





Review

A Survey on IoT-Enabled Smart Grids: Emerging, Applications, Challenges, and Outlook

Arman Goudarzi ^{1,*} , Farzad Ghayoor ² , Muhammad Waseem ³ , Shah Fahad ⁴  and Issa Traore ¹¹ Department of Electrical and Computer Engineering, University of Victoria, Victoria, BC V8P 5C2, Canada² Discipline of Electrical, Electronics and Computer Engineering, University of KwaZulu-Natal, Durban 4001, South Africa³ School of Electrical Engineering, Zhejiang University, Hangzhou 310027, China⁴ Department of Electrical and Computer Engineering, Missouri University of Science and Technology, Rolla, MO 65409, USA

* Correspondence: agoudarzi@uvic.ca

Abstract: Swift population growth and rising demand for energy in the 21st century have resulted in considerable efforts to make the electrical grid more intelligent and responsive to accommodate consumers' needs better while enhancing the reliability and efficiency of modern power systems. Internet of Things (IoT) has appeared as one of the enabling technologies for smart energy grids by delivering abundant cutting-edge solutions in various domains, including critical infrastructures. As IoT-enabled devices continue to flourish, one of the major challenges is security issues, since IoT devices are connected through the Internet, thus making the smart grids vulnerable to a diverse range of cyberattacks. Given the possible cascading consequences of shutting down a power system, a cyberattack on a smart grid would have disastrous implications for the stability of all grid-connected infrastructures. Most of the gadgets in our homes, workplaces, hospitals, and on trains require electricity to run. Therefore, the entire grid is subject to cyberattacks when a single device is hacked. Such attacks on power supplies may bring entire cities to a standstill, resulting in massive economic losses. As a result, security is an important element to address before the large-scale deployment of IoT-based devices in energy systems. In this report, first, we review the architecture and infrastructure of IoT-enabled smart grids; then, we focus on major challenges and security issues regarding their implementation. Lastly, as the main outcome of this study, we highlight the advanced solutions and technologies that can help IoT-enabled smart grids be more resilient and secure in overcoming existing cyber and physical attacks. In this regard, in the future, the broad implementation of cutting-edge secure and data transmission systems based on blockchain techniques is necessary to safeguard the entire electrical grid against cyber-physical adversaries.

Keywords: smart grid; Internet of Things (IoT); cybersecurity strategies; cyber-physical power system (CPPS); 5G wireless telecommunication; smart meters; blockchain



Citation: Goudarzi, A.; Ghayoor, F.; Waseem, M.; Fahad, S.; Traore, I. A Survey on IoT-Enabled Smart Grids: Emerging, Applications, Challenges, and Outlook. *Energies* **2022**, *15*, 6984. <https://doi.org/10.3390/en15196984>

Academic Editors: Wenjian Yang and Huawei Chang

Received: 25 August 2022

Accepted: 20 September 2022

Published: 23 September 2022

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



Copyright: © 2022 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

1.1. Emerging Smart Grids

With the expansion of cities and proliferation of the population, the need for a flexible and intelligent type of electrical grid that could accommodate the diverse demand of different customers has increased. In 2007, the National Institute of Standards and Technology (NIST) proposed a framework for the future electrical grid to guarantee the reliable, scalable, secure, interoperable, and manageable operation of electrical grids while being cost-effective [1]. Figure 1 shows the evolution of electrical grids toward the future grid, known as the smart grid system.

In a smart grid system, renewable energy resources such as wind, solar, and power storage units are integrated into the grid system. These new power generation technologies, which may be smaller, more widely distributed, and more ecologically friendly, could

preserve grid resilience and disperse overload centers [2]. The smart grid employs a widespread sensor network supported by a two-way communication system for constant monitoring of the grid status. The bidirectional communication network allows the exchange of measurement data and control signals between grid entities, improving the grid and user asset monitoring and management. Moreover, to process the collected data within the required time frames, the smart grid should be supported by sufficient computational resources. The control and monitoring are conducted in a more distributed way, as the volume of the collected data is enormous, and the sensors are dispersed across the entire grid.

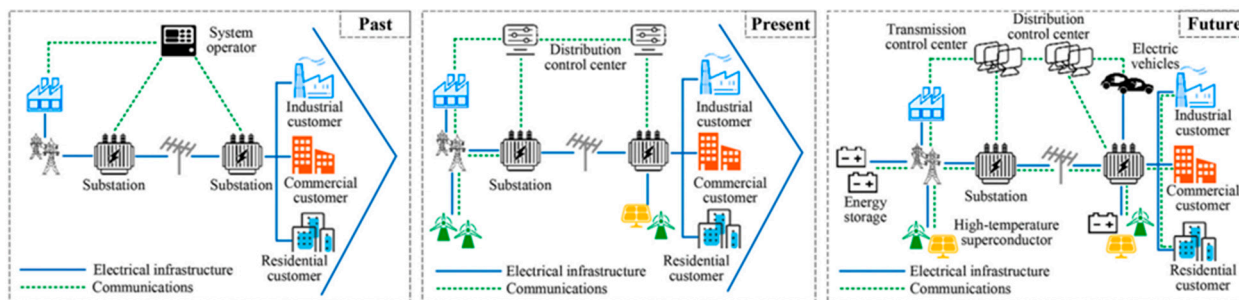


Figure 1. Evolution of electrical grids—from traditional grids to smart grids [2].

As a result of such capabilities, the smart grid can manage the supply–demand balance of energy more effectively, securely, and reliably. Moreover, the smart grid can be considered an enabler for the realization of smart homes and electric transportation, providing a platform for customers’ participation with utility companies and helping reduce carbon emissions. The merits of smart grids in comparison to traditional electrical grids are presented in Table 1 [3,4]. However, these advantages would be obtained at the cost of increasing the grid’s complexity and infrastructure, which demands an ongoing effort to overcome challenges using emerging technologies and solutions [5,6].

Table 1. Advantages of smart grids over traditional grids.

Features	Traditional Grid	Smart Grid
Communication	One-way communication	Two-way communication with interaction
Power generation	Centralized	Distributed generation, provides support during peak hours when load demand increases
Topology	Radial	Different network topology
Operation and maintenance	Manual monitoring, periodic equipment maintenance	Real-time monitoring, prognostic, and event-driven maintenance
Power restoration	Manual equipment checks and time-based maintenance	Self-healing; smart grid can anticipate, identify, and respond to faults and outages
Reliability	Prone to failure and cascading outages	Pro-active, real-time, and islanding
Metering	Electro-mechanical	Advanced metering arrangement that drives the facility to track and regulate energy consumption
Customer participation	Limited interaction or none	Extensive interaction
Power quality control	Less use of sensors and less power quality	Contains numerous modules, for example, sensors, smart meters, and technologies on the distribution grid that aid in managing the parameters, such as voltage and power factor, to improve the power quality
Renewable power source integration	Optimized for non-renewable resources	Offers essential insights and enables automation for renewable power resources to supply electricity to grids while their management is being optimized
Operational cost and wastage at peak hour	High at peak hours	Low at peak hour due to distributed generation and control over the power consumption

1.2. Rise of Internet of Things (IoT) Devices in Smart Grids

One of the cutting-edge solutions in the field of telecommunication is the Internet-of-Things (IoT) concept. The IoT is generally considered a network of devices embedded with electronics, software, sensors, and actuators capable of exchanging information through communication networks, such as the Internet. The IoT supports bidirectional communications and distributed computational capabilities, so it can be considered a potential solution to address inescapable difficulties in transitioning traditional energy networks into updated smart grid systems [7,8].

In a smart grid environment, services such as large-scale integration of distributed renewable energy resources, the establishment of live, real-time data communication between consumers and service providers regarding tariff information and energy consumption, and infrastructure to collect and transfer statistics of the grid's parameters for analysis, and mechanisms to implement necessary actions based on such analyses are required [9]. For intelligent decision-making, the smart energy grid creates a large amount of data and information that have to be transported, processed, and stored [10]. In this regard, the IoT, considering its multifaceted benefits in numerous industries, appears to be a suitable solution with significant potential to be used in the smart energy grid system. In addition to the increased accuracy and competency that can be added to the system through the IoT's intelligent and proactive features, the IoT can assist in a smooth transformation of the legacy power grid into a smart energy system that would be more efficient [11].

The main concerns in a traditional power grid system are power quality and dependability, both of which may be addressed with the help of the IoT as it offers better control of these issues. By introducing intelligent information-processing features during the electricity flow between the service provider and consumers, advanced metering infrastructure (AMI) assisted by smart metering (SM) technologies can facilitate the transformation of a conventional power grid system into a smart grid system [12]. Through the combination of sensing and actuation systems in the AMI, the IoT offers significant potential for optimizing and regulating energy use. This integrated system collects a massive quantity of data and information from many parts of the grid system, including energy usage, voltage readings, current readings, and phase measurements. Cutting-edge IoT technology can collect large amounts of data and transmit and analyze them intelligently, allowing for better energy grid management [13]. Power generation infrastructure management, supervisory control, and data acquisition (SCADA) connected systems for managing transmission and distribution operations, advanced metering infrastructure, and carbon footprint and environmental monitoring are all examples of areas where IoT technologies can have a significant impact on smart energy grid systems. Advanced cloud and edge computing technologies can enable distributed monitoring and management of dispersed energy resources, and provide answers to the old centralized SCADA system's cyber vulnerabilities [14].

Moreover, the IoT-enabled smart grid can operate and manage the electrical grid more efficiently as it can seamlessly be integrated with other smart entities, such as smart appliances, smart homes, smart buildings, and smart cities, to access and control more devices over the Internet. However, this requires using more advanced computational capabilities and resource-allocation mechanisms. Despite gaining more efficiency in monitoring and operation of the energy system, the IoT-enabled smart grid implementation comes with a set of obstacles. For instance, IoT cyber adversaries can impose smart grids onto several attacks that can be classified into three main categories: operational, economic, and system security. Several examples of these damages are listed as follows [15,16]:

- Localized and large-scale power outages.
- Significant business loss to the utilities and electricity markets.
- Social security threats to customers by publicizing their information.
- Manipulation of energy consumption records.
- Interrupting the process of transactive energy systems.

To counterattack the aforementioned challenges, several technologies, such as machine learning methods, artificial intelligence (AI), blockchain, and multifactor authentication systems, have been developed [17].

1.3. Motivational Factors and Contributions

The latest improvements in IoT-enabled smart grids and energy systems inspired this survey. The IoT offers the structure and protocols for the smart system's sensing, actuation, communication, and processing technologies. Moreover, the fast growth of technology in several IoT industries has created new prospects for developing smart grids smoothly. This paper will aid potential researchers, industrial experts, and stakeholders in comprehending the architecture of an IoT-enabled smart grid system. It will also familiarize readers with different applications of IoT technologies, security vulnerabilities, and mitigation strategies to maintain the safe operation of smart energy systems. In this regard, the key contributions of the study are as follows:

- The concept of an IoT-enabled smart grid and recent practical advances are investigated, especially the application, challenges, and opportunities of communication technologies in modern power systems.
- The study examines the use of 5G-based IoT technologies for smart grids, considering the technology's fast data transfer speed for remote control, strong security for preserving customer privacy, and high dependability for guaranteeing smart grid efficacy.
- This study investigated and classified energy grid IoT security vulnerabilities, and it also included mitigating strategies. We concentrated on how a cyber adversary might take advantage of vulnerabilities in IoT systems and conduct malicious attacks that could jeopardize the security of the IoT energy system. Energy theft in smart meter data, injection attacks in IoT home automation systems, denial-of-service attacks on IoT data analytics, manipulation attacks on transactive energy systems and the electricity market, etc., are only a few of the threats that have been researched. Potential lightweight intrusion-detection technologies for IoT systems and prospective solutions to mitigate threat and device-level vulnerabilities have also been studied. Although they were not given much attention in the past, these issues will soon rank among the most important. Moreover, it is significant to mention that, to our knowledge, no study has ever conducted such a precise survey on the cybersecurity architecture of IoT-enabled smart grids.
- The study covered the potential for end-users of distributed ledger systems based on blockchain. The protection of data privacy during peer-to-peer energy trade and information exchange was also underlined. To examine the potential prospects and applications in an IoT context, emerging machine learning methods for IoT-enabled energy systems were also explored.
- A detailed future work recommendation is made to achieve the application of 5G-based IoT devices and their security protection equipment and software to smart grids. Future research also recommends several approaches to improve the effectiveness and dependability of IoT-enabled smart grids, including ubiquitous data acquisition, data visualization, real-time state awareness, intelligent distribution networks, precise load control, edge computing, network security, and new business models.

It is important to mention that, to further demonstrate this study's novel contributions, a comparison table is provided in the Appendix A as Table A1.

1.4. Paper Organization

The organization of this paper is as follows: Section 2 briefly explains the motivations behind the implementation of IoT-enabled smart grids, followed by the IoT technologies, architecture, and protocols, which are briefly described in Section 3. The applications and security aspects (including challenges and solutions) of IoT-enabled smart grids through several examples are presented in Sections 4 and 5, respectively. Ultimately, Section 6 provides conclusions on the findings of this survey.

2. Motivation behind Implementation of IoT-Enabled Smart Grids

The key features of IoT technology are depicted in Figure 2, showing its potential to provide an excellent solution to recent issues of transitioning a traditional electrical grid into a modernized smart grid. The adoption of IoT technology is growing in popularity for current smart grid applications in residential and commercial structures. The use of sensors and smart metering in a smart power grid would allow for more efficient operation at all levels of power generation, transmission, and distribution, resolving most of the industry's problems. It also has a smart option for real-time monitoring of power flow throughout the electrical grid [18]. The IoT, backed up by big data analysis, may help with critical power-source and end-user demand decisions [19]. On the same grounds, real-time insight analysis may influence the creation of new rules by policymakers and power-generating service providers to readily react to market fluctuations, which requires establishing a mechanism to raise or reduce output to increase energy efficiency. Furthermore, these technologies enable the effective analysis of the acquired data for future state estimation purposes. Furthermore, customers would be able to monitor real-time energy pricing and properly limit their power usage with the aid of mobile devices that are equipped with IoT technology [20].

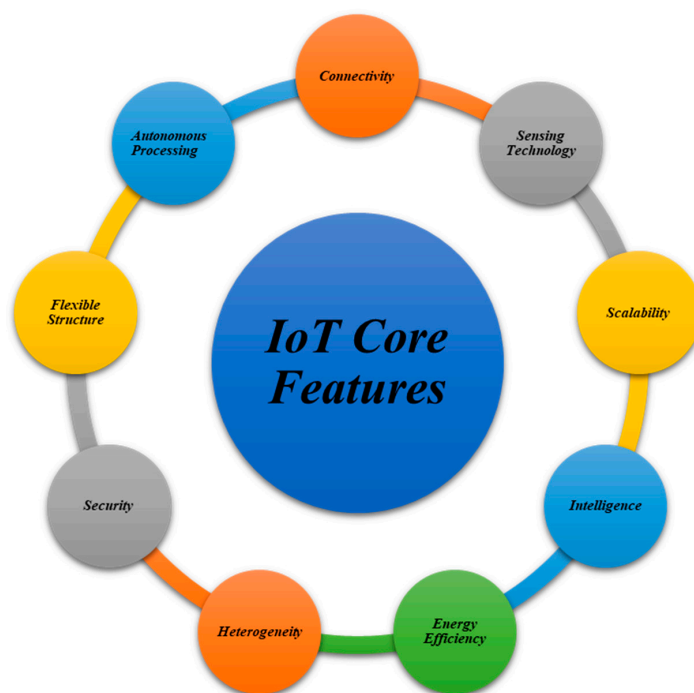


Figure 2. Key characteristics of IoT devices.

