

Review

A Survey on Energy Efficiency in Smart Homes and Smart Grids

Lisardo Prieto González ¹, Anna Fensel ^{2,3,4,*}, Juan Miguel Gómez Berbís ¹, Angela Popa ⁴
and Antonio de Amescua Seco ¹

¹ Software Architect Group, Department of Computer Science, Carlos III University of Madrid, 28911 Leganés, Spain; lisardo.prieto@uc3m.es (L.P.G.); juanmiguel.gomez@uc3m.es (J.M.G.B.); antonio.amescua@uc3m.es (A.d.A.S.)

² Wageningen Data Competence Center (WDCC), Wageningen University and Research, 6708 PB Wageningen, The Netherlands

³ Consumption & Healthy Lifestyles Group, Wageningen University and Research, 6708 PB Wageningen, The Netherlands

⁴ STI (Semantic Technology Institute) Innsbruck, Department of Computer Science, University of Innsbruck, 6020 Innsbruck, Austria; popa.angela@gmail.com

* Correspondence: anna.fensel@wur.nl; Tel.: +31-6185-23825

Abstract: Empowered by the emergence of novel information and communication technologies (ICTs) such as sensors and high-performance digital communication systems, Europe has adapted its electricity distribution network into a modern infrastructure known as a smart grid (SG). The benefits of this new infrastructure include precise and real-time capacity for measuring and monitoring the different energy-relevant parameters on the various points of the grid and for the remote operation and optimization of distribution. Furthermore, a new user profile is derived from this novel infrastructure, known as a prosumer (a user that can produce and consume energy to/from the grid), who can benefit from the features derived from applying advanced analytics and semantic technologies in the rich amount of big data generated by the different subsystems. However, this novel, highly interconnected infrastructure also presents some significant drawbacks, like those related to information security (IS). We provide a systematic literature survey of the ICT-empowered environments that comprise SGs and homes, and the application of modern artificial intelligence (AI) related technologies with sensor fusion systems and actuators, ensuring energy efficiency in such systems. Furthermore, we outline the current challenges and outlook for this field. These address new developments on microgrids, and data-driven energy efficiency that leads to better knowledge representation and decision-making for smart homes and SGs.

Keywords: energy efficiency; smart home; semantic technology; knowledge graphs; security; fraud; detection; encryption; smart grid; communication; microgrid



Citation: Prieto González, L.; Fensel, A.; Gómez Berbís, J.M.; Popa, A.; de Amescua Seco, A. A Survey on Energy Efficiency in Smart Homes and Smart Grids. *Energies* **2021**, *14*, 7273. <https://doi.org/10.3390/en14217273>

Academic Editor: André Madureira

Received: 31 August 2021

Accepted: 28 October 2021

Published: 3 November 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Smart grids (SGs) are comprised of advanced and complex technological components [1], both physical and logical. Their popularization and development are growing across the globe [2,3], given the multiple benefits this kind of infrastructure provides over the former electricity distribution network [4]. Some of them include:

- a safer and more resilient electricity distribution network,
- self-healing protection mechanisms,
- advanced monitoring capabilities and load management,
- a cost reduction in network operations due to the dynamic balancing between production and demand,
- a cleaner, decentralized production of electricity,
- a reduction of the traditional costly peak production capacity,
- bidirectional flow of electricity.

All these benefits make the energy distribution system more versatile, reliable, and efficient.

The creation of a SG is tightly associated with the need to set up a complex, advanced communications network, enabling monitoring and piloting the grid through the observation of the electricity generation and distribution flow. Such a high-density communication network will gather a vast quantity of data that needs to be processed and analyzed within intelligent workflows to make the best possible use of the underlying information.

With the increase of computing power that has led to varied and increasingly powerful techniques based on AI, together with big data generation and analysis, a broad set of novel features are starting to emerge to tackle existing problems that had not been an easy solution before [5–8]. AI-related techniques utilized to analyze the vast amount of data gathered by the SG provide tools to perform reasoning, efficient planning, knowledge gathering, and quickly and effectively manage possible outages, detect fraud, optimize the distribution of power, and manage potential security breaches, among others.

On the other hand, the towering collection of data within SG also creates new critical threats that must be addressed from an information security (IS) perspective. Otherwise, they may bring disastrous consequences. The threats mostly happen at three different levels [9–12]:

- The architecture level, where it is necessary to consider problems as credentials distribution to enable end-to-end security between devices and applications. It also features dynamic fine-grain authorization management to control which application is entitled to use which data.
- Smart devices compose the hardware part of the grid. They can be hardened via secure elements in the devices [13]. Also, a challenge is defining low-cost, highly scalable secure element solutions, including hardware, provisioning, and deployment components, to use certain secure embedded elements well suited to SG applications.
- Software applications to manage the SG components.

It is essential to ensure that the data collected within the grid is stored and distributed securely and only to authorized parties. It is also crucial to ensure that the devices, sensors, and actuators deployed within the grid are trusted and cannot be easily cloned and replaced by malicious ones. The security of the grid is therefore of extreme importance. It will involve the definition of advanced security architectures well suited to SG and the definition of a new generation of standardized, secure element solutions compatible in cost and ease of deployment with SG's business models.

As shown in Figure 1, the use of the SG starts at the first link of the value chain: the energy production; the power plants make the production data available through the grid. Its use continues with the transportation chain, where the different meters inform about the energy circulating through the transportation means. The distribution units also submit the data about their performance via the grid. Customers make intensive use of the SG since they use and produce data transmitted through the grid. Remarkably, the interaction with customers occurs through smart homes, which are ICT-empowered homes that assist their residents with energy consumption. Finally, outsourcing companies or other business units of the energy companies may interact with the grid by retrieving or transmitting any data.

In conclusion, all the links of the energy value chain use the SG, so any energy market actors are subject to attacks. In this regard, several recent studies propose technologies such as blockchain [14–16] to mitigate problems such as centralization of the management system, support the operation of crowdsourced energy systems, remove single points of failure, and prevent fraud and the ability to forge energy transactions. However, these technologies are mainly applied theoretically or in testing environments to SGs.

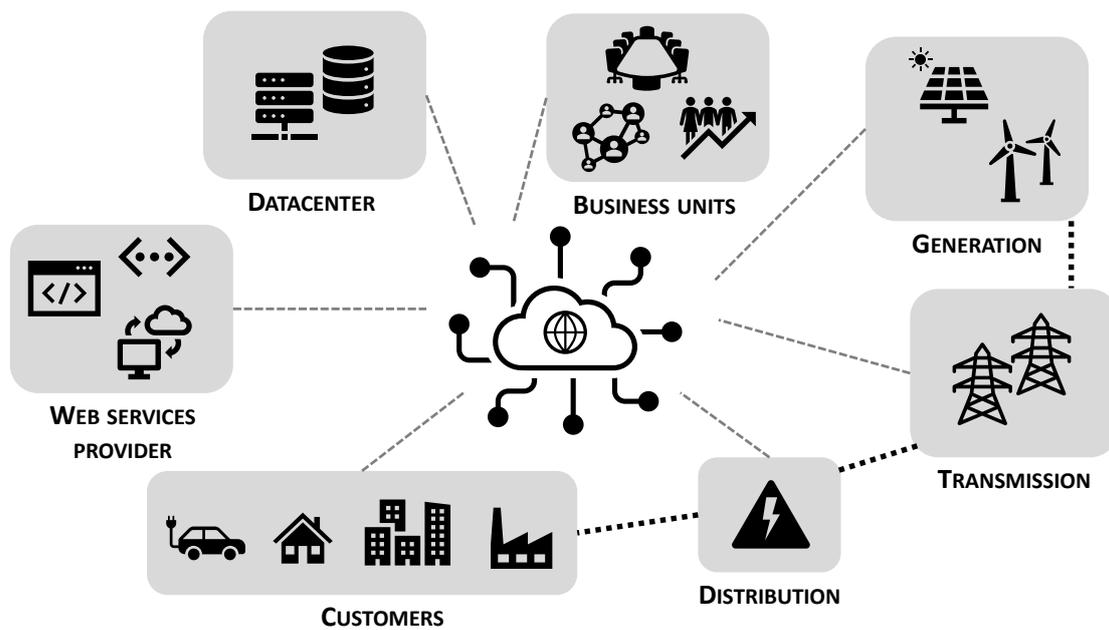


Figure 1. Smart Grid energy market.

