IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 20 March 2025, accepted 1 April 2025, date of publication 4 April 2025, date of current version 11 April 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3558143

RESEARCH ARTICLE

Power Theft Detection in Smart Grids Using Quantum Machine Learning

KONSTANTINOS BLAZAKIS[1], **NIKOLAOS SCHETAKIS**[2,3], **MAHMOUD M. BADR**[4], **DAVIT AGHAMALYAN**[5], **KONSTANTINOS STAVRAKAKIS**[6,7], **AND GEORGIOS STAVRAKAKIS**[8]

[1]Department of Electrical and Computer Engineering, Hellenic Mediterranean University, 714 10 Heraklion, Greece
[2]School of Production Engineering and Management, Technical University of Crete, 731 00 Chania, Greece
[3]Alma Sistemi Srl, 00012 Guidonia, Italy
[4]Department of Network and Computer Security, College of Engineering, SUNY Polytechnic Institute, Utica, NY 13502, USA
[5]Institute of High Performance Computing, Agency for Science, Technology, and Research (A*STAR), Singapore 138632
[6]Department of Quantum and Computer Engineering, Delft University of Technology, 2628 CD Delft, The Netherlands
[7]Quantum Innovation PC, 731 00 Chania, Greece
[8]School of Electrical and Computer Engineering, Technical University of Crete, 731 00 Chania, Greece

Corresponding author: Konstantinos Blazakis (kblazakis@hmu.gr)

This work was supported in part by the EYE Project from European Commission under Grant 101007638, and in part by the CResDER Project from H.F.R.I. under Grant 03698.

ABSTRACT Electricity theft can lead to enormous economic losses and cause operational and security problems for electricity networks and utilities. Most current research has focused on electricity theft detection in the consumption sector. However, the high penetration rate of distributed generation (DG) can lead to an increase in power theft attacks in this sector via smart meter manipulation. This study is an extension of prior works focused on electricity theft detection in the consumption and generation domains of a smart grid environment with DG. This study proposes a novel electricity theft detection framework based on quantum machine learning (QML). The elegant field of QML has been used to demonstrate that data classification becomes more efficient in higher-dimensional spaces. An extensive numerical study was conducted to determine the type of QML architecture that can perform well and efficiently in electricity theft detection cases. The technique presented here has not yet been extensively studied in the domain of energy theft detection. Extensive experiments were conducted to assess this approach, and an accuracy of 0.87 was achieved with respect to the classical consumption domain, whereas an accuracy of 0.977 was achieved with respect to the net metering domain.

INDEX TERMS Distributed generation, net metering, photovoltaic (PV) electric energy, power theft detection, quantum machine learning, smart grid.

I. INTRODUCTION

Smart grids incorporating renewable energy sources (RESs) are innovative breakthroughs that use new RES technologies to transform a conventional power grid into a clean, valuable, and resilient system. Advanced metering infrastructure (AMI), where smart meters (SMs) are installed at consumers' homes to transmit power consumption data to the utility provider on a regular basis for load monitoring and billing, is one of the most crucial parts of recent smart grids [1], [2], [3]. Recent smart grids have tended to produce the majority of their electricity from RESs to reduce greenhouse gas emissions and transition to a more sustainable electricity system [4], [5].

Solar power is one of the most widespread RESs is renewable energy sources. Many houses have installed photovoltaic (PV) panel electricity generators. The consumption metering system, the sole metering system that utilities employ for residential customers without access to RESs, transmits electricity-usage data to the utility provider.

The associate editor coordinating the review of this manuscript and approving it for publication was Lei Chen.

On the other hand, homeowners who use PV energy can take advantage of two metering schemes, feed-in tariffs (FITs) and net metering, which enable them to sell the excess electricity they generate [4], [5], [6]. The two FIT policies that are currently the most prevalent are the fixed FIT and the feed-in premium, which can be characterized as either independent of or dependent on the market price for electricity, which arises from the deliberated electricity market structure [7].

Only one SM is utilized in the net metering system to report the difference between the electricity generated by the consumer and that consumed [4]. The meter reading is negative when the amount of power generated exceeds the amount of power consumed, and positive if the opposite is true. Consumers are reimbursed for negative values and taxed for positive ones.

Customers who are dishonest can take advantage of these metering systems by providing false readings to gain unlawful profits; that is, they can submit lower consumption values to lower their bills [1], [8]. Similarly, fraudulent clients may report greater PV generation values in the FIT system to improve their financial gains [4]. Utilities worldwide are currently experiencing problems with the reporting of erroneous consumption or generation data, resulting in significant financial losses. It is estimated that worldwide losses from electricity theft totaled $96 billion annually [9]. Therefore, it is critical, from both economic and social perspectives, to effectively detect electricity theft.

Moreover, false consumption or generation values can negatively affect the performance of the grid, not only by causing financial losses, but also by harming network integrity because the reported readings are systematically used for energy management decisions [10]. Owing to the increasing number of incorrect readings worldwide, that is, falsely reported readings in smart grid AMI, several strategies for detecting power theft attacks have been proposed in the literature [6], [10], [11], [12], [13], [14], [15], [16].

Before discussing the proposed approach based on quantum machine learning (QML), power theft detection using QML was proposed in ref. [17] so far. In [17], the first study on this topic, the results presented were preliminary. Additionally, owing to the small sizes of the test and validation sets, the accuracy achieved by the authors was 55% for the test set and 75% for the validation set, which is considered a rather poor performance in the field of power theft. The quantum classifier described in [17] shares similarities with the quantum node (QNODE) proposed here. The proposed QNODE provides enhanced customizability by allowing the selection of the number of blocks and entangling layers. Furthermore, the proposed QNODE is incorporated between classical layers, creating a hybrid deep learning network that combines the strengths of classical and quantum domains. In the noisy intermediate-scale quantum (NISQ) era, where the number of qubits is limited, hybrid computation is crucial. In addition, much higher accuracy was achieved. In comparison with [17], instead of using one performance metric, five were calculated; instead of restricting to 64 days of data, 1096 days of data were considered; and instead of six qubits, 16 qubits were examined.

In the present study, a second serious contribution is made to the aforementioned topic by introducing the use of quantum deep learning (QDL) to investigate the identification of false reading attacks in both consumption metering systems and net-metering systems utilizing well-established benchmarked datasets with embedded power theft scenarios from prior studies [13], [16].

The emerging field of QML has been used to devise algorithms that are capable of speeding up the learning process and have crucial importance in real-life applications because they have the potential to deliver a practical quantum advantage. QML algorithms, compared with the basic linear algebra subroutines, such as those solving certain types of linear equations (the quantum version known as the Harrow-Hassidim-Lloyd (HHL) algorithm), finding eigenvectors and eigenvalues, and performing principal component analysis (PCA), exhibit exponential/polynomial speedups [18], [19], [20], [21], [22], [23]. QML algorithms can learn from smaller amounts of data, process more complex structures, and handle noisy data more effectively. This is particularly useful in the context of energy production and consumption databases, where noisy datasets are prevalent [22], [23], [24].

QML is a rapidly emerging field that combines the principles of quantum computing with traditional machine learning algorithms. With QML, certain types of calculations can be performed much faster than with classical computers, making QML especially useful for solving complex problems, such as optimization, pattern recognition, and clustering.

In a QML neural network, the traditional neurons found in the layers of a classical deep learning neural network are replaced with qubits and quantum gates, which work in conjunction with quantum measurements to serve as activation functions. The three main building blocks of any QML algorithm are data encoding, unitary evolution of the system, and state readout performed through measurements [22], [23], [24], [25], [26].

Data are typically input into a quantum model through sequences of quantum gates. The data are encoded into the initial state of the qubits, and a quantum circuit is then used to perform operations on the data [23], [24], [25]. There are various methods for encoding classical data into quantum states, such as amplitude, phase, and basis encoding [23], [24], [25], [26], [27], [28], [29]. The choice of the encoding method depends on the specific quantum algorithm used and the type of data used as input. In this study, we chose to use angle embedding, which encodes N features into the rotational angles of n qubits, where $N <= n$. Quantum embedding uses classical data and projects it to a high-dimensional Hilbert space in which a higher degree of separation between data classes is desired in comparison to the original coordinate system. This type of encoding was successfully used in [23]. Additionally, by training quantum embedding to obtain the greatest possible separation between the data clusters in the Hilbert space (a technique known as ''quantum metric learning''), paving the way for the development of more robust quantum classifiers. It is known that data classification becomes easier by moving to higher-dimensional spaces when QML is utilized. A good example is the XOR classification problem, which cannot be solved with support vector machines (SVMs) in two-dimensional space, but can be solved easily by moving to three-dimensional space. This is one of the rationales for the introduction of the QML algorithm. Another rationale is to conduct an extensive numerical study to determine the types of QML architecture that can perform efficiently in electricity theft detection.

The energy industry and smart grids frequently employ noisy datasets; thus, this research uses QML to enhance classification models for these datasets [23], [25], [26], [27], [28], [29]. The three main advantages of QML are as follows [23], [24], [25], [26], [27], [28], [29], [30]:

1. Improvements in runtime leading to earlier final results.
2. Learning enhancements that increase the capacity of associative or content-addressable memories.
3. Improvements in learning efficiency when less training information or simpler models are required to achieve the same results, or when more complex relationships can be learned from the same data.

The most important contributions of the present work can be summarized as follows:

1. An advanced QML approach is proposed to analyze electricity theft in the consumption and net-metering domains of a smart grid.

2. Using this software package, three different fundamental QML designs were examined: hybrid neural networks, parametric quantum circuits, and data reuploading.

3. A novel machine learning (ML) approach, referred to as full hybrid QML (FHQML), was developed for the classification problem of power theft, utilizing a combination of techniques, such as hybrid neural networks, parametric circuits, and data-reuploading.

4. It was shown that using QML, data classification becomes more efficient in higher-dimensional spaces. An extensive numerical study was conducted to determine the type of QML architecture that can perform well and efficiently in electricity theft detection cases.

The remainder of this paper is organized as follows.