Several functionalities that IoT-enabled smart grids can achieve are listed below [21,22]:

- Self-healing capability enables grid operators to intelligently detect the exact location of faults while assessing their impacts on the entire grid and responding promptly.
- Large-scale integration of renewable energy resources.
- Further implementation of state estimation devices, phasor measurement units (PMUs), and smart devices (AI-enabled devices) to enhance the power quality, coordination monitoring, and resilience of smart grids.
- Providing an interactive platform for utility and consumers to exchange information instantly. Moreover, consumers would have control over their energy use and tariff selection based on the time-of-use (ToU).
- Providing operational and managerial services for real-time charging, such as vehicle-to-grid, vehicle-to-home, and home-to-grid (prosumers) solutions and easing additional growth of electrification levels.

- Avoiding/responding to most cyber and physical attacks by real-time monitoring of the grid components' behavior.

3. Description of IoT Technologies: Architecture and Protocols

3.1. Clearing the Confusion—IOE, IoT, and IoE

Before the commencement of this survey, it is necessary to clarify three terminologies that are frequently used in the literature: (1) Internet-of-Everything (IOE), (2) Internet-of-Things (IoT), and (3) Internet-of-Energy (IoE). The IOE, as shown in Figure 3, expresses a broad range of meanings, including the IoT. Nevertheless, the IoT and IoE have been used interchangeably on many occasions to convey similar conceptual ideas, yet hold their differences in terms of field applications. The IoE has a five-layered architecture with respect to its functionality: (1) infrastructure layer, (2) networking of energy internet, (3) energy router, (4) smart energy management system, and (5) smart terminals [23–25]. This study focuses on the IoT, which aids the efficient management of energy systems.

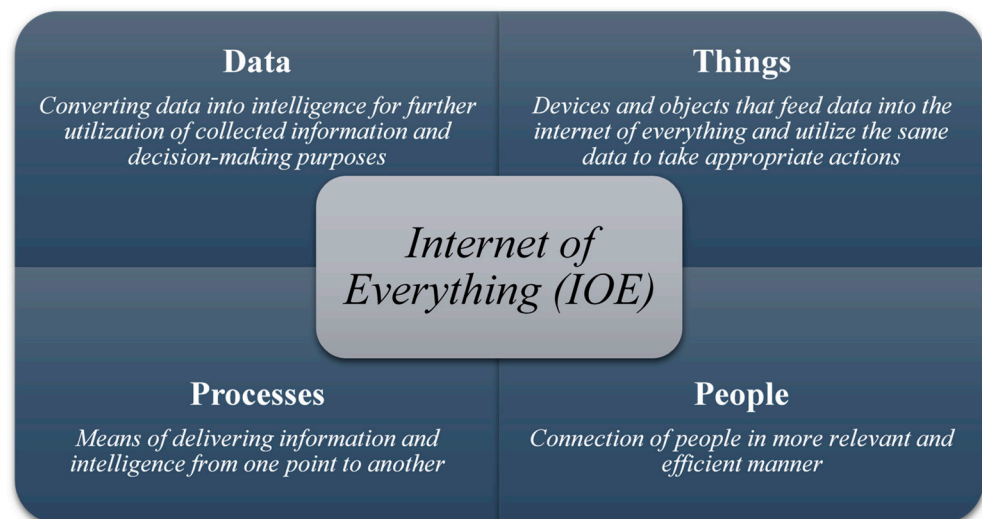


Figure 3. Categories of Internet of Everything (IOE).

3.2. Architecture of IoT Technologies

3.2.1. IoT Layered Slicing

The design of IoT-based systems is completely reliant on the operation of the associated components through the utilization of a variety of technologies in different locations. The architecture is often recognized based on a layer-by-layer articulation where each layer is assigned to a specific task that it must accomplish [26]. Figure 4 shows a four-layered design applicable to the integration of the IoT with the smart power grid, which is more important in terms of the IoT application and compliance with energy system regulations [27].

The four-layered IoT-enabled smart grid design includes [28]:

- (1) **Physical layer:** The physical layer is the foundation of the architecture of the IoT-enabled smart grid and includes the grid's physical facilities and executors. All distributed and decision-making instructions are carried out at this layer to provide the system's desired functionality. Additionally, the bidirectional energy flow between power generation, transmission, distribution, and customers happens inside this layer.
- (2) **Communication network layer:** The key layer of the IoT-enabled smart grid architecture is the communication network layer, which serves as a link between the lower physical and upper cyber layers. It covers the general activities of the information network, such as the interaction between electrical facilities and heterogeneous components and transferring the higher layer's control instructions and the lower layer's collected data.

- (3) Cyber layer: The cyber layer, or more accurately, the decision-making layer, is the core of the portrayed architecture, which comprises a cloud-based central processing mechanism and distributed computing intelligence to optimize both computing and control techniques. This decision-making layer serves as the system's executive brain, providing a human-computer interface to the top layer to enable it to coordinate all lower levels by developing and issuing suitable orders.
- (4) Application layer: The highest level of decision-making layer is the application layer, also known as the management and control layer, which encompasses service providers, markets, and operations. To conduct power generation and consumption in the physical world, decision-makers analyze all concerns from the economic, social, and environmental viewpoints by considering market regulation, pricing, and incentive measures. The optimum operations are carried out based on two-way information and value flows between markets and service providers, which is a distinguishing feature of this layer.

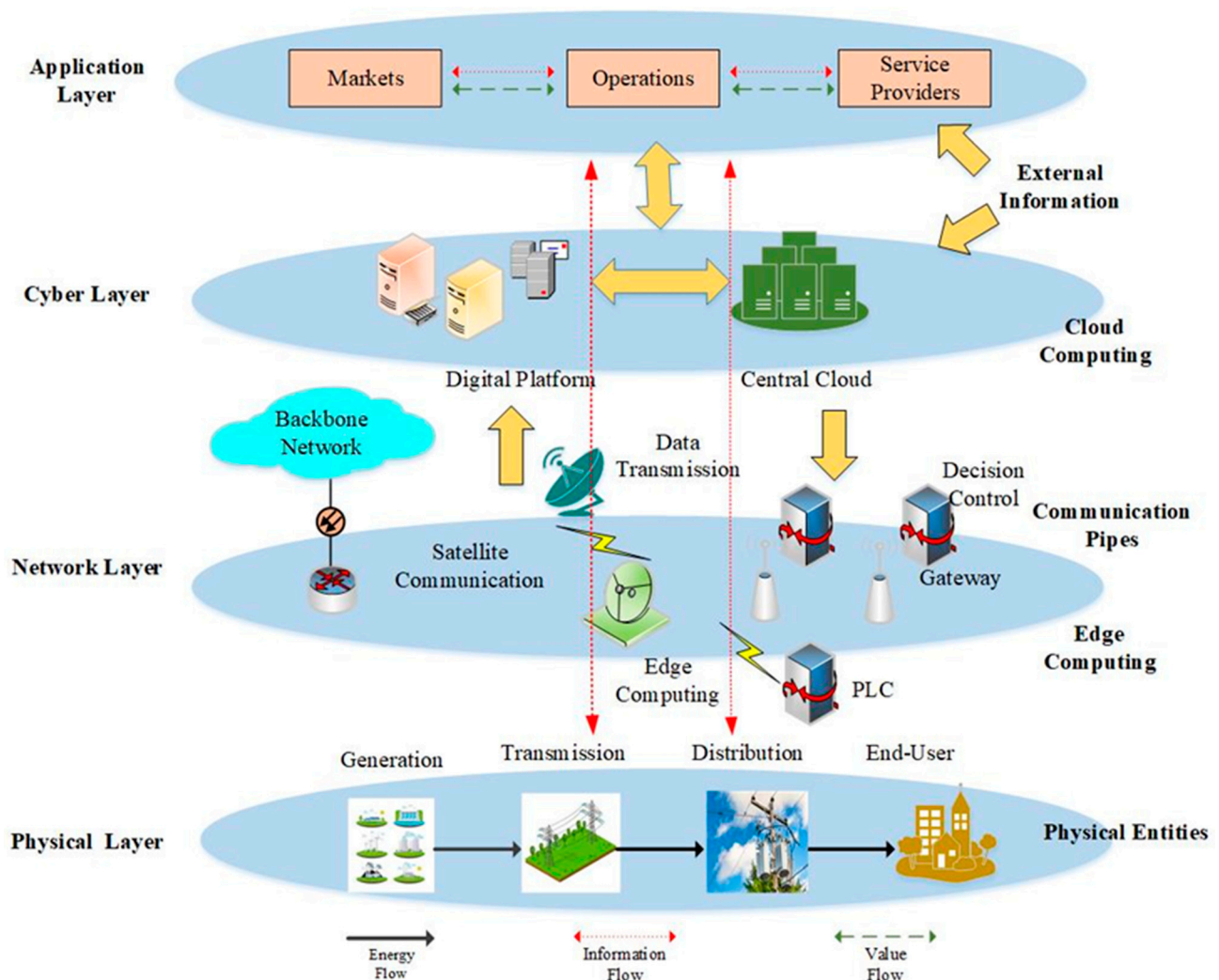


Figure 4. Four-layered architecture for the IoT-enabled smart grid.

3.2.2. IoTs, from the Perspective of Information and Communications Technology

The four enablers of information and communications technologies (ICTs) in the IoT-based smart grid architecture are cloud computing, communication network, edge computing, and physical entities [27]. Each of these components is explicitly defined below [29,30]:

- (1) Cloud computing: Cloud computing can handle big data's networking, storage, and computational needs and offers extensive application services. Cloud computing, with the help of virtualization technology, can combine hardware and software resources from several geographical areas to establish a virtual platform with powerful storage and processing capabilities. It is important to emphasize that cloud computing is critical for enabling common, suitable, and on-demand network access to a distributed group of configurable computing resources, which can be automatically provisioned and released with minimal effort on the part of service providers. The term "cloud" is often used to characterize data centers that are scattered across several geographic areas and can be made available to many customers over the Internet. Cloud computing allows large data storage and extremely dependable, scalable, and autonomous processing. Cloud services are used to aggregate data and information from various elements, such as sensors, appliances, and other devices. They also process and analyze the collected data and provide the results to consumers and service providers for more insights. Different features of cloud computing are shown in Figure 5 [31].
- (2) Communication network: Communication networks consist of data transmission links between the physical and cyber layers that connect user terminals, edge devices, and cloud computing resources to build the smart grid's omnipresent information network. Since each electrical service has unique communication, computation, and storage requirements, establishing specialized physical facilities for different types of applications in the IoT-enabled smart grid architecture is costly and may undermine grid connectivity and interoperability [32]. Therefore, the precise selection of communication technologies is an essential aspect of IoT-enabled smart energy grids. Tables 2 and 3 classify and compare the widely used wired and wireless communication network technologies in smart grid systems [33–37].
- (3) Edge computing: Edge computing refers to the deployment of distributed intelligent agents at the edges of the network and closer to IoT-enabled devices to provide computation, storage, and application services near data sources. Although cloud computing can provide the required computational capabilities to the smart grid, the central cloud is located at a large distance from the data source, resulting in lengthy latency. However, many electricity applications and services could benefit from offloading computational and storage tasks to the proximity of IoT-enabled devices, which results in much lower service response latency and a reduction in communication overhead and traffic load to the central network, and an improvement in context-awareness. The offloading of computational tasks to the embedded resources available on IoT devices is known as edge computing. However, for some applications, the computational power in embedded devices is not sufficient, and the latency of the cloud is intolerable, which brings in the necessity for a processing layer between the network's edges and the cloud, known as the fog server. Nevertheless, the computational capacity of fog servers is far less than that of cloud servers. To overcome this limitation, the architectural standard of multi-access edge computing (MEC) has been proposed for IoT applications, aiming to move cloud resources to the edge of a network. The edge computing classifications are depicted in Figure 6 [38,39]. Peak-load shifting and real-time load–demand balancing to provide optimal options for power generation scheduling are examples of using edge computing proposed in smart grid applications [40].
- (4) Physical entities: The term "physical entities" refers to different electrical components of the power grid, spread across the power grid as basic components of the power system, conducting distributed sensing, and acting. In the IoT-enabled smart grid, physical entities could benefit from AI methods to gain the ability to learn from their experiences and environments, react to new inputs and execute human-like activities. Moreover, through device-to-device (D2D) communication, neighboring entities can create direct communication among themselves, without using a third party, to exchange information directly [41].

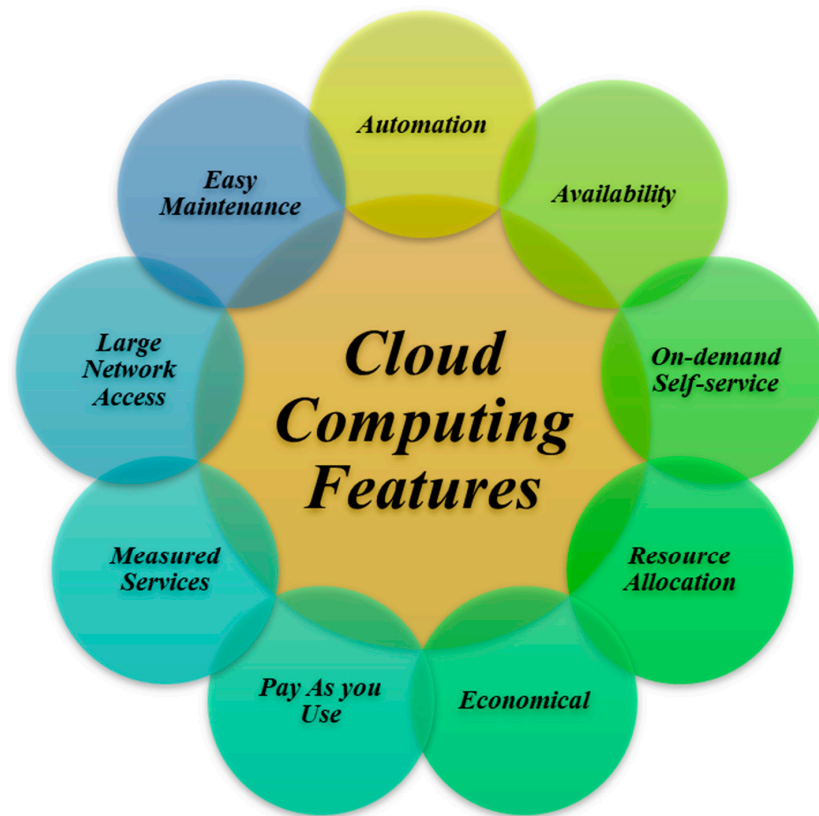


Figure 5. Cloud computing features.