In this paper, we contribute with an overview of the state-of-the-art developments comprising the area of energy-efficient SGs and smart homes. We cover the whole domain relevant for ICT use, starting from the physical infrastructure and proceeding towards the end-users of smart homes and grids. Also, relevant topics related to the solutions such as decentralization, security, and blockchain applications are discussed. This state-of-the-art survey is concluded by the outlook and future work areas derived based on the reviewed literature and projects.

The rest of the article is organized as follows. Section 2 outlines the followed methodology for this survey. Section 3 presents relevant technical solutions to achieve energy efficiency within smart homes and grids. Section 4 gives an outlook and outlines future lines of work. Section 5 contains conclusions.

2. Survey Methodology

To create this paper, a typical survey methodology has been followed; namely, we have been following a method for systematic literature review [17]. The peer-reviewed publications as the primary resource have been identified using the typical for ICT literature scholarly indexing services: Google Scholar, IEEE Xplore, the ACM Digital Library, Scopus, and DBLP. We considered a representative number of studies primarily ranging from 2016 to 2021, focusing on the most recent and relevant ones. The query terms included relevant keywords for both addressed domain and specific technology, such as energy efficiency, smart home, semantic technology, ontology, knowledge graphs, big data, security, fraud, detection, encryption, SG, communication, and behavioral change. Authors and affiliations of the publications were also used as keywords to find additional relevant sources of knowledge, and the authors' many years of research experience and their knowledge of the covered field are relied on. Moreover, the citation count of the papers has been a relevant criterion to select and review them by. To provide a comprehensive investigation for ICT-enabled energy efficiency approaches, they are reviewed in separate sections dedicated to the SGs and to smart homes.

3. Technical Solutions for Energy Efficiency with SGs and Homes

Big data is intended to put together all data coming from automated metering infrastructure (AMI).

From the customer's perspective (electricity companies), revenue protection (in more straightforward language, theft detection) is a crucial application to secure their revenues. This has been the object of several works [6,18–22]. Also, demand response analysis and management is an important task, getting customers to reduce their energy consumption, and hence, system peak loads. It can also focus on customer behavior (inducing privacy-aware issues) [23] or the combination of messaging and incentives that are best at getting customers to reduce energy usage at the lowest possible cost to utilities.

The outage management system (OMS) enhancements are the primary way to use AMI-gathered data to perform operational improvements from the network perspective. For instance, there are successful implementations of AMI-assisted outage restorations in post-disaster scenarios (weather events or cyber-attacks) [24–26]. These systems facilitate the ability to fix as-yet-unreported outages, like those that happen when the affected users may be asleep or away from home, and the health diagnoses of SG systems themselves [26].

Finally, utility regulators can use predictive analytics to create precise financial models to consider the costs and benefits of future deployments [27,28]. Accurate demand forecasting is crucial to perform efficient energy planning and trading. Predictions are even more impressive when applied to disaster prevention. Systems could accurately predict where thunderstorms may damage the SG [29] and allow utilities to stage specific crews and required equipment accordingly.

The SG allows users to automate their connection-disconnection of devices by enabling time-of-use pricing in the home automation field. However, it could also be shifted to the area of personal services. Users may want to include specific task automation rules to interact with their smart homes, e.g., *“turn on the heating system 30 min before I arrive home”*. Here the smartphone, or maybe the car, which is not connected to the SG by default, is involved since it provides the user's location. Nevertheless, hackers can immediately manipulate their energy costs or forge fake energy meter readings by compromising a smart meter. Even more, in some cases, they can do the same with any other smart device connected to the grid [30]. Thus, in modern SG architectures, home automation is orchestrated through security channels and supervised by the network.

Securing communications in a system and a SG in particular always involves achieving both data protection and resilience to sabotage. Data protection requires the secure distribution of credentials used to harden data transmission and storage. It also needs an authorization management mechanism to define how devices and applications may interact together. Moreover, a second issue is involved since the data used to coordinate these rules is personal and must be deleted as long as it is not needed to automate the task. Novel approaches include using specific blockchain-based networks and smart contracts to address most of these issues [16,31,32]. Besides, the right security level usually involves protecting long-term credentials stored in the cloud platforms and the devices to prevent credential theft. Stolen credentials retrieved from an unprotected device may enable the cloning and impersonation of the device and open the way to destructive attacks. The concept of an efficient solution to protect credential storage on an insecure device is a real challenge. The use of secure embedded elements inside the devices constitutes a proven solution to enhance credential storage security [13]. Also, effective computational and storage cost solutions based on the blockchain can overcome the problems related to trusted control access by IoT-based smart meters in untrusted environments by decentralizing the trusted control access scheme and protecting the data transmission requests sent and received by smart meters to the network [14].

From another perspective, the availability of a large quantity of user-related data collected within the SG raises a privacy issue. Network intrusion prevention systems and network intrusion detection systems should enhance host-based defenses to protect the system from outside and inside attacks [33]. In this regard, solutions that combine blockchain-based energy exchange and deep learning networks that detect attacks and fraudulent transactions have been proposed [34]. Also, a particular use case consists of defining and elaborating the intelligent security monitoring and control layer that will

monitor the bidirectional communication between supervisory control and data acquisition (SCADA) systems and remote devices. For operators of power plants and grids, it is of utmost importance to be aware. This raises the bar for new available commercial solutions. This is especially true for remotely located devices, which are installed in non-secure environments and require innovative security solutions. Simultaneously, these devices are typically connected to critical central systems, like SCADA, an element manager (for IT maintenance and support centrally), and a monitoring server (including the backup). This means that a complex communication environment requires better tunable security solutions for keeping the operators in a state of awareness. Some studies [35–37] propose a viable solution for SG in an intelligent security monitoring and control layer, adapted and enhanced with smart artificial intelligent anomaly detector systems (ADS). The intelligent monitoring and control systems actively follow the communication messages and compare these with the “learned” normal situation. So, it can detect anomalies that will trigger specifications (i.e., an alarm on the operator screen). A more context-based description, where in-depth monitoring and control are of vital importance, is provided in the following paragraphs.

In the energy production and distribution chain, ICT-based automation is increasingly involved, and this phenomenon will grow even more in the future by integrating information technologies (IT) and operational technologies (OT) into new operational information technologies (OIT) systems. Liberalization of the market and the rise of decentralized production add different communication interfaces between the other parties [38]. From a security perspective, all these various communication interfaces need to be monitored, and in case of anomalies, to adopt the appropriate mitigation actions. The typical communication structures in the energy production and distribution environment use SCADA systems as a hub [39]. The actual physical communication path ranges from copper and/or optic fiber to wireless solutions, meaning that third parties can provide the physical infrastructure. This fact induces extra incentives to monitor and control the communication mechanism carefully. Figure 2 shows a high-level representation using the Smart Grid Architecture Model (SGAM) reference model [40].

