Renewable and Sustainable Energy Reviews 184 (2023) 113544

Contents lists available at ScienceDirect

Renewable and Sustainable Energy Reviews

journal homepage: www.elsevier.com/locate/rser

Review article

Systematic review of energy theft practices and autonomous detection through artificial intelligence methods

Erika Stracqualursi [a], Antonello Rosato [b], Gianfranco Di Lorenzo [a], Massimo Panella [b], Rodolfo Araneo [a,*]

[a] Electrical Engineering Division of DIAEE, University of Rome "La Sapienza", Via Eudossiana 18, Rome, 00184, Italy
[b] Department of Information Engineering, Electronics and Telecommunications, University of Rome "La Sapienza", Via Eudossiana 18, Rome, 00184, Italy

ARTICLE INFO

Keywords:
Artificial intelligence
Autonomous theft detection
Electricity theft
Energy meter tampering
Machine learning
Non-technical losses
Smart grids

ABSTRACT

Energy theft poses a significant challenge for all parties involved in energy distribution, and its detection is crucial for maintaining stable and financially sustainable energy grids. One potential solution for detecting energy theft is through the use of artificial intelligence (AI) methods. This systematic review article provides an overview of the various methods used by malicious users to steal energy, along with a discussion of the challenges associated with implementing a generalized AI solution for energy theft detection. In this work, we analyze the benefits and limitations of AI methods, including machine learning, deep learning, and neural networks, and relate them to the specific thefts also analyzing problems arising with data collection. The article proposes key aspects of generalized AI solutions for energy theft detection, such as the use of smart meters and the integration of AI algorithms with existing utility systems. Overall, we highlight the potential of AI methods to detect various types of energy theft and emphasize the need for further research to develop more effective and generalized detection systems, providing key aspects of possible generalized solutions.

1. Introduction

The massive electrification of consumers' appliances, unit products, and energy services is an ongoing trend in the current energy transition to a low-carbon economy and climate neutrality [1]. Electric energy is inherently pervasive: it is an essential part of modern life, a necessary component for economic production and growth, and its cost is often a critical part of the total costs for private households and the industry. Researchers assessed that there is bidirectional causality between electric energy consumption and gross domestic product in a country [2]. Hence, electric energy not only shapes the energy systems but also impacts human beings' everyday life on a national and international scale, calling into question energy policymakers and stakeholders and setting the agenda for development policies [3].

Electricity can be stolen as any other good with an economic value, yet, for its aforementioned characteristics, it is affected by stealing attempts. After the pioneering work of Smith [4] that explored the issue of electricity theft (ET) in a global context, several studies, albeit with an emphasis on particular countries (e.g., Turkey [5], Indian States [6], Pakistan [7]), confirmed that ET is a worldwide predicament. The various types of ET that have been conceived and are often realized under the risk of severe injuries, electrocution, or even death of the culprit [8] demonstrate the widespread of this rampant fraudulent and illegal activity. ET, as well as petty corruption, graft and pilfering, which are closely intertwined phenomena, frequently occur in countries with under-developed or developing economies [9]. Greater occurrence of ET is generally encountered in countries with low values of the six Worldwide Governance Indicators published by the World Bank [10]. They are, namely, the regulatory effectiveness, the efficiency of the legal system, the control of corruption, the degree of the voice of accountability, the political stability, and the government effectiveness. Additionally, socio-economic factors influence ET, including literacy rate, poverty, crime rate, consumption per capita, urbanization, income, human development index, and population size and density [11]. In developed countries, because of the more advanced monitoring and metering systems that bring transparency in electricity distribution, ET is more difficult, yet present [12]. Today's soaring energy prices will fuel the number of people stealing electricity, which is expected to increase in the near future.

ET is one of the major chunks of Non-Technical Losses (NTLs) in electricity [13,14]. Grid losses are the difference between the amount of electricity entering the grid minus the amount of electricity metered

* Corresponding author.
E-mail addresses: erika.stracqualursi@uniroma1.it (E. Stracqualursi), antonello.rosato@uniroma1.it (A. Rosato), gianfranco.dilorenzo@uniroma1.it (G. Di Lorenzo), massimo.panella@uniroma1.it (M. Panella), rodolfo.araneo@uniroma1.it (R. Araneo).

https://doi.org/10.1016/j.rser.2023.113544
Received 27 February 2023; Received in revised form 21 June 2023; Accepted 6 July 2023
Available online 26 July 2023

and sold. Such losses are divided into two categories [12]: Technical Losses (TLs), which are caused by power dissipation in transmission lines and cannot be fully eliminated due to physical constraints, and NTLs, which are caused by factors external to the power system. NTLs are a severe concern for distribution operators (DSOs - or utility companies) and electricity providers (or traders) because they result in a lack of profits for both. Losses in the distribution system are generally renewed through average flat percentage coefficients of the energy delivered; hence, lower or higher losses result in economic revenues or losses for the DSOs. Furthermore, ET may impact the quality of electricity supply, can cause power disruption and infrastructure damage [15], and ultimately can provoke blackouts or even threaten public safety. Once the theft is uncovered, the DSO is called to reconstruct the consumer's consumption, identifying the initial moment of the illegal consumption. Then, the electricity provider who supplied the energy to the client when a contract exists (or whom the client is attributed to by law enforcement when a contract does not exist) must generally take on a protracted legal dispute to obtain a judicial enforcement order of payment. Lengthy litigations and unpaid bills are translated into consumer increments in tariffs. This latter phenomenon worsens when the stealing users cannot be disconnected from the grid for peculiar reasons (e.g., they feed public services or healthcare devices). In this case, the whole community pays for them through appropriate components inserted into the electricity billing structure, uprising the problem's perception. Ultimately, NTLs can significantly jeopardize the current green transition towards a CO_2-free energy production [16].

Detecting ET is a complex task due to the many thieving methods that greedy customers put in place. Czechowski and Kosek write in [17] that, according to an electric energy supplier, there are about 300 theft techniques. Widespread methods for illegal electric consumption are reviewed in Section 3. The present study does not consider billing alteration, irregularities, and unpaid bills since they are administrative issues.

The primary measure adopted to curb ET is deploying smart (electricity) meter (SMs) that can be remotely supervised and read. The surveillance carried out by DSOs on meters is performed in a rolling fashion. Anyway, many meters may be located inside the private property and not be accessible, or they may be easily physically obstructed. In light of this, modern and future smart metering infrastructures, currently adopted by DSOs within smart grid (SG) frameworks, may facilitate anomaly detection [18].

First-generation (1G) SMs have been operating in Europe since the early 2000s. They are based on the European Union (EU) Directive 2004/22/CE about measuring instruments (called MID Directive). According to the recent EU Directives concerning common rules for the internal market for electricity and gas (2009/72/EC and 2009/73/EC), energy efficiency (2012/27/EU), and measuring instruments (2014/32/EU and 2015/13/EU), Member States are nowadays rolling-out "*open intelligent metering systems*" of second generation (meters 2G). Meters 2G provide greater functionalities for all the players involved, end users (customers or prosumers), DSOs, and energy providers, in terms of intelligence, communication, and integration in smart environments (grids, buildings, and homes). In [19], the authors introduce the benefits of SMs for identifying illegal consumers, while in [20], Ahmad illustrates with a broader view the advantages of a SM infrastructure.

What is disruptive in the present context is that 2G meters provide consumption data every quarter of an hour and a channel of communication from the SM directly to the customer or third parties. Additionally, they can display absorbed power in real time at any moment. 1G meters had no such functionalities. In low voltage connections, meters usually treat monthly consumption data on time slots through registers that store index reads (e.g., cumulative absorbed active energy). Every month, index reads are subtracted from previous ones to provide aggregate consumption data on the past month. Only in medium voltage installations or low voltage installations with contractual power higher than a prescribed threshold (e.g., in Italy, 55 kW), meters record values every 15 min. On the one hand, these improvements help customers be aware of their consumption profiles in everyday life to encourage competition in post-meter services and participation in transactive markets [21]. On the other hand, they provide the DSOs with a tremendous amount of data that can be used to identify illegal energy consumption.

There is a body of literature on the potentialities offered by an SM infrastructure viewed as a component of a SG to detect (and deject) illegal consumers. In [13], well before the advent of SMs 2G, the authors designed an advanced architecture composed of an SM, external control station, harmonic generator, and filter circuit to provide various parameters related to instantaneous power consumption. In their overview on smart metering systems [22], Sharma and Saini indicate how an automatic metering infrastructure that relies on SMs can help minimize ET. However, the problem of false positives requires particular care. In [23], Yip et al. introduce two new metrics, defined as the loss factor and error term, to estimate the amount of TLs and capture the measurement noise in case of consumers' malfeasance or faulty meter. Then, the authors develop an anomaly detection framework based on an energy balance that uses these metrics, and that is solved through linear programming. The authors claim the method can distinguish intermittent cheating consumers and faulty equipment; anyway, it requires sampling the consumption over each day, i.e., advanced SMs. In [24], Park and Kim use the data streams generated from SMs in conjunction with an anomaly pattern detection method to detect ET. Again, this approach requires daily energy usage data. In [25], de Souza et al. use data from SMs and phasor measurement units and process them using a multilayer perception artificial neural network to detect anomalous consumption patterns. The data from SMs are so necessary that even intermediate monitor meters are proposed in [26]. Indeed, the fine-grained data about consumers' consumption that SMs can record in near real-time pose a problem in handling this big amount of data; Wen et al. make an overview of the compression techniques to reduce the transmission pressure and storage overhead in [27].

The issue is that ET, especially when intermittent, is difficult to distinguish from a fault or a natural variation of the consumer's load. In order to implement efficient Artificial Intelligence (AI) fault-detections methods, as the ones discussed in the reminder of the paper, both knowledge of the network topology and data recorded by relevant measuring systems are required. Consequently, the difficulty is strictly linked to the quantity and quality of metering data. What plays an important role are the amount of available data (e.g., active power, reactive power, and power peaks) and the time sampling T of the measured data (e.g., hour, day, or month). Since DSOs employ qualified inspection teams to assess on the field any possible fraudulent behavior, any false classification of an honest customer as fraudulent entails vast costs.

The smart metering infrastructure may offer a broad range of potential benefits when its dataset is used in conjunction with AI. Innovative AI algorithms enable the analysis and process of large datasets and the extraction of features from massive and varying load profiles, in order to detect the consumers' absorption patterns and find anomalous consumption behaviors referred to ETs.

Reviews on the topic available in the literature focus on ET practices [17] or on algorithms only, either for non-technical losses detection [12,28] or for maintenance prediction [29]; instead, this review aims at providing the reader with a clear view both on the practical aspects related to ET and on the available detection algorithms, also considering their limits of applicability, starting from understanding of the problem on the practical level to choosing suitable solutions for its detection.

2. Artificial intelligence in the energy sector

The energy sector plays a pivotal role in the economic development of nations, providing power for industries, transportation, and residential needs. As the global demand for energy continues to rise, optimizing energy generation, distribution, and consumption has become an urgent priority. In recent years, the integration of AI techniques in the energy sector has emerged as a game-changer, offering innovative solutions to enhance operational efficiency, promote sustainability, and tackle the persistent challenge of ET.

Traditional methods of detecting ET rely heavily on manual inspections, which are time-consuming, costly, and often ineffective in identifying sophisticated theft practices. However, with the advent of AI-based methods, there is new found hope for automating the detection process, enabling utilities to detect and respond to ET incidents more efficiently.

AI encompasses a diverse range of technologies that empower machines to simulate intelligent behavior, perceive their environment, reason, learn, and autonomously make decisions. These capabilities make AI an ideal tool for addressing the complexities of the energy sector, where vast amounts of data need to be analyzed, patterns identified, and real-time decisions made. By harnessing AI, the energy sector can optimize resource allocation, improve grid management, enhance energy efficiency, and facilitate the seamless integration of renewable energy sources.

One of the most notable applications of AI in the energy sector is the detection and prevention of ET practices. By leveraging AI algorithms like machine learning and Deep Learning (DL), utility companies can analyze extensive data collected from SMs, sensors, and other monitoring devices. These algorithms have the ability to identify patterns and anomalies associated with ET, enabling utilities to differentiate between legitimate energy consumption and unauthorized usage. Moreover, AI systems can continuously learn and adapt to new theft techniques, improving the accuracy and effectiveness of detection systems over time.

The implementation of AI-powered energy management systems also presents significant benefits in optimizing energy generation and consumption. By utilizing real-time data from SGs and Internet of Things (IoT) devices, AI algorithms can accurately forecast energy demand, dynamically adjust power generation, and optimize distribution networks. This empowers utilities to enhance load balancing, reduce transmission losses, and maximize the utilization of renewable energy sources. Additionally, AI can facilitate demand response programs, allowing consumers to adjust their energy usage based on price signals or grid conditions, thereby promoting energy efficiency and mitigating peak demand challenges.

While the integration of AI holds immense promise for the energy sector, several challenges and considerations must be addressed, with ET being a crucial aspect. Data privacy and security concerns, ethical implications of automated decision-making, regulatory frameworks, and the necessity for skilled AI professionals in the energy industry are all critical areas that require attention. Collaboration among utility companies, policymakers, researchers, and technology providers is essential to overcome these challenges effectively.

Among the techniques of the AI, the most stable and reliable ones for complex decision making and pattern recognition problems revolve around DL. In fact, the potentialities of DL algorithms for energy time series analysis are widely acknowledged and many contributions were proposed in this regard over the past few years. One of the main problems concerning energy distribution issues is about time series classification: energy-related data are notoriously hard to classify because they may exhibit fluctuating behaviors or heterogeneous profiles. In recent years, a variety of approaches based on Machine Learning (ML) and DL have been proposed to deal with time series classification tasks [30–32].

Thanks to its flexibility and modularity, DL can easily be applied to different pattern recognition problems without the necessity of performing heavy data preprocessing steps; it allows to automatically extract meaningful features and relevant information, thus leading to high expressive power and resilience to ill-posed input data. A multivariate strategy within a DL architecture integrates manifold data sources to provide a substantial improvement on the quality of the solution, useful when dealing with highly dynamic sequences and complex systems in the energy domain [33,34].

The recent advances in the metering infrastructure contributed to the development of effective data-driven anomaly detection algorithms in the distribution grid [63]. The possibility of performing high frequency data sampling in different distribution contexts (e.g. Virtual Power Plant, Power Systems, Energy Communities) led to an optimal management of energy loads and dispatching. Therefore, the development of modern approaches based on spatial and temporal data correlation is of crucial importance [64].

