Journal of
Sensor and Actuator Networks

MDPI

Article

Edge Intelligence in Smart Grids: A Survey on Architectures, Offloading Models, Cyber Security Measures, and Challenges

Daisy Nkele Molokomme [1,*], Adeiza James Onumanyi [2] and Adnan M. Abu-Mahfouz [1,2]

[1] Department of Electrical, Electronic and Computer Engineering, University of Pretoria, Pretoria 0028, South Africa
[2] Next Generation Enterprises and Institutions, Council for Scientific and Industrial Research (CSIR), Pretoria 0001, South Africa
* Correspondence: u11261766@tuks.co.za

Abstract: The rapid development of new information and communication technologies (ICTs) and the deployment of advanced Internet of Things (IoT)-based devices has led to the study and implementation of edge computing technologies in smart grid (SG) systems. In addition, substantial work has been expended in the literature to incorporate artificial intelligence (AI) techniques into edge computing, resulting in the promising concept of edge intelligence (EI). Consequently, in this article, we provide an overview of the current state-of-the-art in terms of EI-based SG adoption from a range of angles, including architectures, computation offloading, and cybersecurity concerns. The basic objectives of this article are fourfold. To begin, we discuss EI and SGs separately. Then we highlight contemporary concepts closely related to edge computing, fundamental characteristics, and essential enabling technologies from an EI perspective. Additionally, we discuss how the use of AI has aided in optimizing the performance of edge computing. We have emphasized the important enabling technologies and applications of SGs from the perspective of EI-based SGs. Second, we explore both general edge computing and architectures based on EI from the perspective of SGs. Thirdly, two basic questions about computation offloading are discussed: what is computation offloading and why do we need it? Additionally, we divided the primary articles into two categories based on the number of users included in the model, either a single user or a multiple user instance. Finally, we review the cybersecurity threats with edge computing and the methods used to mitigate them in SGs. Therefore, this survey comes to the conclusion that most of the viable architectures for EI in smart grids often consist of three layers: device, edge, and cloud. In addition, it is crucial that computation offloading techniques must be framed as optimization problems and addressed effectively in order to increase system performance. This article typically intends to serve as a primer for emerging and interested scholars concerned with the study of EI in SGs.

Keywords: computation offloading; cyber security; edge computing; edge intelligence; internet of things; smart grid

Citation: Molokomme, D.N.; Onumanyi, A.J.; Abu-Mahfouz, A.M. Edge Intelligence in Smart Grids: A Survey on Architectures, Offloading Models, Cyber Security Measures, and Challenges. *J. Sens. Actuator Netw.* **2022**, *11*, 47. https://doi.org/10.3390/jsan11030047

Academic Editor: Mingjun Xiao

Received: 20 June 2022
Accepted: 16 August 2022
Published: 21 August 2022

1. Introduction

Smart grids (SG) are widely recognized as the "next-generation power grids" comprising sophisticated cyber-secured information and communication technologies (ICT), bidirectional information and electricity infrastructure, and network-integrated computational intelligence [1–3]. The concept of SGs evolved around the year 2000 as a feasible solution to the substantial challenges connected with the old (legacy) power grid system [4–6]. Among these difficulties are a lack of automated analysis, insufficient accessibility, a lack of situational awareness, and slow response times [7]. To put things into context, legacy electrical grids were developed, planned, built, and deployed decades ago in a significantly different political, social, and technological environment than exists now [8]. However, with the passage of time, it is evident that aging infrastructures have played a major role in the decline of these grids, in addition to other inherent characteristics

such as their one-way communication structure, centralized generation, restricted sensors, manual restoration, and limited monitoring capabilities [9,10]. However, despite the fact that legacy power systems have seen little to no alteration in decades, the number of customers connected to the grids continues to grow at a rapid pace. As a result, the design and development of new infrastructure is critical to resolving the aforementioned issues.