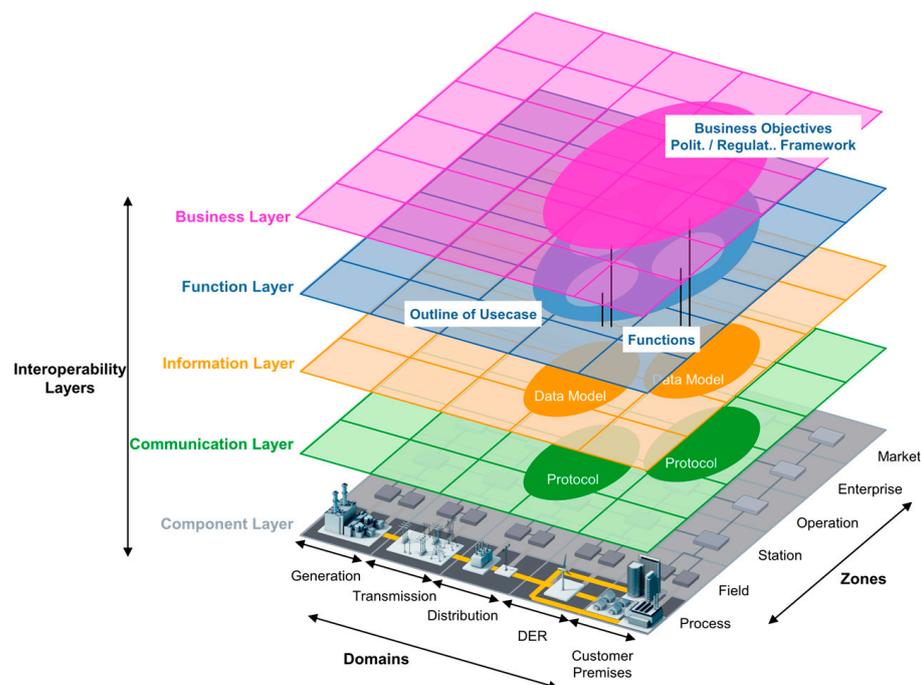


Figure 2. High level representation SGAM [40].

The general build-up of the primary layers that interface to monitor and control a power plant or grid is shown. Most of the applied ICT automated device vendors

(i.e., intelligent electronic devices—IEDs) have not included security mechanisms in their devices; thus, security by design is not always implemented. In installed systems, some unprotected devices can still be found. This requires stringent security procedures for technical, operational people (both vendors employees) when updating, commissioning, or configuring these remote devices. However, the bidirectional monitoring and control of the communication between these remote devices and the centralized SCADA systems are vital to keeping the energy systems up and running. Figures 3 and 4 show the smart grid according to SGAM zones.

In the future, SG will evolve in an even more intelligent environment where the remote devices in substations will communicate with each other. An example is the self-healing ring concept that makes it possible that the network itself will heal after a malfunction in the medium voltage meshed or ring networks (e.g., a cable cut). This brings extra challenges for the security application because the IEDs will communicate directly without consulting the SCADA. After restoration, the SCADA system needs to be informed of the new medium-voltage network status [41]. In this case, an AI-based approach needs to follow up on the monitoring and control messages between the IEDs and the SCADA system. The future SG needs updates in the environment of station level, typically in the layer where the aggregation devices are found that communicate to the SCADA systems. Special attention is paid to security architecture [42]. As shown in the example below, the demilitarized zone (DMZ) needs to be defined, the communication messages that flow to and from the different devices and to and from the SCADA system must be identified, described, and, in the end, this information and the intelligence on how to act after an anomaly detection has to be programmed in ADS. This also means that these enhanced ADSs need to be adapted, tested and implemented.

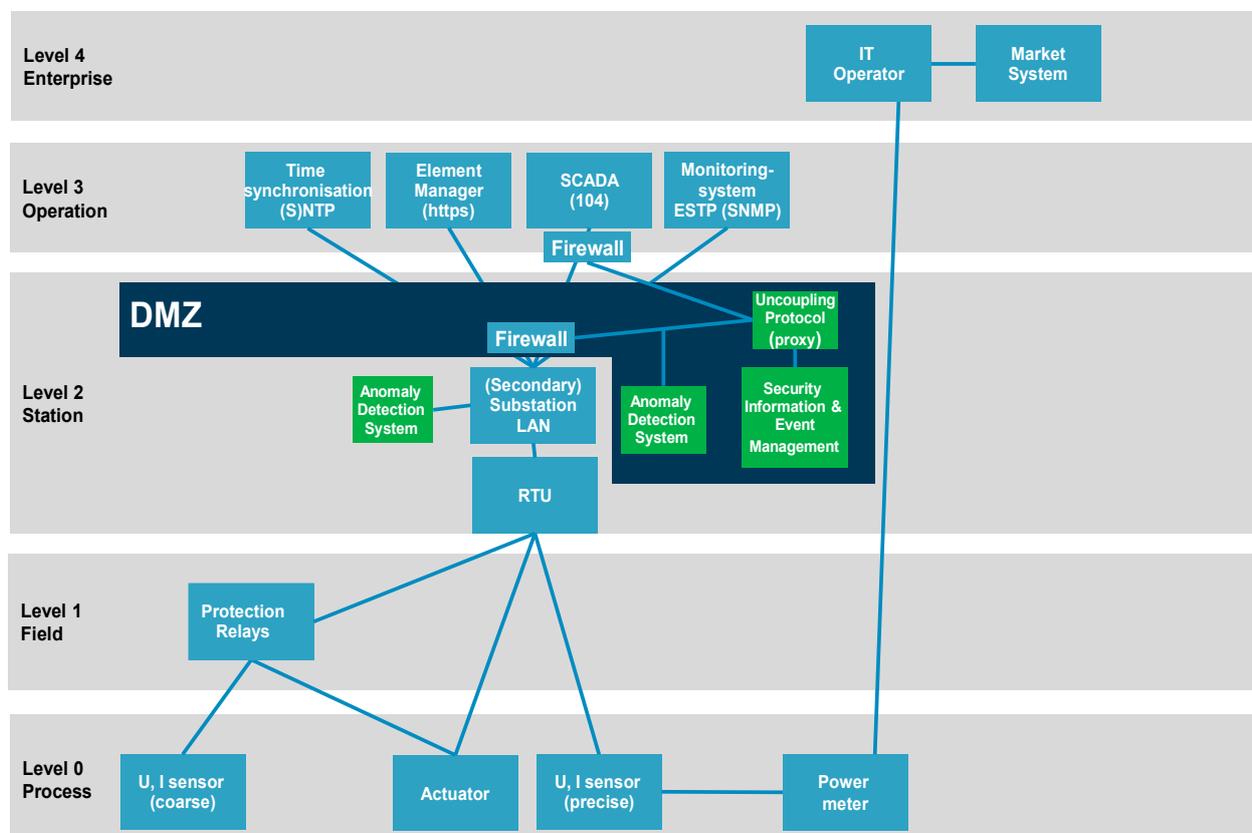


Figure 3. Smart Grid overview.