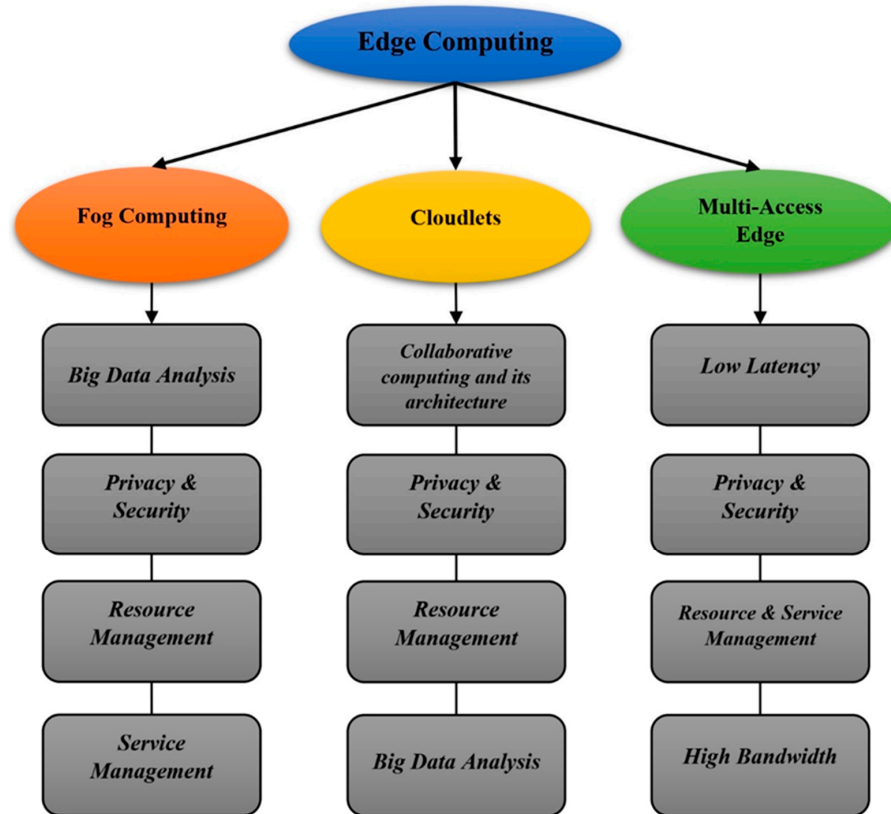


Figure 6. Edge computing classifications.

Table 2. Commonly used wireline communication technologies in smart grid systems.

Technology	Date Rate	Coverage	Application	Advantages	Disadvantages	Network Type
Ethernet	Up to 100 Gbps	Up to 100 m	In-home communication and backbone communication	Good for short distances	Coverage limitations	Premise Network, NAN, FAN, and WAN
Broadband PLC	Up to 300 Mbps	Up to 1500 m	SCADA and backbone communication in power generation sector	Existing infrastructure, standardized and high reliability	Noisy channel environment and disturbance	NAN, FAN, and WAN
Narrowband PLC	10–500 Kbps	Up to 3 km	SCADA and backbone communication in power generation sector	Existing infrastructure, standardized and high reliability	Noisy channel environment and disturbance	NAN, FAN and WAN
HomePlug	4, 5, and 10 Mbps	Up to 200 m	In-home communication and smart appliances	Low cost and energy	Coverage limitations and disturbance	Premise Network
Fiber Optic	Up to 100 Gbps	Up to 100 km	SCADA and backbone communication in power generation sector	High bandwidth, high data rate and not susceptible to electromagnetic interference	Costly	WAN

Table 3. Commonly used smart grid wireless communication technologies.

Technology	Date Rate	Coverage	Application	Advantages	Disadvantages	Network Type
WiMAX	75 Mbps	Up to 50 km	In-home communication and smart meter reading	Low cost and low energy	Not widespread, coverage highly reduced if loss in line of sight	NAN, FAN, and WAN
ZigBee	20–250 Kbps	Up to 100 m	In-home communication, energy monitoring, smart appliances, and home automation	Mesh capability, simplicity, mobility, low cost and energy	Low data rate, short range and poor interference	Premise Network, NAN, and FAN
Z-Wave	9–40 Kbps	Up to 30 m	Wireless mesh network	Mesh capability, simplicity, mobility, low cost and energy	Low data rate, short range and poor interference	Premise Network
Wi-Fi	2 Mbps–1.7 Gbps	Up to 100 m	In-home communication, smart appliances. Home automation and SCADA	Good for short distances	Security	Premise Network, NAN, and FAN
3G	Up to 42 Mbps	70 km	SCADA and smart meter reading	Already-existing network, high security, low cost, and large coverage	Network shared with customers may result in congestion	NAN, FAN, and WAN
4G/LTE	Up to 979 Mbps	Up to 16 km	SCADA and smart meter reading	Already-existing network, high security, low cost, and large coverage	Network shared with customers may result in congestion	NAN, FAN, and WAN
LTE-M	7 Mbps	Up to 10 km	Smart meter reading	Low cost and energy and scalability	Low data rate	NAN and FAN
NB-IoT	159 Kbps	Up to 10 km	Smart meter reading	Low cost and energy and scalability	Low data rate	NAN and FAN
5G	Up to 20 Gbps	Up to 500 m	SCADA, remote control and smart meter reading	Low energy, low latency, high data rate, and scalability	—	NAN, FAN, and WAN
Satellite	50 Mbps	—	Backup, remote location communication	Good when no other alternative is feasible	High cost	WAN

3.2.3. Operating Software for IoT Devices

The IoT consists of gateway nodes and end devices connected by various communication methods and controlled by microcontroller units (MCUs). The end devices in an IoT architecture take different forms, such as sensors, actuators, and switches, which can often execute a restricted range of actions. End-devices are usually compact, featuring a resource-constrained MCU (RAM, ROM, and energy), and can communicate via short-range low-power communication protocols [42]. The MCU firmware plays a vital part in IoT operations. It is now possible to install firmware that can perform more on the device itself and receive automatic security updates (OTA). This firmware can be a whole operating system (OS) that enhances the device's functionality and security. Because the resources of these end devices are still restricted, data must be gathered and transferred in real-time, with no buffering. These operating systems are referred to as real-time operating systems (RTOS). The usage of an RTOS also allows a programmer or system integrator to be more productive, as the OS provides access to the majority of low-level tasks [43].

Gateway devices, which operate as a bridge between various IoT devices, support communication protocols and have a greater capacity to capture and analyze data. When cloud services are part of a design, gateway devices, which reside at the junction between the external Internet and the internal local Intranet, are also known as edge gateways. Gateway devices require an operating system that can handle a variety of communications. They must also be secure and resistant to external cyberattacks. Unlike end devices, gateway devices typically provide a user interface for controlling various aspects of the network or visualizing data [43].

3.3. Standards and Protocols for IoT Technologies

The physical or data collection layer's standard is determined by the devices utilized in that layer. Since there are so many different types of sensors and device makers, international organizations such as the ISO, IEC, and IEEE have developed a multitude of standards. For instance, the following ISO standards are used for different RFID applications [4,44–46]:

- ISO 11784: regulation of data structure.
- ISO 15459: identification of transport product.
- ISO 18000: goods tracking systems.
- ISO 18047: equipment performance testing.
- ISO/IEC 18092: near-field communication (NFC).
- ISO/IEC 20248: fog and edge computing.
- ISO 29182: sensor network reference architecture (SNRA).
- ISO/IEC 30118: UPnP.

Additionally, the following IEEE standards are used in wireless communication technologies [46]:

- IEEE 802.15.4: communication standard.
- IEEE 802.15: short-range communication.
- IEEE 802.15.1: Bluetooth.
- IEEE 802.11., 802.11a, 802.11b, 802.11g, 802.11n, 802.11h, 802.11i, 802.11-2007, 802.11-2012, 802.11ac, 802.11ad, 802.11af, 802.11-2016, 802.11ah, 802.11ai, 802.11aj, 802.11aq, 802.11ax, 802.11ay: Wi-fi, Wi-Fi 4, Wi-Fi 5 and Wi-Fi 6.

4. Applications of IoT Technologies in Smart Energy Grids

Efficient management of the power generation sector, SCADA-connected transmission network, AMI in the distribution systems, emission gases monitoring, smart home, and building systems, and many other areas of energy systems have prospective uses for IoT technologies. As a cutting-edge IoT solution, fog computing opens a world of possibilities for improving and managing the SCADA-connected transmission network. Most smart home appliances have been completely automated in the past few years thanks to IoT

technologies. In this section, several solutions for smart grid applications that have been facilitated based on IoT technology are discussed.

4.1. Fog-Based Energy Grids through the Utilization of SCADA

SCADA systems are critical for regulating and monitoring electrical energy generation, transmission, and distribution. The SCADA system collects data and information from the energy systems, and oversees automation procedures to manage and regulate various system parameters to ensure that the operation continues smoothly. In recent years, with further accessibility of IoT solutions, such as fog computing, the operation of the SCADA system has become more efficient [47]. The architecture of a fog-based SCADA system for the energy grid is given in Table 4 [48].

Table 4. Fog-based SCADA system architecture.

Fog-Based SCADA Parts	Components	Connection Type	Tasks
Terminal devices	Sensors, actuators, and appliances	Wireless sensor network (WSN), Wi-Fi, Bluetooth, and ZigBee	Information collection
Fog computing devices	Switches, access points, firewalls, cloudlets, and routers	Local area networks (LANs) and wide area networks (WANs)	Analyze and process the collected data from terminal devices
Cloud systems	Cloud data centers, cloud storage, and gateway devices	Local area networks (LANs), wide area networks (WANs), virtual private networks (VPNs), and/or APIs	Aggregate and process the collected statistical information
SCADA systems	Field instrumentation, field controllers (RTUs/PLCs), and human-machine interfaces (HMIs)	Combinations of wired and wireless connections	Based on the collected results from the cloud, the system operator takes control decision and regulates different parameters of the energy grid

4.2. AMI-Connected Distribution Networks

AMI is an architecture for bidirectional, planned communication between customers' IP-based smart meters and the service provider. The goal of an AMI is to keep utility service providers informed about the real-time power consumption of power users. It is anticipated that, within the next 5 years, users should be able to make energy-efficient decisions based on real-time tariffs provided by the AMI system [49]. Through effective smart meter connections, IoT-based AMI offers considerable potential for optimizing and regulating the energy use of customers. AMI can be connected to a variety of appliances such as lights, fans, dishwashers, switches, power outlets, and geysers to collect and transfer real-time data to utility providers to support optimal energy management [50]. Figure 7 depicts different integration layers of IoT devices and their protocols in distribution networks [26].

4.3. IoT for Smart Meters

IoT technologies aid smart meters in managing homes, cities, and grids intelligently by collecting consumers' energy consumption in real time and transferring them to utility service providers for the optimal management of energy grids. Smart meters can be used to monitor the state of different parameters such as voltage readings, current readings, temperature, moisture status, and the capacity to alter those parameters, as well as energy usage, remotely [51]. Table 5 presents the advantages and disadvantages of using IoT-enabled smart meters [52–54].

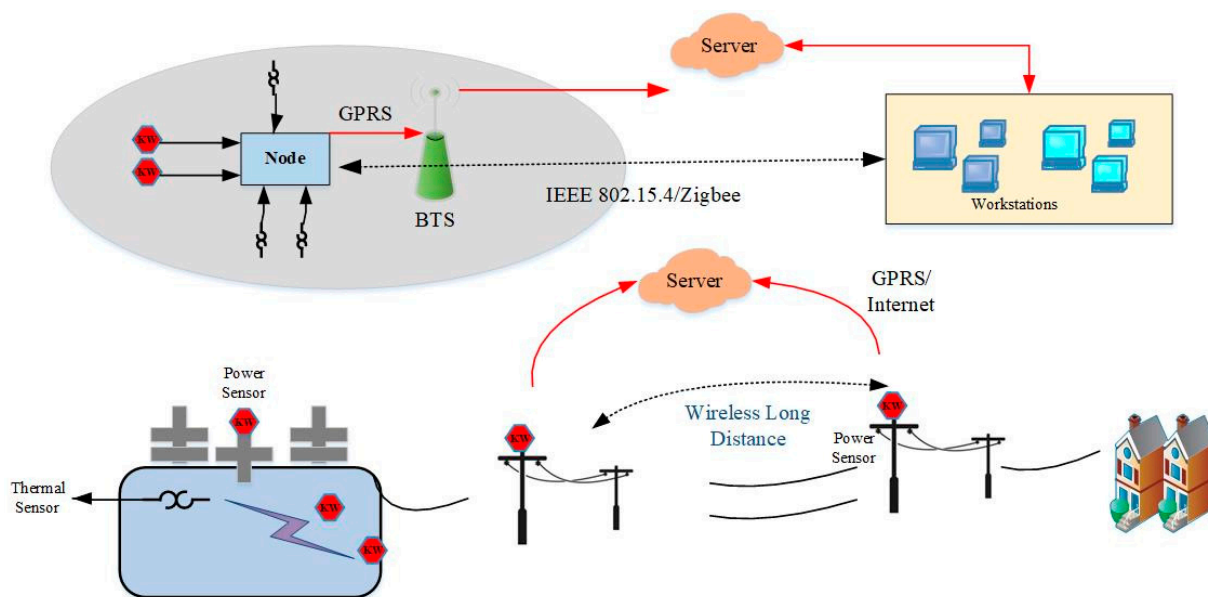


Figure 7. Examples of IoT integration in distribution networks.

Table 5. Characteristics of IoT-enabled smart meters.

Categories	Itemized Description	Explanation
Advantages	Free Installation	No payment is required for the meter installation
	Savings opportunities	Smart meters can help families cut their energy costs by providing insight into their energy usage and assisting them in changing their consumption behavior to save money
	Emission reduction	Customers can alter their consumption not only to save money on bills but also to lessen their carbon footprint
	Energy consumption monitoring	Smart meters can help energy users to understand how their energy habits convert into costs by displaying their energy consumption not just in kilowatt hours but also in dollars
	No meter readings needed	Smart meters transmit information about the customers’ energy usage automatically, eliminating the need for manual readings.
	No bill estimation is required	Daily, weekly, and monthly bill projections can be accessed through the users’ accounts
	Pre-payment meters option	Households on pay-as-you-go rates can benefit from smart prepayment meters, which can help them keep track of their credit balances and even send out notifications when the meters are running low
	Enabling time-of-use (ToU) tariffs	Some service providers have the ability to inform the customers about the ToU tariffs ahead of time with the help of IoT-enabled meters
	Auto-switching ability	In the near future, IoT-enabled smart meters could automatically and effortlessly switch energy suppliers for customers
	High customer satisfaction	According to a conducted survey in the UK, 80% of customers indicated that they are happy with smart meters’ functionality [55]
Disadvantages	Awareness of deals	This option includes personalized tariffs tailored to a home’s specific energy needs and use
	Requires proactive use for savings	Smart meters do not automatically save you money. Customers must actively engage with the meter and adjust their behavior in response to its data, or their bills will not decrease
	Smart meters may lose functionality after switching	The majority of smart meters now in use are first-generation devices that frequently “go dumb” or lose functionality once customers switch energy providers
	Not available to some consumers on prepayment and time-of-use tariffs	Smart meters are technically available for houses on prepayment and time-of-use tariffs, and while they can make these tariffs easier to monitor and save money with, their use is restricted
	Privacy concerns for some customers	Unfortunately, cyber-physical attacks through the breach of information and privacy are increasing day by day

4.4. Application of 5G in IoT-Based Demand Response Programs (DRPs)

Demand response programs (DRPs) are defined as a shift in customers' electrical consumption patterns from their usual patterns in response to a variety of factors, such as price changes during a specific period of operation, receiving incentivized payments from power market operators to reduce their electricity usage during high prices, or when system reliability is threatened due to unpredicted contingency events [56]. In general, 5G-based IoT devices are expected to play a significant role in regulating demand response in future energy networks. Since most of the recently integrated IoT devices are cloud-based platform types of devices, software applications operating on the cloud platform can make data integration and exchange easier [57,58]. Furthermore, the IoE framework allows prosumers and utilities to independently coordinate supply and demand with the help of sophisticated forecasting algorithms that utilize weather predictions, anticipated traffic patterns, and other intelligent aspects of IoT-based energy systems [59]. To further investigate the 5G networks' applications for enhancing the demand response programs in smart energy grids, they are summarized in Table 6 [60,61].