Section II presents an overview of related literature. Section III describes the well-established datasets and power theft scenarios used. Section IV presents the novel quantum machine learning approach applied in this study. Section V presents a comparison of the FHQML approach with other promising classical approaches, and the results obtained. Finally, in Section VI, the article is concluded and possible future work is discussed.

II. RELATED RESEARCH WORK

Only a few research papers in the literature have examined electricity theft detection in the generation domain, while the majority of previous research has mostly concentrated on power theft detection in the consumption domain. Studies conducted to detect electricity theft can be divided into four categories: game theory-based methods, power grid analysis-based methods, hardware-based methods, and machine learning-based methods [31]. Physical and cyber-data attacks are the two main nontechnical loss (NTL) attack types in smart grids. The use of strong magnets, illegal tapping, reversing meters, splicing pipes or wires to bypass meters, and meter malfunction are examples of physical attack techniques. Eavesdropping, denial of service, covert attacks, malware injection, and false data injection attacks (FDIAs) are a few examples of cyberattacks. Attacks can result in service interruptions, infrastructure destruction, energy and information theft, and other outcomes [32].

A. POWER THEFT DETECTION IN CONSUMPTION METERING DOMAIN

In the presence of smart meters, a new data analysis technique for the detection and localization of NTLs performed by unauthorized connections of loads to distribution networks was proposed in [33].

A hidden electricity theft (HET) attack that uses the newly developed multiple pricing (MP) method was presented in [34].

The objective of the study in [35] was to identify malicious users using a small number of monitoring tools within the shortest possible detection time.

The use of temperature sensors has been suggested as a new way to enhance the calculation of technical losses (TLs), leading to a better estimate of NTL in [36]. A new method for locating potential energy theft locations using voltage drop differences was also described.

A multitask feature-extracting fraud detector (MFEFD) and a deep learning-based model were created to recognize electricity fraud in an advanced metering system [37].

SVMs are used in conjunction with voltage sensitivity analysis, power system optimization, and other techniques to accurately identify NTLs in the distribution grid under various circumstances [38].

Because the value of the electricity theft loss (ETL) should be more correlated to the meter readings of energy thieves than to those of honest consumers, the authors in [39] formulated the problem of identifying electricity theft as a time-series correlation analysis problem that does not require a linearity assumption of attack modes or any cost of training.

In [40], a deep learning-based method was proposed to extract sophisticated features from vast amounts of smart-meter data.

In [41], a deep convolutional neural network (CNN) is used efficiently to distinguish between periodic and nonperiodic energy consumption while maintaining the basic characteristics of the power consumption data.

In [11], a wide and deep CNN model was tested on a realistic power consumption database made available by the State Grid Corporation of China (SGCC). The results demonstrated that the proposed wide and deep CNN structure outperforms other well-known techniques, such as linear regression (LR), random forest (RF), Wide CNN, SVM, and CNN.

A conditional deep belief network (CDBN) technique for real-time false data injection (FDI) attack detection was proposed in [12].

In [13], using the dataset ETD 2022, [42], five machine learning approaches, i.e., k-nearest neighbor (KNN), random forest (RF), decision tree (DT), bagging, and ANN, were used to construct intelligent autonomous power theft detection techniques.

In [43], synthetic binary discriminator models (SYNBDM) and legacy unsupervised models (LUM) were introduced for electricity theft detection in smart homes, utilizing fine-grained appliance consumption data to distinguish between normal and malicious usage.

In [44], parameter estimation and power quantities of an unbalanced distribution line and a hybrid general regression neural network model equipped with multirun optimization (GRNN–MRO) were developed for power theft detection.

In [45], a practical privacy-preserving electricity-theft detection scheme was presented, and the impact of the detection period was explored through communication overhead analysis.

B. POWER THEFT DETECTION IN FEED-IN-TARIFF (FIT) DOMAIN

In [6], a variety of cyber-attacks that alter reliable data from the SMs of DG units in a way that imitates malicious customers stealing electricity were presented. The application of deep feed-forward, deep recurrent, and deep convolutional recurrent neural networks has been investigated to construct a deep learning power theft detection method.

In [14], the research in [6] was extended and an anomaly detector was suggested for identifying power theft in distributed generation that is trained solely on benign data.

In [15], a deep learning-based theft detector was proposed, which captures the temporal properties in a time-series dataset using the gated recurrent unit (GRU) neural network model.

To identify false-reading assaults in the FIT system's generating domain, Krishna et al. [4] presented several strategies for developing custom anomaly detectors based on ARIMA and Kullback–Leibler divergence (KLD).

C. POWER THEFT DETECTION IN NET-METERING DOMAIN

Reference [16] is the first attempt to investigate this problem in the net-metering domain, which uses a single smart meter to indicate the difference between the electricity generated and consumed. By analyzing a genuine dataset of power generation and consumption, a benign dataset for the net metering system was created and used to achieve successful power theft incident detection via deep learning techniques.

III. DATASETS AND POWER THEFT SCENARIOS GENERATOR

A. DATASET ORIGIN

The data used in this study for detecting electricity theft in the consumption domain were the same as those used in [13]. The dataset is from the Open Energy Data Initiative (OEDI, [42]) platform, which is a central repository for high-quality energy research data provided by the U.S. Department of Energy Programs, Offices, and National Laboratories.

The dataset includes the actual hourly energy consumption for 16 different three-phase connection consumer types over a period of a year for a number of consumers.

A dataset from the work in [16] was used to detect power theft in the net metering domain. The largest electricity provider on Australia's east coast, Ausgrid, released this publicly accessible dataset [46]. Actual measurements of power generation and consumption at a half-hour sampling for a group of consumers located in Sydney and the region of New South Wales with PV solar panels installed on their roofs are included in the Ausgrid dataset. These measurements were taken between July 1, 2010, and June 30, 2013. Each consumer has two SMs: one SM used to track electricity consumption, and the other SM used to track electricity generated by the PV solar panels. Additionally, the Ausgrid dataset contains information on the generation capacity or Cmax, which represents the maximum amount of electricity that can be produced by each consumer's solar panels in an hour. The dataset also contains the location of each consumer and a category indicating whether an SM reading is for consumption or generation, day, and season.

Information about solar irradiance and temperature was gathered from SOLCAST [47] using consumer locations given in the Ausgrid dataset.

B. DATA PREPROCESSING

Anomalous readings were removed from the consumption and net metering databases, and a clean dataset was created. Despite the fact that all participants are honest customers, equipment malfunctions and mistakes, such as those involving the SM and PV solar panel inverters, can result in unintentionally anomalous readings (outliers). To reduce the variance of the training data and produce a well-trained machine learning model, it is legitimate and standard practice to remove these outliers from the dataset.

For every customer in the net metering database, the readings for the generation SM and consumption SM were subtracted to obtain net readings. As the amount of electricity purchased/injected by/to the utility at each time instant is equal to the difference between the electricity consumed and the electricity generated by the consumer at that time instant, these readings correspond to the readings that would be recorded if the two SMs were replaced by a single net metering smart meter. Eventually, a clean dataset of 31 consumers was produced with one-hour sampling net meter values for 1096 days between July 1, 2010, and June 30, 2013. For both datasets, the data were further divided into training, validation, and test sets at a ratio of 75/15/10, respectively. The training, validation, and test sets are then normalized to bring all feature values to a common scale, ensuring that each feature makes a fair contribution to the detector's classification. Table 1 presents the features of each dataset.

TABLE 1. Dataset features.

	Ausgrid dataset	OEDI dataset
Features	Net meter readings (kW)	Electricity (kW)
		Fans (kW)
	Solar irradiance (kW)	Cooling (kW)
		Heating (kW)
	Temperature (°C)	Interior lights (kW)
		Interior equipment (kW)
	Day	Gas (kW)
	Season	Heating (kW)
	C_{Max} (kW, maximum capacity of installed solar panel)	Interior equipment gas (kW)
		Water heater (kW)
Label	Binary value indicating whether there is electricity fraud or not (benign/malicious)	Multiclass value indicating whether there is electricity fraud or not (benign/malicious)

C. POWER THEFT SCENARIOS GENERATOR

A set of energy theft cyberattacks was created and imported into the datasets for both the consumption and net-metering domains, because malicious samples are not publicly available.

As described in the relevant research studies [1], [13], [48], [49], [50], [51], six different types of the most frequent fraud were considered, and two additional scenarios were examined to further consider stochasticity in the consumption domain. These are the various forms of theft that certain customers might engage in. A notable drop in electricity consumption during the day constitutes the first type of theft (T_1). The consumption is multiplied by a number randomly determined between 0.1 and 0.8 to estimate this reduction. The second type of theft (T_2) occurs when the power usage drops to zero at a random time instant and for a random duration. The third type of theft (T_3) is similar to the first type, except that each consumption value (per hour) is multiplied by a dynamic, randomly determined number between 0.1 and 0.8. A randomly determined portion of the average consumption is produced in a dynamic manner to create the fourth type of electricity stealing case (T_4). The average consumption is presented in the fifth theft type (T_5) and the readings are reversed in the sixth electricity theft type (T_6). The seventh type of electricity theft (T_7) is similar to the second type of theft (T_2), but the consumption drop is a random percentage of the real consumption, that is, it starts at random time instants and occurs for random time durations. In the eight types of theft (T_8), abrupt instantaneous drops in consumption occurred at random time instants. An electricity theft generator was created that made it possible to produce these eight categories of electricity theft in a random manner for the database.

The following is a formal representation of the suggested method for producing the eight different types of electricity theft: Consider the following daily electricity consumption vector (X): $X = \{x_1, x_2, x_3, \ldots\ldots, x_{24}\}$, where x_i is the hourly consumption reading for $i = 1 \ldots 24$; then, the eight electricity theft types can be created as shown in Table 2.

TABLE 2. Power theft scenarios in the consumption domain.