Supervision and management procedures are used in different systems in the energy context, whether the final decision-making process is more or less automatized (i.e., with different levels of “smartness”). The most common environments in which AI is engaged can be categorized into five groups, listed in descending order of size: SGs, district microgrids, buildings, appliances, and machines. All of these groups of smart systems represent a significant context in which ML has been employed with good results for fault detection, diagnosis, and management, being the penetration of AI in the system's structure more important than the nature and scale of the system itself. It is worth noting that, despite their different dimension and scale, all of them share the same challenges when relying on AI algorithms for supervision:

- Real-time measurement: For enabling fast and accurate detection of anomalies and response, it is necessary that all the available data are as close as possible to the actual, present status of the power grid. As a consequence, the smart sensors and SMs deployed in the system need not only to be fast in acquiring data but also need to be prompt to send it through the communication network. While the ubiquitous sensors' computational power can be just low enough to compute physical measurements, the sensors' analysis and communication capabilities must be boosted, tentatively using ML, to take into account the possible overhead in forwarding through the network [65].
- Large datasets: Clearly, the more data is acquired from the physical operation of the grid, the better the diagnosis could be, given enhanced data analytics [66]. For this reason, there is the tendency to overreach the dimension of the datasets used, for the sake of facilitating the diagnostic AI models. This bears some difficulties regarding not only the speed of the transmission of information but most importantly processing and storing the amount of data, which must be done efficiently and smartly [67,68].
- Two-way secure communication: Apart from the network capacity necessary for handling large and fast data sharing, the communication protocol put in place in a smart environment must be bidirectional. The core characteristic of ML-enhanced SGs is the capacity of optimizing energy management by continuously exchanging data to and from sensors, appliances, machines, and control points. Also, since some exchanged data is sensible and since important distribution-level decisions are shared in the network [69], the communication needs to be secure and resilient to attacks; once again, AI techniques have been applied for this purpose with great success [70].

These concepts can be viewed not only as structural concerns restraining the development and performance of AI applications in the energy framework but, given their ubiquitous nature, as enablers for more reliable energy management logic. In other words, nowadays real-time measurement and fast communication can be considered almost a given in any modern energy system, thus it would be unwise not to take advantage of them by implementing sophisticated ad-hoc AI algorithms. Furthermore, energy management systems are often developed by relying on the same premises nonetheless, disregarding their

Table 1
Techniques and methods for data analysis for the solution of energy transmission, distribution, and dispatching issues.

Publication	Scope	Method	Framework	Application
[35]	Fault detection in smart metering	Impedance	SG	Distribution
[36]	Detection and location	Impedance	SG	Dispatch
[37]	Fault localization	Impedance	SG	Transmission
[38]	Fault detection	Impedance	Microgrid	Distribution
[39]	Detection and location	Impedance	SG	Distribution
[40]	Detection	Impedance	SG	Transmission
[41]	Detection	Impedance	SG	Dispatch
[42]	Fault detection and discrimination	Impedance	SG	Transmission
[43]	Disturbance detection	Analytical	SG	Distribution
[44]	Anomaly detection	Analytical	SG	Distribution
[45]	Fault detection and classification	Analytical	SG	Transmission
[46]	Fault detection	Analytical	Building	Dispatch
[47]	Fault detection	Learning	SG	Transmission
[48]	Fault detection	Learning	Microgrid	Distribution
[49]	Diagnosis	Learning	HVAC	Dispatch
[50]	Fault detection	Learning	Microgrid	Distribution
[51]	Fault detection	Learning	Microgrid	Distribution
[52]	Fault detection	Learning	Microgrid	Dispatch
[53]	Fault analysis and protection	Learning	BESS	Dispatch
[54]	Diagnosis	Learning	SG	Distribution
[55]	Detection and diagnosis	Learning	Building	Distribution
[56]	Fault detection	Learning	PV	Dispatch
[57]	Fault detection, Identification and location	Learning	SG	Distribution
[58]	Fault tolerance	Learning	SG	Transmission
[59]	Prediction	Learning	Microgrid	Transmission
[60]	Classification	Learning	SG	Distribution
[61]	Fault detection	Learning	Building	Dispatch
[62]	Predictive control	Learning	Microgrid	Distribution

underlying logic and analytical implementation, and facing the same challenges.

In the light of the emerging problems in managing distributed generation with relation to prosumers and renewable sources, fault diagnosis has become the mainstay for an efficient and reliable modern SG, thus attracting scientists from different fields. While the general issues are about electrical, industrial, and power engineering, in recent years, more and more techniques have been borrowed from data science and information technology, showing favorable results in solving energy transmission, distribution, and dispatching issues. Ordinarily, the techniques and algorithms found in literature can be divided into three different groups, based on their analysis mode and used data:

- *Impedance-based methods*: These are a plethora of methods which rely on steady-state measurements of current and voltage. These measurements are carried out to tentatively estimate an apparent reactance or impedance during the fault. The latter is used to estimate the distance to the fault. One of the main weaknesses is the impossibility of resolving the ambiguity caused by multiple faults occurring at the same time. Apart from using the same physical concepts, impedance-based methods can be different in their range of applications. As a general note, they are particularly suited for legacy power systems but lack good performance when following the evolution of SG topologies. For reference, a list of works inherent in the most prominent impedance-based method is presented in Table 1.
- *Analytical methods*: This group of techniques is more generic, as they combine the use of a formal process with the system model, using knowledge to create an analytical mathematical model. Their fault detection estimation is polyvalent and, being fundamentally signal processing methods, their quality hinges on the complexity of the employed algorithm and on the system sampling rate. A broad range of approaches is available, differing in the choice of the analytical model; a comprehensive list is given in Table 1.
- *Learning based*: As already stated, AI techniques are employed in fault detection leveraging their automatic learning procedure, which has great advantages in modern SG scenarios as they can follow the changes in the grid physical structure and power flow. It is also clear that learning-based methods are more demanding in terms of resources, also needing supportive forecasting knowledge to infer structures over data and diagnosing faults. In most cases, supervised learning is played out, as the characteristics of the faults that may occur in the study framework are well-known. The most influential fault detection methods with ML are listed in Table 1. As a remark, while being the most sought-after solutions given their great generalization capability, sometimes ML algorithms bear difficulties in human tuning and adjustments since they could be viewed as a so-called “black-box”, with difficult access to their hyperparameters. For this reason, it is only advisable to deploy AI methods when the training scheme is well-defined, giving access to researchers well-versed in ML theory. For this reason, some of the works listed in Table 1 are taken from strict communication and AI fields.

3. Overview on theft methods and malicious users behavior

A review of common fraudulent practices regarding ET is presented in this section, limiting to malicious strategies relevant to SGs. The analysis focuses on ET by users connected to the low-voltage (LV) and medium-voltage (MV) networks, schematically summarized in Fig. 1. The analysis distinguishes between methods dealing with direct operation on energy metering devices, and those providing non-authorized connections in order to tap energy from the network or to bypass the metering systems. Depending on the voltage level of the point of connection and the type of energy supply as from the contract signed with the distributor (e.g., three-phase or single-phase, if present), brief reference is made to simple approaches allowing to compute a first estimate of the actual energy consumption during to the period of fraud.

3.1. Users connected to the MV network

The typical technical practice of the Italian DSO is to provide the User with a suitable point of connection to the MV network. Private substations, as in Fig. 2, can often be considered as terminal type substations, i.e. substations where the MV line ends at the installation

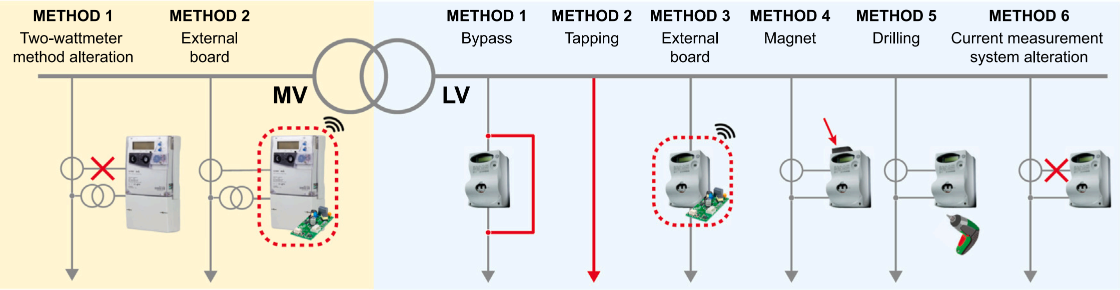
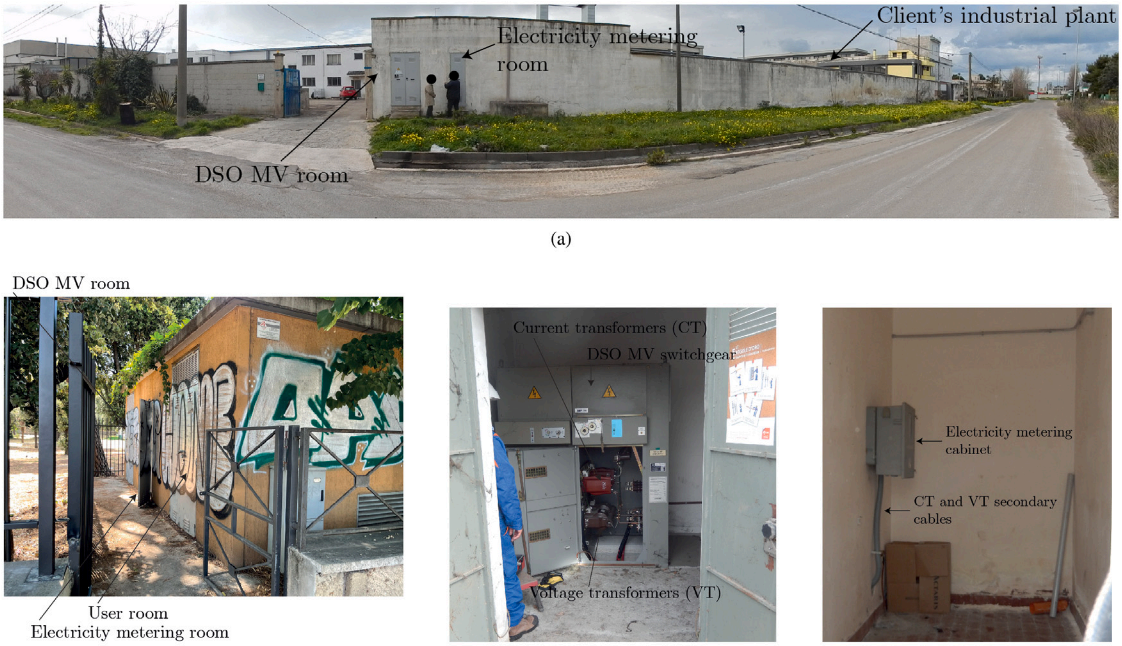


Fig. 1. Schematic representation of different methods for energy theft from the LV and MV networks.


Electricity metering room
Client's industrial plant
DSO MV room
DSO MV room
User room
Electricity metering room
Current transformers (CT)
DSO MV switchgear
Voltage transformers (VT)
Electricity metering cabinet
CT and VT secondary cables

(a)

(b)

(c)

(d)

Fig. 2. Example of a private substation.

point of the substation itself. They are owned by the User and can supply both civil users (schools, hospitals, etc.) and industrial users connected to the public MV grid. The user must make available to the distributing company a special room, accessible to the staff of the company, where the equipment for which the distribution company is responsible will be installed. There can be various design solutions, although in recent times the use of prefabricated substations, consisting of a distributor room, a metering room and a user room, is increasingly widespread.

- Distributor room (D): Where the switching devices of the Distributor are installed. This room must be large enough to allow for possible construction of the incoming–outgoing system that the Distributor is entitled to implement, even to satisfy new requirements at a later stage. The delivery room houses the sampling point that represents the boundary and the connection between the public grid and the user installation.
- Metering room (M): Where the metering equipment is located. This room must be accessible from a public road, to allow maintenance by authorized personnel regardless of whether the User is present.
- User room (U): Intended to contain the MV and LV switchgear and protection devices of the User. This room is normally adjacent to the other two rooms.

Since room M should be accessible also to the User, the latter may tamper the measuring system in order to illegally alter in his/her favor the measured power. The most frequent tampering method consists in shunting (e.g., through a pin or a rigid conducting wire with resistance R_{sh}) the secondary winding of one of the two measuring current transformers (CTs) employed by the Aron circuit (e.g., the *two-wattmeter method*) for the measurement of the absorbed three-phase power (see Fig. 3). The general working principle is illustrated in Fig. 4, where $\mathbf{I}_r+\mathbf{I}_s+\mathbf{I}_t = 0$ is assumed; herein, bold upper case quantities are complex quantities and upper case quantities are their corresponding rms values.

Two CTs, with turns ratio k_c, are used to measure the currents $\mathbf{I}_r$ and $\mathbf{I}_t$, carried by phase conductors r and t; two voltage transformers, with turns ratio k_v, are used to measure the line-to-line voltage $\mathbf{V}_{rs} = \mathbf{V}_r - \mathbf{V}_s$ and $\mathbf{V}_{ts} = \mathbf{V}_t - \mathbf{V}_s$. Hence, referring with prime quantities to the secondary (low-voltage and low-current) windings of the measuring transformers, the measured active and reactive power, P_m and Q_m, in normal operating conditions (i.e., with $R_{sh} \to \infty$) can be retrieved

$$P_m = k_v k_c \left[V'_{rs} I'_r \cos\left(\varphi + \frac{\pi}{6}\right) + V'_{ts} I'_t \cos\left(\varphi - \frac{\pi}{6}\right)\right] \tag{1}$$

$$Q_m = k_v k_c \left[V'_{rs} I'_r \sin\left(\varphi + \frac{\pi}{6}\right) + V'_{ts} I'_t \sin\left(\varphi - \frac{\pi}{6}\right)\right] , \tag{2}$$

where a balanced three-phase circuit is assumed. If the metering apparatus gets hacked through an unknown resistance R_{sh} as in Fig. 4, assuming $R_{sh} \approx 0$ (hence, $I'_t \approx 0$), the measured powers after tampering

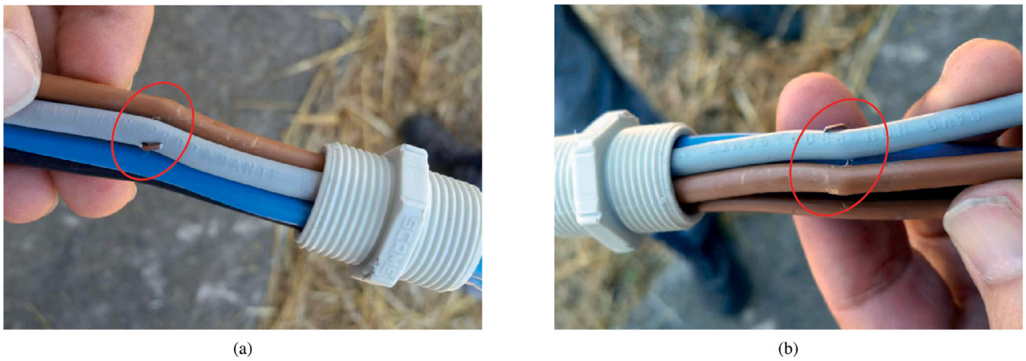


Fig. 3. Example of shunt on MV metering systems.