Table 6. Comparison of 5G-based IoT-enabled smart grids for the DRPs.

Items	Advantages	Challenges
Massive links among flows for more accurate and fairer DRP control	<ol style="list-style-type: none"> (1) More precise and accurate DR control thanks to the terminal and built-in controllers (2) Monitoring user's consumption in shorter time intervals 	<ol style="list-style-type: none"> (1) Necessity to set accurate financial compensations for users (2) Users participating in DR programs need to be controlled for their electricity intake
Fast transfer speed and low latency	<ol style="list-style-type: none"> (1) Removing instability and oscillations during the frequency regulation process (2) Considering RES in the frequency regulation services in the maintenance of system balance 	<ol style="list-style-type: none"> (1) Costs of adapting faster communication methods (2) Dealing with the issue of power deviation, system frequency, and area control
Robust security and data privacy	<ol style="list-style-type: none"> (1) Enabling data transfer security and diversified services (2) Generating network function sets for tailor-made customer services (network slices) 	Implementing a 5G network slices individual structures
High system stability and reliability	<ol style="list-style-type: none"> (1) Optimized power consumption by the system (2) Lower system failure rate 	<ol style="list-style-type: none"> (1) Logistical problems due to linking a large number of appliances (2) Costs of installing the 5G terminal controllers
Energy-saving and low power consumption	<ol style="list-style-type: none"> (1) Higher energy transfer capability (2) Compliance with the sustainable development goals and priorities 	<ol style="list-style-type: none"> (1) Low number of real-life practical testing and applications (2) Few implementations around the world

5. Cyber-Physical Security Vulnerabilities and Challenges in IoT-Enabled Smart Grids

5.1. General Definitions, Framework, and Guidelines

The energy grid systems have become more intelligent and interactive with the widespread use of IoT-based technologies, which improves the system's consistency, efficiency, and adaptability. Cybersecurity vulnerabilities, on the other hand, are becoming increasingly common. Thus, this section will discuss the security issues in IoT-connected smart energy systems and their corresponding mitigation strategies. Figure 8 portrays the general paradigm of cyber-physical security in smart energy grids [62]. Five significant causes make the smart grids vulnerable to cyberattacks [63]:

- (1) Ever-increasing development of intelligent electronic devices (IEDs): The number of attack sites grows in lockstep with the number of devices in the network. Even if a single point's security is breached, the entire network system is affected.
- (2) Unregulated installation of third-party components: Experts advise against using third-party components because they make the network more vulnerable to hacking. These devices might be infected with Trojans, which could then spread to other network devices.
- (3) Insufficient personal training: To use any technology, appropriate training is required. When employees are not properly trained, they are more likely to fall prey to phishing scams.
- (4) Insecure Internet protocols: In terms of data transfer, not all protocols are secure. Unencrypted data transport is used by several protocols. As a result, they are easy targets for man-in-the-middle attacks that extract data.
- (5) Maintenance: The primary objective of maintenance is to keep things running smoothly. It can also be used as a vector for cyberattacks. Operators frequently deactivate a security system during maintenance to undertake tests.

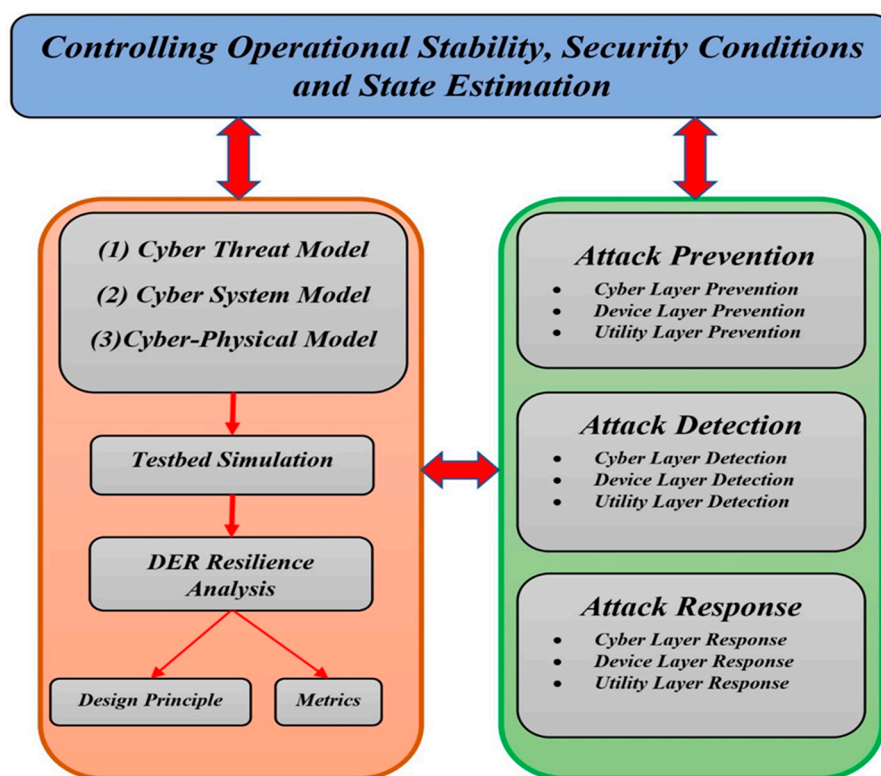


Figure 8. General paradigm of cybersecurity in smart grids.

The abovementioned five causes may compromise one of the five main goals of the cybersecurity framework in smart grids [64–66]:

- (1) Authentication: The ability to verify the identity of any smart grid communication device. For example, to bill the relevant user, the energy provider must validate each smart meter.
- (2) Authorization: Ensures that an authenticated person or an object is authorized to accomplish certain tasks or has been granted the necessary privileges to access a certain category of resources. For example, an agent requires authorization to access and conduct manual configuration on a smart meter.
- (3) Availability: Ensures that when a user needs some resources and/or data, they are always available for usage.

- (4) **Confidentiality:** Guarantees that only the intended recipients have access to data that have been stored or transmitted. For example, only smart grid operators and energy providers should be aware of the end users' consumption patterns and data.
- (5) **Integrity:** Certifies that received data have not been tampered with in any manner. For example, smart meters must ensure the integrity of software updates as well as the source origin.

A framework for improving smart grid cybersecurity was established by the NIST, which suggests 14 requirements for smart grids to safeguard themselves against different types of cyber-physical attacks:

- (1) Staff awareness training.
- (2) Access control and configuration management.
- (3) Physical and environmental security.
- (4) Continuous audit and accountability.
- (5) Security assessment and authorization.
- (6) Continuity of operations (individual and systematic).
- (7) Development and maintenance planning.
- (8) Well-implemented identification and authentication procedures.
- (9) Document and information management processes.
- (10) Incident response plan.
- (11) Media management and protection.
- (12) Security management program (personnel and premises).
- (13) Risk assessment and management.
- (14) Smart grid information system, services acquisition, communication protection, and information integrity.

5.2. Historical Cybersecurity Attacks (in the Context of IoT-Enabled Smart Grids)

To better comprehend the risks posed by cyberattacks on the critical infrastructure of electrical grids, in this section, we will discuss a number of significant instances of cyberattacks around the globe [67].

5.2.1. Tram Hack Lodz, Poland (2008)

A tram system was hacked in Lodz city and escalated to the point where a dozen passengers were severely injured. This was the first cyber-kinetic attack that resulted in human injury.

5.2.2. Texas Power Company (2009)

An employee of Texas power company (TPC) who had recently been dismissed hacked the company's network to disable power forecasting systems. They took advantage of logins that had not yet been deactivated.

5.2.3. Iran Nuclear Facility Attack (2010)

Stuxnet was created to disrupt and destroy Iran's nuclear program, but it also demonstrated that it has the capability to do considerable physical damage to vital infrastructures by focusing on computer controllers and SCADA systems that oversee industrial equipment [68].

5.2.4. Bowman Avenue Dam Cyberattack (2013)

Hackers were able to acquire control of the floodgates of the Bowman Avenue Dam in New York. Investigations revealed that they could have simply modified water flow parameters or even the quantity of chemicals used in water treatment to lead to devastating consequences. It would have had disastrous implications if this had happened.

5.2.5. Ukraine Power Grid Attack (2015)

Cyberattacks on the energy sector are rising, posing a growing danger to the reliability and safety of smart grids. The successful strikes on Ukraine's electrical grid in 2015 demonstrate this threat. Attackers obtained access to distribution grid operator consoles and remotely closed breakers on several occasions, causing local blackouts. The attack shut down 30 substations, affecting about 230,000 people. In similar incidents, attackers might compromise communications channels and change data, or they could flood the highly connected network with data traffic, limiting operators' ability to monitor and operate the grid [69].

5.2.6. Dyn Distributed Denial-of-Service (DDoS) Cyberattack (2016)

Dyn, an internet service provider, was hit by a cyberattack that brought down large areas of the Internet in the United States of America (USA) and interrupted access to famous websites. The hackers carried out widespread denial-of-service assaults. The DDoS attack took control of the Mirai botnet, which scours the Internet for inadequately protected IoT devices with factory default usernames and passwords. They then took control of a large number of unsecured IoT devices and used them to make requests to Dyn servers for services. The site was swamped by fake traffic, which caused it to crash.

5.2.7. Attack on the Smart Building Facilities in Lappeenranta, Finland (2016)

During the middle of the Finland winter in the city of Lappeenranta, a targeted DDoS attack shut off the heat and hot water systems in two apartment complexes.

5.2.8. Cyberattack on the UK Electrical Grid (2017)

A power infrastructure that distributes electricity to the United Kingdom and Ireland was targeted in July 2017. The cyberattack was aimed at penetrating power management systems, allowing them to shut down a section of the energy grid. It was accomplished with the help of several falsified emails sent to senior executives at the power business.

5.2.9. Cyberattack at the Petrochemical Plant in Saudi Arabia (2017)

A failed cyberattack on a Saudi Arabian petrochemical factory was meant to not only impair the plant's operations but also produce an explosion that could have killed people. Fortunately, a glitch in the attackers' computer programming stopped the explosion from taking place.

5.3. Main Cyberattack Strategies in IoT-Enabled Smart Grids

Cyber adversaries utilize four key access and control methods to target devices: scanning, surveillance, maintenance, and manipulation. During the first step, reconnaissance, the attacker collects and acquires information about their target. They seek to discover the system's weaknesses in the second step. These moves are intended to help understand and recognize the services available and running on the open ports and the hosting device characteristics (e.g., operating system, manufacturer). During the target exploitation time, they aim to gain concession control over the entire system. After gaining target administrator access, the final step must be completed so that access may be maintained indefinitely. This is accomplished by installing a covert and undetectable application that allows them to quickly return to the target system. Security requirements are a concession in the smart grid, as attackers take the same procedures. At each stage, they use a variety of tactics to breach a specific system [17,70]. Figure 9 demonstrates a stepwise procedure of cyberattacks during the exploitation of cyber adversaries [71], where Table 7 presents how each type of attack can compromise system security [63,72]. Figure 10 vividly shows how cyber attackers can breach systems' security [73].

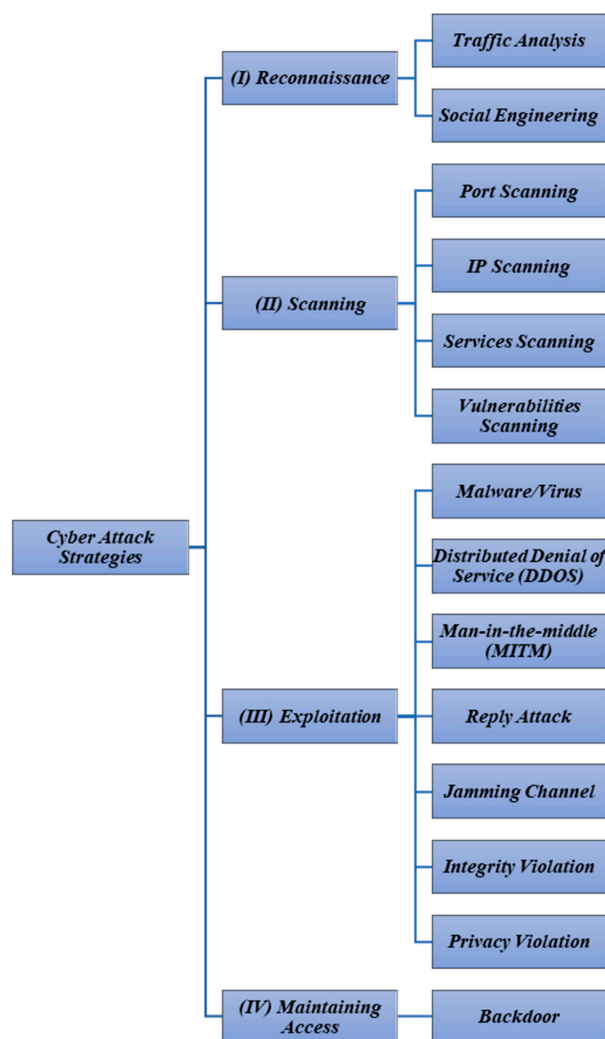


Figure 9. Stepwise cyberattack strategies in IoT-enabled smart grids.

Table 7. Goals of security that have been jeopardized because of an attack.