Essentially, SGs are aimed at improving energy generation, transmission, and distribution by connecting intelligent monitoring, two-way communication, control, and self-healing technologies with innovative products and services [8]. Another advantage of SGs is their new enabling network management strategies, which provide for the use of distributed generation (DG) in demand side management (DSM), energy storage for DG load balancing, and for the deployment of advanced metering infrastructure (AMI) for two-way communication between consumers, prosumers, and control centers [10]. Additionally, SGs enable a complete paradigm change from the old communication infrastructure to a contemporary electric grid architecture capable of increased sensing, sophisticated communication, and computation.

Smart devices (e.g., smart meters, sensors, and smart electrical appliances) are utilized in SGs to generate data via different applications and services. Currently, many SG designs rely significantly on cloud computing to store, analyse, and process data in preparation for future control commands and decision-making purposes [1,11,12]. However, existing traditional cloud computing platforms, on the other hand, have a number of shortcomings, including large communication latency, network and deployment complexities, all of which restrict their use in real-time applications [13]. Various strategies have been proposed in the literature to overcome the aforementioned problems of cloud computing services. These techniques are nonetheless subject to a number of constraints as a result of the foundational architecture of the cloud computing framework. Some of these constraints include efficiency, privacy, and security, amongst others. In a bid to address these issues, the authors of [14] proposed a heuristic algorithm in an attempt to intelligently optimize the energy efficiency across geographically distant data centers that are connected by cloud networks. Similarly, optimization strategies were used to solve the issue of power consumption in cloud infrastructure in [15].

To further solve these issues effectively in traditional cloud computing, edge computing was introduced recently. This developing paradigm of edge computing goes beyond the concept of re-evaluating cloud computing and aims for a dramatic movement away from distance storage and processing centers in order to reduce latency and cost, as well as to improve security and dependability [16]. Specifically, the term "edge computing" refers to the process of transferring certain storage and computation resources away from a remote central data center (cloud) and closer to the data source. The technological improvements in smart IoT and mobile devices allows for the development of new applications and services that meet these evolving demands. As computing and storage capabilities migrate closer to the edge, some edge devices may struggle to run high-intensity applications and services due to their low battery capacity and energy consumption characteristics [17]. Thus, an appropriate solution has been established, which is based on the concept of computation offloading. This strategy entails offloading high computational or latency-sensitive operations to edge devices or servers in order to comply with quality of service (QoS) requirements [18,19]. However, such a strategy being implemented in a highly diverse and distributed edge computing network ultimately raises concerns regarding security and privacy issues. Thus, as a possible solution to the aforementioned issues, the subject of artificial intelligence (AI) has begun to garner research interest in both academia and industry.

To this effect, the collaborative integration of AI with edge computing has sufficed as a suitable solution to a number of issues associated with conventional edge computing, such as limited computational power, processing capabilities, security, and storage capacity problems. Such a convergence of AI with edge computing is referred to as edge intelligence (EI) [5,20–26]. EI is not only the fusion of these two terminologies, but more of a broad and complex subject area that encompasses a wide variety of concepts and technologies [22].

Presently, the deployment of EI in SGs is still in its infancy. However, by locating computing capabilities closer to data sources, edge intelligence promises to optimize the overall network performance of SG networks in terms of lowering their network processing and maintenance costs, easing the strain of data transfer via network backhauls, and enabling rapid decisions [5,27]. To this effect, instead of transferring raw data (generated by computationally expensive processes) directly to the cloud, EI will consist of incorporating intelligent elements into edge devices that will serve to process and analyze the data generated locally. However, despite the fact that EI promises great potentials for SG systems, there are several limitations inherent in contemporary AI systems that may limit its use.