Input: X, Output: T_N; where N = 1, 2,…, 6
$T_1(x_i) = a \cdot x_i$, a: randomly determined in (0.1, 0.8)
$T_2(x_i) = \beta_i \cdot x_i,\ \beta_i = \begin{cases} 0, & time_{start} < i < time_{end} \\ 1, & \text{Otherwise} \end{cases}$
$T_3(x_i) = \gamma_i \cdot x_i$, γ_i: randomly determined in (0.1, 0.8)
$T_4(x_i) = \gamma_i \cdot \text{mean}(X)$, γ_i: randomly determined in (0.1,0.8)
$T_5(x_i) = \text{mean}\ (X)$
$T_6(x_i) = x_{24\text{-}t}$
$T_7(x_i) = \delta_i \cdot x_i,\ \delta_i = \begin{cases} \varepsilon_i\ , & time_{start} < i < time_{end} \\ 1\ , & Otherwise \end{cases}$ ε_i: randomly determined in (0.1, 0.8)
$T_8(x_i) = \zeta_i x_i,\ \zeta_i = \begin{cases} 0 & At\ time\ t \\ 1 & Otherwise \end{cases}$

*$time_{start}$: randomly determined in (0, 23-$time_{off}$)
Duration: random ($time_{off}$, 24)
$time_{end}$ = $time_{start}$+duration
$time_{off}$>= 4 time instants

Both the choice of theft duration and the reduction factor in different theft types involve a random element. This method summarizes the actions of most thieves. They wanted to reduce their reported consumption reading for an arbitrary amount of time. To perform multiclass classification, these categories were applied to the dataset for this study in a fair and random manner.

The detection of false reading attacks in net metering systems differs from that in traditional metering systems. In consumption-metering systems, the detector can be calibrated to the consumer's consumption habits, whereas in FIT systems, the detector can be calibrated to the solar PV panel generation patterns of the customer to spot false readings. Detecting false-reading attacks in net metering systems is a more complex task because of the impact of various factors, such as the behavior of building occupants, solar irradiation, and solar PV panel generation capacity on net meter readings. To address this challenge, a new detection approach that considers both consumption and generation patterns is required. The investigation of attacks specific to net metering systems is essential for the following reasons.

In attacks on the consumption-metering system, the attacker's goal is to reduce the metered values while replicating the consumption pattern. In contrast, attacks on FIT systems aim to increase the metered values of electricity

TABLE 3. Power theft scenarios in the net metering domain.

#	Attack		Consumption>Generation	Consumption<Generation
1	**Intermittent**		$\begin{cases} b_t * TR_t, & t_{start} \le t \le t_{end} \\ TR_t, Otherwise \end{cases}$	$\begin{cases} -max(p_t * C_{max,}\lvert TR_t\rvert, & t_{start} \le t \le t_{end} \\ TR_t, Otherwise \end{cases}$
2	**Continuous**	**Scaling -based**	a*TR_t	$-min(\lvert\beta * TR_t\rvert, C_{max})$
3			a$_t$*TR_t	$-min(\lvert\beta_t * TR_t\rvert, C_{max})$
4		**History -based**	$M_{1_t} * min(PR, TR_t)$	$-M_{2_t}max(\lvert NR\rvert, \lvert TR_t\rvert)$

generation while imitating the generation pattern. However, when generating fraudulent readings for net metering systems, attackers must consider both consumption and generation patterns to gain financial advantages.

Therefore, a series of subtle attacks has been proposed to mimic the behavior of malicious customers [16]. The authors of [16] practically modeled these attacks as clever attackers that wish to modify the true readings into false readings for binary classification, making it challenging for the utility to identify the attack. Table 3 lists these attacks.

To benefit financially from the net metering system, attackers aim to increase their reported net values when the power consumed is less than the power generated (negative readings), and decrease their reported values when the power consumed is greater than the power generated (positive readings).

The suggested attacks can also be categorized as intermittent or continuous attacks. In intermittent attacks, the attacker presents false readings during some time windows and genuine readings during other time windows to deceive the detector. However, in continuous attacks, the attacker presents false readings continuously to maximize gain.

Attack #1, which deceives for a random time period beginning at t$_{\text{start}}$ and ending at t$_{\text{end}}$ while otherwise reporting the correct measurements, is a common type of intermittent attack. Within the deception period, the attacker submits a value equal to the larger of a significant percentage (p_t) of the maximum solar PV generation capacity (Cmax) or the absolute value of the current true reading ($|TR_t|$) when the power consumed is less than the power generated (negative readings), and provides a modified version of the current true reading ($|TR_t|$) reduced by a time-varying factor b_t during positive reading intervals (positive readings). Three attacks based on either scaling or history have been proposed in the context of continuous attacks. In scaling-based attacks, the attacker scales both positive and negative readings up and down, without considering the values of earlier measurements. In a history-based attack, the attacker uses previous readings to calculate the incorrect value.

In *Attack #2*, the attacker deceives the system by constantly reporting a version of $|TR_t|$ that is decreased by a factor of $\boldsymbol{\alpha}$ when the readings are positive, and a version that is increased by a factor of $\boldsymbol{\beta}$ when the readings are negative. As shown in Table 3, the attack assumes that the reported value does not exceed Cmax, which is represented by the term $-min(|\beta * TR_t|, C_{max})$.Here, $\boldsymbol{\alpha}$ is a randomly determined value between 0 and 1 and $\boldsymbol{\beta}$ is a randomly determined value greater than 1.

Attack #3 is also a type of scaling-based attack; however, in contrast to Attack #2, both downscaling and upscaling randomly determined parameters $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ depend on time.

In *Attack #4*, a method based on historical data, the attacker deceives the system by submitting the highest value between $|TR_t|$ and the last recorded negative reading (NR) during negative reading intervals, and the lowest value between $|TR_t|$ and the last reported positive reading (PR) during positive reading intervals. In Attack #4, factors M_{1_t} and M_{2_t} serve as masks rather than scaling factors to prevent reporting the exact same reading in consecutive time slots and misleading the detector. The values of M_{1_t} and M_{2_t} are slightly less than 1 and slightly higher than 1, respectively.

The attacker plugs the genuine readings into equations that correspond to the proposed attacks instead of reporting the true values directly. Consequently, these equations provide false readings that the attacker provides to the utility company to obtain illegal financial gain.

IV. THE PROPOSED FULL HYBRID QUANTUM DEEP LEARNING NEURAL NETWORK ELECTRICITY THEFT DETECTOR

In this section, the QDL model used in this study is described in detail. In this model, quantum layers are sandwiched between classical layers. This model is implemented using Pennylane, a Python-based tool for QML, and the optimization of hybrid quantum-classical computations [52]. The full code of the QDL model used in this study can be found in [53]. Before proceeding to describe several architectures that serve as building blocks to form QDL, the authors attempt to justify why they have chosen QDL as a specific architecture for the power theft classification problem. As mentioned in the introduction, unbalanced noisy datasets are prevalent in power theft classification problems. In ref. [54] the detailed benchmarking of quantum architectures (which are similar to QDL) against the best classical counterparts for both synthetic and real-world unbalanced datasets is presented. It has been demonstrated that the QDL-like architecture serves as an excellent framework for tackling classification issues in unbalanced datasets that have non-convex boundaries. Moreover, in [54], through extensive numerical studies, it was shown that in the presence of high

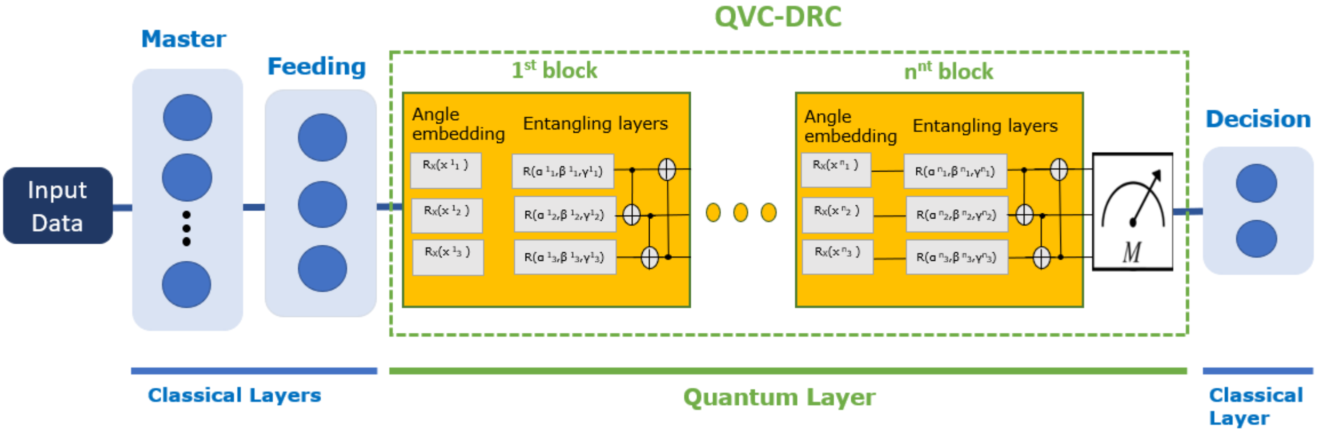
QVC-DRC
Master
Feeding
Input Data
1st block
nnt block
Angle embedding
Entangling layers
$R_x(x^1_1)$
$R_x(x^1_2)$
$R_x(x^1_3)$
$R(\alpha^1_1, \beta^1_1, \gamma^1_1)$
$R(\alpha^1_2, \beta^1_2, \gamma^1_2)$
$R(\alpha^1_3, \beta^1_3, \gamma^1_3)$
$R_x(x^n_1)$
$R_x(x^n_2)$
$R_x(x^n_3)$
$R(\alpha^n_1, \beta^n_1, \gamma^n_1)$
$R(\alpha^n_2, \beta^n_2, \gamma^n_2)$
$R(\alpha^n_3, \beta^n_3, \gamma^n_3)$
M
Decision
Classical Layers
Quantum Layer
Classical Layer

FIGURE 1. **Block diagram flowchart of the proposed FH-QVC-DRC classifier where a QVC-DRC circuit of n-blocks is inserted between the feeding classical layer and the classical decision layer.**

noise in the dataset, the quantum QDL-like deep learning model performs better than the corresponding classical models. These findings provide a rationale for using the QDL architecture for the power theft detection method presented here. The quantum layer of the proposed QDL is as follows. The core of the quantum layer is a *quantum variational circuit*(QVC) consisting of two parts (angle embedding, entangling layers), as shown in Fig. 1.