Attack Category	Security Goals	Description	References
Flooding attack	Availability	Deterring users from utilizing resources	[74,75]
Denial of service	Availability	Stop serving of user’s request	[76]
Jamming channel	Availability	Jamming the network	[77,78]
Buffer overflow	Availability and confidentiality	Overwriting the memory of the buffer	[79]
False data injection (FDI)	Integrity	Tampering the real data	[80,81]
Social engineering	Integrity and confidentiality	Attacking humans instead of machines or networks	[82,83]
MITM	Confidentiality	Extracting packet information between sender and receiver	[63,84]
Packet sniffing	Confidentiality	Analyzing the packet	[85]
Session hijacking	Integrity and confidentiality	Obstructing the user from resources for a particular amount of time	[86]
Data manipulation	Integrity	Data tampering	[87]
Replay attack	Integrity	Send data continuously	[88,89]

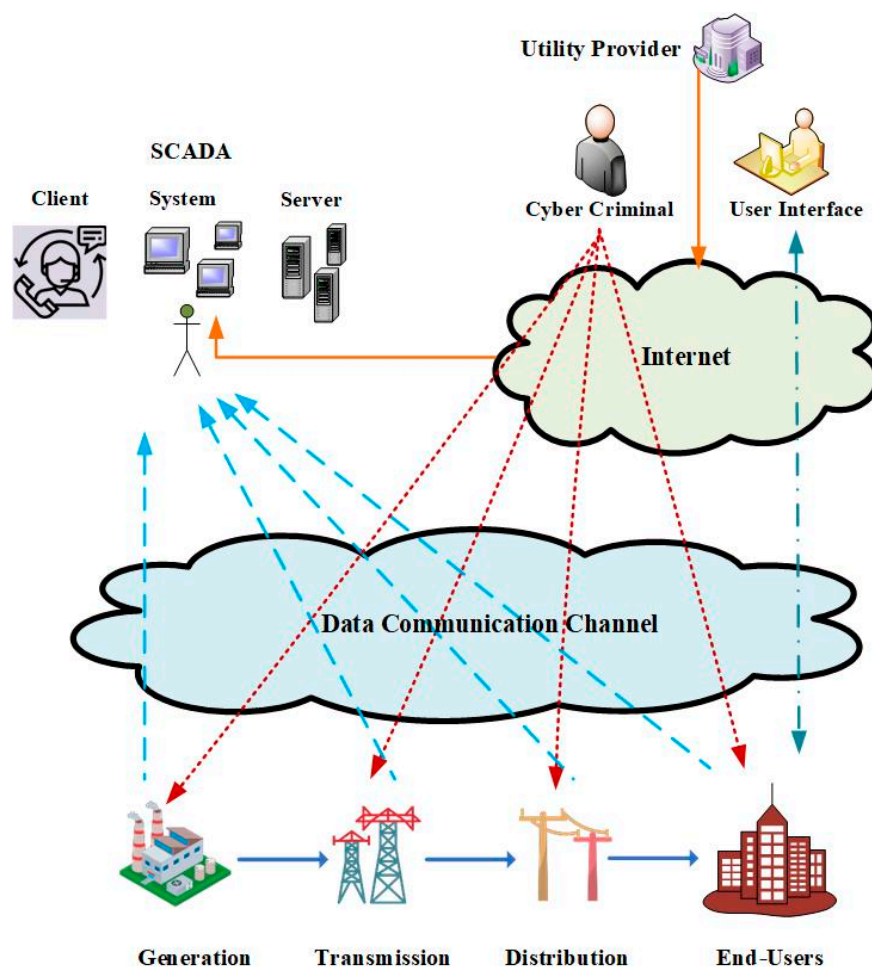


Figure 10. Different cyberattack approaches in IoT-enabled smart grids.

5.3.1. Reconnaissance Definition and Strategies

The reconnaissance procedure includes attacks such as traffic analysis and social engineering. In social engineering, instead of focusing on technology abilities, the focus is on the human connection and social engineering that revolves around it. Persuasion and communication gain are used by an attacker to earn the user's trust in order to access private and credential information, such as PINs or passwords to log in to the server [82]. Password and phishing attempts, for example, have become commonplace in social engineering. The traffic analysis monitors and analyzes network traffic to determine which machines and hosts connect to the network, obtaining their IP addresses. Social engineering and traffic analysis are the main threats to information security [85,90].

5.3.2. Scanning Strategies

The scanning is the next step in detecting all the available network machines and hosts. IP addresses, ports, utilities, and security issues are all factors to consider while scanning. An intruder would normally start identifying the network by scanning the hosts connected to their newly acquired IP addresses. Then, they examine each port to establish which ones are available. This scan is performed on any found host network. The attacker then runs a service scan to see what service or device is running behind each open port [91]. Vulnerability scanning is the final stage, which identifies defects, goals, and vulnerabilities associated with each service system on the target devices to be attacked at a later stage. Modbus and DNP3 are two industrial protocols that are vulnerable to scan attacks. Instead of utilizing the scanning Modbus network approach, TCP/Modbus was created to safeguard it. The attack involves delivering an innocuous message to all

networked computers to capture their data. On the SCADA Modbus network, Modscan is a well-known scanner that can discover and open TCP/Modbus connections, and identify system IP addresses and slave IDs [92].

5.3.3. Exploitation Strategies

The third step, exploitation, involves hostile operations attempting to acquire control of the IoT-enabled smart energy system components and exploiting vulnerabilities [82]. Viruses, worms, and Trojan horses infecting the human-machine interface (HMI). Privacy violations, channel jamming, integrity breaches, and other assaults, such as denial of service (DOS), man-in-the-middle (MITM), and replay attacks, are all instances of these activities [93,94]. Viruses are programs that infect computers, devices, and/or machines in smart energy systems. A worm is a self-replicating program. It infects the system and other devices by spreading across the network, copying itself, and infecting them. A Trojan horse is computer software that impersonates a beneficial function on the target computer [95,96].

5.3.4. Maintaining Access

In the final step, the attacker utilizes a specific attack to gain permanent access to the target, such as backdoors, infections, and Trojan horses. Undetectable software, such as a backdoor, is installed on the target surreptitiously so that it may be accessed fast and simply [97]. Assume that the attacker has successfully created a backdoor into the SCADA server control: in such a situation, they will be able to launch a series of attacks against the system, having a severe impact on the entire power system. On the IT network, the security requirements are established in order of importance: (1) confidentiality, (2) integrity, and (3) availability [98].

5.4. Adverse Impacts of Cyberattacks on Smart Grids

In the following, we will discuss several examples related to the negative impacts of cyberattacks on the safe operation (from economic and stability points of view) of the IoT-enabled smart grids.

5.4.1. Electricity Market Losses

Cyberattacks on smart energy systems have significant potential economic and physical consequences. Even though the current study has focused on cyber technical/physical attacks on smart grids, it is also critical to pay greater attention to cyberattacks in terms of associated economic risks. Smart grids have had severe economic difficulty with cyberattacks, particularly renewable energy resources with a high penetration level. Electricity markets are a mix of real-time and day-ahead trading [99,100]. The day-ahead market is primarily concerned with finding the most cost-effective solution to optimization and load forecasting problems. Since load forecasting is impacted by fake data injection (FDI) cyberattacks in the day-ahead market, the optimization algorithms would be unable to accurately determine the location marginal prices (LMPs) of the grid [101,102]. On the other hand, the real-time market assesses the dispatched power from each generating unit to meet the required load demand of each bus [103,104]. It is also necessary to calculate the power that flows through transmission lines to achieve the congestion pattern and consequently evaluate real-time LMPs. Thus, FDI attacks can impact precise state estimation of the power grids in the real-time electricity markets [105,106].

5.4.2. Power System Stability

The FDI attacks have had major technological and physical consequences for IoT-enabled smart grids. In the case of FDI attacks, smart grids must usually deal with steady-state stability and transient effects [107]. The impact of FDI attacks on steady-state stability on voltage control demand current/voltage/power management and energy management of smart grids is very significant [108,109]. Furthermore, the cyberattacks have a negative influence on electrical grid steady-state functioning, whereas the FDI

attacks have harmed the dynamic and transient stability of smart grids. FDI can also impact the smart grid frequency control system. However, the goal will be to maintain rotor angle stability [110,111].

5.4.3. Energy Theft

The widespread use of IoT-aided AMI in the smart energy grid allows for the transmission of massive energy data and information in a more reliable, efficient, and effective manner for smart grid system management. It replaced the existing analog meter reading and data gathering system with a digital system. Those massive volumes of acquired data and information are wirelessly transferred for further processing with the help of IoT technology, which significantly reduces labor-intensive operations [112]. In the energy sector, energy theft has become a major cause of concern. Both energy service providers and consumers have suffered significant financial losses because of energy theft. The most basic kind of energy theft is tampering with an energy meter so that it can no longer record real energy use and thereby alter the energy bill. Energy theft usually entails circumventing the energy meter so that energy may be consumed without being recorded for billing purposes [80].

5.4.4. Disruption of Service in Critical and Non-Critical Facilities

Cyberattacks against automation equipment in critical and non-critical facilities can be conducted to achieve the goals listed below [4,113,114]:

- (1) To gain initial access, for example, via hacking smart lights, to gain Wi-Fi authentication and eventually control of Wi-Fi network devices.
- (2) To cause an indirect service disruption, for example, by using a thermostat to manage the building's air conditioning system from afar.
- (3) To obtain and disseminate information. Use an application that hacks smart gadgets, such as smart televisions, to make them act as though they are turned off and then use the microphone to record and leak conversations surrounding them.
- (4) For system abuse, such as producing light flashing at a certain frequency that might trigger epileptic seizures in individuals.
- (5) To initiate an intensified attack against critical facilities such as hospitals through a number of targeted smart devices. To deactivate smart home automation systems by targeting a large number of IoT-enabled smart home automation devices in a short amount of time.

5.4.5. Disruption of Transactive Energy Systems

The transactive energy system employs this integrated notion of economic and operational mechanisms to dynamically maintain demand and supply balance across the grid system, hence improving the energy grid's efficiency and reliability. For decision-making and demand response programs, the transactive energy control mechanism is heavily reliant on the cyber system of distributed edge computing and IoT-enabled technologies. This system necessitates a large amount of data to be transmitted across various market processes. Cyberattacks can be performed through the following procedure in order to disrupt the safe operation of transactive energy systems [115,116]:

- (1) Malware injection in the system can result in a large-scale power outage or data theft.
- (2) Cybercriminals can tamper with or damage smart meters for several purposes.
- (3) To interrupt the transactive system by manipulating the control signals of the relay and circuit breaker.

5.4.6. Environmental Security

Environmental security is critical in the implementation of smart energy grids because it aids in the control and avoidance of potentially catastrophic effects on infrastructures caused by natural or artificially induced environmental hazards such as floods, tremors, earthquakes, landslides, falling trees, and bushfires. In such circumstances, smart action

based on environmental concerns is performed primarily by delivering appropriate threat alerts based on collected data and providing alternate feeders for vital infrastructure. Although this feature of smart grids' security is classified as non-technical in this study, it has both technical and non-technical ramifications in some areas.

The capacity of a system's response to failure, in terms of its ability to restore service (by utilizing an improvised alternate feeder if appropriate) or provide adequate data to enable system operators to restore service, is of the highest importance in smart grids. This is accomplished mostly by automatic switching in the event of outages or failures. Natural catastrophes, harsh temperatures, peak, and fossil oil depletion, global energy market instability, terrorism, sabotage, vandalism, and other similar variables all have adverse impacts on the system's resiliency [117,118]. A geographic information system (GIS) is based on the real-time data that are captured by deployed IoT devices such as smart meters to aid data analytics methods that predict natural disasters and thus have a crucial role in providing timely and accurate environmental threats alerts.

5.5. Detection and Mitigation of IoT-Enabled Cyberattacks

Customers (consumers and prosumers), electric utilities, power system operators, and third-party service providers can be assumed to be stakeholders of smart grids. The data administration of smart grids, particularly in terms of smart meters, becomes a demanding task due to the participation of various stakeholders. There are several frameworks that provides guidelines for integrating security and privacy across several domains to enhance the security and privacy protection of all involved entities. Security is divided into three categories by the framework: communication security, secure computing, and system control security. Cryptography, route security, and network privacy are all aspects of communication security [119].

A key goal in the management of communication security is to successfully achieve end-to-end encryption and multiple hop routing that can assure the security of transferred data. In [120], the authors described the major functionalities of smart meters, which includes tracking the quantity of utilized energy as well as voltage and frequency. The implemented smart meters are also in charge of providing data to the grid via a secure communication channel, as well as managing load switches by operators to prevent black-outs in emergency situations. Additionally, this research showed that high-assurance smart meters could be implemented (HASM).

Various techniques have been proposed in the literature to address cybersecurity backgrounds, elements, challenges, and potential solutions for smart energy grids. However, as the complexity of the grid increases with the significant deployment of smart IoT devices, most recent studies have found that the integration of AI techniques is one of the most effective solutions [121–126]. According to several research findings, the smart grid is similarly vulnerable to human errors, which can be caused by social engineering attacks [127,128]. Therefore, in this study to investigate the most promising recent methods for safeguarding IoT-enabled smart grids, we have divided these methods into two main categories: non-human-centric and human-centric methods.

5.5.1. Non-Human-Centric Methods

The non-human-centric methods can be categorized into three classes: (1) machine-learning-based methods, (2) cloud-computing-based methods, and (3) blockchain-based methods. In the following, we will briefly discuss each of the mentioned methods.

Machine-Learning-Based Methods

In the smart grid infrastructure, thousands of sensors are deployed. These sensors continually monitor the states of the devices to which they are connected, generating a massive quantity of data in the form of log files or time-series data. The data that are produced by sensors are saved on a cloud server, which must be preprocessed before being sent. Local servers are another option for servers. However, the maximum level of data

security is achieved by storing data on a local server. Nevertheless, they constrain the ability of pattern recognition features or forecasts by advanced optimization algorithms [129,130].

In the past few years, machine-learning methods have proved to be effective in detecting cyberattacks. Machine learning identifies intrusions based on past data, as opposed to rule-based techniques. To anticipate power system disruptions, a combination of JRipper and Adaboost was formulated in [131]. The model generated three groups based on the attack data, natural disturbances, and the state of no event. False data injection attack (FDIA) is another popular type of attack that can seriously damage smart energy systems. By tampering with data that are collected from smart meters, FDIA can financially impact utilities and consumers. In [132], a model was analyzed on an IEEE 14-bus test system. The efficiency and performance of the ensemble-based learning (EBL) model were compared with several algorithms such as linear regression (LR), naïve-Bayes (NB), decision tree (DT), and support vector machine (SVM), where the obtained results demonstrated that the unsupervised EBL model outperformed all the other algorithms with accuracy of 73%. In [133], the authors proposed a robust deviation-based detection method to efficiently defend the system against an FDIA. Additionally, an exponential weighting function in combination with a Kalman filter was implemented to retain the original weighted least squares estimator. The experimental results confirmed the efficacy of the proposed detection method against FDIA attacks. In this study, the influence of various attack strengths and noise on detection performance was also investigated. In [134], a deep learning technique based on a conditional deep belief network model was proposed to identify the behavioral characteristics of FDI attacks on a real-time basis. In the presented method, the detection mechanism relaxes the beliefs for the potential attack scenarios and attains high accuracy. Moreover, the formulated optimization model was able to distinguish similar behavior that takes place in the process of energy theft. The performance of the presented method was illustrated through two simulation cases on IEEE 118-bus and IEEE 300-bus test systems, where the scalability of the proposed model was also examined.

Occasionally, a smart grid may be subjected to distributed denial-of-service (DDoS) attacks. DDoS attacks jeopardize the availability of communication servers. The fundamental goal of a DDoS attack is to flood the communication server with false requests, causing it to become unusable for communication. In [135], the authors proposed a DDoS attack detection method based on a multilevel auto-encoder formulation. Multiple levels of shallow and deep auto-encoders were trained in an unsupervised approach which was employed to encode training and test data for feature extraction and generation purposes. In the final stage of the algorithm, a unified detection model was constructed by combining the multilevel features using a kernel learning algorithm. The obtained results of their algorithm showed its functionality by achieving high prediction accuracy where it outperforms all the other compared methods.