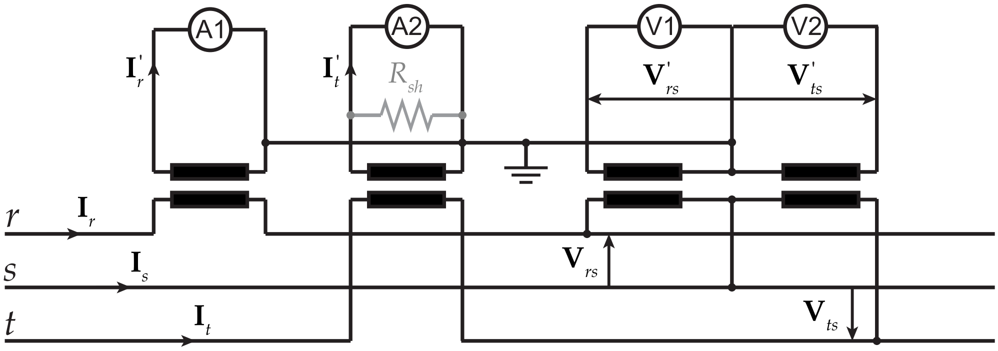


Fig. 4. Circuit representation of the three-phase power measuring system by means of current and voltage transformers, and of the system tampered through a shunt resistance R_{sh} (in gray).

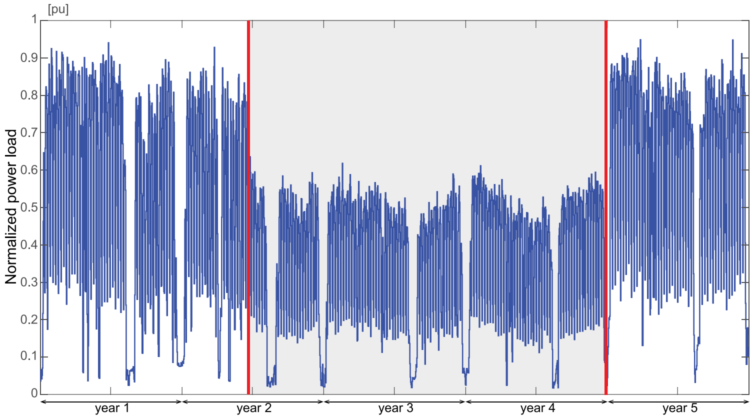


Fig. 5. Average daily power absorption of an industrial User normalized with respect to the contractual power over a five years interval. The period of anomalous absorption is enclosed in the red observation window.

reduce to $\tilde{P}_m$ and $\tilde{Q}_m$

$$\tilde{P}_m = k_v k_c V'_{rs} I'_r \cos\left(\varphi + \frac{\pi}{6}\right) = k_v k_c \frac{V'_{rs} I'_r}{2\sqrt{3}} \left[3\cos\varphi - \sqrt{3}\sin\varphi\right] \tag{3}$$

$$\tilde{Q}_m = k_v k_c V'_{rs} I'_r \sin\left(\varphi + \frac{\pi}{6}\right) = k_v k_c \frac{V'_{rs} I'_r}{2\sqrt{3}} \left[3\sin\varphi + \sqrt{3}\cos\varphi\right] . \tag{4}$$

An anomalous pattern due to tampering or unintentional anomalies in the metering system is to be spotted in Fig. 5, in which the power profile of an industrial load (normalized with respect to the User contractual power) is displayed over a five years interval.

Approximated expressions of a *restoring coefficient* C_a can be used to retrieve a first estimate of the actual power $P_a = C_a \tilde{P}_m$ absorbed by the User from the measured $\tilde{P}_m$ and $\tilde{Q}_m$. From (3), $\tilde{P}_m$ depends on the load balance and power factor $\cos\varphi$, and on the measured rms values of phase currents and line-to-line voltages. Under the aforementioned hypothesis of balanced three-phase circuit, i.e., $V_{rs} = V_{ts} = V$ and $I_r = I_t = I$, C_a is derived as follows:

$$C_a = \frac{P_a}{\tilde{P}_m} = \frac{\sqrt{3} V I \cos\varphi}{k_v k_c \frac{V' I'}{2\sqrt{3}} \left[3\cos\varphi - \sqrt{3}\sin\varphi\right]} = \frac{3}{2} + \frac{\sqrt{3}}{2} \frac{\left(3\sin\varphi + \sqrt{3}\cos\varphi\right)}{\left(3\cos\varphi - \sqrt{3}\sin\varphi\right)} = \frac{3}{2} + \frac{\sqrt{3}}{2}\frac{\tilde{Q}_m}{\tilde{P}_m} . \tag{5}$$

In Fig. 6, C_a is shown as a function of the power factor with the aforementioned simplificative hypotheses; for common power factors in the range $0.85 < \cos\varphi < 1$, $2 < C_a < 3$. It should be noted that the value $R_{sh} = 0$, assumed in the derivation of (5), penalizes the User

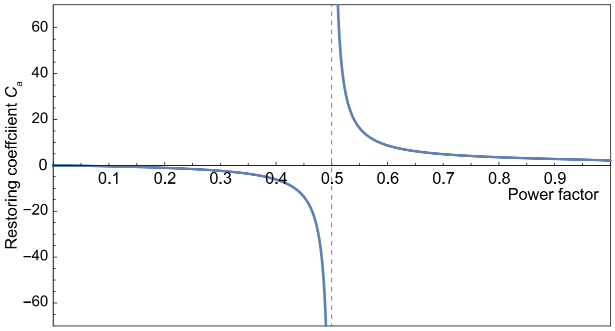


Fig. 6. Restoring coefficient C_a as a function of the power factor in a balanced three-phase circuit with $R_{sh} = 0$.

when the actual power consumption P_a is being estimated, nullifying the power contribution measured through meters A2–V2 (in Fig. 4) to $\tilde{P}_m$.

Energy meters usually perform a numerical integration of the product of the measured currents and voltages (after performing an analog-to-digital transform). The energy or the average power absorbed by the load during fixed intervals of 15 min is recorded as to calculate the load curve. Fig. 7 displays a second method to disguise the actual power absorption in favor of the User, i.e., equipping the electronic energy meter with an external board. Evidences of this scam were documented also in Brazil [71]. Operating on the current measuring system is the rationale. Among other circuit elements in Fig. 7, the board hosts a radio transceiver module, a microcontroller and two change-over relays. Unauthorized lead connections are derived from the terminals of the Mutual Current Transformers (MCTs) to the relays' pins.

The microcontroller is programmed to periodically switch the position of the relays' contacts, so to short-circuit the MCTs terminals for a time interval T_1, and keep their normal position for an interval T_2, resulting in a dimming control logic. The intervals T_1 and T_2 should be shorter than 15 min, so to always avoid measuring zero energy consumption in a 15 min interval: the power absorbed exceeds the measured one, still not generating any diagnostic alarm or an evidently suspicious absorption pattern.

The circuit board can be activated by a remote control, communicating with the radio transceiver within some meters from the tampered energy meter. When turned off, the external board does not alter the correct measurement of the actual absorbed power.

It is noteworthy that the tampering of an energy meter is not an easy task. Indeed, these electronic devices are always equipped with security seals, and may be programmed to report any opening of the external case after installation (through tamper violation sensors), along with other diagnostic information. Whenever an experienced and targeted intervention by the User in bypassing anti-tampering systems is not an option, collusion of the personnel working for the distributor should not be excluded.

3.2. Users connected to the LV network

LV Users often resort to tapping the energy from the distribution network through an illicit intervention on the power carrying circuit, avoiding any alteration of the measurement apparatus.

The first theft practice is to be identified with User-made connections to bypass the energy meter. Despite the legal stipulation of a supply contract between the User and the energy supplier, hence the existence of a point of connection and a dedicated energy meter, the measuring circuit is bypassed by illegal parallel connections, installed a posteriori. These connections are only rarely easy to detect by simple inspection: in Fig. 8(a), the bypass is realized through cables connected to the aerial network of the distributor in a rural area, resulting in zero current amplitude measured by the current clamps at the energy meter, but non-zero current flowing through the bypass connections (Fig. 8(b)); bypassing cables are easily observed in Fig. 9(b). However, cable connections are far more frequently buried underground, or placed in concealed locations (Figs. 9(c) and 9(d)).

A second theft practice consists in direct energy tapping from the distribution network. This stealing method may be distinguished from the one aforementioned by the absence of a point of connection, hence, of a metering system. Since the terminal block in Fig. 9(a) is not provided with an energy meter (due to the termination of the previous energy contract), this illegal connections may be classified as a case of energy tapping.

As to advanced techniques for the tampering with energy meters, Users provided with a three-phase connection to the LV network may steal energy by short-circuiting the lead connections used for a single-phase current measurement, as shown in Fig. 10(a). At least one current measuring circuit is left intact so not to record null power consumption. On this basis, an additional precautionary practice consists in replacing short circuit connections with low-resistance paths (Fig. 10(b)). In this way, the contribution of the hacked single-phase measuring circuits to the total measured power is reduced through a resistive divider (and never nullified).

Fig. 11 displays drilling through the external case of the energy meter, aimed at interrupting one of the current measuring circuits, permanently nullifying the corresponding contribution to the total measured power. This practice requires prior knowledge of the accurate position for drilling, the hole being of small dimension, carefully disguised by overlapped writing.

A non-invasive alteration of the measured energy consumption consists in exploiting external magnetic fields [72] to prevent the proper operation of MCTs. The interference is generated by means of permanent magnets producing high-intensity magnetic fields; additional ferromagnetic slabs, located between the permanent magnet and the meter case, may be exploited to customize the magnetic field distribution (as shown in Fig. 12).

The fast installation and removal of the magnet, in case of inspection by the distributor personnel, make the method captivating. Occasionally, evidences of drawn traces on the meter case may be found (e.g., the black square shape in Fig. 12), guiding the accurate placing of the magnet. Fig. 13 displays the power absorption of a User as recorded by the energy meter every 15 min over an interval of 6 years. The portion of the load profile enclosed by the observation window stands out for the reduced density of relevant measured values of power (in blue) and for an anomalous reduction in the User base load (the minimum absorbed power in back). Indeed, the User was discovered to place a magnet in order to infer the correct functioning of the energy meter.

Additional difficulties may raise in gathering evidences of anomalies in the recorded load curves, also depending on the combined effect of the periodicity of the available meter records with the unknown strategies adopted by the User for the magnet placing and removal. A second case of fraud with permanent magnet is related to the daily average power consumption over a 13 years time interval shown in Fig. 14. The displayed three curves refer to the average power absorbed during different Time-of-Use (ToU) tariff slots (ToU slots 2 and 3 referring to weekends, and evening and night consumption during weekdays). With reference to the period enclosed within the observation window, the User used to put the magnet in place mainly in correspondence of ToU slots 2 and 3 to decrease the measured power; this is confirmed by the trend of the power load during ToU slot 1 (blue curve), which does not change noticeably over the years.

Tests on a magnet-tampered energy meter were carried out in a calibration center in the configuration illustrated in Fig. 12, i.e., with the energy meter plugged to its standard removable terminal block, provided by the distributor. The error committed when measuring the

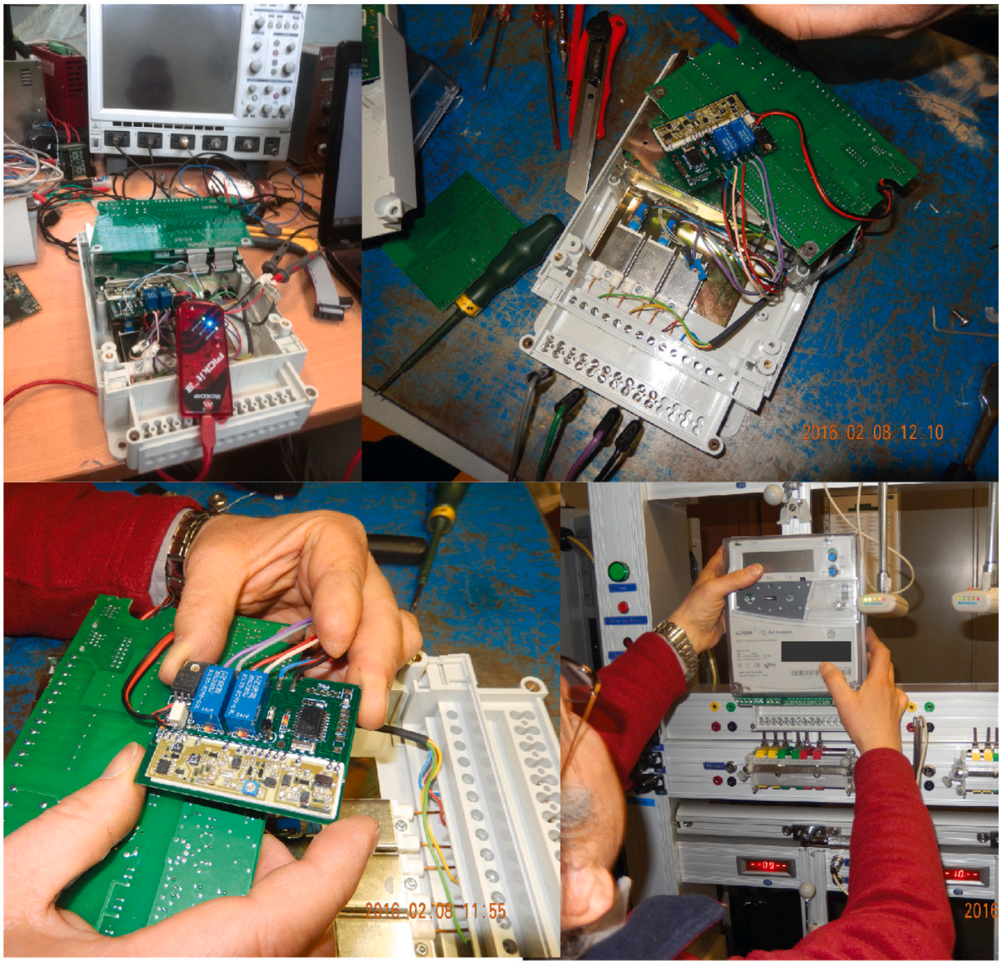
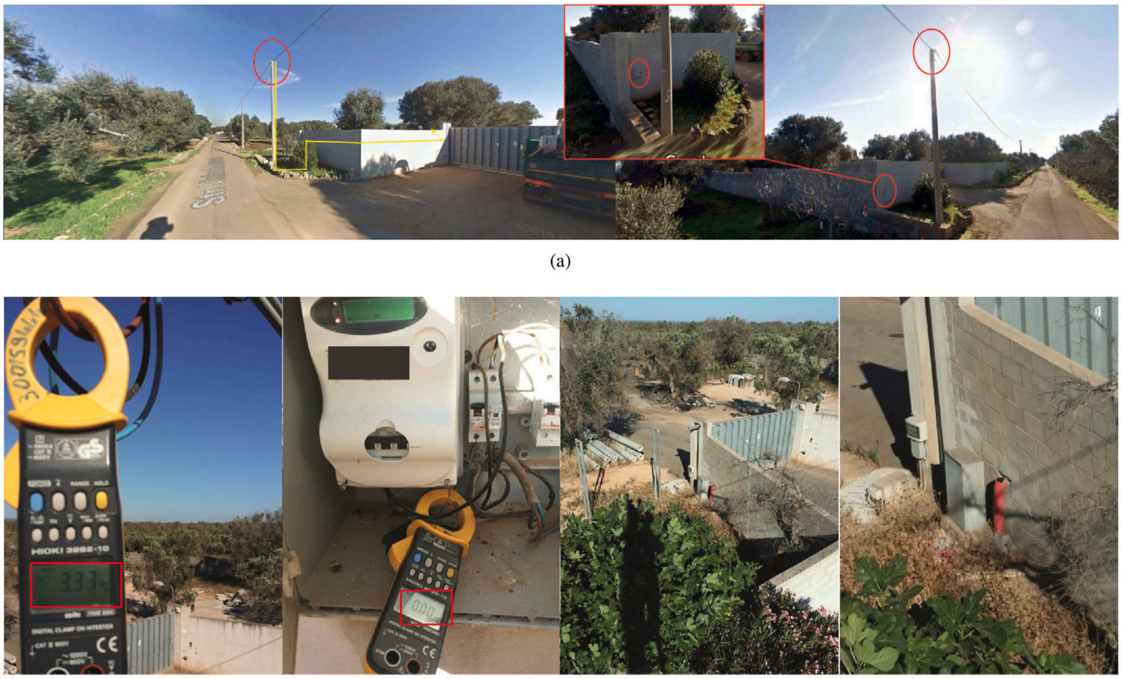