The first part is an angle-embedding layer that encodes the output of a classical neural layer (feeding layer) to the qubits using angle rotation encoding. One of the main advantages of angle embedding is that it can be performed in a constant time with parallelism; each qubit will go through a rotation gate in parallel. The second part comprises a series of CNOT and rotational gates with trainable parameters. Using one gate to encode each qubit reduces noise, which is important in noisy intermediate-scale quantum (NISQ) computers, as multiqubit gates are more prone to noise and are harder to implement. In addition, angle embedding is intuitive and simple to implement. These two parts create the blocks. The third part is the measurement stage in which the quantum output of the previous stages is converted into classical information that can be fed into the next classical layer. QML architectures can be recovered (for low to moderate amounts of noise) by simply training quantum neural networks for more epochs.

Essentially, by adding more blocks to a QVC, the data are reintroduced into the quantum circuit. This technique is known as the *data-reuploading circuit* (DRC) [26], [27], [54], in which a new deep learning NN model called QVC-DRC is obtained.

The last decision layer consists of only one layer of neurons with a sigmoid activation function. The architecture defined and described above is illustrated in Fig. 1.

A more detailed description of the FH-QVC-DRC deep learning neural network architecture can be found in [23] and [54]. Further details on the optimization process, loss function, etc., to train the quantum layer and a comparison with the classical deep learning model can also be found in [23] and [54]. Next, the QVC-DRC was sandwiched between an arbitrary number of classical NN layers to obtain the *full hybrid* (FH) QVC-DRC model. The constraint is that the classical layer before the QVC-DRC should have the same number of neurons as the number of qubits in the QVC-DRC.

These references also provided a very detailed benchmark of quantum architectures against the best classical counterparts for both synthetic and real-world unbalanced datasets. In [23] and [54] demonstrated that the FH-QVC-DRC deep learning architecture is an excellent framework for addressing classification issues in unbalanced datasets. Moreover, in [54] demonstrated that in the presence of high noise in the dataset, the quantum FH-QVC-DRC deep learning model performed better than the corresponding classical models.

Limitations regarding the necessary computer power have set the upper limit for the number of qubits to 16, owing to run-time constraints. The training epoch for the QVC-DRC needs approximately one hour on a PC with 64 GB of RAM and an AMD Ryzen7 processor [23]. Specifically, Fig. 5 in ref. [23] illustrates the training time as a function of the total number of qubits and the number of blocks in the data re-uploading approach. To ensure a justifiable comparison, the quantum and classical deep-learning models were trained for the same number of epochs, which was set to 250. This value was selected after observing that the quantum deep learning models tended to overfit after 250 epochs, on average. Nonetheless, the classical deep learning model exhibited slight enhancement when the training was extended to 3,500 epochs.

The batch size of the FH QVC-DRC was reduced to 16 training examples per iteration owing to the memory restrictions. The optimizer used was a stochastic gradient descent (SGD) optimizer, and the loss function was a binary cross-entropy. For consistency, the same training, validation, and test datasets were used in all simulations. For every specified configuration, the average outcome scores were extracted over the simulations.

The scalability of the proposed quantum machine learning (QML) approach for handling large-scale smart-grid deployment is a critical consideration. The FH QVC-DRC model offers scalability because classical layers can take up a heavy computational load; thus, the quantum layer is not currently restricted by large datasets. When more qubits are available, more computational load can be directed to the quantum layer by removing the classical layers.

V. EFFECTIVE POWER THEFT DETECTION RESULTS AND DISCUSSION

This section presents detailed experimental results for the proposed power theft detection approach with respect to the classical approaches in the consumption and net metering domains using the proposed FH-QVC-DRC QML. The FH-QVC-DRC algorithm was developed, applied, and run using Pennylane [52], a framework for differentiable open-source quantum computer programming. It is worth mentioning that PennyLane offers three different methods for implementing noise in quantum circuits: classical parametric randomness, PennyLane's built-in default mixed device and plugins for other platforms. Quantum circuits can operate on various backends, some of which have their own programming languages and simulators. PennyLane interfaces with these languages via plugins, such as Cirq and Qiskit. To satisfy the present research requirements, methodical hyperparameter tuning was performed to analyze the effect of changing the number of repeating units in the data-reuploading approach, number of epochs, batch size, qubits, and number of strongly entangling units on the area under receiver operating characteristic curve (AUC/ROC) metric (see below).

A. CLASSIFICATION EVALUATION METRICS

Accuracy (ACC), F1 score, precision or positive predictive value (PPV), recall or sensitivity or hit rate or true-positive rate (TPR) is a critical metric in classification tasks that assesses the model's ability to correctly identify positive incidents, and area under the receiver operating characteristic curve (AUC/ROC) are the classification metrics used here to numerically assess the findings. These metrics are defined by equations (1)–(4) as follows and are calculated for each classification case using the corresponding confusion matrices, that is, tables with two rows and two columns that report the number of true positives (TP), false negatives (FN), false positives (FP), and true negatives (TN) [13], [15]:

$$Accuracy = \frac{TP + TN}{TP + TN + FN + FP} \tag{1}$$

$$F1 = \frac{2TP}{2TP + FP + FN} \tag{2}$$

$$Precision = \frac{TP}{TP + FP} \tag{3}$$

$$Recall = \frac{TP}{TP + FN} \tag{4}$$

The confusion matrices created in this work yielded four types of results:

(1) True positive (TP) is the dishonest consumer correctly classified as dishonest.

(2) A false negative (FN) is a dishonest consumer incorrectly classified as honest.

(3) FP (false positive) is the honest consumer incorrectly classified as dishonest.

(4) TN (true negative) is an honest consumer correctly classified as honest.

A small drop in the metric's maximum values defined above was observed after 10 qubits in the QVC-DRC layer, and no significant change was observed if the number of blocks was more than three, as shown in Figs. 2 and 3, respectively. In this study, simulations were performed and the corresponding results are presented for a 3 blocks and 10 qubits FH QVC-DRC structure in the following. The observed decrease in recall below 3 blocks/10 qubits is due to the model being underparameterized, indicating a need for additional trainable parameters to improve its performance. Generally, increasing the number of qubits allows for the creation of more complex entangled states, which are essential resources in quantum computing and quantum machine learning. These entangled states enhance the model's capacity to capture intricate patterns, thereby improving overall recall. Moreover, changing the number of epochs may improve sensitivity (recall) and other performance metrics.

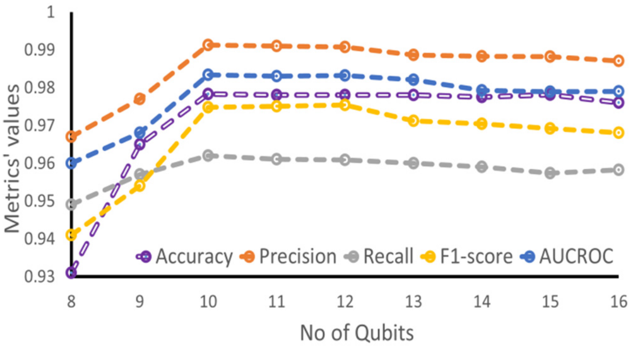

FIGURE 2. Metric values vs. number of qubits for 3 blocks.

B. COMPARATIVE RESULTS OF THE FH-QVC-DRC DEEP LEARNING CLASSIFICATION METHOD WITH CLASSICAL APPROACHES APPLIED IN THE CONSUMPTION DOMAIN CASE

In Tables 5, 6, and 7, the results of applying the FH-QVC-DRC QML approach, LSTM [55], XGBoost [56], LightGBM [57], and CatBoost [58] classical approaches can be seen for all classes of consumers and per class for the first six power theft scenarios (PT6) and for all power theft scenarios (PT8) for power theft detection in the consumption domain. To select the appropriate hyperparameters for every

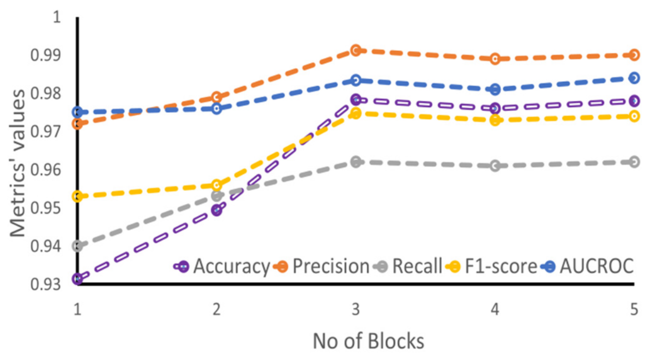

FIGURE 3. Metric values vs. number of blocks for 10 qubits.

classification algorithm, trial-and-error was applied to tune the hyperparameters. The FH-QVC-DRC model architecture was set as close as possible to that of the classical neural network structure. The structures of both the classical LSTM and the quantum model are shown in Table 4. Several activation functions were examined, and it was observed that the best classification performance was achieved with the *Softmax* activation function. Similar or equal performances were observed with the *Tanh* activation function.

TABLE 4. Structure of LSTM and FH-QVC-DRC deep learning classifiers.

LSTM			**FH-QVC-DRC**		
Hyperparameters			Hyperparameters		
Layer	Number of units	Activation function	Layer	Number of units	Activation function
Input	10	ReLU	Input	10	ReLU
Dense	25	ReLU	Dense	25	ReLU
Dense	10	ReLU	Dense	10	ReLU
Dense	10	ReLU	QVC-DRC	10(qubits)	-
Output	2	Softmax	Output	2	Softmax

TABLE 5. Average results for all power theft detection classes examined for the first 6 (PT6) and for all the 8 (PT8) power theft scenarios.

	ACC		F1	
	PT6	PT8	PT6	PT8
FH-QVC-DRC	0.87	0.87	0.86	0.86
LSTM	0.84	0.81	0.83	0.78
XGBoost	0.85	0.85	0.82	0.84
LightGBM	0.85	0.85	0.84	0.85
CatBoost	0.86	0.85	0.83	0.83

TABLE 6. Comparative results per class for the first 6 power theft scenarios (PT6).