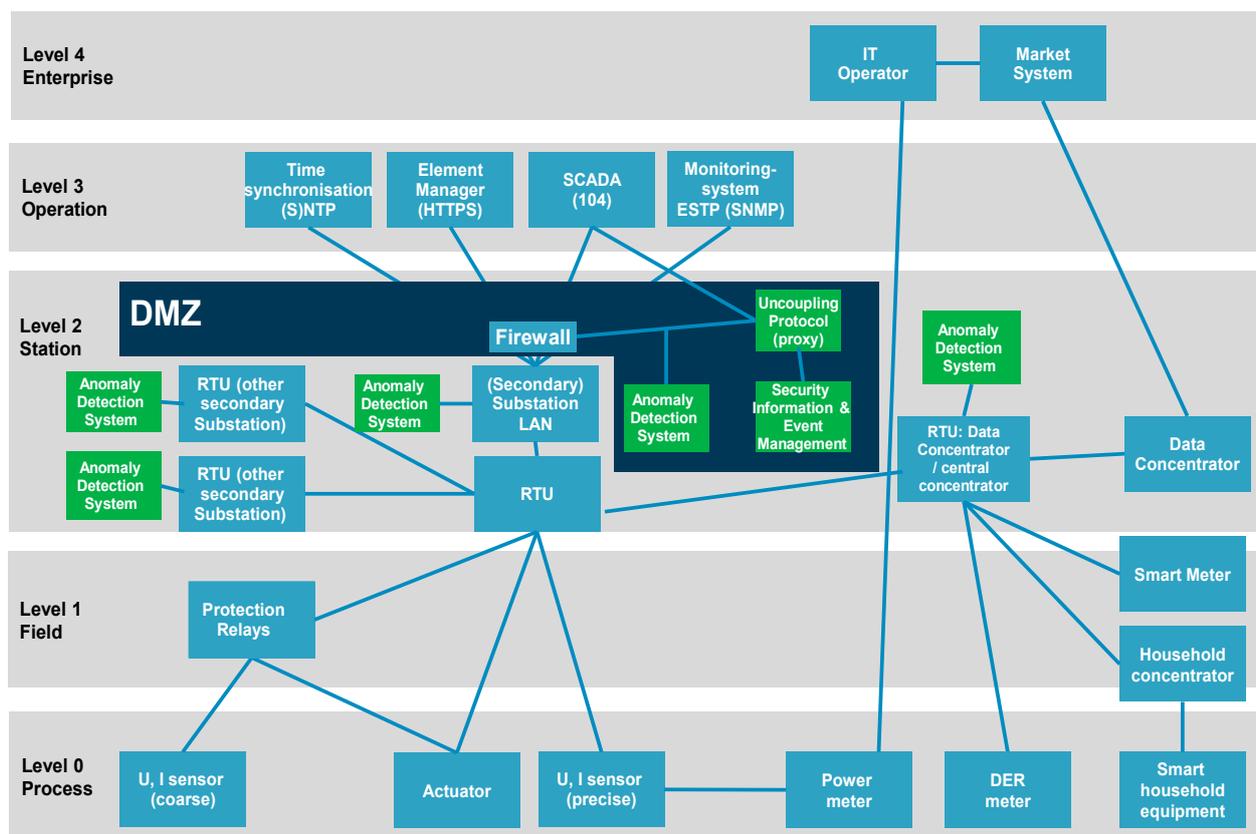


Figure 4. Future secure Smart Grid.

3.1. Smart Homes

Smart homes are technically equipped dwellings that can monitor and improve their energy consumption among several other tailored services for users [43]. Extending this idea to buildings, we also have the term “smart buildings”. Smart buildings are energy-efficient, technically integrated, safe and sustainable buildings that are part of broader energy grids. Technologies that involve heterogeneous approaches and frameworks include the internet of things (IoT), integration and interoperability solutions, energy consumption awareness, energy consumption prediction, and decentralized deployment.

IoT developments become relevant in addressing the challenge to lower the impact of humanity on the environment. One of the techniques that is already in use is home automation [44,45]. The smart meters installed in buildings, together with sensors and actuators, keep track of and even optimize energy consumption. Smart meters are technical devices that automatically measure the energy consumption of a building unit. In the European Directive for Energy Buildings [46], at least 80% of energy consumers should be equipped with smart meter systems by 2020.

The goal of the usage of smart meters is the ability to offer accurate and frequent billing details. AI technologies might enhance smart meters in the future so that they can manage and improve the energy consumption levels autonomously [47].

Smart cities are comprised of interconnecting homes, offices, data centers, warehouses, and public infrastructure. European cities are actively working on ideas and prototypes to accomplish the vision of smart cities. An example is the city of Innsbruck, where the notion of a holistic energy identity in 2050 is only possible by an overall consideration of the city as a system in which energy, buildings, supply networks, mobility, information, and people are viewed in an integrated manner [48].

For the integration of information in smart homes, semantic technology increasingly serves as an enabler for semantic interoperability for smart homes. An example of such development is the SESAME project that offers a plug-and-play solution for integrating

building automation systems with advanced metering systems to facilitate an energy-aware home automation system [49]. The project uses semantic rules to describe how appliances within the environment will be operated. These rules enable reasoning on the measured data. For the SESAME project, three ontologies were developed [50]:

- The Automation Ontology includes general concepts such as Resident and Location, but also ideas in the automation and the energy domain, such as device (with consumption per hour, peak power, on/off status), and Configuration (configuration data of an appliance),
- The Meter Data Ontology enables communication protocols for data exchange with the metering equipment,
- The Pricing Ontology is used for selecting the optimal tariff model for a specified time and energy load. It defines weighted criteria, which are then used by the reasoning engine for choosing the best tariff model.

Involvement of the end users and engaging them as active prosumers creates challenges in building systems that implement energy consumption awareness. As an example of an energy awareness approach, the Entropy project [51] aims to sensitize tenants to their dwellings' consumed energy [52]. These dwellings are equipped with special sensors that collect energy consumption data. The tenants are kept informed by a specially developed application about their energy consumption. The Entropy project focuses mainly on the tenants' behavior and suggested lifestyle changes to reduce the energy consumption via their services, but in a user-friendly manner.

As described in [52], the entropy services collect and process data from sensor nodes in real-time and manage historical sensor data. The Entropy project uses semantic web technologies like semantic models and ontologies for unified data representation of the previously collected sensor data. The two developed semantic models are the energy efficiency semantic model, which represents the energy consumption data collected from the sensors, and, the behavioural semantic model, which focuses on the energy consumption profile of end users.

These models facilitate the further management and exploitation of the collected sensor data. With LinDa workbenches [53], the semantically annotated data from the semantic models are transformed into linked data. This approach is of use to the building sector because comparisons between the collected data and the exchange with other open linked data like meteorological data are needed. The data is stored in the JSON-LD [54] data format, a lightweight linked data format. The recommender system behind Entropy is based on the Drools framework [55], which is a rule-based management system. In the Entropy project, a rule is expressed by a condition element and a recommendation template. Entropy's recommender system uses machine learning techniques and provides the user with personalized suggestions taking into account the user attributes and behavioral traits [55]. For example, if a context changes, the recommender system creates personalized recommendations for each user in the targeted user group using the recommendation template. The targeted user group is based on users that satisfy specific user attributes defined in the template. Through the Entropy project an application was developed that joins energy and behavioural data and, as a consequence, leads to the improvement of energy efficiency in smart buildings [51].

Energy consumption prediction in smart homes and grids is another important aspect that involves AI. Building thermodynamics is a complex non-linear phenomenon, which is strongly influenced by weather conditions, building operating modes, and occupant schedules and requires, for example, predictive data-driven models [56]. These models were developed with the help of machine learning techniques. The machine learning algorithms are trained with a set of data and run on a different set, applying what they learned during the training period. The developed predictive models are of two categories. On one side is the black-box, in contrast to white-box model models (e.g., support vector regression, regression forest), and on the other side is the grey-box models (e.g., Gaussian). This research proved that the predictions generated by the black-box models applied to

temperature values outperformed the grey-box models used for energy consumption values because the first captured human behavior. Human behavior has a more significant impact on energy consumption than the envelope of the building. According to the researchers, the random forest had the best prediction results [56].

From the standpoint of security and decentralisation, it is a challenge to monitor in real-time the SG and all the devices connected to it. ICTs are crucial for the success and implementation of the SG concept. Several communication technologies could support SG communication in the distribution system, ranging from optical fiber to power line carrier (PLC) to wireless technologies.

A three-level hierarchy can be defined to support an SG communications network. It includes the home area network (HAN), neighborhood area network (NAN), and wide area network (WAN). An overview of the AMI communication scheme is shown in Figure 5.