Cloud-Computing-Based Methods

In [136], risks and opportunities that cloud computing avails to utility companies and energy suppliers of IoT-enabled smart grids were discussed while considering characteristics of cloud computing that may be able to enhance the system defense capability in dealing with DDoS attacks. An extensive literature review was also conducted to determine which DDoS defense techniques can be employed by means of cloud-computing techniques in the context of smart energy systems. In [137], to ease the inconvenience of working on encrypted data, an attribute-based online/offline searchable encryption scheme was proposed. In the first step, encryption and trapdoor algorithms were divided into two phases. In the second step, both the encryption and attribute control policy were performed in the offline mode. In the next step, the proposed scheme was secured against two attacks: (1) chosen plaintext and (2) chosen keyword attacks. Ultimately, the applicability of the presented method in a cloud-based smart grid was tested. In [138], the authors analyzed a fundamental security problem in the scalable architecture of the smart grid cloud services. They evaluated risks involved in IoT-enabled smart grid security in terms of five distinctive

features: (1) policy and organizational risks, (2) general technical risks, (3) SaaS risks, (4) PaaS risks, and (5) IaaS risks. The presented evaluation model was based on deep belief networks, which comprised multiple RBMs and a BP neural network (BPNN). The RBMs were trained by means of a greedy training algorithm, and then BPNN was employed for fine-tuning purposes. Their obtained results found that the mean absolute error (MAE), mean relative error (MRE), and mean square error (MSE) of the proposed model are the lowest in comparison to all the other methods [139].

Blockchain-Based Methods

The integration of blockchain with IoT-enabled smart grids is becoming a complicated key solution for accelerating a broad range of security functionalities in smart energy systems [140]. The current centralized ledger system can be transferred by blockchain-based techniques into a distributed ledger thanks to the existence of public key algorithms. Blockchain methods offer end-to-end encryption technology based on their distributed processing structure that guarantees the safety and reliability of communication [141]. In [142], a blockchain-based security method that facilitates secure and authorized access to smart city resources was presented. The proposed method comprised an authentication and authorization process for constrained environments based on two models: (1) a blockchain model and (2) object security architecture (OSCAR) for the IoT. The blockchain-based method laid out an adaptable and untrustworthy authorization system, while OSCAR used a public ledger to construct multicast classes for authorized customers. Furthermore, a meteor-based application was created to provide a user-friendly interface for heterogeneous smart city technology. Through this application, users were able to interact and operate with smart city resources such as traffic lights, smart energy meters, and security cameras. In [143], a new distributed authentication and authorization protocol for IoT-enabled smart grids based on blockchain-based methods was proposed to address information leaks, illegal access, and identity theft issues. The protocol introduced combined the decentralized authentication and immutable ledger properties of blockchain architectures that are applicable for power systems to achieve both identity authentication and resource authorization for smart energy systems. In [144], a model-based architecture was proposed that considered an interoperable blockchain-based local energy market for consumers and prosumers in a residential microgrid (MG) framework. The research identified 21 organizational, informational, technological, and blockchain needs for a local energy market and its underlying information system using the IoT-enabled smart grid architecture. According to the Landau Microgrid case study, the biggest hurdle was a clear value proposition for key stakeholders, standardization of data exchange, and appropriate physical implementation [145].

5.5.1.4. Human-Centric Methods

Multifactor Authentication

When two successive authentication procedures are combined, the password-breaking algorithm becomes exponentially more complicated. Unauthorized users will have less access to the data because of the multifactor authentication process. Multifactor authentication approaches include SMS token authentication, email token authentication, hardware token authentication, software token authentication, and phone authentication [146].

Employee Training

Hackers are increasingly targeting humans because of technological advancements that have made attacks on smart equipment more complicated. Attackers are using machine-learning technologies to recognize human behaviors and create a variety of scenarios. Thus, employee training plays a critical role in limiting the hackers' success in their malicious intent.

Password Strength

The use of strong passwords minimizes the likelihood of an attack on the integrity or confidentiality of data. Password-guessing attacks are more likely with weak passwords. Password guessing is a method of gaining access to a system by guessing passwords and

gaining access to a targeted device. In addition, the attacker consumes network resources and bandwidth to carry out several attacks that consequently limit the access of legitimate users to the resources [147].

Operating System (OS) Protection

Users are one of the weakest links in the context of cybersecurity, and one of the biggest challenges with users is that they cannot be taught in the same way as staff. Thus, smart devices such as smart meters and smart inverters must be protected against cyberattacks. Tamper-proofing the devices' internal operating systems is one of the most effective approaches for protecting devices against cybercriminals [148].

Customers Protection against Third-Party Applications

Customers should always be wary of applications that request authorization. Customers keep sensitive data on their devices, and some third-party apps request more information than they require. Around 98.5 percent of consumers ignore or just sometimes accept the permissions requested by applications without thinking twice. It has been reported that 93.6 percent of users accept the applications' terms and conditions instantaneously or within one minute [149].

Reporting of Malicious Behavior

Customers should be able to readily report any suspected attack on a platform created by utilities. The destruction would grow exponentially as the time gap between the attack and the time of report increases. A delay in reporting an attack jeopardizes not only the privacy of one client but also the privacy of other connected customers in the grid [63].

6. Conclusions and Future Directions

The Internet of Things (IoT) is the next step toward a worldwide and widespread connection to every communication and computation-enabled device, independent of its access technology, available resources, or geographical location. The smart grid is the largest IoT deployment, with smart devices distributed throughout the energy chain from the generating power plants to the end-users. The IoT will improve existing smart energy grids by facilitating real-time control and monitoring of the grid components. However, in the past decade, as discussed in the literature, cybersecurity has been viewed as one of the major roadblocks to IoT acceptance and further deployment in smart energy grid systems around the world. It is a challenging task to ensure the safety of grid-connected devices, and this is due to the massive number of devices that are connected to the communication networks, which increases the chances of a cyberattack and the potential risks of severe repercussions. It has been predicted that 30.9 billion IoT devices will be deployed around the world by 2025, of which 19% will be installed in the energy sector, which increases the focus of cyberattacks on this sector by 54% [67,150]. In this regard, the extent of the susceptible attack surface will rise dramatically with the further implementation of IoT-enabled devices in the smart grids. To address the abovementioned concerns and challenges, the following recommendations for the improvement of IoT-based smart energy systems are made:

- The framework and modeling of smart energy grids should be improved, and suitable reconfiguration technologies must be developed for the restoration aspect of electrical grids.
- Secure AMI technologies must be widely deployed in combination with advanced cloud and edge-computing facilities and 5G telecommunication technologies to enhance the functionality and security of the smart grids.
- Smart grids must be equipped with more secure communication protocols that consider the heterogeneity of IoT devices while enabling the deployment of AI algorithms onto the device itself instead of being controlled from afar to reduce the likelihood of communication breaches.

- Advanced secure and data communication systems based on blockchain methods must be extensively implemented in IoT-based smart energy systems.
- Game-theoretic models (specifically for the energy markets), and cognitive and deep-learning methods (for system behavioral modeling and forecasts) must be used effectively for the smooth and reliable operation of electrical grids.

Author Contributions: Writing—original draft, A.G.; Conceptualization, F.G.; writing, S.F.; formal analysis, M.W.; Writing—review & editing, A.G. and F.G.; Supervision, I.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

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

Appendix A

Table A1 provides a thorough comparison of this study with the existing literature to demonstrate further this work’s novel contributions to the state-of-the-art IoT-enabled smart grid field.

Table A1. Novel characteristics of this study as compared with the existing literature.

Ref	IoT	5G	Blockchain	Cyber Attacks	Edge Computing	Cloud Computing	Demand Response	Smart Energy Management	RESs	Smart Homes	Grid Restoration
[30]	X	X					X				
[141]			X	X							
[36]		X									
[142]		X			X						
[143]	X						X				
[3]	X										X
[144]	X	X					X				
[149]		X						X			
[150]		X	X	X							
[57]		X							X		
[151]	X		X								
[29]		X			X						
[152]	X		X	X							
[58,64,153]	X		X	X							
[33]		X									
[17]	X		X								
[154]	X					X					
[43]	X									X	
This Study	X	X	X	X	X	X	X	X		X	

References

1. Amin, M. A smart self-healing grid: In pursuit of a more reliable and resilient system [in my view]. *IEEE Power Energy Mag.* **2013**, *12*, 110–112. [\[CrossRef\]](#)
2. Goudarzi, A.; Li, Y.; Xiang, J. Efficient energy management of renewable resources in microgrids. In *Renewable Energy Microgeneration Systems*; Elsevier: Amsterdam, The Netherlands, 2021; pp. 285–321.
3. Fan, D.; Ren, Y.; Feng, Q.; Liu, Y.; Wang, Z.; Lin, J. Restoration of smart grids: Current status, challenges, and opportunities. *Renew. Sustain. Energy Rev.* **2021**, *143*, 110909. [\[CrossRef\]](#)
4. Abir, S.A.A.; Anwar, A.; Choi, J.; Kayes, A. IoT-enabled smart energy grid: Applications and challenges. *IEEE Access* **2021**, *9*, 50961–50981. [\[CrossRef\]](#)
5. Espe, E.; Potdar, V.; Chang, E. Prosumer communities and relationships in smart grids: A literature review, evolution and future directions. *Energies* **2018**, *11*, 2528. [\[CrossRef\]](#)

6. Tuballa, M.L.; Abundo, M.L. A review of the development of Smart Grid technologies. *Renew. Sustain. Energy Rev.* **2016**, *59*, 710–725. [[CrossRef](#)]
7. Ullah, A.; Azeem, M.; Ashraf, H.; Alaboudi, A.A.; Humayun, M.; Jhanjhi, N. Secure healthcare data aggregation and transmission in IoT—A survey. *IEEE Access* **2021**, *9*, 16849–16865. [[CrossRef](#)]
8. Pau, M.; Patti, E.; Barbierato, L.; Estebansari, A.; Pons, E.; Ponci, F.; Monti, A. A cloud-based smart metering infrastructure for distribution grid services and automation. *Sustain. Energy Grids Netw.* **2018**, *15*, 14–25. [[CrossRef](#)]
9. Makkar, A.; Garg, S.; Kumar, N.; Hossain, M.S.; Ghoneim, A.; Alrashoud, M. An efficient spam detection technique for IoT devices using machine learning. *IEEE Trans. Ind. Inform.* **2020**, *17*, 903–912. [[CrossRef](#)]
10. Doan, Q.-T.; Kayes, A.; Rahayu, W.; Nguyen, K. Integration of iot streaming data with efficient indexing and storage optimization. *IEEE Access* **2020**, *8*, 47456–47467. [[CrossRef](#)]
11. Xiao, L.; Wan, X.; Lu, X.; Zhang, Y.; Wu, D. IoT security techniques based on machine learning: How do IoT devices use AI to enhance security? *IEEE Signal Proc. Mag.* **2018**, *35*, 41–49. [[CrossRef](#)]
12. Geneiatakis, D.; Kounelis, I.; Neisse, R.; Nai-Fovino, I.; Steri, G.; Baldini, G. Security and privacy issues for an IoT based smart home. In Proceedings of the 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 22–26 May 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1292–1297.
13. Chang, J.; Kadry, S.N.; Krishnamoorthy, S. Review and synthesis of Big Data analytics and computing for smart sustainable cities. *IET Intell. Transp. Syst.* **2020**, *14*, 1363–1370. [[CrossRef](#)]
14. Li, W.; Au, M.H.; Wang, Y. A fog-based collaborative intrusion detection framework for smart grid. *Int. J. Netw. Manag.* **2021**, *31*, e2107. [[CrossRef](#)]
15. Hammad, E.; Nag, A.K.; Chennamaneni, A.; Aghashahi, M.; Dogdu, E. A Deep-Defense Approach for Next-Gen Cyber-Resilient Inter-Dependent Critical Infrastructure Systems. In Proceedings of the 2021 Resilience Week (RWS), Salt Lake City, UT, USA, 18–21 October 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–7.
16. Lázaro, J.; Astarloa, A.; Rodríguez, M.; Bidarte, U.; Jiménez, J. A Survey on Vulnerabilities and Countermeasures in the Communications of the Smart Grid. *Electronics* **2021**, *10*, 1881. [[CrossRef](#)]
17. Hasan, M.K.; Alkhalifah, A.; Islam, S.; Babiker, N.; Habib, A.; Aman, A.H.M.; Hossain, M. Blockchain Technology on Smart Grid, Energy Trading, and Big Data: Security Issues, Challenges, and Recommendations. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 9065768. [[CrossRef](#)]
18. Goudarzi, A.; Kazemi, M. In DC Optimal Power Flow through the Linear Programming—in Context of Smart Grid. In Proceedings of the 24th Southern African Universities Power Engineering Conference, Vereeniging, South Africa, 26–28 January 2016.
19. Moreno Escobar, J.J.; Morales Matamoros, O.; Tejeida Padilla, R.; Lina Reyes, I.; Quintana Espinosa, H. A Comprehensive Review on Smart Grids: Challenges and Opportunities. *Sensors* **2021**, *21*, 6978. [[CrossRef](#)]
20. Pal, R.; Chavhan, S.; Gupta, D.; Khanna, A.; Padmanaban, S.; Khan, B.; Rodrigues, J.J. A comprehensive review on IoT-based infrastructure for smart grid applications. *IET Renew. Power Gener.* **2021**, *15*, 3761–3776. [[CrossRef](#)]
21. Aman, A.H.M.; Shaari, N.; Ibrahim, R. Internet of things energy system: Smart applications, technology advancement, and open issues. *Int. J. Energy Res.* **2021**, *45*, 8389–8419. [[CrossRef](#)]
22. Ghasempour, A. Internet of things in smart grid: Architecture, applications, services, key technologies, and challenges. *Inventions* **2019**, *4*, 22. [[CrossRef](#)]
23. Cao, J.; Yang, M. Energy internet—towards smart grid 2.0. In Proceedings of the 2013 Fourth International Conference on Networking and Distributed Computing, Los Angeles, CA, USA, 21–24 December 2013; IEEE: Piscataway, NJ, USA, 2013; pp. 105–110.
24. Wu, J.; Guo, S.; Li, J.; Zeng, D. Big data meet green challenges: Big data toward green applications. *IEEE Syst. J.* **2016**, *10*, 888–900. [[CrossRef](#)]
25. Wang, K.; Yu, J.; Yu, Y.; Qian, Y.; Zeng, D.; Guo, S.; Xiang, Y.; Wu, J. A survey on energy internet: Architecture, approach, and emerging technologies. *IEEE Syst. J.* **2017**, *12*, 2403–2416. [[CrossRef](#)]
26. Shahinzadeh, H.; Moradi, J.; Gharehpetian, G.B.; Nafisi, H.; Abedi, M. IoT architecture for smart grids. In Proceedings of the 2019 International Conference on Protection and Automation of Power System (IPAPS), Tehran, Iran, 8–9 January 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 22–30.
27. Liu, Y.; Yang, X.; Wen, W.; Xia, M. Smarter Grid in the 5G Era: Integrating Power Internet of Things with Cyber Physical System. *Front. Commun. Netw.* **2021**, *2*, 23. [[CrossRef](#)]
28. Kabalci, Y.; Kabalci, E.; Padmanaban, S.; Holm-Nielsen, J.B.; Blaabjerg, F. Internet of things applications as energy internet in smart grids and smart environments. *Electronics* **2019**, *8*, 972. [[CrossRef](#)]
29. Tufail, A.; Namoun, A.; Alrehaili, A.; Ali, A. A Survey on 5G Enabled Multi-Access Edge Computing for Smart Cities: Issues and Future Prospects. *Int. J. Comput. Sci. Netw. Secur.* **2021**, *21*, 107–118.
30. 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. [[CrossRef](#)]
31. Ray, P.P. A survey of IoT cloud platforms. *Future Comput. Inform. J.* **2016**, *1*, 35–46. [[CrossRef](#)]
32. Liu, Q.; Han, T.; Ansari, N. Learning-assisted secure end-to-end network slicing for cyber-physical systems. *IEEE Netw.* **2020**, *34*, 37–43. [[CrossRef](#)]