	FH-QVC-DRC		LSTM		XGBoost		LightGBM		CatBoost	
	ACC	F1	ACC	F1	ACC	F1	ACC	F1	ACC	F1
Full serv. rest.	0.86	0.85	0.84	0.83	0.86	0.83	0.86	0.85	0.86	0.83
Hospital	0.86	0.86	0.84	0.85	0.85	0.82	0.85	0.84	0.85	0.82
Large hotel	0.86	0.84	0.85	0.83	0.85	0.82	0.83	0.82	0.84	0.81
Large office	0.86	0.85	0.85	0.84	0.86	0.83	0.84	0.83	0.86	0.84
Medium office	0.86	0.84	0.84	0.83	0.84	0.81	0.84	0.83	0.85	0.83
Midrise apart.	0.85	0.82	0.84	0.80	0.80	0.76	0.81	0.80	0.84	0.80
Outpatient	0.85	0.84	0.83	0.82	0.83	0.80	0.83	0.82	0.87	0.84
Primary school	0.87	0.86	0.85	0.84	0.86	0.83	0.86	0.85	0.88	0.85
Q. serv. res.	0.87	0.85	0.85	0.82	0.87	0.84	0.87	0.86	0.87	0.84
Sec. school	0.87	0.85	0.84	0.83	0.85	0.82	0.85	0.84	0.87	0.83
Small hotel	0.88	0.86	0.86	0.84	0.86	0.83	0.84	0.83	0.86	0.83
Small office	0.87	0.86	0.84	0.83	0.87	0.84	0.87	0.86	0.87	0.84
Stand-alone retail	0.88	0.86	0.85	0.83	0.86	0.83	0.87	0.86	0.87	0.84
Supermarket	0.88	0.86	0.85	0.84	0.86	0.83	0.86	0.85	0.86	0.83
Strip mall	0.87	0.86	0.85	0.83	0.86	0.83	0.87	0.85	0.86	0.84
Warehouse	0.86	0.85	0.84	0.85	0.84	0.80	0.85	0.84	0.85	0.82

TABLE 7. Comparative results per class for all the 8 power theft scenarios (PT8).

	FH-QVC-DRC		LSTM		XGBoost		LightGBM		CatBoost	
	ACC	F1	ACC	F1	ACC	F1	ACC	F1	ACC	F1
Full serv. rest.	0.87	0.86	0.84	0.80	0.86	0.85	0.86	0.85	0.87	0.84
Hospital	0.87	0.87	0.81	0.79	0.87	0.86	0.87	0.86	0.85	0.83
Large hotel	0.87	0.85	0.82	0.79	0.84	0.83	0.84	0.83	0.85	0.82
Large office	0.84	0.84	0.78	0.76	0.83	0.82	0.84	0.83	0.84	0.82
Medium office	0.87	0.85	0.80	0.77	0.86	0.85	0.86	0.85	0.86	0.84
Midrise apart.	0.84	0.83	0.79	0.76	0.83	0.81	0.82	0.81	0.83	0.81
Outpatient	0.87	0.86	0.83	0.80	0.85	0.84	0.85	0.84	0.86	0.85
Primary school	0.89	0.86	0.81	0.79	0.87	0.85	0.87	0.86	0.87	0.85
Q. serv. res.	0.89	0.87	0.85	0.82	0.88	0.87	0.88	0.87	0.88	0.86
Sec. school	0.84	0.83	0.72	0.69	0.84	0.83	0.84	0.84	0.84	0.81
Small hotel	0.88	0.87	0.80	0.77	0.86	0.85	0.86	0.86	0.86	0.84
Small office	0.85	0.85	0.80	0.77	0.86	0.84	0.86	0.85	0.85	0.83
Stand-alone retail	0.86	0.86	0.82	0.80	0.85	0.84	0.85	0.85	0.85	0.83
Supermarket	0.89	0.88	0.85	0.82	0.86	0.85	0.86	0.85	0.87	0.85
Strip mall	0.87	0.85	0.83	0.79	0.86	0.84	0.86	0.85	0.85	0.83
Warehouse	0.85	0.86	0.80	0.77	0.84	0.82	0.85	0.84	0.84	0.82

C. COMPARATIVE RESULTS OF THE FH-QVC-DRC DEEP LEARNING CLASSIFICATION METHOD WITH CLASSICAL APPROACHES APPLIED IN THE NET-METERING DOMAIN CASE

Photovoltaic (PV) systems are installed on rooftops, in buildings surfaces or in open spaces of /nearby urban areas, allowing homeowners to generate electricity from sunlight with moderate investment cost. This PV produced electricity can be used even directly to cover the household's electricity needs, to be stored in batteries for later use while the excess electricity can be fed into the grid, all the above through net metering. Adding the effect of an eventual wind system would require additional relevant metrics on the power flow and quality. In Table 3 above the power theft scenarios in the net-metering domain are presented.

The structure of the FH-QVC-DRC classifier architecture is presented in Table 8. In Table 9, the results of the FH-QVC-

DRC-QML approach and the LSTM, CatBoost, XGBoost, and LightGBM classical approaches are presented for every stage of the net-metering domain. To select the appropriate hyperparameters for every classification algorithm, trial-and-error was applied to tune the hyperparameters. Six types of data from distinct sources were used. The initial data source consisted of fine-grained net readings obtained over a day. Fine-grained values of irradiance and temperature were the second and third input data, respectively, obtained for the same day. The remaining input data consisted of Cmax values, day, and season. Additionally, the detector is created in three stages, each of which considers more input data to enhance the detection performance of the proposed detector. Stage 1 examines only net readings as the input data type. Stage 2 considers Stage 1 input data as well as the temperature and irradiance (three inputs in total). Finally, Stage 3 considers all the input data from Stages 1 and 2 in addition to the Cmax, day, and season (six inputs in total). The correlation coefficients between all the input data are shown in Fig. 4.

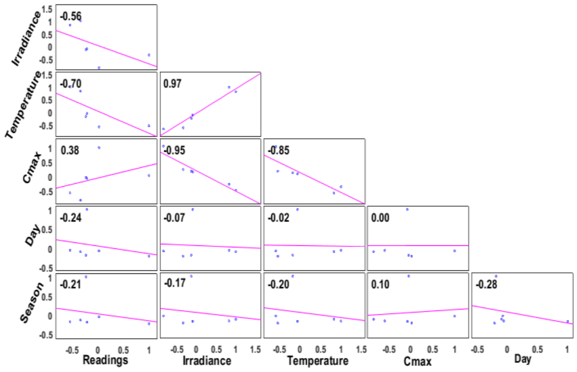

FIGURE 4. Correlation coefficients between all inputs.

TABLE 8. Structure of the FH-QVC-DRC model for the net-metering application.

Hyperparameters		
Layer	Number of units	Activation function
Input	24	Linear
Dense	128	Linear
Dense	128	Sigmoid
Dense	128	Sigmoid
Dense	256	Sigmoid
Dense	18	ReLU
QVC-DRC	10 (qubits)	-
Output	2	Softmax

D. COMPARATIVE RESULTS AND DISCUSSION

Comparing the simulation results from Table 5, Table 6, and Table 9 with the corresponding results from the studies in [13], [16], [59], and [60], it is clearly observed that the proposed FH-QVC-DRC QML approach has similar or even better results in every metric. The runtime, capacity, and learning efficiency of the FH-QVC-DRC QML approach can be found in [23].

TABLE 9. Results for the net-metering domain application.

	Accuracy	Precision*	Recall	F1-score	AUC/ROC
		FH-QVC-DRC			
Stage 1	0.962	0.988	0.958	0.973	0.981
Stage 2	0.963	0.989	0.960	0.974	0.982
Stage 3	0.977	0.991	0.962	0.976	0.983
		LSTM			
Stage 1	0.928	0.931	0.928	0.929	0.938
Stage 2	0.930	0.935	0.930	0.932	0.940
Stage 3	0.948	0.951	0.948	0.949	0.946
		CatBoost			
Stage 1	0.952	0.956	0.952	0.954	0.950
Stage 2	0.956	0.959	0.956	0.957	0.952
Stage 3	0.972	0.972	0.972	0.972	0.956
		XGBoost			
Stage 1	0.958	0.986	0.960	0.973	0.954
Stage 2	0.958	0.987	0.960	0.973	0.954
Stage 3	0.973	0.984	0.972	0.978	0.960
		LightGBM			
Stage 1	0.945	0.985	0.946	0.965	0.945
Stage 2	0.946	0.985	0.947	0.966	0.946
Stage 3	0.961	0.983	0.968	0.975	0.951

Concerning power theft detection in the consumption domain, the FH-QVC-DRC QML has better average results (Table 5) for all metrics, for both the PT6 and PT8 approaches, when compared with the LSTM, CatBoost, XGBoost, and LightGBM algorithms.

Compared with relevant studies [13], [59], [60], which utilized the same dataset and the same power theft scenarios (PT6), the FH-QVC-DRC QML approach has better results in relation to [13] and [59] and equivalent results with [60]. More specifically, the proposed FH-QVC-DRC approach achieved an ACC of 0.87 and an F1-score of 0.86. In the Table 11 of ref. [13] an ACC of 0.8500 and F1-score of 0.8406 were achieved. In ref. [59] an ACC of 0.7006. Table 1 and Table 2 of ref. [60], ACC of 0.8800, and F1-score of 0.8549 were achieved.

Concerning power theft detection in the net-metering domain case presented for the first time in ref. [16] (Table 9 of [16]), the FH-QVC-DRC QML approach has slightly improved results for Stage 1 and similar results for Stages 2 and 3 (Table 9). Comparing the FH-QVC-DRC QML approach with the LSTM, CatBoost, XGBoost, and LightGBM approaches, the FH-QVC-DRC QML approach yielded better results for almost all metrics and stages (Table 9). *T*he greater values for the AUC/ROC metric of the FH-QVC-DRC QML approach compared with the other approaches of the present study, shows that it has the best performance in distinguishing between the benign and malicious samples combined with the rest metrics.

Furthermore, the improved stage 3 results for all the applied algorithms and almost every metric demonstrate that the detectors can create a more complex classification boundary between benign and malicious samples by considering additional important features.