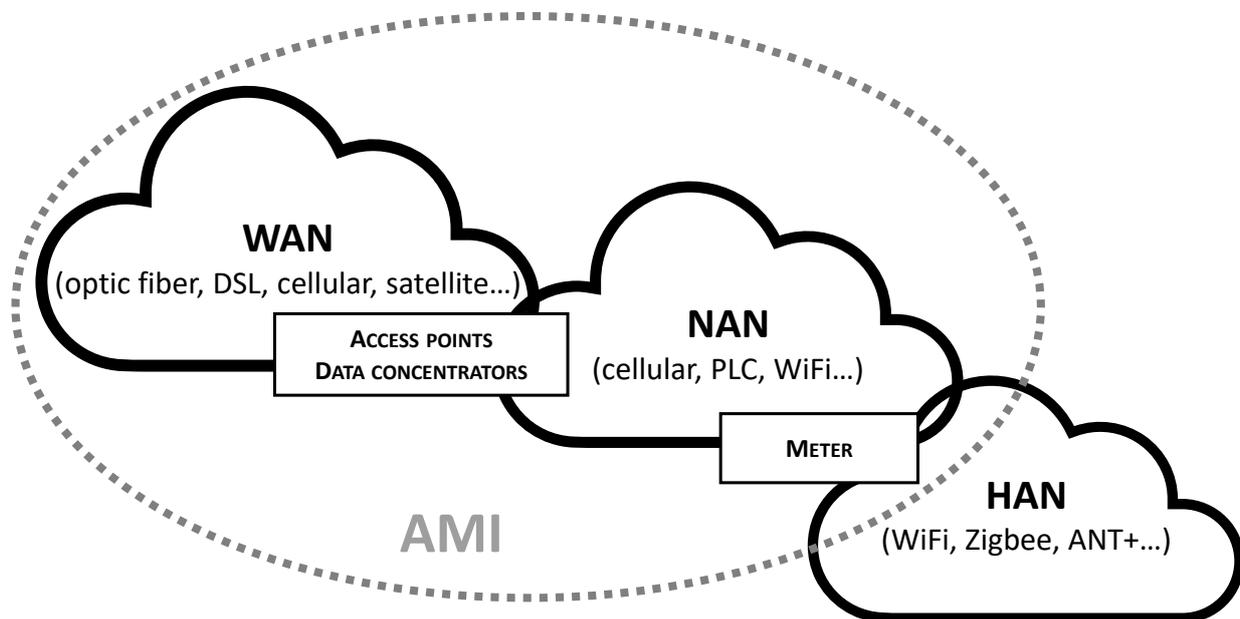


Figure 5. AMI scheme.

With ICT-enhanced infrastructures, grids are evolving from centralized and hierarchical topologies to distributed and holonic architectures. They provide substantial added value in terms of efficiency, eco-friendliness, and savings. However, a significant impediment to their adoption is the security issues they raise. With enhanced communication, load balancing automation, and important heterogeneous data analysis capabilities, the grid becomes vulnerable to large-scale cyber-attacks [9,10]. Hence, security is to be a “market enabler” to smart grids. An identified method of attacking the meters involves placing a strong magnet on the devices, which causes them to stop measuring usage while still providing electricity to the customer [57]. Some customers are using this method to disable the meter at night when air-conditioning units are operational. This is an example of a physical attack related to significant concern in the power systems planning and operation, which is commercial losses (also known as non-technical losses). This type of loss has consequences from the grid operational point of view, as it causes unexpected loads in system elements, as well as from the economic point of view. Some works on non-technical losses’ minimization and identification have been developed [58–60], but this is still an area to be improved. At the same time, new data becomes available and suitable to be analyzed utilizing AI-based techniques.

3.2. Smart Grids

While cyber-security emerged as a very IT-focused discipline when the interconnection of local networks to the internet became a standard, we now acknowledge that the machine-to-machine (M2M) communication, particularly the adoption of SG, gets more and more entangled. Hence the emergence of the concept of a cyber-physical system (CPS) embracing supervisory control and data acquisition (SCADA), industrial automation and control systems (ICAS), embedded command and control systems, and the IoT. Novel cyber-physical attacks have emerged [61], as well as advanced defenses. However, a significant limitation is that the security of a cyber-physical system cannot just be tackled by adding physical security at the OT level and cyber-security at the IT level. A new federative approach is required to assess the impact of cyber-incidents and countermeasures on grid operation and processes, identify vulnerabilities of state-of-the-art SCADA protocols in use, and identify the most likely attack scenarios in this environment.

Nations are dependent on the reliable functionality of critical infrastructure, such as electrical, gas, and water grids. Significant concerns have been highlighted in documents such as “Smart Grid Cyber Security Potential Threats, Vulnerabilities and Risks” [62], from the California State University Sacramento, the NIST “Guidelines for Smart Grid Cyber Security” [63], and at the European SG standards proposed by the European Smart Grids Task Force [64].

Smart grids applications are typically based upon client-server architecture. The security of those applications is primarily addressed to secure point-to-point communication between the gateway and applications servers. The role of the M2M service platform appears known as a critical component to ensuring interoperability between heterogeneous applications. Such a platform offers several services that simplify the coding of M2M applications and, more specifically, it enables a dynamic definition of the data flow. Furthermore, efforts have been undertaken by standardization bodies such as IETF, ETSI (now ONEM2M) to define standards for interoperable M2M service platforms [65,66]. However, with the advent of the M2M services platform, the communication model evolves from a point-to-point client-server model towards a point-to-multipoint peer-to-peer communication model.

From the security standpoint, the management of credentials used to secure M2M applications has been fairly static, and this also needs to evolve: The problem is not anymore to secure the communication from devices to the application server, but rather to secure communications from devices to every single application needing and authorized to interact with devices [67]. M2M applications commonly address authentication and data protection issues, but authorization is seldom addressed, which is regrettable. Fine-grain authorization management is an essential component of secure architecture, defining with precision which applications may interact with one device and how.

Also, implementing a security scheme is commonly related to the distribution of credentials [42]. Protecting the storage and use of those credentials is essential to avoid compromising security. The problem is challenging on the device side, where the theft of credentials opens the way to device cloning. Secure elements offer a proven solution to protect the storage of credentials in embedded appliances. Their enrolment and the management of the credentials stored in their memory are performed using specialized secure element management platforms that have been traditionally operated by the business entities issuing a secure element. Nevertheless, recent years have seen the emergence of the “security domain,” enabling a single secure element to be exposed as a shared platform used by independent service providers.

The underlying business model involves the secure element issuer “leasing” secure element space to third parties’ providers for them to remotely store and manage their credentials in their private, secure space [68]. This model could apply to smart grids and smart grid devices as it opens the possibility for multitenant administration of the credentials stored in the devices. It supports emerging business models for smart grid operation. Modern approaches also propose the usage of blockchain-based decentralized and secure keyless signature schemes [31,69].

This idea of multitenant administration has emerged to enable multiple providers to offer mobile services requiring strong security for client-side credentials. Unfortunately, the use cases involved for mobile applications are incredibly diverse and sometimes very complex compared to IoT and, more specifically, smart grid use cases.

The need to support a large variety of use case configurations has a very significant impact on the cost of the process to manage the credentials on the secure elements remotely. Although mobile and IoT vertical domains share the same initial idea of multitenant secure element administration, different solutions should be used in each market segment, and cost-effective and straightforward secure element solutions are needed to make wide deployment possible.

4. Outlook and Future Work

In this section, we discuss current trends and future research and innovation directions for the surveyed areas of smart homes and grids. First of all, both smart homes and smart grids have become strong points of major innovation since they will benefit from the renewable energy sources (RES) revolution. They will also play a significant role in the advent of microgrids. We will elaborate on these topics in the following paragraphs. At the start, we provide an outlook on the new area of microgrids and then discuss further foreseen developments in our overviewed areas of smart homes and grids.

4.1. Microgrids

A microgrid is a decentralized group of electricity sources and loads that normally operates connected to a SG (or, more traditionally, a classic grid distribution infrastructure).

Microgrids can disconnect from the interconnected grid and function autonomously in “island mode” as technical or economic conditions dictate. In this way, microgrids improve the security of supply within the microgrid cell and supply emergency power, changing between the island and connected modes.