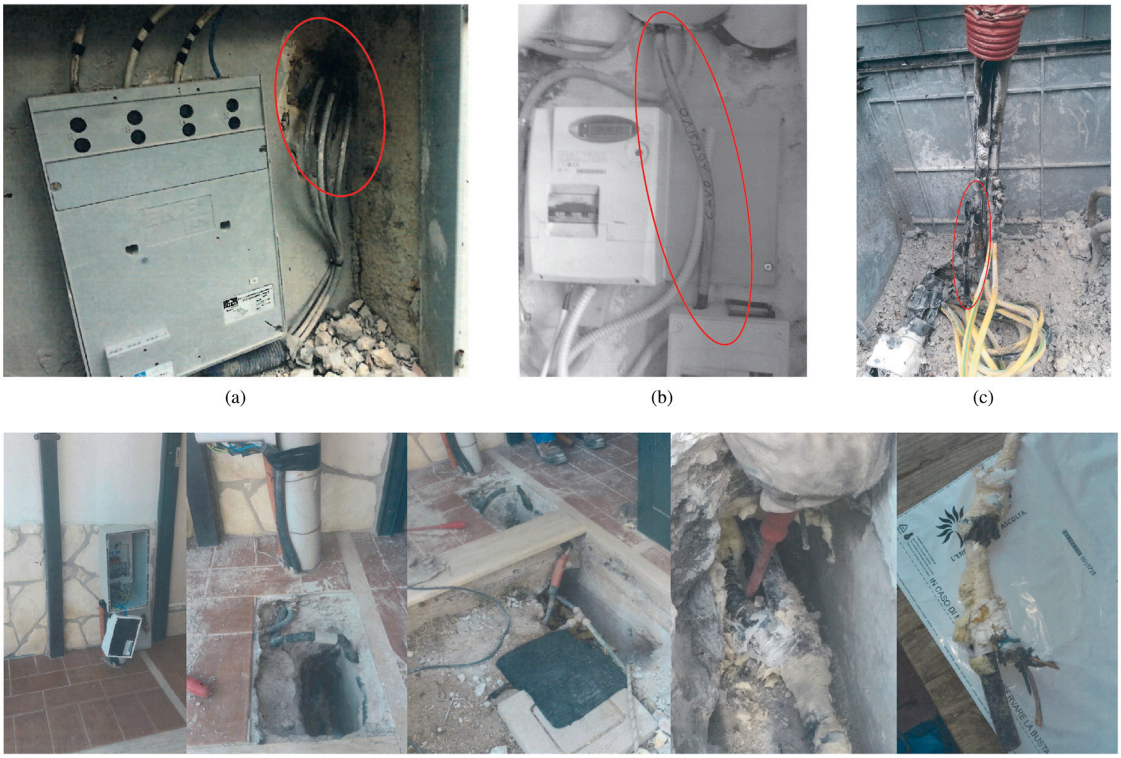
Fig. 7. Example of MV meter tampering with external board.



(a)

(b)

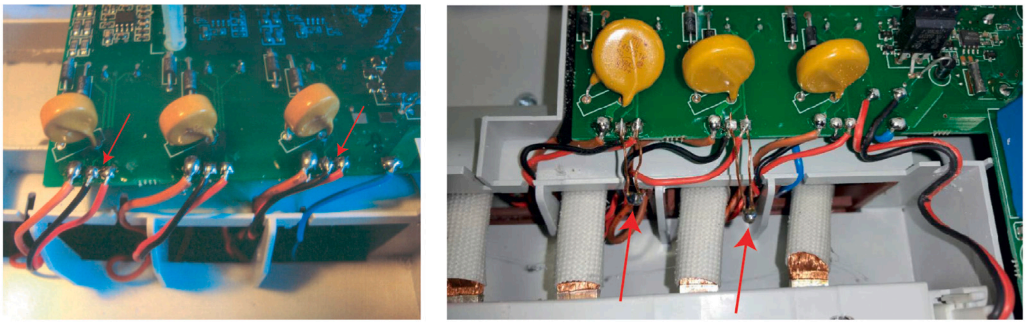
Fig. 8. Examples of LV bypassing in aerial rural electrification.



(a) (b) (c)

(d)

Fig. 9. Examples of LV tapping and non-authorized cables bypassing the electricity meters.



(a) (b)

Fig. 10. Examples of shunt of LV electricity meter.

three-phase energy dissipated by a fictitious load at 50 Hz with and without the permanent magnet is derived, considering different current amplitudes absorbed by a resistive–inductive load (with $\cos\varphi = 1$ and $\cos\varphi = 0.8$). The test results listed in Table 2 demonstrate an impressive impact of the magnet in sharply reducing the measured absorbed energy. It can be observed that the effectiveness of the tampering method decreases with the power factor, indicating a non-negligible effect of the load current phase in weakening the field inside the meter produced by the magnet.

Energy meters for LV applications may be also tampered through the same working principle described in Section 3.1, i.e. by means of an external dimming board equipped with a radio transceiver, a microcontroller, and two relays (Fig. 15).

After the fraud has been ascertained, the necessity of charging the User requires his/her load curve to be estimated during the period of illicit consumption. If a valid contract exists between the User and the energy supplier (as for cases of bypass connections, tampering with magnets, etc.), the energy consumption recorded by the energy meter in the past should be available. These data may be exploited to identify the duration of the fraud, as well as to estimate the actual load curve. Different approximate criteria can be applied, also depending on the amount of available data (e.g., averaging the energy absorbed in corresponding months during years of regular consumption).

Table 2
Energy measuring error for a three-phase LV energy meter with and without tampering by means of a permanent magnet.

	Test conditions			Energy measuring error	
	V	I	$\cos\varphi$	Without magnet	With magnet
	[V]	[A]	–	[%]	[%]
1	230	1.00	1.0	−0.131	−97.24
2	230	5.00	1.0	−0.139	−98.63
3	230	10.00	1.0	0.025	−98.14
4	230	15.00	1.0	0.031	−99.77
5	230	5.00	0.8	−0.121	−95.36
6	230	10.00	0.8	0.014	−95.46
7	230	15.00	0.8	0.032	−96.61

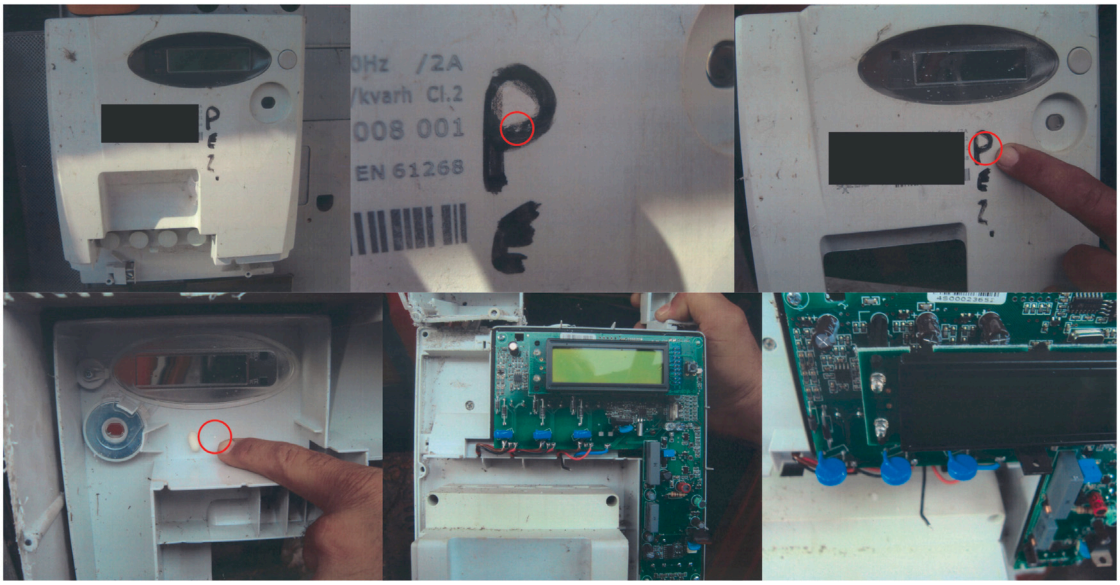
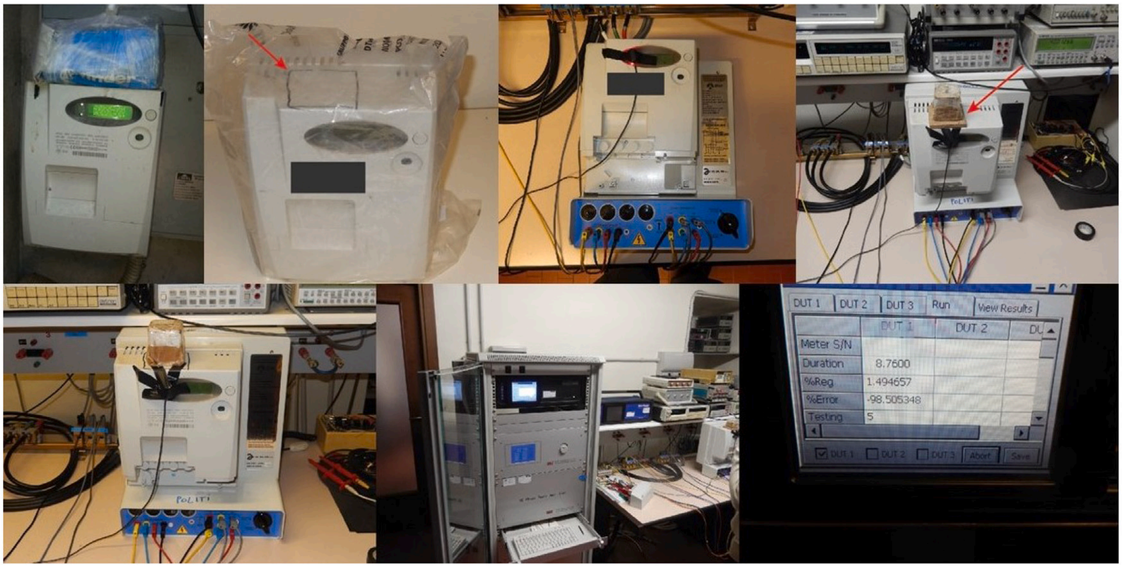


Fig. 11. Example of LV meter tampering through disguised small holes.


DUT 1 | DUT 2 | DUT 3 | Run | View Results

Meter S/N
Duration 8.7600
%Reg 1.494657
%Error -98.505348
Testing 5

Fig. 12. Example of tampering through permanent magnet with high-intensity field.

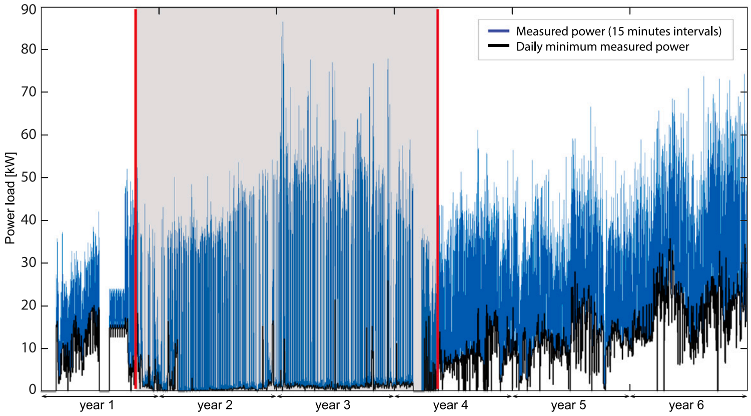


Fig. 13. Power absorption as recorded by the energy meter every 15 min over an interval of 6 years (blue line), and daily minimum power absorption (black line). The observation window identifies the period of fraud by meter tampering through a permanent magnet.

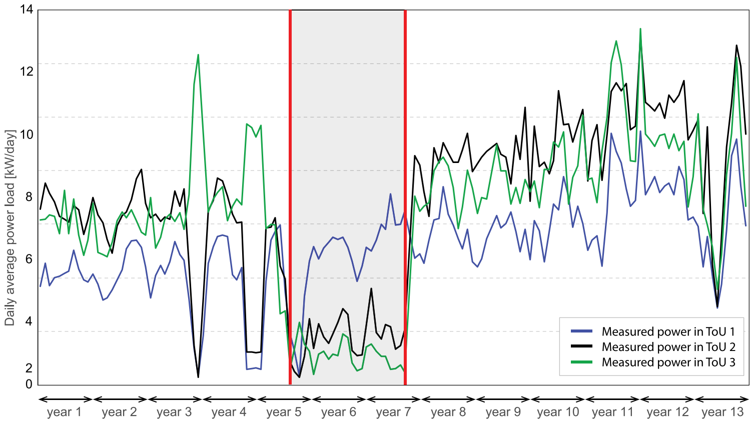


Fig. 14. Daily average power load absorbed with reference to the three Time-of-Use tariff slots over a 13 years interval. The observation window identifies the period of fraud, the energy meter being tampered with a permanent magnet.

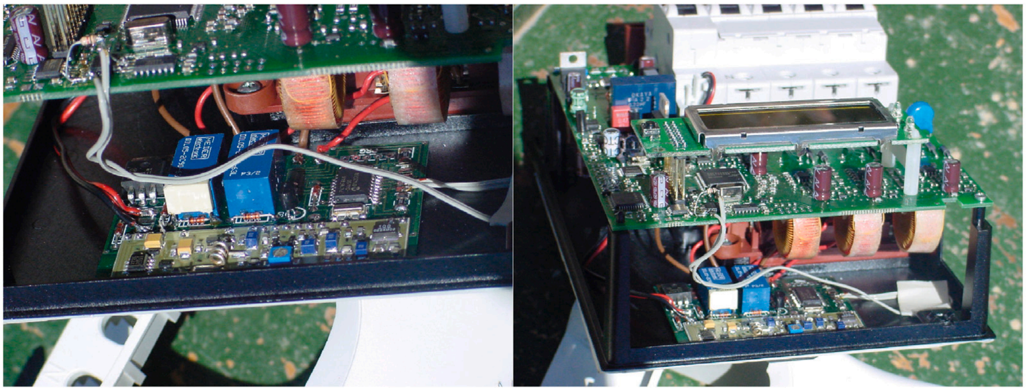


Fig. 15. Example of LV meter tampering with external board.