Even a small metric improvement can remarkably decrease financial losses for the electricity provider, which is interpreted as enhanced power theft detection (e.g., improvement achieved in the recall metric) and fewer consumer inspections needed (e.g., improvement achieved in precision metric).

Because of the similar datasets and power theft scenarios with the research in [13], [16], [59], and [60], the comparisons are credible regarding the consumption and net metering domains.

While classical methods such as XGBoost, CatBoost, and LSTMs are powerful, the motivation for exploring a quantum-based approach lies in its potential for scalability, speed and the ability to handle complex data structures differently than classical models [61].

QML algorithms use quantum mechanics with its inherent unusual effects to process information more efficiently, establishing QML as a promising new paradigm [19]. Here the intuition is as follows: if small quantum information processors can produce statistical patterns that are computationally difficult to be produced by a classical computer, then they can also recognize patterns that are equally difficult to recognize classically.

The classification metrics calculated by equations (1)–(4) above are certainly influenced by dataset variability, hyperparameter sensitivity and inherent quantum circuit noise. To mitigate these uncertainty factors, a rigorous dataset preprocessing pipeline, including outlier removal, feature normalization, and the generation of synthetic power theft scenarios based on established fraudulent behavior models is ensured. Figs. 2 and 3 above demonstrate how the model performance trends to stabilize beyond 10 qubits and 3 quantum blocks, indicating that performance gains plateau due to the quantum circuit's structure. The dataset preprocessing and refinement process was carefully designed to preserve real-world data characteristics while eliminating anomalies that could skew model performance, ensuring that the obtained results accurately reflect the detection capabilities of the proposed approach.

While the performance difference in accuracy may appear marginal in some cases (e.g., Tables 5, 9), this study aims to investigate whether quantum machine learning (QML) can provide an alternative path for achieving competitive results in power theft efficient detection based on future quantum hardware improvements.

The box 1 table of ref. [62] presents a summary of quantum speedups obtained in QML computing compared with their classical counterparts.

The execution time for the FH-QVC-DRC model on the simulator per epoch and per training step for an increasing number of total qubits and for an increasing number of blocks with a constant number of 8 qubits is given in the Fig. 5 of ref. [23]. Indicatively, for 3 blocks and 10 qubits which is the case here the time per epoch is approximately 50 sec while the time per training step is approximately 0.3 sec using an Intel core i7 processor. The average calculation time of the above algorithms, using the same case studies/data for their evaluation, is given in the Table 10 below, while their corresponding precision is given in Table 9.

TABLE 10. Calculation times w.r.t precision*.

Model	Time per epoch (sec)	Time per training step (sec)
FH-QVC-DRC (Quantum)	~50	~0.30
LSTM	~ 5 - 20	~ 0.03 - 0.10
XGBoost	~ 2 - 10	~ 0.01 - 0.05
LightGBM	~ 1 - 8	~ 0.005 - 0.03
CatBoost	~ 3 - 12	~ 0.01 - 0.04

VI. CONCLUSION AND FUTURE DIRECTIONS

In this paper, a novel approach called full hybrid-quantum variational circuit-data reuploading circuit (FH-QVC-DRC), developed by combining techniques such as hybrid-neural networks and quantum variational, data reuploading, and parametric circuits, is proposed for the first time to detect electricity theft in the consumption and net-metering domains in smart grids. The full FH-QVC-DRC approach was tested for efficient power theft detection by running simulations on quantum simulators, and compared with assessed related works (i.e., [13], [16], [59], [60]) on power theft detection in conventional power grids and net-metering domains. Moreover, to support the hypothesis for the need for quantum ML over classical ML, a comparison with the well-known classical LSTM and state-of-the-art algorithms CatBoost, XGBoost, and LightGBM was performed. The performance of the proposed approach compared with the previously published related works [13], [16], [59], [60] reveals that with the QML approach a high accuracy is achieved, i.e. 0.87 (see Table 5) in the classical consumption domain, whereas 0.977 (see stage 3, Table 9) in the net metering domain. The size, skewness, and noise of each dataset, as well as their differences in attributes, and the fact that net metering underwent binary classification, whereas consumption underwent multiclass classification, caused the results from the net-metering domain to differ from those from the conventional consumption domain. Smart grid metering systems are adopted worldwide, where homes are equipped with SMs to report fine-grained readings to electric utility companies for billing, monitoring, load forecasting, and energy management. In this paper, we show how the reported readings can be checked using a QML-based detector to efficiently identify electricity theft.

Regarding data privacy, many research works in the literature have shown that detecting electricity theft while preserving customers' privacy is feasible. One approach is to encrypt the reported readings received from the customers before sending and registering them, as shown in [45]. QML is a powerful framework that holds significant promise for accelerating ML algorithms and routines [61], [62], [63], [64]. In ref. [54] the authors also reported higher results with the QML model than with its classical counterpart in certain classification cases. These results show that they are not needed as many ''stable'' qubits as one believes to reach a quantum ML advantage. Given the rapid advancements in quantum computing (hardware and software), the accessibility and applicability of the proposed methodology are competitive.

In future work, quantum machine learning will be applied to imbalanced datasets that are prevalent in every aspect of classification problems [64]. It would also be challenging to run simulations on an actual quantum computer (IBM, Amazon Bracket, Regetti) to determine how actual hardware noise affects the results. This step could also be achieved on the quantum emulator by using Kraus operators applied to common noise channels, such as depolarizing channels, spin-flips, amplitude damping, and phase damping [65], [66].

It is crucial to consider that the errors and noise in qubits and quantum gates are significant obstacles to scalable universal quantum computers. Therefore, it is beneficial to examine how the results are affected by implementing noise models for realistic quantum backends.

Generally, a noisy quantum system is described by the open system model, whereas the system dynamics within the Born-Markov approximation are governed by the Lindblad master equation for the density matrix of the system [65]. Another approach for describing different noise channels is based on Kraus operators, which are the most general physical operations acting on density matrices [66].

Sensitivity to input errors such as adversarial robustness is a significant issue in quantum classifiers [67], [68]. The robustness of the FH-QVC-DRC QML architecture introduced in this study is a topic for future research. However, as demonstrated in [68], practical quantum classification tasks classify a subset of encoded states by using common qubit encoding schemes. For such tasks, the concentration of the measure phenomenon can be used to derive the robustness of any quantum classifier when the distribution of states to be classified can be smoothly generated from a Gaussian latent space.

It is worth noting the need to assess the full hybrid quantum algorithm examining the case where industry and domestic loads are mixed in equal proportions and to examine single/three-phase connection consumer cases [69], [70], [71].

Implementing QML in the NISQ era faces limitations related to data quality and availability due to technological issues in converting classical information to quantum information (e.g., noisy qubits, limited qubit count), which exacerbates the problems of poor quality or insufficient data.

In [72], the authors suggested that hybrid models (such as the one proposed in the present paper), which combine quantum and classical computation, can leverage the strengths of both worlds. For instance, classical circuits can be used for feature extraction and data handling, whereas quantum methods can efficiently perform optimization [62].

Moreover, QML has the theoretical potential to use less data than classical machine learning (CML) methods in certain scenarios. For instance, in quantum chemistry [73], QML algorithms can efficiently simulate molecular structures and predict chemical properties using fewer data points. Similarly, in optimization problems, quantum algorithms such as the Quantum Approximate Optimization Algorithm (QAOA) [74] can find optimal or near-optimal solutions faster and with less data than the classical algorithms. Finally, Quantum embeddings have the potential to encode large datasets into quantum states more compactly than classical counterparts [75]. This efficient data encoding can lead to better utilization of available data and faster convergence of the learning algorithms.

Studies have shown that hybrid Neural Networks often require a comparable or even lower number of training epochs than their classical counterparts to achieve similar performance [23]. Regarding actual quantum experiments on quantum backends (AWS Braket, Rigetti, IBMQ, IonQ): execution time depends on queue wait times, quantum gate execution times (typically in microseconds) and measurement overhead. A single forward pass (circuit execution) for 4 qubits can take milliseconds to seconds.

As quantum hardware advances, training costs decrease and QML algorithms become more viable in domains where classical ML algorithms face scalability bottlenecks.

Quantum models offer the potential for rapid inference, especially in hybrid quantum-classical architectures while these advantages will gradually be realized as quantum hardware progresses.

These advantages are owing to the quantum properties of superposition and entanglement in quantum computing, which enable a more efficient exploration of the solution space and a more compact representation of complex data structures.

REFERENCES

[1] P. Jokar, N. Arianpoo, and V. C. M. Leung, ''Electricity theft detection in AMI using customers' consumption patterns,'' *IEEE Trans. Smart Grid*, vol. 7, no. 1, pp. 216–226, Jan. 2016.

[2] A. Arif, T. A. Alghamdi, Z. A. Khan, and N. Javaid, ''Towards efficient energy utilization using big data analytics in smart cities for electricity theft detection,'' *Big Data Res.*, vol. 27, Feb. 2022, Art. no. 100285.

[3] Y. Zhu, Y. Zhang, L. Liu, Y. Liu, G. Li, M. Mao, and L. Lin, ''Hybrid-order representation learning for electricity theft detection,'' *IEEE Trans. Ind. Informat.*, vol. 19, no. 2, pp. 1248–1259, Feb. 2023.

[4] V. B. Krishna, C. A. Gunter, and W. H. Sanders, ''Evaluating detectors on optimal attack vectors that enable electricity theft and DER fraud,'' *IEEE J. Sel. Topics Signal Process.*, vol. 12, no. 4, pp. 790–805, Aug. 2018.

[5] N. Bhusal, M. Gautam, R. M. Shukla, M. Benidris, and S. Sengupta, "Coordinated data falsification attack detection in the domain of distributed generation using deep learning," *Int. J. Electr. Power Energy Syst.*, vol. 134, Jan. 2022, Art. no. 107345.

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

[7] A. C. Marques, J. A. Fuinhas, and D. P. Macedo, "The impact of feed-in and capacity policies on electricity generation from renewable energy sources in Spain," *Utilities Policy*, vol. 56, pp. 159–168, Feb. 2019.