A microgrid can also use blockchain-related services to enable the “prosumer/consumer” mode. That means, in a nutshell, that each node/member from the microgrid could either generate/consume many energy services (energy). Blockchain is used in the microgrid scenario to exchange the remaining parts of the energy pool, called tokens. Each token represents an acceptable amount of energy that can be exchanged. We are currently working on these evolutions at the EU iDELTA project iDELTA: <http://idelta.eu> (accessed on 31 October 2021).

4.2. Smart Homes

While many works have been conducted on managing the buildings’ energy efficiency, still too few efforts have been dedicated to standardized accounting of the energy performance of buildings. Legislatively, the European directives on building energy state that the member states should apply national energy efficiency schemes for energy service providers, energy audits, and other energy-saving measures. There are efforts towards energy standards, where enterprises can certify themselves in one of the available certifications, such as EN ISO 14000—Energy Management Systems, EN 16247-1—Energy Audits, or EN ISO 14000—Environmental Management Systems. Yet, the semantic representation of various energy performance certificates (EPCs) and the context of their use is still lacking, as well as their practical deployment.

Smart home technology has also undergone a huge revolution in terms of the so-called “domotic technology” that was very much focused on how to coordinate a number of elements, belonging to the home atmosphere, which could be activated, deactivated, and regulated from a remote perspective.

The evolution of smart home technology has come to an impasse, with several proprietary platforms which compete to get market share in a crowded business space.

4.3. Smart Grids

Smart meters are electronic devices that record/measure customer consumption, and other parameters, in time intervals of an hour or less and send that information over a communications network to the utility for monitoring and billing.

It is important to highlight the difference between automatic meter reading (AMR) and advanced metering infrastructure (AMI). All AMI systems contain AMR functionality, but all AMR systems are not AMI systems. Because of the inherent differences in AMR and AMI, the data available from each system differentiates them. AMI differs from traditional automatic meter reading (AMR) in that it enables two-way communications with the meter and typically provides substantial information, including cumulative electric energy usage, daily electric energy usage, power peak demand, last interval demand, load profile, voltage value, voltage profile; phase information, outage counts, tamper notification, electric energy time-of-use (TOU), and power peak readings.

With AMI systems, nearly all this information is available in real-time and on-demand, allowing for improved operations and customer management. AMI systems can also be used to verify power outages and service restoration, perform remote-service disconnects and reconnects, allow automated net metering, transmit demand-response and load-management messages, interrogate and control distribution-automation equipment and facilitate prepaid metering.

AMI provides the data that can be handled through AI and big data techniques to smooth these uncertainties. In addition, demand response and pricing programs that can be implemented via AMI systems allow the utility and customers many options to manage their usage.

Smart meter equipment in Europe, but also at a worldwide level, is ever increasing. Therefore, the SG becomes a huge source of insights coming from the combination of trailblazing algorithms and interaction data.

Future work in energy markets is also about the sustainable energy research on green Hydrogen that the EU is powering through their Next Generation funding lines. Green Hydrogen joins the new technological challenge of producing and supplying hydrogen from clean energy sources. To do so, 100% renewable electricity must be used in the electrolysis process, thus responding to the electrification and decarbonization needs of sectors such as industry or heavy transport.

5. Conclusions

Many substantial improvements have been accomplished with regard to the SG and smart home infrastructure in the past years, e.g., operational improvements, energy management improvements (including the increasing the awareness of user energy consumption), improvements in the field of predictive analytics, improvements in the interaction between the consumer, the technical home pieces of equipment and the smart grid). Further developments in various areas are outlined in the Energies journal's recent special issue, "Energy Efficiency in Smart Homes and Smart Grids" [70]. Based on this work, the conducted literature review, and our project experiences, we have described this field.

Security remains a major concern for smart grid and smart home systems, and will require special attention in future developments. Some security aspects that should be improved are secure communication among the smart grid actors, secure credentials and sensitive data storage, improvement of the security architecture (including secure communication protocols), and the safety of the technical devices. We also expect many further developments stemming from the fact that more and more data in the addressed areas will become available, such as the deployment of more intelligent systems on all levels and also ability to simulate and predict the smart grid and home environments, for which there is still not enough data. The trend towards decentralization will continue, including the evolution of the current developments in the area of blockchain, as well as developments in the new area of microgrids. Also, further combination and interoperation

with other areas, e.g., manufacturing, logistics, and health are expected, as is the appearance of new corresponding scenarios.

Author Contributions: Conceptualization, L.P.G., A.F. and J.M.G.B.; methodology, A.F.; formal analysis, L.P.G., A.F.; investigation, L.P.G., A.F., A.P.; writing—original draft preparation, L.P.G., A.F., A.P.; writing—review and editing, L.P.G., A.F., A.P., A.d.A.S.; visualization, L.P.G.; supervision, A.F.; project administration, A.F.; funding acquisition, A.F., J.M.G.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research was co-funded by Interreg Österreich-Bayern 2014–2020 programme project KI-Net: Bausteine für KI-basierte Optimierungen in der industriellen Fertigung (AB 292). This work is also supported by the ITEA3 OPTIMUM project and ITEA3 SCRATCH project, all of them funded by the Centro Tecnológico de Desarrollo Industrial (CDTI), Spain.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

Abbreviations

ADS	Anomaly Detector Systems
AI	Artificial Intelligence
AMI	Automated Metering Infrastructure
CPS	Cyber-Physical System
DMZ	Demilitarized Zone
HAN	Home Area Network
ICAS	Industrial Automation and Control Systems
ICT	Information and Communication Technologies
IDS	Intrusion Detection System
IED	Intelligent Electronic Device
IoT	Internet of Things
IS	Information Security
IT	Information Technologies
M2M	Machine-to-Machine
NAN	Neighborhood Area Network
OMS	Outage Management System
OT	Operational Technologies
PLC	Power Line Carrier
SCADA	Supervisory Control and Data Acquisition
SG	Smart Grid
SGAM	Smart Grid Architecture Model
WAN	Wide Area Network

References

1. Khan, B.; Getachew, H.; Alhelou, H.H. 17-Components of the smart-grid system. In *Solving Urban Infrastructure Problems Using Smart City Technologies*; Vacca, J.R., Ed.; Elsevier: Amsterdam, The Netherlands, 2021; pp. 385–397. ISBN 978-0-12-816816-5.
2. Bigerna, S.; Bollino, C.A.; Micheli, S. Socio-economic acceptability for smart grid development—A comprehensive review. *J. Clean. Prod.* **2016**, *131*, 399–409. [[CrossRef](#)]
3. Chen, Z.; An, H.; Sun, Z.; Cen, B.; Li, S. Comprehensive Evaluation of Smart Grid Development Level Under Electricity Market Layout. *E3S Web Conf.* **2018**, *53*, 02013. [[CrossRef](#)]
4. Nafi, N.S.; Ahmed, K.; Gregory, M.A.; Datta, M. A survey of smart grid architectures, applications, benefits and standardization. *J. Netw. Comput. Appl.* **2016**, *76*, 23–36. [[CrossRef](#)]
5. Han, W.; Xiao, Y. Edge computing enabled non-technical loss fraud detection for big data security analytic in Smart Grid. *J. Ambient. Intell. Humaniz. Comput.* **2020**, *11*, 1697–1708. [[CrossRef](#)]
6. Hasan, M.; Toma, R.N.; Nahid, A.-A.; Islam, M.; Kim, J.-M. Electricity theft detection in smart grid systems: A CNN-LSTM based approach. *Energies* **2019**, *12*, 3310. [[CrossRef](#)]

