PhD in Computer Science (2011) from Lancaster University and held lectureships, postdoctoral and visiting researcher positions at Lancaster University (UK), Carnegie Mellon University (USA), University of Porto (Portugal) and University College London (UK).