In the case of tampering with the energy meter, the actual energy consumption to charge to the User may be estimated as well through analytical expressions of restoring coefficients, as the one introduced in Section 3.1 for MV applications, to be derived thorough investigation of the unauthorized modifications made to the metering circuit and devices.

Instead, the criterion of maximum power carrying capacity of the line is applied when the User is not provided with a recognized point of connection to the network (as for cases of tapping). The criterion establishes annual equivalent hours of energy absorption based on the load type: ≈900 h and ≈1800 h for domestic and non-domestic LV loads, respectively, fed by the LV network. These equivalent hours are to be scaled to the confined interval of fraud duration, assuming the energy to be tapped at a constant power, equal to the maximum power carrying capacity of the line, with an average power factor (a common choice is $\cos\varphi \approx 0.8$). It is noteworthy that this approach is likely not to favor the deceitful User, not accounting for the possible variability and randomness of the connected load. Technical considerations and caution turn necessary when applying this reconstruction method.

4. AI goals and tasks for autonomous theft detection

AI is a fundamental tool in energy management systems; given its strong generalization capabilities, it is used for solving a plethora of problems in the energy supervision framework. Since one of the main advantages of AI is the flexibility of its learning-based scheme, it provides a strong solution for general protection problems, also considering its generalization and adaptation capabilities. As a matter of principle, we can identify five main goals by which a management system can fulfill its purpose: prediction, monitoring, detection & localization (diagnosis), classification, solving. Broadly speaking, all of them fall under the same general scope of the system, which is put in place to serve mainly a protection objective of the smart environment framework. The function of the energy supervision system is to operate as safety and diagnostic tool to ensure the smooth operation of the managed structure. The said purposes are all equally essential for handling anomalies (primarily faults) and, ideally, must be all exploited together, intertwining their functions, to reach the crucial ultimate goal of solving heterogeneous problems arising in the system.

We now give a denotation to these objectives:

1. Prediction: In this set of goals, this is the one which is shared the most with the others. Forecasting is ubiquitous in many ML frameworks and it serves the purpose of predicting future states of a complex system by looking at future values of a related time series. As a building block or even as elementary addition of information, forecasting is of paramount importance in every energy management system [73]. It gives the system its essence in resilience by exploiting the possibility of looking into the future state of the whole grid and serving the fault diagnosis in advance. This is important because smart automation can take place several steps before the actual fault in the chain of events, ensuring proper protection and sound failure management. Also, the predicted information can be employed to enhance the detection and localization monitoring process, by yielding up the overall knowledge regarding the evolution of the system. The learning of data-driven models is employed throughout the SG literature for prediction [74].

2. Monitoring: It serves the purpose of collecting data and analyzing the behavior of physical quantities. The relative infrastructure is composed mainly of smart sensors and SMs, connected and deployed in a so-called Wide Area Measurement System [75]. Monitoring is carried out substantially by a Meter Data Management System (MDMS) [66] and the correspondent Advanced Metering Infrastructure (AMI) [76]. AMIs have the role of linking the sensed data quantities to the other elements of the diagnosis and management system, by exploiting a two-way fast communication network between meters and DSOs. The goal is to facilitate the operation of distribution operator services by taking advantage of the SMs and sensors, coupled with intelligent data handling by the MDMS. In this framework, the function of AI is to shorten collection times [77] and intelligently share data and resources throughout the operators and energy agents [78].
3. Detection & localization: Diagnosis of faults in energy protection systems is classically implemented by a failure detection scheme. In practice, detection and localization have been the most used, implementing algorithms with different logics (which will be discussed later). The broad purpose is to give the smart system the possibility of automatically discovering a fault, potentially locating it in the physical plane/scheme [79]. Since diagnosis is inherently guided by data collected in the system, it is evident that to this end infrastructure of hardware (HW) and software (SW) elements must be solidly in place to handle the information on which the detection and localization are based. Those functions of the supervision can be considered as the "brain" of the smart system, since they perform the fundamental part of the automated fault management processing, translating and extracting fault information from raw data. It is also worth noting that, for a highly functional comprehensive system, the fast network infrastructure must be a two-way communication system, to ensure sharing fault detection with monitoring tools and enable feedback loops in the inference process. Several ML techniques can be employed for this purpose: from standard pattern recognition tools [57] to complex distributed unsupervised learning algorithms [80].
4. Classification: Similar to the detection and localization, the classification goal of the supervisory system is a mostly data-driven automating process in which information is extracted from data, to gain insights into the state of physical systems. Often, supervised learning models are used in practice, as classification itself is one of the strongest and renowned applications of AI models [81]. Regarding faults management, classification is important because it gives the ability, after detection, to automatically recognize the fault's nature and characteristics, enabling the suited response.
5. Solving: Ideally, all the above-listed goals are focused on diagnosing and learning faults, to empower the management system to solve the failures. Indeed, the solving necessitates a hard implementation of solutions, both in physical and algorithmic terms. In most instances, a good fault diagnosis is enough to develop a resilient smart system, because the acquired knowledge and prediction provide the backbone for taking discrete staple maintenance decisions. In advanced SGs [82], the solving can be automated too, but only at the expense of installing a much more complex smart infrastructure involving advanced AI, composed of actuators and automatic control mechanisms translating ML insights in the physical plane.

A general framework of methods and AI algorithms that can be adopted to achieve the potential goals of a management system is displayed in Fig. 16.

As said, at best, ML can be utilized to address all of these purposes, solving problems in a centralized or distributed way by employing several different techniques. Ordinarily, one could identify the role of AI algorithms as the cornerstone of modern fault protection systems, enabling fast and reliable fault management/handling/solving. More in detail, several ML algorithms have assessed performance for all the purposes just presented, herein we will point to selected comprehensive state of the artworks in the specific field: prediction [83], monitoring [84], detection [85], classification [81], solving [86].

A schematization of the process of AI for theft detection in SGs is reported in Fig. 17, where all of the general steps are given, highlighting the different roles of human and AI agents when provided with data and contextual information. Indeed, data is gathered via the AMI, as previously explained, coming from different sources and physical processes; the preprocessing stage is needed to homogenize and to make data usable for an autonomous model. Provided additional context information on additional environment variables such as meteorological phenomena and both information and distribution network, along with power quality, the AI model is generally able to give output information for an alert, provided the guide of an human expert, either in the training and/or inference phase. The final output and decision are governed by intrinsic logic and thresholds that are given a priori but could dynamically change based on the system and human intervention.

The goals and tasks just described refer to the ideal condition of having good data and soft computational power constraints to deploy the AI in the field. But, in recent times, a lot of attention has been devoted to try to solve the theft detection problem in SGs, with the goal to reach an autonomous recognition that could be employed as a general solution as resilient to SG implementation differences.

In fact, most, if not all, the approaches in literature fail to provide a framework that could be generalized for different situations where, as described in the next section, there are differences in the nature of the retrievable data (and its evolution), in the network and grid behavior, in the models and resources available. In this subsection we provide a comprehensive review of the most recent AI methods for theft detection in SGs, highlighting their properties and their application boundaries. Starting with other reviews in the field, in [87] a taxonomy is given, especially regarding Support Vector Machines (SVMs). Although it is not a comprehensive review, and the performance are evaluated on a synthetic dataset, it is clear that the reported methods can be used for detecting NTLs in general, but they lack generalization capability, especially when dealing with real-world data.

In [88] authors give a systematic overview of the theft detectable by ML focusing only on applications where the AMI is relevant, using SMs for data retrieval. For sure, this is a competent work but there are few cases analyzed without really clarifying the various options regarding ML algorithms' choices. A fair comparison of advantages and disadvantages of different solutions for autonomous theft detection (not only related to ML) is given in [89]. They come to the conclusion that the main culprit is represented by data and resource availability. While it is certainly true that it is quite challenging to train and implement deep neural network (NN) models for this kind of problem, we believe that with the help of distributed learning and newer algorithmic techniques, the generalization problem and resource bottleneck can be partially mitigated. Also, authors do not give the right importance to the practical side of the theft (see Section 3). Since we are dealing with practices adopted by single users, it is worth mentioning the work in [90] where an analysis of the motivations and behavioral aspects of the ET are studied.

Apart from general reviews, by restricting the analysis to deep NN techniques, as they can be considered the state-of-the-art in solving these kind of problems, it is evident that a combination of Recurrent Neural Networks (RNN) and Convolutional Neural Network (CNN) seems to be the most powerful solution. Indeed, this evidence is backed by several works in this domain. In particular, among the most recent ones, the work in [91] proposes an analysis of various CNN algorithms in comparison with Artificial Neural Networks (ANNs), SVMs and

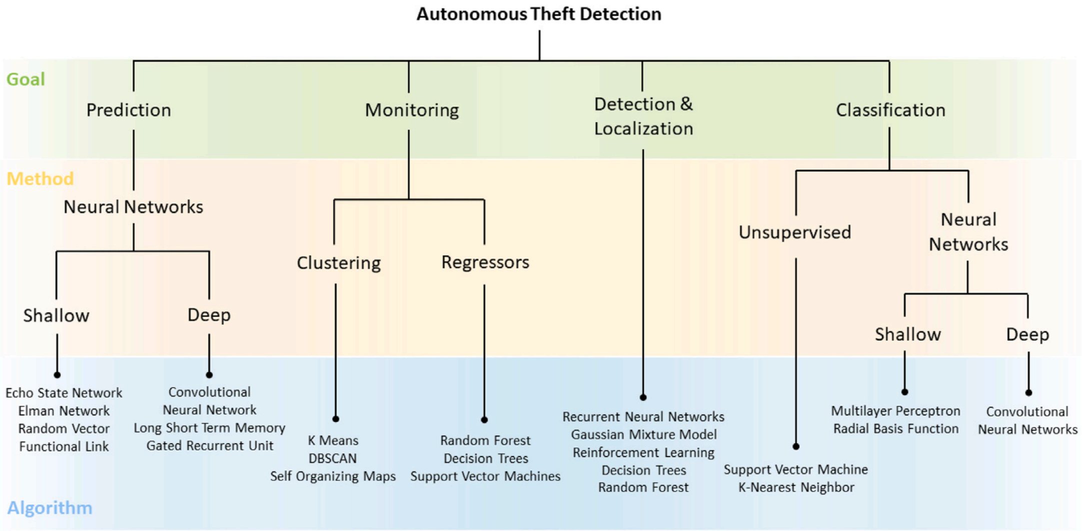


Fig. 16. General framework of methods and AI algorithms that can be adopted to achieve the potential goals of a management system.

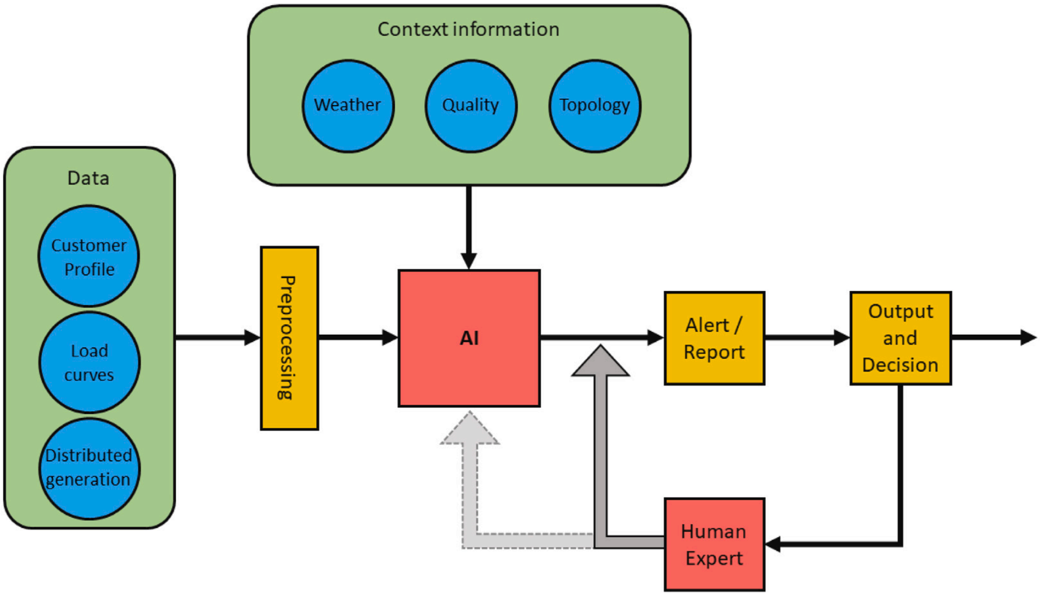


Fig. 17. General scheme for AI detection of theft in the energy sector.

Random Forest (RF). Although the work is sound by all means, the final goal of constructing the expert samples and training the model is scarcely applicable in scenarios where data is difficult to move or is very noisy. An efficient approach to design a neural network architecture for solving the theft detection problem is by combining CNN with other techniques; in particular RNNs seem to be the most appropriate choice to this aim. In fact, while CNNs are very good at extracting patterns from (matrix) data, due to their feed-forward information flow, they tend to be less accurate and more difficult to handle when using time-series data. For this reason, using recurrent gated models such as Long Short-Term Memory (LSTM) [92] or BiGRU [93] can be beneficial. Furthermore, the possibility of using such models in a distributed and/or federated way could enable faster retraining times, but it is still scarcely studied in real-world applications. The use of CNN in combination with other classifiers, such as SVM [94], is appropriate too, but it lacks depth and generalization capability when dealing with high dimensional time series data. Also, apart from the combination with CNNs, LSTM models can achieve good results in classification of theft with sequence data, when used alone or along other simpler classification approaches (such as SVM [95]). As a matter of recent example, using LSTM with an Autoencoder approach, as in [96], can allow the training of a very robust model for time series classification, which can in turn be prone to overfitting or sport high training times.

Since the optimization and search in the hyperparameter space of the architecture of an NN model is difficult and case dependent, some authors propose theft detection solutions employing genetic algorithms or other evolutionary computation techniques [88]. In particular, when dealing with multivariate data, delegating a genetic algorithm for feature selection can be beneficial [97], at the cost of high training times and difficult retraining. Other techniques for feature extraction are also studied in [98]. Apart from specific computational methods to enhance the performance, distributed learning is a class of approaches that could radically improve the deployment of theft detection solutions, based on the high parallelization and inherent privacy-preserving characteristics of such methods. In particular, authors in [99] propose techniques based on ensembling that are effective with big data, while in [100] the paradigm of federated learning over a set of agents is explored. As well put in [101], energy privacy preservation in the SG is of great importance, and autonomous ET detection cannot leave it aside. These are all popular research paths nowadays, especially in information theory and communications [102], but are still relatively underexplored for such vertical problems. Quantum machine learning is just happening to be studied, e.g. [103], but it exceeds the scope of this work since the feasibility of such algorithms is still debatable for large scale applications. It could be worth just mentioning that there are different (boosting, filtering) techniques explored among others in [104–106], but those too can be considered outside of the scope of this work, since they do not rely specifically on AI methods.