7. Samudrala, A.N.; Amini, M.H.; Kar, S.; Blum, R.S. Distributed outage detection in power distribution networks. *IEEE Trans. Smart Grid* **2020**, *11*, 5124–5137. [[CrossRef](#)]
8. Yuan, Y.; Dehghanpour, K.; Bu, F.; Wang, Z. Outage Detection in Partially Observable Distribution Systems using Smart Meters and Generative Adversarial Networks. *IEEE Trans. Smart Grid* **2020**, *11*, 5418–5430. [[CrossRef](#)]
9. Chhaya, L.; Sharma, P.; Kumar, A.; Bhagwatikar, G. Cybersecurity for Smart Grid: Threats, Solutions and Standardization. In *Advances in Greener Energy Technologies*; Springer: New York, NY, USA, 2020; pp. 17–29.
10. Gunduz, M.Z.; Das, R. Cyber-security on smart grid: Threats and potential solutions. *Comput. Netw.* **2020**, *169*, 107094. [[CrossRef](#)]
11. Marksteiner, S.; Vallant, H.; Nahrgang, K. Cyber security requirements engineering for low-voltage distribution smart grid architectures using threat modeling. *J. Inf. Secur. Appl.* **2019**, *49*, 102389. [[CrossRef](#)]
12. Lamba, V.; Šimková, N.; Rossi, B. Recommendations for smart grid security risk management. *Cyber-Phys. Syst.* **2019**, *5*, 92–118. [[CrossRef](#)]
13. Yekini, T.A.; Jaafar, F.; Zavorsky, P. Study of trust at device level of the internet of things architecture. In Proceedings of the 2019 IEEE 19th International Symposium on High Assurance Systems Engineering (HASE), Hangzhou, China, 3–5 January 2019; pp. 150–155.
14. Naseer, O.; Ullah, S.; Anjum, L. Blockchain-Based Decentralized Lightweight Control Access Scheme for Smart Grids. *Arab. J. Sci. Eng.* **2021**, *46*, 8233–8243. [[CrossRef](#)]
15. Khalid, R.; Samuel, O.; Javaid, N.; Aldegheshem, A.; Shafiq, M.; Alrajeh, N. A Secure Trust Method for Multi-Agent System in Smart Grids Using Blockchain. *IEEE Access* **2021**, *9*, 59848–59859. [[CrossRef](#)]
16. Hasankhani, A.; Mehdi Hakimi, S.; Bisheh-Niasar, M.; Shafie-khah, M.; Asadolahi, H. Blockchain technology in the future smart grids: A comprehensive review and frameworks. *Int. J. Electr. Power Energy Syst.* **2021**, *129*, 106811. [[CrossRef](#)]
17. Gough, D.; Oliver, S.; Thomas, J. *An Introduction to Systematic Reviews*; Sage: Thousand Oaks, CA, USA, 2017.
18. Toma, R.N.; Hasan, M.N.; Nahid, A.-A.; Li, B. Electricity theft detection to reduce non-technical loss using support vector machine in smart grid. In Proceedings of the 2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT), Dhaka, Bangladesh, 3–5 May 2019; pp. 1–6.
19. Abdulrahman Okino Otuoze, M.W.M.; Sofimieari, I.E.; Dobi, A.M.; Sule, A.H.; Abioye, A.E.; Saeed, M.S. Electricity theft detection framework based on universal prediction algorithm. *Indones. J. Electr. Eng. Comput. Sci.* **2019**, *15*, 758–768. [[CrossRef](#)]
20. Jindal, A.; Schaeffer-Filho, A.; Marnerides, A.K.; Smith, P.; Mauthe, A.; Granville, L. Tackling energy theft in smart grids through data-driven analysis. In Proceedings of the 2020 International Conference on Computing, Networking and Communications (ICNC), Big Island, HI, USA, 17–20 February 2020; pp. 410–414.
21. Punmiya, R.; Choe, S. Energy theft detection using gradient boosting theft detector with feature engineering-based preprocessing. *IEEE Trans. Smart Grid* **2019**, *10*, 2326–2329. [[CrossRef](#)]
22. 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*, 7659–7669. [[CrossRef](#)]
23. Kement, C.E.; Gultekin, H.; Tavli, B. A Holistic Analysis of Privacy Aware Smart Grid Demand Response. *IEEE Trans. Ind. Electron.* **2020**, *68*, 7631–7641. [[CrossRef](#)]
24. Aydeger, A.; Saputro, N.; Akkaya, K.; Uluagac, S. SDN-enabled recovery for Smart Grid teleprotection applications in post-disaster scenarios. *J. Netw. Comput. Appl.* **2019**, *138*, 39–50. [[CrossRef](#)]
25. Singh, N.K.; Mahajan, V. Smart Grid: Cyber Attack Identification And Recovery Approach. In Proceedings of the 2019 2nd International Conference on Innovations in Electronics, Signal Processing and Communication (IESC), Shillong, India, 1–2 March 2019; pp. 1–5.
26. Haggi, H.; Song, M.; Sun, W. A Review of Smart Grid Restoration to Enhance Cyber-Physical System Resilience. In Proceedings of the 2019 IEEE Innovative Smart Grid Technologies-Asia (ISGT Asia), Chengdu, China, 21–24 May 2019; pp. 4008–4013.
27. Mohamed, A.; Refaat, S.S.; Abu-Rub, H. A review on big data management and decision-making in smart grid. *Power Electron. Drives* **2019**, *4*, 1–13. [[CrossRef](#)]
28. Mishra, S.; Glaws, A.; Palanisamy, P. Predictive Analytics in Future Power Systems: A Panorama and State-Of-The-Art of Deep Learning Applications. In *Optimization, Learning, and Control for Interdependent Complex Networks*; Springer: New York, NY, USA, 2020; pp. 147–182.
29. Kabir, E.; Guikema, S.D.; Quiring, S.M. Predicting thunderstorm-induced power outages to support utility restoration. *IEEE Trans. Power Syst.* **2019**, *34*, 4370–4381. [[CrossRef](#)]
30. Kumar, P.; Lin, Y.; Bai, G.; Paverd, A.; Dong, J.S.; Martin, A. Smart grid metering networks: A survey on security, privacy and open research issues. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2886–2927. [[CrossRef](#)]
31. Musleh, A.S.; Yao, G.; Muyeen, S. Blockchain applications in smart grid—review and frameworks. *IEEE Access* **2019**, *7*, 86746–86757. [[CrossRef](#)]
32. Alladi, T.; Chamola, V.; Rodrigues, J.J.P.C.; Kozlov, S.A. Blockchain in Smart Grids: A Review on Different Use Cases. *Sensors* **2019**, *19*, 4862. [[CrossRef](#)]
33. Jow, J.; Xiao, Y.; Han, W. A survey of intrusion detection systems in smart grid. *Int. J. Sens. Netw.* **2017**, *23*, 170–186. [[CrossRef](#)]
34. Ferrag, M.A.; Maglaras, L. DeepCoin: A Novel Deep Learning and Blockchain-Based Energy Exchange Framework for Smart Grids. *IEEE Trans. Eng. Manag.* **2020**, *67*, 1285–1297. [[CrossRef](#)]