[8] M. I. Ibrahem, M. Mahmoud, M. M. Fouda, F. Alsolami, W. Alasmary, and X. Shen, "Privacy preserving and efficient data collection scheme for AMI networks using deep learning," *IEEE Internet Things J.*, vol. 8, no. 23, pp. 17131–17146, Dec. 2021.

[9] PR Newswire. *96 Billion is Lost Every Year to Electricity Theft*. Accessed: Jan. 2023. [Online]. Available: https://www.prnewswire.com/news-releases/96-billion-is-lost-every-year-to-electricity-theft-300453411.html

[10] M. M. Buzau, J. Tejedor-Aguilera, P. Cruz-Romero, and A. Gómez-Expósito, "Detection of non-technical losses using smart meter data and supervised learning," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 2661–2670, May 2019.

[11] 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.

[12] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2505–2516, Sep. 2017.

[13] S. Zidi, A. Mihoub, S. M. Qaisar, M. Krichen, and Q. A. Al-Haija, "Theft detection dataset for benchmarking and machine learning based classification in a smart grid environment," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 35, no. 1, pp. 13–25, Jan. 2023.

[14] M. Shaaban, U. Tariq, M. Ismail, N. A. Almadani, and M. Mokhtar, "Data-driven detection of electricity theft cyberattacks in PV generation," *IEEE Syst. J.*, vol. 16, no. 2, pp. 3349–3359, Jun. 2022.

[15] M. Ezeddin, A. Albaseer, M. Abdallah, S. Bayhan, M. Qaraqe, and S. Al-Kuwari, "Efficient deep learning based detector for electricity theft generation system attacks in smart grid," in *Proc. 3rd Int. Conf. Smart Grid Renew. Energy (SGRE)*, Mar. 2022, pp. 1–6.

[16] M. M. Badr, M. I. Ibrahem, M. Mahmoud, M. M. Fouda, F. Alsolami, and W. Alasmary, "Detection of false-reading attacks in smart grid net-metering system," *IEEE Internet Things J.*, vol. 9, no. 2, pp. 1386–1401, Jan. 2022.

[17] L. Xue, L. Cheng, Y. Li, and Y. Mao, "Quantum machine learning for electricity theft detection: An initial investigation," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData) IEEE Congr. Cybermatics (Cybermatics)*, Dec. 2021, pp. 204–208.

[18] W. Qi, A. I. Zenchuk, A. Kumar, and J. Wu, "Quantum algorithms for matrix operations and linear systems of equations," *Commun. Theor. Phys.*, vol. 76, no. 3, Mar. 2024, Art. no. 035103.

[19] Y. Du, X. Wang, N. Guo, Z. Yu, Y. Qian, K. Zhang, M.-H. Hsieh, P. Rebentrost, and D. Tao, "Quantum machine learning: A hands-on tutorial for machine learning practitioners and researchers," 2025, *arXiv:2502.01146*.

[20] P. Rebentrost, A. Steffens, I. Marvian, and S. Lloyd, "Quantum singular-value decomposition of nonsparse low-rank matrices," *Phys. Rev. A, Gen. Phys.*, vol. 97, no. 1, Jan. 2018, Art. no. 012327.

[21] S. Stein, Y. Mao, J. Ang, and A. Li, "QuCNN: A quantum convolutional neural network with entanglement based backpropagation," in *Proc. IEEE/ACM 7th Symp. Edge Comput. (SEC)*, Dec. 2022, pp. 368–374.

[22] S. A. Stein, B. Baheri, D. Chen, Y. Mao, Q. Guan, A. Li, S. Xu, and C. Ding, "QuClassi: A hybrid deep neural network architecture based on quantum state fidelity," in *Proc. Mach. Learn. Syst.*, 2022, pp. 251–264.

[23] N. Schetakis, D. Aghamalyan, M. Boguslavsky, A. Rees, M. Rakotomalala, and P. R. Griffin, "Quantum machine learning for credit scoring," *Mathematics*, vol. 12, no. 9, p. 1391, May 2024.

[24] K. Blazakis, Y. Katsigiannis, N. Schetakis, and G. Stavrakakis, "One day ahead wind speed forecasting based on advanced deep and hybrid quantum machine learning," in *Proc. 1st Int. Conf. Frontiers Artif. Intell., Ethics Multidisciplinary Appl.*, Athens, Greece, Sep. 2023, pp. 155–168.

[25] M. Schuld and N. Killoran, "Quantum machine learning in feature Hilbert spaces," *Phys. Rev. Lett.*, vol. 122, no. 4, Feb. 2019, Art. no. 040504.

[26] A. Pérez-Salinas, A. Cervera-Lierta, E. Gil-Fuster, and J. I. Latorre, "Data re-uploading for a universal quantum classifier," *Quantum*, vol. 4, p. 226, Feb. 2020.

[27] A. Pérez-Salinas, D. López-Núñez, A. García-Sáez, P. Forn-Díaz, and J. I. Latorre, "One qubit as a universal approximant," 2021, *arXiv:2102.04032*.

[28] S. Lloyd, M. Schuld, A. Ijaz, J. Izaac, and N. Killoran, "Quantum embeddings for machine learning," 2020, *arXiv:2001.03622*.

[29] Z. Li, J. Peng, Y. Mei, S. Lin, Y. Wu, O. Padon, and Z. Jia, "Quarl: A learning-based quantum circuit optimizer," in *Proc. ACM Program. Lang.*, vol. 8, Apr. 2024, pp. 555–582.

[30] F. Phillipson, "Quantum machine learning: Benefits and practical examples," in *Proc. QANSWER*, Jan. 2020, pp. 51–56.

[31] Z. Yan and H. Wen, "Performance analysis of electricity theft detection for the smart grid: An overview," *IEEE Trans. Instrum. Meas.*, vol. 71, pp. 1–28, 2022.

[32] M. G. Chuwa and F. Wang, "A review of non-technical loss attack models and detection methods in the smart grid," *Electr. Power Syst. Res.*, vol. 199, Oct. 2021, Art. no. 107415.

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

[34] Y. Liu, T. Liu, H. Sun, K. Zhang, and P. Liu, "Hidden electricity theft by exploiting multiple-pricing scheme in smart grids," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2453–2468, 2020.

[35] X. Xia, Y. Xiao, and W. Liang, "SAI: A suspicion assessment-based inspection algorithm to detect malicious users in smart grid," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 361–374, 2020.

[36] H. O. Henriques, R. L. S. Corrêa, M. Z. Fortes, B. S. M. C. Borba, and V. H. Ferreira, "Monitoring technical losses to improve non-technical losses estimation and detection in LV distribution systems," *Measurement*, vol. 161, Sep. 2020, Art. no. 107840.

[37] T. Hu, Q. Guo, X. Shen, H. Sun, R. Wu, and H. Xi, "Utilizing unlabeled data to detect electricity fraud in AMI: A semisupervised deep learning approach," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 30, no. 11, pp. 3287–3299, Nov. 2019.

[38] G. M. Messinis, A. E. Rigas, and N. D. Hatziargyriou, "A hybrid method for non-technical loss detection in smart distribution grids," *IEEE Trans. Smart Grid*, vol. 10, no. 6, pp. 6080–6091, Nov. 2019.

[39] P. P. Biswas, H. Cai, B. Zhou, B. Chen, D. Mashima, and V. W. Zheng, "Electricity theft pinpointing through correlation analysis of master and individual meter readings," *IEEE Trans. Smart Grid*, vol. 11, no. 4, pp. 3031–3042, Jul. 2020.

[40] X. Lu, Y. Zhou, Z. Wang, Y. Yi, L. Feng, and F. Wang, "Knowledge embedded semi-supervised deep learning for detecting non-technical losses in the smart grid," *Energies*, vol. 12, no. 18, p. 3452, Sep. 2019.

[41] E. U. Haq, C. Pei, R. Zhang, H. Jianjun, and F. Ahmad, "Electricity-theft detection for smart grid security using smart meter data: A deep-CNN based approach," *Energy Rep.*, vol. 9, pp. 634–643, Mar. 2023.

[42] OEDI. *Open Energy Data Initiative Platform*. Accessed: Sep. 2022. [Online]. Available: https://data.mendeley.com/datasets/c3c7329tjj/1

[43] O. A. Abraham, H. Ochiai, M. D. Hossain, Y. Taenaka, and Y. Kadobayashi, "Electricity theft detection for smart homes: Harnessing the power of machine learning with real and synthetic attacks," *IEEE Access*, vol. 12, pp. 26023–26045, 2024.

[44] A. Sen and N.-C. Yang, "Power theft detection using advanced neural network in three-phase distribution systems," *IEEE Trans. Instrum. Meas.*, vol. 73, pp. 1–10, 2024.

[45] Z. Zhao, G. Liu, and Y. Liu, "Practical privacy-preserving electricity theft detection for smart grid," *IEEE Trans. Smart Grid*, vol. 15, no. 4, pp. 4104–4114, Jul. 2024.

[46] Ausgrid. *Solar Home Electricity Data*. Accessed: Sep. 2022. [Online]. Available: https://www.ausgrid.com.au/Industry/Our-Research/Data-to-share/Solar-home-electricity-data

[47] *Solcast*. Accessed: Sep. 2022. [Online]. Available: https://solcast.com/historical-and-tmy/

[48] A. Takiddin, M. Ismail, U. Zafar, and E. Serpedin, "Deep autoencoder-based anomaly detection of electricity theft cyberattacks in smart grids," *IEEE Syst. J.*, vol. 16, no. 3, pp. 4106–4117, Sep. 2022.

[49] R. Punmiya and S. Choe, "Energy theft detection using gradient boosting theft detector with feature engineering-based preprocessing," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 2326–2329, Mar. 2019.

[50] S. K. Gunturi and D. Sarkar, "Ensemble machine learning models for the detection of energy theft," *Electric Power Syst. Res.*, vol. 192, Mar. 2021, Art. no. 106904.