5. Key aspects and guidelines for a generalized AI solution

As already highlighted, there are many issues happening all at once which hinder the feasibility of an effective all-encompassing approach to the given problem. In particular, in practical applications, the heterogeneous nature of some elements poses a great challenge for a solution based on ML that tries to minimize the human intervention: the different users' profile (industrial, home, prosumer), the different grid connections (both physical and information-wise), and the different nature of the theft (shunting, smart meter tampering, etc.). Indeed, the human factor, while essential in this field (in particular regarding the counter-active measures and verification of the theft), is very costly; it is almost impossible to ensure a manual control of all the profiles of every user in the distribution grid to find anomalies and NTLs. For this reason, ML and AI in general are promising in this field of work, but, as said, the heterogeneity of the main features of the theft are quite a troubling matter. In the following, we will analyze the aforementioned troubling matters and devise the main aspects and core proprieties of a tentative solution based on the consumer profile, which is among the easiest data to gather for energy providers. Of course, given the abundance of data collected via the metering infrastructure, it is straightforward to imagine that data-driven models will continue to stay relevant in the grid diagnostic field. In fact, the most useful tools in terms of fault protection are supervised data-driven methods based on ML [107], as the fault properties are known before the operational phase and the models are highly flexible and adaptable to learn new failure characteristics anyway.

5.1. Data processing and related challenges

All ML and AI algorithms used for addressing (supervised or unsupervised) problems involving data processing are quite sensible to both the nature and the characteristics of the used data; we report here some actions that could enable a great deal of automation in the solution to the automatic theft detection problem.

As it is clear, the ET detection in modern SGs with ML can be either a supervised or unsupervised problem, depending on whether labeled data are available at training time. In fact, if the grid operator has access to past users' profiles in which thefts are certified by the authorities to be happened, a common practice that is in place since the beginning of these studies is to use those as the foundation of the training of a supervised ML method [108]; nevertheless, the characteristics of the data can be quite different in terms of dynamics and temporal evolution [109]. Furthermore, composing a training set with few examples of theft can result in extremely imbalanced classes, which is a notoriously difficult problem to handle [110].

Data augmentation is among the various techniques to strengthen the representational power of the gathered samples. Generally speaking, it can be done through synthetic generation [111] and resampling [112]. This has been applied specifically in the theft detection problem, in particular by [113] using variational auto-encoders (CVAEs), with mixed results. On the one hand the primary benefit of using this technique in generating stealing power curves is that it does not require assuming their probability distribution and only a small number of samples are necessary for training the model. However, CVAEs work well within the premises of a very definite use case of a single attack model, and they tend to perform less when detecting cases of ET of different nature, since it is a difficult task due to the proficient concealment tactics used by perpetrators as well as the limited resources available for conducting audits.

However, there are several limitations to consider, such as the possibility of negative transfer and bias in the feature extraction process. Moreover, transfer learning requires a substantial amount of labeled data in the source domain to be effective, which may be difficult to obtain in this context. Despite these challenges, transfer learning remains a promising tool for improving energy theft detection, especially when using predictive models [114] or when data needs to be adjusted with seasonal and trend information [115].

Similarly, ensembling methods have also emerged for ET detection, combining multiple models trained on different subsets of data, which can improve the overall accuracy of the model. There are of course some limitations, since ensembling requires significant computational resources, and it can be challenging to select the appropriate models and determine how to combine them, especially in a SG scenario. Moreover, ensembling can be sensitive to the quality and quantity of the data used to train the individual models, which is in turn much variable in the specific case.

Data preprocessing plays a crucial role in ensuring the quality and relevance of the data used for detection and achieving good detection performance. There are several key actions involved in data preprocessing (summarized in Fig. 18), each of which is essential, especially given the large set of cases analyzed in the previous sections.

5.2. Network infrastructure and grid heterogeneity

NTLs recognition is essential in the enhancement of smart energy system's performance and minimization of interruption in their service. As already stated, the detection, location, and clearance of faults are of paramount importance for any power system operation; the intelligent control required for these tasks is bounded with the physical framework of the system itself, as quickness and efficiency are most sought-after. While the theoretical approach of ML solutions could be considered independent concerning the context of the problem (since data-driven learning can always try to exploit a model), in the analysis of the faults occurring in energy systems it is still important to categorize the layer at which the fault itself arises. This is due to the different requirements of each system application necessitating specifically tailored responses, driven by different appropriate ML algorithms. That is to say that, depending on the system level of application in which the failure occurs, different resilience methods are needed, with different AI algorithms for diagnosing. SGs, and smart energy systems in general, are designed to handle different systems and applications, with integrating services with diverse purposes, i.e. different system-level of application: transmission, distribution, commercial/residential, DG, EV, all coexisting in the same framework. Regardless of the management system in place, in all of these scenarios, there are three layers in which a fault can occur:

- Physical devices/components (cables [116], PV [117], turbines [118], transformers [119], converters [120], sensors [121]);
- Communication (timing [122], backbone [123], wireless [124], interference [125], privacy [126]);
- SW/HW (data storage units [127], information systems [128]).

It has to be noted that in some applications, the importance of analyzing one of these layers can be more critical than the others. For instance, in a small industrial grid, the whole system is designed around the functioning of physical devices, thus necessitating a more thoughtful fault localization in the relative layer; conversely, the communication and SW/HW control resources are usually designed to be stable and/or self-resilient to failure (holding a lower impact on the overall structure).

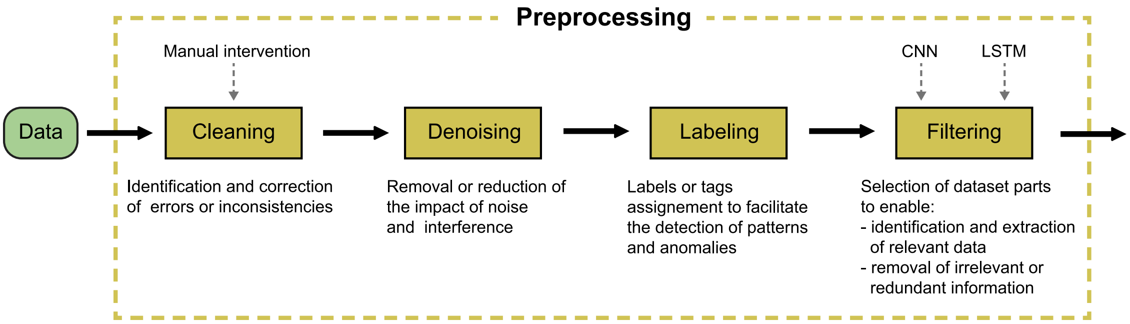

Preprocessing
Manual intervention
CNN
LSTM
Data
Cleaning
Denoising
Labeling
Filtering
Identification and correction of errors or inconsistencies
Removal or reduction of the impact of noise and interference
Labels or tags assignement to facilitate the detection of patterns and anomalies
Selection of dataset parts to enable:
- identification and extraction of relevant data
- removal of irrelevant or redundant information

Fig. 18. Fundamental steps for data preprocessing.

The complexity of the grid and its intrinsic dynamicity as a system, with multiple agents and communication protocols can make it challenging to gather and transmit data, as well as to model the interactions between different agents in the network. The complexity of the grid can also make it difficult to interpret the results produced by an AI model. There are three main reasons for the whole interaction between system complexity and data that can be synthesized in: (i) Measurements, (ii) Data Gathering, (iii) Information presence. To develop an effective ET detection system, it is essential to understand and account for the physical structure of the grid and the network of interconnected agents.

In this context, it is also to highlight the advent of reliable machine-to-machine communication [129], and most relevantly 5G communication, that will enhance the performance of the communication infrastructure in a smart system [130]; it will be both more reliable and cheaper to exchange high volume of data in a network with high frequency. This would make approaching real-time analysis a common practice, with great protection benefits [131].

5.3. Neural network optimization and training

It has been shown that neural models can be considered powerful tools for this applications. However, building effective neural models can be a challenging task, as it involves selecting the right architecture, defining the right set of hyperparameters, optimizing the model's weights, while avoiding overfitting at the same time.

One of the challenges in developing effective detection methods is dealing with the complexity of the data, which includes multiple classes of consumption patterns and NTLs across different feeders. As a primary analysis to extract features and to ensure information compression, CNNs can be used, as they are well-suited for image-based data, but they can also be applied to time-series data, such as electricity consumption data. They are able to extract features from the data at different scales and levels of abstraction, which makes them effective in identifying subtle patterns in the data that are indicative of ET. Also, LSTM networks are able to process sequences of data with long-term dependencies, such as the patterns of electricity consumption over time. This makes them suitable for detecting theft that occurs over an extended period, rather than in a single anomalous event. Often, there are also multiclass classification problems hidden in the theft detection one, since different malicious users could resort to different theft practices, giving rise to diverse behaviors.

Overall, machine learning and AI have the potential to significantly improve the accuracy and efficiency of ET detection, but there are still challenges to be addressed. These include the need for large amounts of labeled data to train the models, the difficulty of optimizing and tuning complex NNs, and the potential for biased or unfair results if the training data are not representative of the entire population. Despite these challenges, the use of machine learning and AI is likely to become increasingly important in ET detection as the volume and complexity of the data continue to grow. In addition, the sheer amount of data required for training can be a challenge, as it may not be feasible to collect enough data to cover all possible scenarios. Transfer learning can help address this challenge by using pre-trained models on similar tasks to fine-tune the model on the target task. Despite these challenges, neural models have shown promising results in theft detection, and they are becoming increasingly important in the field of AI. With the widespread deployment of SMs and the increasing availability of data, AI-based theft detection is poised to become a key component of SG systems in the future.

5.4. Guidelines for theft detection methods

It is worth to summarize and identify four stages in which the theft detection process is divided: detection of NTLs at the distribution system feeder level, detection of abnormal electricity consumption behavior at the individual level, on-site inspection, and evidence collection.

- *Detection of NTLs at the distribution level*: Power grid analysis-based methods are effective for detecting NTLs, estimating them through power balance calculations or distribution network state estimation to identify feeders with high NTLs that may indicate illegal usage;
- *Detection of abnormal electricity consumption at the individual level*: ML-based methods are effective to analyze load profiles, current profiles, active power, and other parameters to identify illegal users who are suspected of stealing electricity;
- *On-site inspection*: On-site inspection by technicians is a costly operation, necessary to confirm the presence and the extent of the theft;
- *Evidence collection*: Hardware-based methods are used to monitor the parameters of incoming and outgoing feeders, as well as the use of anti-device ET devices to narrow down the searching area.

The amount of data required for training ET detection models and how frequently retraining should occur are areas of active research, although SMs have enabled the widespread availability of training data. Successful theft detection using SMs can range from multiple days to years, with a longer observed period yielding higher accuracy.

Overall, while detecting ET requires a multi-stage approach that involves a combination of data analysis, hardware-based methods, and on-site inspections, we are advocating for a smarter, two-stages approach to successfully identify and prosecute illegal users. In fact, after the data collection (which is intrinsically hardware-based, given the particular AMI), the NTLs detection at each level (individual, distribution and grid) can be automated in a single stage, flagging the malicious behaviors, with the human intervention reduced to the bare minimum of validating the flagged cases. This AI-based approach (HW data gathering, AI detection, analysis and flagging, and human validation) has sustainable benefits and permits cost-shrinking for AI retraining and human inspection.

6. Final remarks on actual fraud detection methods used by DSOs

In recent years, attempts have been made by the Italian DSOs towards adopting third-party software based on AI algorithms for ET detection. However, due to the high number of false-positive fraud cases detected, resulting in time consuming and costly procedures to verify actual frauds, the use of AI based software has not solidly established yet.

Some heuristic yet effective methods are mostly adopted in the current practice. The first ones are periodical inspections of the users energy absorption by the specialized personnel of the DSO; thanks to his solid presence on the territory, not only spot-checks are performed, but also anomalous users behaviors may be detected (mainly as small industries and commercial activities are concerned).

As a second method, thorough controls are performed on selected absorption profiles as a result of unexpected fault events, not compatible with the expected operating conditions of sections of the network and/or protection equipment; for instance, anomalous breakers switching or cable joints faults may alert the DSO on unforeseen energy over-absorptions.

The last method consists in comparing the sum of energy recordings associated with users connected to the MV network and with MV/LV transformers (feeding LV users), with the total energy measured at the HV side of the corresponding primary substation (i.e., the node of the network where the conversion from high to medium voltage is operated through dedicated HV/MV transformers). If excessive NTLs are detected, additional investigations are conducted by the DSO, as the surplus may be justified by possible fraudulent activities.

7. Conclusion

One of the most difficult problems to be solved for distribution operators is detection of electricity thefts operated by the final users. In particular, while SMs are employed for automatic monitoring and analysis of the energy consumption, automatic detection of actual thefts is a challenging task, yet too demanding to be faced by the sole human intervention. This is because such thefts are put in place via numerous techniques of physical tampering of equipment at the user side, resulting in just as many load profiles.

In this article we provided a comprehensive survey of the state of the art AI techniques to detect energy thefts of various nature. We showed the main characteristics of the malicious users behaviors, referring to theft practices by users connected to the LV and MV networks; to the best of our knowledge, there is no recent work that provides such analysis on modern technologies at the service of smart infrastructures.

On top of that, the present work reviews a plethora of ML solutions, focusing on their strength and weaknesses, with the purpose of providing the key aspects of a generalized AI solution for the energy theft detection problem.

This work paves the way to a more comprehensive system that can be further developed by analyzing comprehensive and generalized data, with possibly a real-time deployment. By describing the main goals and tasks for autonomous theft detection, and drawing guidelines to overcome the main implementation difficulties (data processing, network and grid infrastructure, and NN optimization), this study delivers a complete framework for AI energy theft detection, emphasizing the importance of collaboration between utility companies, regulators, and AI experts to address the challenges associated with the reduction of non-technical losses and sustainability of energy grids.

CRediT authorship contribution statement

Erika Stracqualursi: Methodology, Software. **Antonello Rosato:** Methodology. **Gianfranco Di Lorenzo:** Methodology, Software. **Massimo Panella:** Methodology. **Rodolfo Araneo:** Conceptualization, Methodology, Software.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The authors have chosen not to specify which data has been used.

References

[1] Dennis K. Environmentally beneficial electrification: Electricity as the end-use option. Electr J 2015;28(9):100–12.

[2] Belaïd F, Zrelli MH. Renewable and non-renewable electricity consumption, environmental degradation and economic development: Evidence from Mediterranean countries. Energy Policy 2019;133:110929.