35. Karimipour, H.; Geris, S.; Dehghantanha, A.; Leung, H. Intelligent anomaly detection for large-scale smart grids. In Proceedings of the 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), Edmonton, AB, Canada, 5–8 May 2019; pp. 1–4.
36. Rossi, B.; Chren, S.; Buhnova, B.; Pitner, T. Anomaly detection in smart grid data: An experience report. In Proceedings of the 2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Budapest, Hungary, 9–12 October 2016; pp. 002313–002318.
37. Karimipour, H.; Dehghantanha, A.; Parizi, R.M.; Choo, K.-K.R.; Leung, H. A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids. *IEEE Access* **2019**, *7*, 80778–80788. [\[CrossRef\]](#)
38. do Prado, J.C.; Qiao, W.; Qu, L.; Agüero, J.R. The next-generation retail electricity market in the context of distributed energy resources: Vision and integrating framework. *Energies* **2019**, *12*, 491. [\[CrossRef\]](#)
39. Sayed, K.; Gabbar, H.A. SCADA and smart energy grid control automation. In *Smart Energy Grid Engineering*; Elsevier: Amsterdam, The Netherlands, 2017; pp. 481–514.
40. CEN-CENELEC-ETSI. *Smart Grid Coordination Group Smart Grid Reference Architecture*; European Commission: Luxembourg, 2012.
41. Sreekumar, S.; Kumar, D.S.; Savier, J. A Case Study on Self Healing of Smart Grid with Islanding and Inverter Volt-VAR function. *IEEE Trans. Ind. Appl.* **2020**, *56*, 5408–5416.
42. Tsitaitse, T.J.; Cai, Y.; Ditta, A. Secure self-healing group key distribution scheme with constant storage for SCADA systems in smart grid. *Wirel. Pers. Commun.* **2018**, *101*, 1749–1763. [\[CrossRef\]](#)
43. Marikyan, D.; Papagiannidis, S.; Alamanos, E. A systematic review of the smart home literature: A user perspective. *Technol. Forecast. Soc. Chang.* **2019**, *138*, 139–154. [\[CrossRef\]](#)
44. Mahmud, S.; Ahmed, S.; Shikder, K. A smart home automation and metering system using internet of things (IoT). In Proceedings of the 2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST), Dhaka, Bangladesh, 10–12 January 2019; pp. 451–454.
45. Harsha, S.S.; Reddy, S.C.; Mary, S.P. Enhanced home automation system using Internet of Things. In Proceedings of the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 10–11 February 2017; pp. 89–93.
46. The European Parliament and the Council of the European Union. *Directive 2012/27/EU of the European Parliament and of the Council of 25 October 2012 on Energy Efficiency, Amending Directives 2009/125/EC and 2010/30/EU and Repealing Directives 2004/8/EC and 2006/32/EC Text. with EEA Relevance*; Office Journal 315; European Union: Maastricht, The Netherlands, 2012.
47. Spencer, R. 5 Ways the Internet of Things Could Help Combat Climate Change. Available online: <https://www.lanner-america.com/blog/5-ways-internet-things-help-combat-climate-change/> (accessed on 1 October 2020).
48. Dobler, C.; Pfeifer, D.; Streicher, W. Reaching energy autonomy in a medium-sized city—three scenarios to model possible future energy developments in the residential building sector. *Sustain. Dev.* **2018**, *26*, 859–869. [\[CrossRef\]](#)
49. Tomic, S.; Fensel, A.; Pellegrini, T. Sesame demonstrator: Ontologies, services and policies for energy efficiency. In Proceedings of the 6th International Conference on Semantic Systems, Graz, Austria, 1–3 September 2010; pp. 1–4.
50. Tomic, S.; Fensel, A.; Schwanzer, M.; Veljovic, M.K.; Stefanovic, M. Semantics for energy efficiency in smart home environments. In *Applied Semantic Web Technologies*; Taylor & Francis Group: New York, NY, USA, 2012; pp. 429–454.
51. H2020 ENTROPY | Smartcities Information System. Available online: <https://smartcities-infosystem.eu/sites-projects/projects/entropy> (accessed on 2 October 2020).
52. Fotopoulou, E.; Zafeiropoulos, A.; Terroso-Sáenz, F.; Şimşek, U.; González-Vidal, A.; Tsiolis, G.; Gouvas, P.; Liapis, P.; Fensel, A.; Skarmeta, A. Providing personalized energy management and awareness services for energy efficiency in smart buildings. *Sensors* **2017**, *17*, 2054. [\[CrossRef\]](#)
53. Kapourani, B.; Fotopoulou, E.; Paspaspyros, D.; Zafeiropoulos, A.; Mouzakitis, S.; Koussouris, S. Propelling SMEs business intelligence through linked data production and consumption. In Proceedings of the OTM Confederated International Conferences “On the Move to Meaningful Internet Systems”, Rhodes, Greece, 21–25 October 2015; pp. 107–116.
54. JSON-LD 1.0. Available online: <https://www.w3.org/TR/json-ld/> (accessed on 3 December 2016).
55. Drools—Business Rules Management System (Java™, Open Source). Available online: <https://www.drools.org/> (accessed on 2 October 2020).
56. González-Vidal, A.; Ramallo-González, A.P.; Terroso-Sáenz, F.; Skarmeta, A. Data driven modeling for energy consumption prediction in smart buildings. In Proceedings of the 2017 IEEE International Conference on Big Data (Big Data), Boston, MA, USA, 11–14 December 2017; pp. 4562–4569.
57. Krebs, B. Smart Meters—Krebs on Security. Available online: <https://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/> (accessed on 2 October 2020).
58. Han, W.; Xiao, Y. Non-technical loss fraud in advanced metering infrastructure in smart grid. In Proceedings of the International Conference on Cloud Computing and Security, Nanjing, China, 29–31 July 2016; pp. 163–172.
59. Han, W.; Xiao, Y. A novel detector to detect colluded non-technical loss frauds in smart grid. *Comput. Netw.* **2017**, *117*, 19–31. [\[CrossRef\]](#)
60. Buzau, M.M.; Tejedor-Aguilera, J.; Cruz-Romero, P.; Gómez-Expósito, A. Detection of non-technical losses using smart meter data and supervised learning. *IEEE Trans. Smart Grid* **2018**, *10*, 2661–2670. [\[CrossRef\]](#)

61. He, H.; Yan, J. Cyber-physical attacks and defences in the smart grid: A survey. *IET Cyber-Phys. Syst. Theory Appl.* **2016**, *1*, 13–27. [[CrossRef](#)]
62. Ghansah, I. *Smart Grid Cyber Security Potential Threats, Vulnerabilities and Risks: Interim Project Report*; California Energy Commission: Sacramento, CA, USA, 2012.
63. Pillitteri, V.Y.; Brewer, T.L. *Guidelines for Smart Grid Cybersecurity*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2014.
64. European Commission Smart Grids Task Force. Available online: https://ec.europa.eu/energy/topics/markets-and-consumers/smart-grids-and-meters/smart-grids-task-force_en (accessed on 2 October 2020).
65. Kovacs, E.; Bauer, M.; Kim, J.; Yun, J.; Le Gall, F.; Zhao, M. Standards-based worldwide semantic interoperability for IoT. *IEEE Commun. Mag.* **2016**, *54*, 40–46. [[CrossRef](#)]
66. Fortino, G.; Savaglio, C.; Palau, C.E.; de Puga, J.S.; Ganzha, M.; Paprzycki, M.; Montesinos, M.; Liotta, A.; Llop, M. Towards multi-layer interoperability of heterogeneous IoT platforms: The INTER-IoT approach. In *Integration, Interconnection, and Interoperability of IoT Systems*; Springer: New York, NY, USA, 2018; pp. 199–232.
67. Tuna, G.; Kogias, D.G.; Gungor, V.C.; Gezer, C.; Taşkın, E.; Ayday, E. A survey on information security threats and solutions for Machine to Machine (M2M) communications. *J. Parallel Distrib. Comput.* **2017**, *109*, 142–154. [[CrossRef](#)]
68. Odelu, V.; Das, A.K.; Wazid, M.; Conti, M. Provably secure authenticated key agreement scheme for smart grid. *IEEE Trans. Smart Grid* **2016**, *9*, 1900–1910. [[CrossRef](#)]
69. Zhang, H.; Wang, J.; Ding, Y. Blockchain-based decentralized and secure keyless signature scheme for smart grid. *Energy* **2019**, *180*, 955–967. [[CrossRef](#)]
70. Fensel, A.; Gómez Berbís, J.M. Energy Efficiency in Smart Homes and Smart Grids. *Energies* **2021**, *14*, 2054. [[CrossRef](#)]