33. Abrahamsen, F.E.; Ai, Y.; Cheffena, M. Communication technologies for smart grid: A comprehensive survey. *Sensors* **2021**, *21*, 8087. [CrossRef]
34. Faheem, M.; Shah, S.B.H.; Butt, R.A.; Raza, B.; Anwar, M.; Ashraf, M.W.; Ngadi, M.A.; Gungor, V.C. Smart grid communication and information technologies in the perspective of Industry 4.0: Opportunities and challenges. *Comput. Sci. Rev.* **2018**, *30*, 1–30. [CrossRef]
35. Bian, D.; Kuzlu, M.; Pipattanasomporn, M.; Rahman, S. Analysis of communication schemes for Advanced Metering Infrastructure (AMI). In Proceedings of the 2014 IEEE PES General Meeting | Conference & Exposition, National Harbor, MD, USA, 27–31 July 2014; IEEE: Piscataway, NJ, USA, 2014; pp. 1–5.
36. Dragičević, T.; Siano, P.; Prabakaran, S. Future generation 5G wireless networks for smart grid: A comprehensive review. *Energies* **2019**, *12*, 2140.
37. De Sanctis, M.; Cianca, E.; Araniti, G.; Bisio, I.; Prasad, R. Satellite communications supporting internet of remote things. *IEEE Internet Things J.* **2015**, *3*, 113–123. [CrossRef]
38. Pflanzner, T.; Kertész, A. A survey of IoT cloud providers. In Proceedings of the 2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 30 May–3 June 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 730–735.
39. Cao, K.; Liu, Y.; Meng, G.; Sun, Q. An overview on edge computing research. *IEEE Access* **2020**, *8*, 85714–85728. [CrossRef]
40. Slama, S.B. Prosumer in smart grids based on intelligent edge computing: A review on Artificial Intelligence Scheduling Techniques. *Ain Shams Eng. J.* **2021**, *13*, 101504. [CrossRef]
41. Savazzi, S.; Nicoli, M.; Rampa, V. Federated learning with cooperating devices: A consensus approach for massive IoT networks. *IEEE Internet Things J.* **2020**, *7*, 4641–4654. [CrossRef]
42. Khan, S.A.; Liu, C.; Ansari, J.A. Centralized fuzzy logic based optimization of pi controllers for VSC control in MTDC network. *J. Electr. Eng. Technol.* **2020**, *15*, 2577–2585. [CrossRef]
43. Mocrii, D.; Chen, Y.; Musilek, P. IoT-based smart homes: A review of system architecture, software, communications, privacy and security. *Internet Things* **2018**, *1*, 81–98. [CrossRef]
44. Tighiz, L.; Yang, H. A comprehensive review on IoT protocols' features in smart grid communication. *Energies* **2020**, *13*, 2762. [CrossRef]
45. Avancini, D.B.; Rodrigues, J.J.; Rabêlo, R.A.; Das, A.K.; Kozlov, S.; Solic, P. A new IoT-based smart energy meter for smart grids. *Int. J. Energy Res.* **2021**, *45*, 189–202. [CrossRef]
46. Trappey, A.J.; Trappey, C.V.; Govindarajan, U.H.; Chuang, A.C.; Sun, J.J. A review of essential standards and patent landscapes for the Internet of Things: A key enabler for Industry 4.0. *Adv. Eng. Inform.* **2017**, *33*, 208–229. [CrossRef]
47. Yousefpour, A.; Fung, C.; Nguyen, T.; Kadiyala, K.; Jalali, F.; Niakanlahiji, A.; Kong, J.; Jue, J.P. All one needs to know about fog computing and related edge computing paradigms: A complete survey. *J. Syst. Archit.* **2019**, *98*, 289–330. [CrossRef]
48. Kumari, A.; Tanwar, S.; Tyagi, S.; Kumar, N.; Obaidat, M.S.; Rodrigues, J.J. Fog computing for smart grid systems in the 5G environment: Challenges and solutions. *IEEE Wirel. Commun.* **2019**, *26*, 47–53. [CrossRef]
49. Repo, S.; Pylvanainen, J.; Kauppinen, M.; Repo, S.; Jarventausta, P. Automatic Meter Infrastructure (AMI) as a part of flexibility market. In Proceedings of the 2018 15th International Conference on the European Energy Market (EEM), Lodz, Poland, 27–29 June 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–5.
50. Agalgaonkar, Y.P.; Hammerstrom, D.J. Evaluation of smart grid technologies employed for system reliability improvement: Pacific northwest smart grid demonstration experience. *IEEE Power Energy Technol. Syst. J.* **2017**, *4*, 24–31. [CrossRef]
51. Al Dakheel, J.; Del Pero, C.; Aste, N.; Leonforte, F. Smart buildings features and key performance indicators: A review. *Sustain. Cities Soc.* **2020**, *61*, 102328. [CrossRef]
52. Avancini, D.B.; Rodrigues, J.J.; Martins, S.G.; Rabêlo, R.A.; Al-Muhtadi, J.; Solic, P. Energy meters evolution in smart grids: A review. *J. Clean. Prod.* **2019**, *217*, 702–715. [CrossRef]
53. Nižetić, S.; Djilali, N.; Papadopoulos, A.; Rodrigues, J.J. Smart technologies for promotion of energy efficiency, utilization of sustainable resources and waste management. *J. Clean. Prod.* **2019**, *231*, 565–591. [CrossRef]
54. Switch, S. The Pros and Cons of Smart Meters. Available online: <https://www.simplyswitch.com/energy/guides/smart-meters-pros-cons/> (accessed on 1 April 2022).
55. Sovacool, B.K.; Kivimaa, P.; Hielscher, S.; Jenkins, K. Vulnerability and resistance in the United Kingdom's smart meter transition. *Energy Policy* **2017**, *109*, 767–781. [CrossRef]
56. Goudarzi, A.; Li, Y.; Fahad, S.; Xiang, J. A game theory-based interactive demand response for handling dynamic prices in security-constrained electricity markets. *Sustain. Cities Soc.* **2021**, *72*, 103073. [CrossRef]
57. Waseem, M.; Lin, Z.; Liu, S.; Jinai, Z.; Rizwan, M.; Sajjad, I.A. Optimal BRA based electric demand prediction strategy considering instance-based learning of the forecast factors. *Int. Trans. Electr. Energy Syst.* **2021**, *31*, e12967. [CrossRef]
58. Waseem, M.; Lin, Z.; Liu, S.; Sajjad, I.A.; Aziz, T. Optimal GWCSO-based home appliances scheduling for demand response considering end-users comfort. *Electr. Power Syst. Res.* **2020**, *187*, 106477. [CrossRef]
59. Waseem, M.; Lin, Z.; Liu, S.; Zhang, Z.; Aziz, T.; Khan, D. Fuzzy compromised solution-based novel home appliances scheduling and demand response with optimal dispatch of distributed energy resources. *Appl. Energy* **2021**, *290*, 116761. [CrossRef]
60. Strielkowski, W.; Dvořák, M.; Rovný, P.; Tarkhanova, E.; Baburina, N. 5G wireless networks in the future renewable energy systems. *Front. Energy Res.* **2021**, *9*, 714803. [CrossRef]

61. Khan, T.; Yu, M.; Waseem, M. Review on recent optimization strategies for hybrid renewable energy system with hydrogen technologies: State of the art, trends and future directions. *Int. J. Hydrogen Energy* **2022**, *47*, 25155–25201. [[CrossRef](#)]
62. Agnew, D.; Aljohani, N.; Mathieu, R.; Boamah, S.; Nagaraj, K.; McNair, J.; Bretas, A. Implementation Aspects of Smart Grids Cyber-Security Cross-Layered Framework for Critical Infrastructure Operation. *Appl. Sci.* **2022**, *12*, 6868. [[CrossRef](#)]
63. Tufail, S.; Parvez, I.; Batool, S.; Sarwat, A. A Survey on Cybersecurity Challenges, Detection, and Mitigation Techniques for the Smart Grid. *Energies* **2021**, *14*, 5894. [[CrossRef](#)]
64. Pillitteri, V.Y.; Brewer, T.L. *Guidelines for Smart Grid Cybersecurity*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2014.
65. Agarkar, A.; Agrawal, H. A review and vision on authentication and privacy preservation schemes in smart grid network. *Secur. Priv.* **2019**, *2*, e62. [[CrossRef](#)]
66. Shuaib, K.; Trabelsi, Z.; Abed-Hafez, M.; Gaouda, A.; Alahmad, M. Resiliency of smart power meters to common security attacks. *Procedia Comput. Sci.* **2015**, *52*, 145–152. [[CrossRef](#)]
67. Kimani, K.; Oduol, V.; Langat, K. Cyber security challenges for IoT-based smart grid networks. *J. Crit. Infrastruct. Prot.* **2019**, *25*, 36–49. [[CrossRef](#)]
68. Kenney, M. Cyber-terrorism in a post-stuxnet world. *Orbis* **2015**, *59*, 111–128. [[CrossRef](#)]
69. Libicki, M.C. Correlations between cyberspace attacks and kinetic attacks. In Proceedings of the 2020 12th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 26–29 May 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 199–213.
70. Abdella, J.A.; Shuaib, K. An architecture for blockchain based peer to peer energy trading. In Proceedings of the 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), Granada, Spain, 22–25 October 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 412–419.
71. Dileep, G. A survey on smart grid technologies and applications. *Renew. Energy* **2020**, *146*, 2589–2625. [[CrossRef](#)]
72. Chen, X.; Li, Y.; Goudarzi, A.; Xiang, J. Leaderless Consensus of a Hierarchical Cyber-Physical System. *arXiv* **2020**, arXiv:2004.07411.
73. Faquir, D.; Chouliaras, N.; Sofia, V.; Olga, K.; Maglaras, L. Cybersecurity in smart grids, challenges and solutions. *AIMS Electron. Electr. Eng.* **2021**, *5*, 24–37.
74. Zhang, F.; Mahler, M.; Li, Q. Flooding attacks against secure time-critical communications in the power grid. In Proceedings of the 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm), Dresden, Germany, 23–27 October 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 449–454.
75. Lu, Z.; Lu, X.; Wang, W.; Wang, C. Review and evaluation of security threats on the communication networks in the smart grid. In Proceedings of the 2010-Milcom 2010 Military Communications Conference, San Jose, CA, USA, 31 October–3 November 2010; IEEE: Piscataway, NJ, USA, 2010; pp. 1830–1835.
76. Huseinovic, A.; Mrdovic, S.; Bicakci, K.; Uludag, S. A taxonomy of the emerging Denial-of-Service attacks in the smart grid and countermeasures. In Proceedings of the 2018 26th Telecommunications Forum (TELFOR), Belgrade, Serbia, 20–21 November 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–4.
77. Kurt, M.N.; Yilmaz, Y.; Wang, X. Real-time detection of hybrid and stealthy cyber-attacks in smart grid. *IEEE Trans. Inf. Forensics Secur.* **2018**, *14*, 498–513. [[CrossRef](#)]
78. Gai, K.; Qiu, M.; Sun, X. A survey on FinTech. *J. Netw. Comput. Appl.* **2018**, *103*, 262–273. [[CrossRef](#)]
79. Sakhnini, J.; Karimipour, H.; Dehghantanha, A.; Parizi, R.M.; Srivastava, G. Security aspects of Internet of Things aided smart grids: A bibliometric survey. *Internet Things* **2021**, *14*, 100111. [[CrossRef](#)]
80. Cui, L.; Qu, Y.; Gao, L.; Xie, G.; Yu, S. Detecting false data attacks using machine learning techniques in smart grid: A survey. *J. Netw. Comput. Appl.* **2020**, *170*, 102808. [[CrossRef](#)]
81. Riggs, H.; Tufail, S.; Khan, M.; Parvez, I.; Sarwat, A.I. Detection of False Data Injection, of PV Production. In Proceedings of the 2021 IEEE Green Technologies Conference (GreenTech), Denver, CO, USA, 7–9 April 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 7–12.
82. El Mrabet, Z.; Kaabouch, N.; El Ghazi, H.; El Ghazi, H. Cyber-security in smart grid: Survey and challenges. *Comput. Electr. Eng.* **2018**, *67*, 469–482. [[CrossRef](#)]
83. Gunduz, M.Z.; Das, R. Cyber-security on smart grid: Threats and potential solutions. *Comput. Netw.* **2020**, *169*, 107094. [[CrossRef](#)]
84. Rajendran, G.; Sathyabalu, H.V.; Sachi, M.; Devarajan, V. Cyber Security in Smart Grid: Challenges and Solutions. In Proceedings of the 2019 2nd International Conference on Power and Embedded Drive Control (ICPEDC), Chennai, India, 21–23 August 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 546–551.
85. Peng, C.; Sun, H.; Yang, M.; Wang, Y.-L. A survey on security communication and control for smart grids under malicious cyber attacks. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *49*, 1554–1569. [[CrossRef](#)]
86. Huang, X.; Qin, Z.; Liu, H. A survey on power grid cyber security: From component-wise vulnerability assessment to system-wide impact analysis. *IEEE Access* **2018**, *6*, 69023–69035. [[CrossRef](#)]
87. Wang, X.; Shi, D.; Wang, J.; Yu, Z.; Wang, Z. Online identification and data recovery for PMU data manipulation attack. *IEEE Trans. Smart Grid* **2019**, *10*, 5889–5898. [[CrossRef](#)]
88. Alohal, B.; Kifayat, K.; Shi, Q.; Hurst, W. Replay attack impact on advanced metering infrastructure (AMI). In *Smart Grid Inspired Future Technol*; Springer: Cham, Switzerland, 2017; pp. 52–59.