[3] Aalto P. Electrification: Accelerating the energy transition. London: Academic Press; 2021.

[4] Smith TB. Electricity theft: a comparative analysis. Energy Policy 2004;32(18):2067–76.

[5] Yurtseven C. The causes of electricity theft: An econometric analysis of the case of Turkey. Util Policy 2015;37:70–8.

[6] Gaur V, Gupta E. The determinants of electricity theft: An empirical analysis of Indian states. Energy Policy 2016;93:127–36.

[7] Babar Z, Jamil F, Haq W. Consumer's perception towards electricity theft: A case study of Islamabad and Rawalpindi using a path analysis. Energy Policy 2022;169:113189.

[8] Kumar V. S, Prasad J, Samikannu R. Overview, issues and prevention of energy theft in smart grids and virtual power plants in Indian context. Energy Policy 2017;110:365–74.

[9] Jamil F, Ahmad E. Policy considerations for limiting electricity theft in the developing countries. Energy Policy 2019;129:452–8.

[10] AlShiab MSI, Al-Malkawi H-AN, Lahrech A. Revisiting the relationship between governance quality and economic growth. Int J Econ Financ Issues 2020-07;10(4):54–63.

[11] Razavi R, Fleury M. Socio-economic predictors of electricity theft in developing countries: An Indian case study. Energy Sustain Dev 2019;49:1–10.

[12] Messinis GM, Hatziargyriou ND. Review of non-technical loss detection methods. Electr Power Syst Res 2018;158:250–66.

[13] Depuru SSSR, Wang L, Devabhaktuni V. Electricity theft: Overview, issues, prevention and a smart meter based approach to control theft. Energy Policy 2011;39(2):1007–15.

[14] Czechowski R, Kosek AM. The most frequent energy theft techniques and hazards in present power energy consumption. In: 2016 joint workshop on cyber- physical security and resilience in smart grids (CPSR-SG). 2016, p. 1–7.

[15] Lewis FB. Costly "Throw-Ups": Electricity theft and power disruptions. Electr J 2015;28(7):118–35.

[16] Daví-Arderius D, Sanin M, Trujillo-Baute E. CO2 content of electricity losses. Energy Policy 2017;104:439–45.

[17] Czechowski R, Kosek AM. The most frequent energy theft techniques and hazards in present power energy consumption. In: 2016 joint workshop on cyber- physical security and resilience in smart grids (CPSR-SG). 2016, p. 1–7.

[18] Pai P-F, Li S, Han Y, Yao X, Yingchen S, Wang J, Zhao Q. Electricity theft detection in power grids with deep learning and random forests. J Electr Comput Eng 2019;2019:4136874.

[19] Depuru SSSR, Wang L, Devabhaktuni V. Electricity theft: Overview, issues, prevention and a smart meter based approach to control theft. Energy Policy 2011;39(2):1007–15.

[20] Ahmad T. Non-technical loss analysis and prevention using smart meters. Renew Sustain Energy Rev 2017;72:573–89.

[21] Capper T, Gorbatcheva A, Mustafa MA, Bahloul M, Schwidtal JM, Chitchyan R, Andoni M, Robu V, Montakhabi M, Scott IJ, Francis C, Mbavarira T, Espana JM, Kiesling L. Peer-to-peer, community self-consumption, and transactive energy: A systematic literature review of local energy market models. Renew Sustain Energy Rev 2022;162:112403.

[22] Sharma K, Mohan Saini L. Performance analysis of smart metering for smart grid: An overview. Renew Sustain Energy Rev 2015;49:720–35.

[23] Yip S-C, Tan W-N, Tan C, Gan M-T, Wong K. An anomaly detection framework for identifying energy theft and defective meters in smart grids. Int J Electr Power Energy Syst 2018;101:189–203.

[24] Park CH, Kim T. Energy theft detection in advanced metering infrastructure based on anomaly pattern detection. Energies 2020;13(15).

[25] de Souza MA, Pereira JL, de O. Alves G, de Oliveira BC, Melo ID, Garcia PA. Detection and identification of energy theft in advanced metering infrastructures. Electr Power Syst Res 2020;182:106258.

[26] Kim JY, Hwang YM, Sun YG, Sim I, Kim DI, Wang X. Detection for non-technical loss by smart energy theft with intermediate monitor meter in smart grid. IEEE Access 2019;7:129043–53.

[27] Wen L, Zhou K, Yang S, Li L. Compression of smart meter big data: A survey. Renew Sustain Energy Rev 2018;91:59–69.

[28] Viegas JL, Esteves PR, Melício R, Mendes V, Vieira SM. Solutions for detection of non-technical losses in the electricity grid: A review. Renew Sustain Energy Rev 2017;80:1256–68.

[29] Carvalho TP, Soares FAAMN, Vita R, da P. Francisco R, Basto JP, Alcalá SGS. A systematic literature review of machine learning methods applied to predictive maintenance. Comput Ind Eng 2019;137:106024.

[30] Hua Y, Zhao Z, Li R, Chen X, Liu Z, Zhang H. Deep learning with long short-term memory for time series prediction. IEEE Commun Mag 2019;57(6):114–9.

[31] Rizzi A, Buccino NM, Panella M, Uncini A. Genre classification of compressed audio data. In: 2008 IEEE 10th workshop on multimedia signal processing. 2008, p. 654–9.

[32] Lim B, Zohren S. Time-series forecasting with deep learning: a survey. Phil Trans R Soc A 2021;379(2194):20200209.

[33] Mellouli N, Akerma M, Hoang M, Leducq D, Delahaye A. Multivariate time series forecasting with deep learning proceedings in energy consumption. In: KDIR. 2019, p. 384–91.

[34] Succetti F, Rosato A, Araneo R, Panella M. Deep neural networks for multivariate prediction of photovoltaic power time series. IEEE Access 2020;8:211490–505.

[35] Chakraborty S, Das S. Application of smart meters in high impedance fault detection on distribution systems. IEEE Trans Smart Grid 2019;10:3465–73.

[36] Pasdar AM, Sozer Y, Husain I. Detecting and locating faulty nodes in smart grids based on high frequency signal injection. IEEE Trans Smart Grid 2013;4:1067–75.

[37] Devi MM, Geethanjali M, Devi AR. Fault localization for transmission lines with optimal Phasor Measurement Units. Comput Electr Eng 2018;70:163–78.

[38] Zhang F, Mu L. A fault detection method of microgrids with grid-connected inverter interfaced distributed generators based on the PQ control strategy. IEEE Trans Smart Grid 2018;PP:1.

[39] Milioudis AN, Andreou GT, Labridis DP. Detection and location of high impedance faults in multiconductor overhead distribution lines using power line communication devices. IEEE Trans Smart Grid 2015;6:894–902.

[40] Saleh KA, Hooshyar A, El-Saadany EF. Hybrid passive-overcurrent relay for detection of faults in low-voltage DC grids. IEEE Trans Smart Grid 2017;8:1129–38.

[41] Wang B, Geng J, Dong X. High-impedance fault detection based on nonlinear voltage-current characteristic profile identification. IEEE Trans Smart Grid 2018;9:3783–91.

[42] Affijulla S, Tripathy P. A robust fault detection and discrimination technique for transmission lines. IEEE Trans Smart Grid 2018;9(6):6348–58.

[43] Seyedi Y, Karimi H, Guerrero JM. Centralized disturbance detection in smart microgrids with noisy and intermittent synchrophasor data. IEEE Trans Smart Grid 2017;8:2775–83.

[44] Yen SW, Morris S, Ezra MA, Huat TJ. Effect of smart meter data collection frequency in an early detection of shorter-duration voltage anomalies in smart grids. Int J Electr Power Energy Syst 2019;109:1–8.

[45] Gopakumar P, Mallikajuna B, Reddy MJB, Mohanta DK. Remote monitoring system for real time detection and classification of transmission line faults in a power grid using PMU measurements. Prot Control Mod Power Syst 2018;3:1–10.

[46] Qi P, Jovanovic S, Lezama J, Schweitzer P. Discrete wavelet transform optimal parameters estimation for arc fault detection in low-voltage residential power networks. Electr Power Syst Res 2017;143:130–9.

[47] Wang S, Dehghanian P. On the use of artificial intelligence for high impedance fault detection and electrical safety. IEEE Trans Ind Appl 2020;56(6):7208–16.

[48] Haes Alhelou H, Golshan M, Hatziargyriou ND, Moghaddam MP. A novel unknown input observer-based measurement fault detection and isolation scheme for micro-grid systems. IEEE Trans Ind Inf 2020;1.

[49] Dey M, Rana SP, Dudley S. Smart building creation in large scale HVAC environments through automated fault detection and diagnosis. Future Gener Comput Syst 2020;108:950–66.

[50] Cepeda C, Orozco-Henao C, Percybrooks W, Pulgarín-Rivera JD, Montoya OD, Gil-González W, Vélez JC. Intelligent fault detection system for microgrids. Energies 2020;13.

[51] Yu JJ, Hou Y, Lam AY, Li VO. Intelligent fault detection scheme for microgrids with wavelet-based deep neural networks. IEEE Trans Smart Grid 2019;10:1694–703.

[52] Eslami R, Sadeghi SHH, Askarian-Abyaneh H, Nasiri A. A novel method for fault detection in future renewable electric energy delivery and management microgrids, considering uncertainties in network topology. Electr Power Compon Syst 2017;45(10):1118–29.

[53] Nahas EW, Mansour DEA, El-Ghany HAA, Eissa MM. Accurate fault analysis and proposed protection scheme for battery energy storage system integrated with DC microgrids. In: 2018 20th international middle east power systems conference, MEPCON 2018 - Proceedings. IEEE; 2019, p. 911–7.

[54] Kordestani M, Saif M. Data fusion for fault diagnosis in smart grid power systems. In: Canadian conference on electrical and computer engineering. IEEE; 2017, p. 1–6.

[55] Lazarova-Molnar S, Mohamed N. A framework for collaborative cloud-based fault detection and diagnosis in smart buildings. In: 2017 7th international conference on modeling, simulation, and applied optimization (ICMSAO). 2017, p. 1–6.

[56] Pires VF, Foito D, Amaral TG. Fault detection and diagnosis in a PV grid-connected T-type three level inverter. In: 2015 international conference on renewable energy research and applications, ICRERA 2015, Vol. 5. 2015, p. 933–7.

[57] Jiang H, Zhang JJ, Gao W, Wu Z. Fault detection, identification, and location in smart grid based on data-driven computational methods. IEEE Trans Smart Grid 2014;5(6):2947–56.

[58] Li D, Aung Z, Williams JR, Sanchez A. Efficient authentication scheme for data aggregation in smart grid with fault tolerance and fault diagnosis. In: 2012 IEEE PES innovative smart grid technologies, ISGT 2012. IEEE; 2012, p. 1–8.

[59] Lima BM, Morato MM, Mendes PRC, Normey-Rico JE. Moving horizon estimation of faults in renewable microgrids. IFAC-PapersOnLine 2019;52(1):311–6, 12th IFAC Symposium on Dynamics and Control of Process Systems, including Biosystems DYCOPS 2019; URL https://www.sciencedirect.com/science/article/pii/S240589631930165X.

[60] De Santis E, Rizzi A, Sadeghian A. A cluster-based dissimilarity learning approach for localized fault classification in Smart Grids. Swarm Evol Comput 2018;39:267–78, URL https://www.sciencedirect.com/science/article/pii/S2210650217300238.

[61] Khan I, Capozzoli A, Corgnati SP, Cerquitelli T. Fault detection analysis of building energy consumption using data mining techniques. Energy Procedia 2013;42:557–66.

[62] Prodan I, Zio E, Stoican F. Fault tolerant predictive control design for reliable microgrid energy management under uncertainties. Energy 2015;91:20–34.

[63] Sun M, Zhang J. Data-driven anomaly detection in modern power systems. In: Karimipour H, Srikantha P, Farag H, Wei-Kocsis J, editors. Security of cyber-physical systems. Cham: Springer; 2020, p. 131–43.

[64] Bhat RR, Trevizan RD, Sengupta R, Li X, Bretas A. Identifying nontechnical power loss via spatial and temporal deep learning. In: 2016 15th IEEE international conference on machine learning and applications (ICMLA). IEEE; 2016, p. 272–9.

[65] Khan RH, Khan JY. A comprehensive review of the application characteristics and traffic requirements of a smart grid communications network. Comput Netw 2013;57(3):825–45, URL https://www.sciencedirect.com/science/article/pii/S1389128612003751.

[66] Wang Y, Chen Q, Hong T, Kang C. Review of smart meter data analytics: Applications, methodologies, and challenges. IEEE Trans Smart Grid 2019;10:3125–48.

[67] He X, Ai Q, Qiu RC, Huang W, Piao L, Liu H. A big data architecture design for smart grids based on random matrix theory. IEEE Trans Smart Grid 2017;8(2):674–86.

[68] Barja-Martinez S, Aragüés-Peãlba M, Munné-Collado Í, Lloret-Gallego P, Bullich-Massagué E, Villafafila-Robles R. Artificial intelligence techniques for enabling Big Data services in distribution networks: A review. Renew Sustain Energy Rev 2021;150:111459.

[69] Herold R, Hertzog C. Data privacy for the smart grid. 2015.

[70] Boroojeni KG, Amini MH, Iyengar SS. Smart grids: Security and privacy issues. Springer International Publishing; 2016, p. 1–113.

[71] De Faria RA, Fonseca KVO, Schneider B, Nguang SK. Collusion and fraud detection on electronic energy meters-a use case of forensics investigation procedures. In: 2014 IEEE security and privacy workshops. IEEE; 2014, p. 65–8.

[72] Chandel P, Thakur T, Sawle B, Sharma R. Power theft: Major cause of non technical losses in Indian distribution sector. In: 2016 IEEE 7th power India international conference (PIICON). IEEE; 2016, p. 1–6.

[73] Rosato A, Panella M, Araneo R, Andreotti A. A neural network-based prediction system of distributed generation for the management of microgrids. IEEE Trans Ind Appl 2019;55(6):7092–102.

[74] Almalaq A, Zhang JJ. Deep learning application: Load forecasting in big data of smart grids. In: Studies in computational intelligence, vol. 865, Springer Verlag; 2020, p. 103–28.

[75] Volskis BH, Moraes RMD. WAMS initiatives in Brazil. IEEE Power Energy Mag 2008;52–65.

[76] Rashed Mohassel R, Fung A, Mohammadi F, Raahemifar K. A survey on advanced metering infrastructure. Int J Electr Power Energy Syst 2014;63:473–84.

[77] Lloret J, Tomás J, Canovas A, Parra L. An integrated IoT architecture for smart metering. IEEE Commun Mag 2016;54:50–7.

[78] Munshi AA, Mohamed YA. Big data framework for analytics in smart grids. Electr Power Syst Res 2017;151:369–80.

[79] Kezunovic M. Smart fault location for smart grids. IEEE Trans Smart Grid 2011;2(1):11–22.

[80] Bezerra CG, Costa BSJ, Guedes LA, Angelov PP. An evolving approach to unsupervised and Real-Time fault detection in industrial processes. Expert Syst Appl 2016;63:134–44, URL https://www.sciencedirect.com/science/article/pii/S0957417416303153.