[51] A. A. Almazroi, F. S. Alsubaei, N. Ayub, and N. Z. Jhanjhi, "Inclusive smart cities: IoT-cloud solutions for enhanced energy analytics and safety," *Int. J. Adv. Comput. Sci. Appl.*, vol. 15, no. 5, pp. 1–10, 2024.

[52] V. Bergholm et al., "PennyLane: Automatic differentiation of hybrid quantum-classical computations," 2018, *arXiv:1811.04968*.

[53] *QML in Smart-Grids*. Accessed: Sep. 2023. [Online]. Available: https://github.com/nsansen/QML-in-smart-grids

[54] N. Schetakis, D. Aghamalyan, P. Griffin, and M. Boguslavsky, "Review of some existing QML frameworks and novel hybrid classical–quantum neural networks realising binary classification for the noisy datasets," *Sci. Rep.*, vol. 12, no. 1, p. 11927, Jul. 2022.

[55] A. Gao, F. Mei, J. Zheng, H. Sha, M. Guo, and Y. Xie, "Electricity theft detection based on contrastive learning and non-intrusive load monitoring," *IEEE Trans. Smart Grid*, vol. 14, no. 6, pp. 4565–4580, Jun. 2023.

[56] T. Chen and C. Guestrin, "XGBoost: A scalable tree boosting system," in *Proc. 22nd ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, Aug. 2016, pp. 785–794.

[57] G. Ke, Q. Meng, T. Finley, T. Wang, W. Chen, W. Ma, Q. Ye, and T. Liu, "LightGBM: A highly efficient gradient boosting decision tree," in *Proc. Adv. Neural Inf. Process. Syst.*, vol. 30, Dec. 2017, pp. 3146–3154.

[58] L. Prokhorenkova, G. Gusev, A. Vorobev, A. V. Dorogush, and A. Gulin, "CatBoost: Unbiased boosting with categorical features," in *Proc. 32nd Int. Conf. Neural Inf. Process. Syst.*, 2018, pp. 1–11.

[59] S. Abbas, I. Bouazzi, S. Ojo, G. A. Sampedro, A. S. Almadhor, A. A. Hejaili, and Z. Stolicna, "Improving smart grids security: An active learning approach for smart grid-based energy theft detection," *IEEE Access*, vol. 12, pp. 1706–1717, 2024.

[60] F. Mohammad, K. Saleem, and J. Al-Muhtadi, "Ensemble-learning-based decision support system for energy-theft detection in smart-grid environment," *Energies*, vol. 16, no. 4, p. 1907, Feb. 2023.

[61] A. Abbas et al., "Challenges and opportunities in quantum optimization," *Nature Rev. Phys.*, vol. 6, pp. 718–735, Oct. 2024.

[62] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, "Quantum machine learning," *Nature*, vol. 549, no. 7671, pp. 195–202, Sep. 2017.

[63] D. Leykam and D. G. Angelakis, "Topological data analysis and machine learning," *Adv. Phys., X*, vol. 8, no. 1, Apr. 2023, Art. no. 2202331.

[64] A. Melnikov, M. Kordzanganeh, A. Alodjants, and R.-K. Lee, "Quantum machine learning: From physics to software engineering," *Adv. Phys., X*, vol. 8, no. 1, Dec. 2023, Art. no. 2165452.

[65] H. Carmichael, "Master equations and sources I," in *An Open Systems Approach to Quantum Optics*, vol. 4. Berlin, Germany: Springer-Verlag, 1991.

[66] M. A. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*. Cambridge, U.K.: Cambridge Univ. Press, 2010.

[67] H. Liao, I. Convy, W. J. Huggins, and K. B. Whaley, "Robust in practice: Adversarial attacks on quantum machine learning," *Phys. Rev. A, Gen. Phys.*, vol. 103, no. 4, Apr. 2021, Art. no. 042427.

[68] N. Liu and P. Wittek, "Vulnerability of quantum classification to adversarial perturbations," *Phys. Rev. A, Gen. Phys.*, vol. 101, no. 6, Jun. 2020, Art. no. 062331.

[69] S. Janthong, R. Duangsoithong, and K. Chalermyanont, "Feature extraction of risk group and electricity theft by using electrical profiles and physical data for classification in the power utilities," *ECTI Trans. Comput. Inf. Technol. (ECTI-CIT)*, vol. 18, no. 1, pp. 51–63, Jan. 2024.

[70] S. Janthong, K. Chalermyanont, and R. Duangsoithong, "Unbalanced data handling techniques for classifying energy theft and defective meters in the provincial electricity authority of Thailand," *IEEE Access*, vol. 11, pp. 46522–46540, 2023.

[71] S. Janthong, K. Chalermyanont, and R. Duangsoithong, "Comparison of feature extraction methods for classifying energy theft and defective meters in automatic meter reading," in *Proc. IEEE Int. Electr. Eng. Congr. (iEECON)*, Mar. 2023, pp. 49–53.

[72] M. Cerezo, G. Verdon, H.-Y. Huang, L. Cincio, and P. J. Coles, "Challenges and opportunities in quantum machine learning," *Nature Comput. Sci.*, vol. 2, no. 9, pp. 567–576, Sep. 2022.

[73] Y. Cao, J. Romero, J. P. Olson, M. Degroote, P. D. Johnson, M. Kieferová, I. Kivlichan, T. Menke, B. Peropadre, N. P. D. Sawaya, S. Sim, L. Veis, and A. Aspuru-Guzik, "Quantum chemistry in the age of quantum computing," *Chem. Rev.*, vol. 119, no. 19, pp. 10856–10915, Aug. 2019.

[74] K. Bharti, A. Cervera-Lierta, T. H. Kyaw, T. Haug, S. Alperin-Lea, A. Anand, M. Degroote, H. Heimonen, J. S. Kottmann, T. Menke, W. Mok, S. Sim, L. C. Kwek, and A. Aspuru-Guzik, "Noisy intermediate-scale quantum algorithms," *Rev. Mod. Phys.*, vol. 94, no. 1, Feb. 2022, Art. no. 015004.

[75] M. A. Khan, M. N. Aman, and B. Sikdar, "Beyond bits: A review of quantum embedding techniques for efficient information processing," *IEEE Access*, vol. 12, pp. 46118–46137, 2024.

KONSTANTINOS BLAZAKIS received the Diploma degree in applied mathematical and physical sciences from the National Technical University of Athens (NTUA), in 2010, and the M.Sc. and Ph.D. degrees in electrical and computer engineering from the Technical University of Crete (TUC), in 2016 and 2024, respectively.

His research interests include machine learning, data mining, wind and solar forecasting, power theft detection, smart grids, and electric vehicles.

NIKOLAOS SCHETAKIS received the B.S. degree from the University of Crete, in 2008, and the M.S. degree from the Technical University of Crete, Crete, Greece, in 2012, where he is currently pursuing the Ph.D. degree.

Since 2022, he has been the CEO of Quantum Innovation Pc. His current research interests include classical and quantum machine learning, computer vision, and reservoir computing.

MAHMOUD M. BADR received the B.S. and M.S. degrees in electrical engineering (electronics and communications) from Benha University, Cairo, Egypt, in 2013 and 2018, respectively, and the Ph.D. degree in electrical and computer engineering from Tennessee Tech University, TN, USA, in 2022.

He is currently an Assistant Professor with the Networks and Computer Security: Cybersecurity Department, College of Engineering, State University of New York (SUNY) Polytechnic Institute, USA. He also holds the position of a Lecturer Assistant with the Faculty of Engineering at Shoubra, Benha University, Egypt. His research interests include machine learning, blockchains, cryptography, 5G networks, and smart grids.

DAVIT AGHAMALYAN has worked in many different areas of quantum physics. Joining CQT's Ph.D. Programme, in 2011, he completed his thesis on "Atomtronics: Quantum Technology with Cold Atoms in Ring Shaped Optical Lattices." After graduating, he moved to France for a postdoctoral stint, where he worked on cold atom collisions. He returned to CQT, in 2017, as a Research Fellow. Then, he was part of a collaboration between CQT and A∗STAR's Institute of High Performance Computing on quantum optical systems. Later, he has moved his quantum expertise into machine learning. He joined Singapore Management University, in July 2020, as a Research Scientist. He had been exploring the potential of quantum machine learning to make better predictive models for credit scoring. Currently, he is with the A∗star's Institute of High Performance Computing (Department of Materials Science and Engineering), where he is working in quantum optics, quantum machine learning, and on quantum control of many-body quantum systems.

KONSTANTINOS STAVRAKAKIS received the Diploma degree from the School of Electrical and Computer Engineering, National Technical University of Athens (NTUA), in 2022.

Recently, he has been a Software Engineer specializing in both classical and quantum machine learning with Alma Sistemi Srl, Rome, Italy. His current research interests include the development and optimization of quantum algorithms and the integration of classical machine learning techniques with emerging quantum computing technologies.

GEORGIOS STAVRAKAKIS received the Diploma degree in electrical engineering from the National Technical University of Athens (NTUA), Greece, in July 1980, the master's (D.E.A.) degree in automatic control and systems engineering from INSA, Toulouse, France, in July 1981, and the Ph.D. degree in automatic control and systems engineering from "Paul Sabatier" University-Toulouse-III, France, in January 1984.

He was a Research Fellow with the Robotics Laboratory, NTUA (1985–1988), and a Visiting Scientist with the Institute for Systems Engineering and Informatics/Components Diagnostics & Reliability Sector of the EC-Joint Research Center (JRC), Ispra, Italy (September 1989–September 1990). He was the Vice President of the Hellenic Center of Renewable Energy Sources (www.cres.gr), from November 2000 to April 2002. He has been a Full Professor in systems engineering with the Electrical and Computer Engineering School, Technical University of Crete (www.ece.tuc.gr), Greece, since November 1995. He performed prototype and advanced engineering research in automation, systems safety and reliability analysis, real-time industrial processes, fault monitoring and diagnosis, modeling and diagnosis in bioengineering systems, AI intelligent DSS-deep learning NN applications in modeling, forecasting, classification in medical diagnosis, power systems, power theft detection, renewable energy sources (RES) forecasting, modeling and automation, smart and micro grids, energy storage and increased RES penetration in non-interconnected power grids, energy efficiency, and building energy management systems (BEMS).