89. Liu, Z.; Wang, Q.; Ye, Y.; Tang, Y. A GAN Based Data Injection Attack Method on Data-Driven Strategies in Power Systems. *IEEE Trans. Smart Grid* **2022**, *13*, 3203–3213. [[CrossRef](#)]
90. Mollah, M.B.; Zhao, J.; Niyato, D.; Lam, K.-Y.; Zhang, X.; Ghias, A.M.; Koh, L.H.; Yang, L. Blockchain for future smart grid: A comprehensive survey. *IEEE Internet Things J.* **2020**, *8*, 18–43. [[CrossRef](#)]
91. Kurt, M.N.; Yilmaz, Y.; Wang, X. Distributed quickest detection of cyber-attacks in smart grid. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 2015–2030. [[CrossRef](#)]
92. Burg, A.; Chattopadhyay, A.; Lam, K.-Y. Wireless communication and security issues for cyber-physical systems and the Internet-of-Things. *Proc. IEEE* **2017**, *106*, 38–60. [[CrossRef](#)]
93. Aldwairi, M.; Alansari, D. n-Grams exclusion and inclusion filter for intrusion detection in Internet of Energy big data systems. *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e3711. [[CrossRef](#)]
94. Alotaibi, B. Utilizing blockchain to overcome cyber security concerns in the internet of things: A review. *IEEE Sens. J.* **2019**, *19*, 10953–10971. [[CrossRef](#)]
95. Sani, A.S.; Yuan, D.; Jin, J.; Gao, L.; Yu, S.; Dong, Z.Y. Cyber security framework for Internet of Things-based Energy Internet. *Future Gener. Comput. Syst.* **2019**, *93*, 849–859. [[CrossRef](#)]
96. Wang, T.; Hua, H.; Wei, Z.; Cao, J. Challenges of blockchain in new generation energy systems and future outlooks. *Int. J. Electr. Power Energy Syst.* **2022**, *135*, 107499. [[CrossRef](#)]
97. Rakas, S.B.; Timčenko, V.; Kabovič, M.; Kabovič, A. Intrusion Detection Systems in Smart Grid. In Proceedings of the 2022 21st International Symposium Infoteh-Jahorina (INFOTEH), East Sarajevo, Bosnia and Herzegovina, 16–18 March 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–6.
98. Mohammadi, Z.; Pinto, S.J.; Panda, G.; Thokchom, S. A Survey of Cyber Security in Smart Microgrid. In *Sustainable Energy and Technological Advancements*; Springer: Singapore, 2022; pp. 687–698.
99. Badar, A.Q.; Patil, P.; Sanjari, M. Introduction and history of virtual power plants with experimental examples. In *Scheduling and Operation of Virtual Power Plants*; Elsevier: Amsterdam, The Netherlands, 2022; pp. 1–26.
100. Li, Y.; Li, T.; Zhang, H.; Xie, X.; Sun, Q. Distributed Resilient Double-Gradient-Descent Based Energy Management Strategy for Multi-Energy System under DoS Attacks. *IEEE Trans. Netw. Sci. Eng.* **2022**, *9*, 2301–2316. [[CrossRef](#)]
101. Brown, M.A.; Zhou, S.; Ahmadi, M. Smart grid governance: An international review of evolving policy issues and innovations. *Wiley Interdiscip. Rev. Energy Environ.* **2018**, *7*, e290. [[CrossRef](#)]
102. Holik, F.; Flå, L.H.; Jaatun, M.G.; Yayilgan, S.Y.; Foros, J. Threat modeling of a smart grid secondary substation. *Electronics* **2022**, *11*, 850. [[CrossRef](#)]
103. Goudarzi, A.; Fahad, S.; Ni, J.; Ghayoor, F.; Siano, P.; Haes Alhelou, H. A sequential hybridization of ETLBO and IPSO for solving reserve-constrained combined heat, power and economic dispatch problem. *IET Gener. Transm. Distrib.* **2022**, *16*, 1930–1949. [[CrossRef](#)]
104. Goudarzi, A.; Zhang, C.; Fahad, S.; Mahdi, A.J. A hybrid sequential approach for solving environmentally constrained optimal scheduling in co-generation systems. *Energy Rep.* **2021**, *7*, 3460–3479. [[CrossRef](#)]
105. Khezri, R.; Mahmoudi, A.; Aki, H. Optimal planning of solar photovoltaic and battery storage systems for grid-connected residential sector: Review, challenges and new perspectives. *Renew. Sustain. Energy Rev.* **2022**, *153*, 111763. [[CrossRef](#)]
106. Ghasemi-Marzbali, A. Fast-charging station for electric vehicles, challenges and issues: A comprehensive review. *J. Energy Storage* **2022**, *49*, 104136.
107. Khan, S.A.; Wang, M.; Su, W.; Liu, G.; Chaturvedi, S. Grid-Forming Converters for Stability Issues in Future Power Grids. *Energies* **2022**, *15*, 4937. [[CrossRef](#)]
108. Nejabatkhah, F.; Li, Y.W.; Liang, H.; Reza Ahrabi, R. Cyber-security of smart microgrids: A survey. *Energies* **2020**, *14*, 27. [[CrossRef](#)]
109. Fahad, S.; Goudarzi, A.; Xiang, J. Demand management of active distribution network using coordination of virtual synchronous generators. *IEEE Trans. Sustain. Energy* **2020**, *12*, 250–261. [[CrossRef](#)]
110. Farraj, A.; Hammad, E.; Kundur, D. On the impact of cyber attacks on data integrity in storage-based transient stability control. *IEEE Trans. Ind. Inform.* **2017**, *13*, 3322–3333. [[CrossRef](#)]
111. Khalghani, M.R.; Solanki, J.; Solanki, S.K.; Khooban, M.H.; Sargolzaei, A. Resilient frequency control design for microgrids under false data injection. *IEEE Trans. Ind. Electron.* **2020**, *68*, 2151–2162. [[CrossRef](#)]
112. Ibrahim, M.S.; Dong, W.; Yang, Q. Machine learning driven smart electric power systems: Current trends and new perspectives. *Appl. Energy* **2020**, *272*, 115237. [[CrossRef](#)]
113. Ali, W.; Din, I.U.; Almogren, A.; Kim, B.-S. A Novel Privacy Preserving Scheme for Smart Grid-Based Home Area Networks. *Sensors* **2022**, *22*, 2269. [[CrossRef](#)]
114. Abdullah, A.M.; Ullah, I.; Khan, M.A.; Alsharif, M.H.; Mostafa, S.M.; Wu, J.M.-T. An Efficient Multidocument Blind Signcryption Scheme for Smart Grid-Enabled Industrial Internet of Things. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 7779152. [[CrossRef](#)]
115. Zamani, R.; Moghaddam, M.P.; Haghifam, M.-R. Dynamic Characteristics Preserving Data Compressing Algorithm For Transactive Energy Management Frameworks. *IEEE Trans. Ind. Inform.* **2022**, *18*, 7587–7596. [[CrossRef](#)]
116. Lin, Y.; Wang, J. Realizing the Transactive Energy Future with Local Energy Market: An Overview. *Curr. Sustain./Renew. Energy Rep.* **2022**, *9*, 1–14. [[CrossRef](#)]
117. Goel, S.; Hong, Y. Security challenges in smart grid implementation. In *Smart Grid Security*; Springer: London, UK, 2015; pp. 1–39.

118. Sharifi, A.; Yamagata, Y. Principles and criteria for assessing urban energy resilience: A literature review. *Renew. Sustain. Energy Rev.* **2016**, *60*, 1654–1677. [[CrossRef](#)]
119. Kalogridis, G.; Sooriyabandara, M.; Fan, Z.; Mustafa, M.A. Toward unified security and privacy protection for smart meter networks. *IEEE Syst. J.* **2013**, *8*, 641–654. [[CrossRef](#)]
120. Mühlberg, J.T.; Cleemput, S.; Mustafa, M.A.; Bulck, J.V.; Preneel, B.; Piessens, F. An implementation of a high assurance smart meter using protected module architectures. In Proceedings of the IFIP International Conference on Information Security Theory and Practice, Heraklion, Greece, 26–27 September 2016; Springer: Cham, Switzerland, 2016; pp. 53–69.
121. Ma, C. Smart city and cyber-security; technologies used, leading challenges and future recommendations. *Energy Rep.* **2021**, *7*, 7999–8012. [[CrossRef](#)]
122. Canaan, B.; Colicchio, B.; Ould Abdeslam, D. Microgrid cyber-security: Review and challenges toward resilience. *Appl. Sci.* **2020**, *10*, 5649. [[CrossRef](#)]
123. Gunduz, M.Z.; Das, R. A comparison of cyber-security oriented testbeds for IoT-based smart grids. In Proceedings of the 2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, 22–25 March 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–6.
124. Sadik, S.; Ahmed, M.; Sikos, L.F.; Islam, A. Toward a sustainable cybersecurity ecosystem. *Computers* **2020**, *9*, 74. [[CrossRef](#)]
125. Yamin, M.M.; Ullah, M.; Ullah, H.; Katt, B. Weaponized AI for cyber attacks. *J. Inf. Secur. Appl.* **2021**, *57*, 102722. [[CrossRef](#)]
126. Abdullahi, M.; Baashar, Y.; Alhussian, H.; Alwadain, A.; Aziz, N.; Capretz, L.F.; Abdulkadir, S.J. Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review. *Electronics* **2022**, *11*, 198. [[CrossRef](#)]
127. Mahajan, V.; Singh, N.K.; Gupta, P.K.; Yadav, A.K.; Mudagal, S. Smart Grid Cyber Security Threats and Solutions. In *Deregulated Electricity Structures and Smart Grids*; CRC Press: Boca Raton, FL, USA, 2022; pp. 233–258.
128. Badihi, H. Smart Grid Resilience. In *Handbook of Smart Energy Systems*; Springer: Cham, Switzerland, 2022; pp. 1–25.
129. Hudani, D.; Haseeb, M.; Taufiq, M.; Umer, M.A.; Kandasamy, N.K. A Data-Centric Approach to Generate Invariants for a Smart Grid Using Machine Learning. *arXiv* **2022**, arXiv:2202.06717.
130. Ahmad, T.; Madonski, R.; Zhang, D.; Huang, C.; Mujeeb, A. Data-driven probabilistic machine learning in sustainable smart energy/smart energy systems: Key developments, challenges, and future research opportunities in the context of smart grid paradigm. *Renew. Sustain. Energy Rev.* **2022**, *160*, 112128. [[CrossRef](#)]
131. Hink, R.C.B.; Beaver, J.M.; Buckner, M.A.; Morris, T.; Adhikari, U.; Pan, S. Machine learning for power system disturbance and cyber-attack discrimination. In Proceedings of the 2014 7th International symposium on resilient control systems (ISRCs), Denver, CO, USA, 19–21 August 2014; IEEE: Piscataway, NJ, USA, 2014; pp. 1–8.
132. Ashrafuzzaman, M.; Das, S.; Chakhchoukh, Y.; Shiva, S.; Sheldon, F.T. Detecting stealthy false data injection attacks in the smart grid using ensemble-based machine learning. *Comput. Secur.* **2020**, *97*, 101994. [[CrossRef](#)]
133. Pei, C.; Xiao, Y.; Liang, W.; Han, X. A Deviation-Based Detection Method Against False Data Injection Attacks in Smart Grid. *IEEE Access* **2021**, *9*, 15499–15509. [[CrossRef](#)]
134. He, Y.; Mendis, G.J.; Wei, J. Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism. *IEEE Trans. Smart Grid* **2017**, *8*, 2505–2516. [[CrossRef](#)]
135. Ali, S.; Li, Y. Learning multilevel auto-encoders for DDoS attack detection in smart grid network. *IEEE Access* **2019**, *7*, 108647–108659. [[CrossRef](#)]
136. Califano, A.; Dincelli, E.; Goel, S. Using features of cloud computing to defend smart grid against DDoS attacks. In Proceedings of the 10th Annual Symposium on Information Assurance (ASIA 15), Albany, NY, USA, 2–3 June 2015; pp. 44–50.
137. Eltayieb, N.; Elhabob, R.; Hassan, A.; Li, F. An efficient attribute-based online/offline searchable encryption and its application in cloud-based reliable smart grid. *J. Syst. Archit.* **2019**, *98*, 165–172. [[CrossRef](#)]
138. Chen, L.; Liu, J.; Ha, W. Cloud service security evaluation of smart grid using deep belief network. *Int. J. Sens. Netw.* **2020**, *33*, 109–121. [[CrossRef](#)]
139. Bagherzadeh, L.; Shahinzadeh, H.; Shayeghi, H.; Dejamkhooy, A.; Bayindir, R.; Iranpour, M. Integration of cloud computing and IoT (CloudIoT) in smart grids: Benefits, challenges, and solutions. In Proceedings of the 2020 International Conference on Computational Intelligence for Smart Power System and Sustainable Energy (CISPSSE), Keonjhar, India, 29–31 July 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–8.
140. Dehalwar, V.; Kolhe, M.L.; Deoli, S.; Jhariya, M.K. Blockchain-based trust management and authentication of devices in smart grid. *Clean. Eng. Technol.* **2022**, *8*, 100481.
141. Mahmood, S.; Chadhar, M.; Firmin, S. Cybersecurity Challenges in Blockchain Technology: A Scoping Review. *Hum. Behav. Emerg. Technol.* **2022**, *2022*, 7384000. [[CrossRef](#)]
142. Asif, M.; Aziz, Z.; Bin Ahmad, M.; Khalid, A.; Waris, H.A.; Gilani, A. Blockchain-Based Authentication and Trust Management Mechanism for Smart Cities. *Sensors* **2022**, *22*, 2604. [[CrossRef](#)] [[PubMed](#)]
143. Zhong, Y.; Zhou, M.; Li, J.; Chen, J.; Liu, Y.; Zhao, Y.; Hu, M. Distributed blockchain-based authentication and authorization protocol for smart grid. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 5560621. [[CrossRef](#)]
144. Kirpes, B.; Mengelkamp, E.; Schaal, G.; Weinhardt, C. Design of a microgrid local energy market on a blockchain-based information system. *IT-Inf. Technol.* **2019**, *61*, 87–99. [[CrossRef](#)]
145. Fischer-Hübner, S.; Alcaraz, C.; Ferreira, A.; Fernandez-Gago, C.; Lopez, J.; Markatos, E.; Islami, L.; Akil, M. Stakeholder perspectives and requirements on cybersecurity in Europe. *J. Inf. Secur. Appl.* **2021**, *61*, 102916. [[CrossRef](#)]

146. Gope, P. PMAKE: Privacy-aware multi-factor authenticated key establishment scheme for advance metering infrastructure in smart grid. *Comput. Commun.* **2020**, *152*, 338–344. [[CrossRef](#)]
147. Dong, H.; Zhao, J.; Yang, X.; Yang, K. Combination of D-AHP and grey theory for the assessment of the information security risks of smart grids. *Math. Probl Eng.* **2020**, *2020*, 3517104. [[CrossRef](#)]
148. Sun, C.-C.; Cardenas, D.J.S.; Hahn, A.; Liu, C.-C. Intrusion detection for cybersecurity of smart meters. *IEEE Trans. Smart Grid* **2020**, *12*, 612–622. [[CrossRef](#)]
149. El May, Z.; Ayed, H.K.B.; Machfar, D. State of the art on Privacy Risk Estimation Related to Android Applications. In Proceedings of the 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), Tangier, Morocco, 24–28 June 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 889–894.
150. Djenna, A.; Harous, S.; Saidouni, D.E. Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. *Appl. Sci.* **2021**, *11*, 4580. [[CrossRef](#)]
151. Yahaya, A.S.; Javaid, N.; Ullah, S.; Khalid, R.; Javed, M.U.; Khan, R.U.; Wadud, Z.; Khan, M.A. A secure and efficient energy trading model using blockchain for a 5G-deployed smart community. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 6953125.
152. Shahinzadeh, H.; Mahmoudi, A.; Moradi, J.; Nafisi, H.; Kabalci, E.; Benbouzid, M. Anomaly Detection and Resilience-Oriented Countermeasures against Cyberattacks in Smart Grids. In Proceedings of the 2021 7th International Conference on Signal Processing and Intelligent Systems (ICSPIS), Tehran, Iran, 29–30 December 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–7.
153. Leszczyna, R. Standards on cyber security assessment of smart grid. *Int. J. Crit. Infrastruct. Prot.* **2018**, *22*, 70–89. [[CrossRef](#)]
154. Allahvirdizadeh, Y.; Moghaddam, M.P.; Shayanfar, H. A survey on cloud computing in energy management of the smart grids. *Int. Trans. Electr. Energy Syst.* **2019**, *29*, e12094. [[CrossRef](#)]