[81] Hlalele T, Sun Y, Wang Z. Faults classification and identification on smart grid: Part-A status review. Procedia Manuf 2019;35:601–6, The 2nd International Conference on Sustainable Materials Processing and Manufacturing, SMPM 2019, 8-10 March 2019, Sun City, South Africa; URL https://www.sciencedirect.com/science/article/pii/S235197891930722X.

[82] Babar M, Tariq MU, Jan MA. Secure and resilient demand side management engine using machine learning for IoT-enabled smart grid. Sustainable Cities Soc 2020;62:102370, URL https://www.sciencedirect.com/science/article/pii/S2210670720305904.

[83] Rosato A, Altilio R, Araneo R, Panella M. Prediction in photovoltaic power by neural networks. Energies 2017;10.

[84] Rivas AEL, Abrão T. Faults in smart grid systems: Monitoring, detection and classification. Electr Power Syst Res 2020;189:106602.

[85] Hussain N, Nasir M, Vasquez JC, Guerrero JM. Recent developments and challenges on AC microgrids fault detection and protection systems-a review. Energies 2020;13.

[86] Spiegel MH, Veith EMSP, Strasser TI. The spectrum of proactive, resilient multi-microgrid scheduling: A systematic literature review. Energies 2020;13(17). URL https://www.mdpi.com/1996-1073/13/17/4543.

[87] Ahmed M, Khan A, Ahmed M, Tahir M, Jeon G, Fortino G, Piccialli F. Energy theft detection in smart grids: Taxonomy, comparative analysis, challenges, and future research directions. IEEE/CAA J Autom Sin 2022;9(4):578–600.

[88] Kaur R, Saini G. Electricity theft detection methods and analysis using machine learning: Overview. Lect Notes Electr Eng 2023;926:527–46. http://dx.doi.org/10.1007/978-981-19-4971-5_38, URL https://www.scopus.com/inward/record.uri?eid=2-s2.0-85142708814&doi=10.1007%2f978-981-19-4971-5_38&partnerID=40&md5=8e1328a4b0ff3c1ded855f0024595c22.

[89] Yan Z, Wen H. Performance analysis of electricity theft detection for the smart grid: An overview. IEEE Trans Instrum Meas 2022;71:1–28. http://dx.doi.org/10.1109/TIM.2021.3127649.

[90] Saini S. Social and behavioral aspects of electricity theft: An explorative review. Int J Res Econ Soc Sci 2017;7(6):26–37.

[91] Chen J, Nanehkaran Y, Chen W, Liu Y, Zhang D. Data-driven intelligent method for detection of electricity theft. Int J Electr Power Energy Syst 2023;148. http://dx.doi.org/10.1016/j.ijepes.2023.108948, URL https://www.scopus.com/inward/record.uri?eid=2-s2.0-85146049659&doi=10.1016%2fj.ijepes.2023.108948&partnerID=40&md5=3f0f2c2208d4a84a40267792ebe3f9c8.

[92] Gao H-X, Kuenzel S, Zhang X-Y. A hybrid ConvLSTM-based anomaly detection approach for combating energy theft. IEEE Trans Instrum Meas 2022;71. http://dx.doi.org/10.1109/TIM.2022.3201569, All Open Access, Green Open Access; URL https://www.scopus.com/inward/record.uri?eid=2-s2.0-85137561156&doi=10.1109%2fTIM.2022.3201569&partnerID=40&md5=0d36e1f2a44d37fd03e256e0474d3f84.

[93] Soares LD, Queiroz AdS, López GP, Carreño-Franco EM, López-Lezama JM, Muñoz-Galeano N. BiGRU-CNN neural network applied to electric energy theft detection. Electronics (Switzerland) 2022;11(5). http://dx.doi.org/10.3390/electronics11050693, All Open Access, Gold Open Access; URL https://www.scopus.com/inward/record.uri?eid=2-s2.0-85125374680&doi=10.3390%2felectronics11050693&partnerID=40&md5=2d9639648bcb4d7c326b5e15826b71f8.

[94] Haq EU, Huang J, Xu H, Li K, Ahmad F. A hybrid approach based on deep learning and support vector machine for the detection of electricity theft in power grids. Energy Rep 2021;7:349–56. http://dx.doi.org/10.1016/j.egyr.2021.08.038, All Open Access, Gold Open Access; URL https://www.scopus.com/inward/record.uri?eid=2-s2.0-85119915080&doi=10.1016%2fj.egyr.2021.08.038&partnerID=40&md5=cc55040d4130bb0c20384b81c27ef44c.

[95] Tanwar S, Kumari A, Vekaria D, Raboaca MS, Alqahtani F, Tolba A, Neagu B-C, Sharma R. GrAb: A deep learning-based data-driven analytics scheme for energy theft detection. Sensors 2022;22(11). http://dx.doi.org/10.3390/s22114048, All Open Access, Gold Open Access, Green Open Access; URL https://www.scopus.com/inward/record.uri?eid=2-s2.0-85130805444&doi=10.3390%2fs22114048&partnerID=40&md5=f3670fdb1f4374b45c4db3634b879ef8.

[96] Takiddin A, Ismail M, Zafar U, Serpedin E. Deep autoencoder-based anomaly detection of electricity theft cyberattacks in smart grids. IEEE Syst J 2022;16(3):4106–17. http://dx.doi.org/10.1109/JSYST.2021.3136683, URL https://www.scopus.com/inward/record.uri?eid=2-s2.0-85122850248&doi=10.1109%2fJSYST.2021.3136683&partnerID=40&md5=954daa1dd7d83fc74fb39d2d312c2bfd.

[97] Umair M, Saeed Z, Saeed F, Ishtiaq H, Zubair M, Hameed HA. Energy theft detection in smart grids with genetic algorithm-based feature selection. Comput Mater Contin 2023;74(3):5431–46. http://dx.doi.org/10.32604/cmc.2023.033884, All Open Access, Gold Open Access, Green Open Access; URL https://www.scopus.com/inward/record.uri?eid=2-s2.0-85145438447&doi=10.32604%2fcmc.2023.033884&partnerID=40&md5=07fff331518832d3319befcc11fbfcf6.

[98] Lepolesa LJ, Achari S, Cheng L. Electricity theft detection in smart grids based on deep neural network. IEEE Access 2022;10:39638–55. http://dx.doi.org/10.1109/ACCESS.2022.3166146, All Open Access, Gold Open Access; URL https://www.scopus.com/inward/record.uri?eid=2-s2.0-85128329230&doi=10.1109%2fACCESS.2022.3166146&partnerID=40&md5=4faefe2f11470a4c803782548d0c2a56.

[99] Arif A, Alghamdi TA, Khan ZA, Javaid N. Towards efficient energy utilization using big data analytics in smart cities for electricity theft detection. Big Data Res 2022;27. http://dx.doi.org/10.1016/j.bdr.2021.100285, URL https://www.scopus.com/inward/record.uri?eid=2-s2.0-85119083127&doi=10.1016%2fj.bdr.2021.100285&partnerID=40&md5=4e2e06fa4b113efbb5ac66b25d9ec4d6.

[100] Ashraf MM, Waqas M, Abbas G, Baker T, Abbas ZH, Alasmary H. FedDP: A privacy-protecting theft detection scheme in smart grids using federated learning. Energies 2022;15(17). http://dx.doi.org/10.3390/en15176241, All Open Access, Gold Open Access, Green Open Access; URL https://www.scopus.com/inward/record.uri?eid=2-s2.0-85137989060&doi=10.3390%2fen15176241&partnerID=40&md5=aca59d9f196b5beaba3bca39aefabcaa.

[101] Yao D, Wen M, Liang X, Fu Z, Zhang K, Yang B. Energy theft detection with energy privacy preservation in the smart grid. IEEE Internet Things J 2019;6(5):7659–69.

[102] Catena T, Eramo V, Panella M, Rosato A. Distributed LSTM-based cloud resource allocation in Network Function Virtualization Architectures. Comput Netw 2022;213:109111. http://dx.doi.org/10.1016/j.comnet.2022.109111, URL https://www.sciencedirect.com/science/article/pii/S1389128622002390.

[103] Xue L, Cheng L, Li Y, Mao Y. Quantum machine learning for electricity theft detection: An initial investigation. In: Proceedings - IEEE congress on cybermatics: 2021 IEEE international conferences on internet of things, iThings 2021, IEEE green computing and communications, GreenCom 2021, IEEE cyber, physical and social computing, CPSCom 2021 and IEEE smart data, SmartData 2021. 2021, p. 204–8. http://dx.doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData-Cybermatics53846.2021.00043, URL https://www.scopus.com/inward/record.uri?eid=2-s2.0-85127419577&doi=10.1109%2fiThings-GreenCom-CPSCom-SmartData-Cybermatics53846.2021.00043&partnerID=40&md5=1aaf17dc36775062d48210f5ad54e281.

[104] Punmiya R, Choe S. Energy theft detection using gradient boosting theft detector with feature engineering-based preprocessing. IEEE Trans Smart Grid 2019;10(2):2326–9.

[105] Salinas SA, Li P. Privacy-preserving energy theft detection in microgrids: A state estimation approach. IEEE Trans Power Syst 2016;31(2):883–94.

[106] Ahir RK, Chakraborty B. Pattern-based and context-aware electricity theft detection in smart grid. Sustain Energy Grids Netw 2022;32:100833. http://dx.doi.org/10.1016/j.segan.2022.100833, URL https://www.sciencedirect.com/science/article/pii/S2352467722001199.

[107] Zhao Y, Li T, Zhang X, Zhang C. Artificial intelligence-based fault detection and diagnosis methods for building energy systems: Advantages, challenges and the future. Renew Sustain Energy Rev 2019;109:85–101.

[108] McLaughlin S, Holbert B, Fawaz A, Berthier R, Zonouz S. A multi-sensor energy theft detection framework for advanced metering infrastructures. IEEE J Sel Areas Commun 2013;31(7):1319–30.

[109] Jacquot P, Beaude O, Gaubert S, Oudjane N. Demand response in the smart grid: The impact of consumers temporal preferences. In: 2017 IEEE international conference on smart grid communications (SmartGridComm). IEEE; 2017, p. 540–5.

[110] Wang X, Yao Z, Papaefthymiou M. A real-time electrical load forecasting and unsupervised anomaly detection framework. Appl Energy 2023;330:120279.

[111] Fang H, Tan H, Kosonen R, Yuan X, Jiang K, Ding R. Study of the data augmentation approach for building energy prediction beyond historical scenarios. Buildings 2023;13(2). http://dx.doi.org/10.3390/buildings13020326, URL https://www.mdpi.com/2075-5309/13/2/326.

[112] Delfosse A, Hebrail G, Zerroug A. Deep learning applied to NILM: Is data augmentation worth for energy disaggregation? In: ECAI 2020. IOS Press; 2020, p. 2972–7.

[113] Gong X, Tang B, Zhu R, Liao W, Song L. Data augmentation for electricity theft detection using conditional variational auto-encoder. Energies 2020;13(17). http://dx.doi.org/10.3390/en13174291, URL https://www.mdpi.com/1996-1073/13/17/4291.

[114] Hooshmand A, Sharma R. Energy predictive models with limited data using transfer learning. In: Proceedings of the tenth ACM international conference on future energy systems. 2019, p. 12–6.

[115] Ribeiro M, Grolinger K, ElYamany HF, Higashino WA, Capretz MA. Transfer learning with seasonal and trend adjustment for cross-building energy forecasting. Energy Build 2018;165:352–63.

[116] Huo Y, Prasad G, Atanackovic L, Lampe L, Leung VC. Cable diagnostics with power line modems for smart grid monitoring. IEEE Access 2019;7:60206–20.

[117] Mellit A, Tina GM, Kalogirou SA. Fault detection and diagnosis methods for photovoltaic systems: a review. Renew Sustain Energy Rev 2018;91:1–17, URL https://www.sciencedirect.com/science/article/pii/S1364032118301370.

[118] Liu W, Tang B, Han J, Lu X, Hu N, He Z. The structure healthy condition monitoring and fault diagnosis methods in wind turbines: A review. Renew Sustain Energy Rev 2015;44:466–72, URL https://www.sciencedirect.com/science/article/pii/S1364032114010570.

[119] Ma H, Saha TK, Ekanayake C, Martin D. Smart transformer for smart grid - Intelligent framework and techniques for power transformer asset management. IEEE Trans Smart Grid 2015;6:1026–34.

[120] Zhang W, Xu D, Enjeti PN, Li H, Hawke JT, Krishnamoorthy HS. Survey on fault-tolerant techniques for power electronic converters. IEEE Trans Power Electron 2014;29(12):6319–31.

[121] Sun R, Guo J, Gill EK. Opportunities and challenges of wireless sensor networks in space. In: 61st international astronautical congress 2010, IAC 2010, Vol. 6. IEEE; 2010, p. 4993–5004.

[122] Allnutt J, Anand D, Arnold D, Goldstein A, Li-Baboud Y-S, Martin A, Nguyen C, Noseworthy R, Subramaniam R, Weiss M. Timing challenges in the smart grid, Vol. 1500. NIST Special Publication, 2017, p. 8.

[123] Cupp JG, Beehler ME. Implementing smart grid communications managing mountains of data opens up new challenges for electric utilities. Communications 2008;57–9.

[124] He D, Chan S, Zhang Y, Guizani M, Chen C, Bu J. An enhanced public key infrastructure to secure smart grid wireless communication networks. IEEE Netw 2014;28(1):10–6.

[125] Baimel D, Tapuchi S, Baimel N. Smart grid communication technologies-overview, research challenges and opportunities. In: 2016 international symposium on power electronics, electrical drives, automation and motion, SPEEDAM 2016. IEEE; 2016, p. 116–20.

[126] Asghar MR, Dán G, Miorandi D, Chlamtac I. Smart meter data privacy: A survey. IEEE Commun Surv Tutor 2017;19:2820–35.

[127] Arenas-Martínez M, Herrero-Lopez S, Sanchez A, Williams JR, Roth P, Hofmann P, Zeier A. A comparative study of data storage and processing architectures for the smart grid. In: 2010 first IEEE international conference on smart grid communications. 2010, p. 285–90.

[128] Wu YN, Chen J, Liu LR. Construction of Chinas smart grid information system analysis. Renew Sustain Energy Rev 2011;15:4236–41.

[129] Dehalwar V, Kalam A, Kolhe ML, Zayegh A. Review of machine to machine communication in smart grid. In: 2016 international conference on smart grid and clean energy technologies, ICSGCE 2016. IEEE; 2017, p. 134–9.

[130] Ahmed S, Gondal TM, Adil M, Malik SA, Qureshi R. A survey on communication technologies in smart grid. In: 2019 IEEE PES GTD grand international conference and exposition Asia (GTD Asia). 2019, p. 7–12.

[131] Hui H, Ding Y, Shi Q, Li F, Song Y, Yan J. 5G network-based Internet of Things for demand response in smart grid: A survey on application potential. Appl Energy 2020;257:113972.