Among these problems are those relating to security and privacy issues. In this regard, several publications have explored the application of blockchain technologies to solve these cybersecurity concerns [28–30]. Despite the number of surveys on edge intelligence, to the best of our knowledge, an extensive review that simultaneously explores the convergence of EI and SGs in terms of architectures, offloading models, and cybersecurity measures has not yet been undertaken. Thus, this article aims to provide an overview of the current state of the art in terms of EI-based SG adoption from these three main angles, and these contributions are summarized as follows:

1. We have provided a synthesis of the most recent studies on the application of EI in SGs. It was discovered that the literature lacked a survey of this nature, and the purpose of the current article is to address this gap, particularly for the benefit of researchers who may interested in developing some knowledge about the subject.
2. We conducted a detailed overview of edge computing architectures and those based on EI for deployment in SGs. Due to the paucity of comprehensive EI-based designs for SG latency-sensitive applications in the existing literature, we also discussed a deployment-friendly architecture for the integration of EI in SGs.
3. We highlighted and emphasized a number of critical cybersecurity issues linked with edge computing, as well as discussed some available solutions to these challenges in SG applications. We provided additional details on how machine learning algorithms and blockchain technologies were used to solve these problems.
4. We discussed the current challenges that are associated with SGs and EI, which have surfaced as a result of the confluence of these two ideas. These challenges include communication at the edge, big data processing, resource management, and effective big data offloading, to mention a few of them. These difficulties and possible paths for the future are presented with an intention to aid the development of potential solutions regarding the adoption of EI in SGs.

A general view of the article's organizational structure is shown in Figure 1, which is further summarized as follows: we discuss related survey articles in Section 2, which is entirely focused on establishing the uniqueness of our article. To establish context for our survey, we provide in Section 3 an in-depth overview of EI and SGs from a variety of perspectives, including important enabling technologies, features, and applications. Following that, in Section 4 we review appropriate architectures for implementing EI in SGs and presented an EI-based architecture for SGs applications. Additionally, key general concepts relating to computation offloading were examined in Section 5, including what and why we require computation offloading and the classification of computation offloading (i.e., multiple user and single user scenarios). Section 6 examines cybersecurity concerns and solutions for SGs powered by EI. In Section 7, we discuss research challenges and future research. Finally, in Section 8, we summarize and give concluding remarks on our survey.

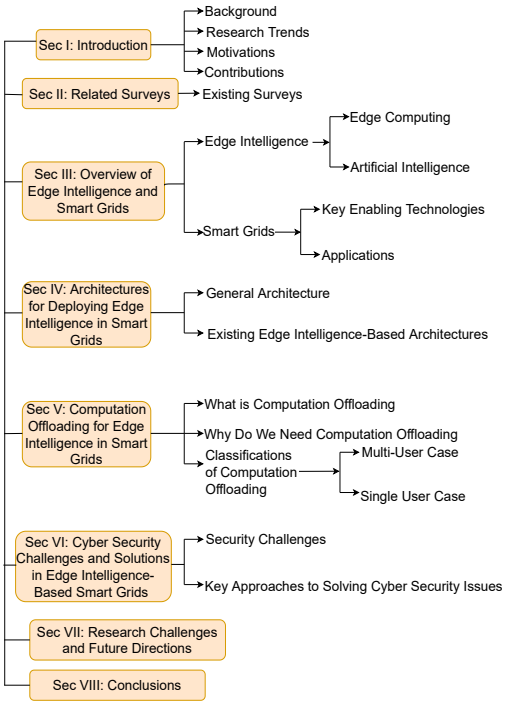

Figure 1. Paper organization structure.

2. Related Surveys

In this section, we aim to provide a comprehensive review of some of the most important survey publications that are primarily concerned with the convergence of EI and SGs. In recent years, a few survey articles, as highlighted in Table 1, have attempted to explore contemporary SG issues and how the incorporation of EI might aid in alleviating them.

The selection criteria of articles considered in our survey focused on the current research works dealing with edge intelligence in smart grids. The following is an explanation of the approach that was utilized in the selection of the papers:

1. The keywords that characterize our area of interest were noted, namely "architectures", "computation offloading", "edge intelligence", "smart grids", "security", and these were used to search within the Scopus and Google Scholar database among others that were taken into consideration.
2. The search process returned more than 16,700 hits, which were then narrowed down based on the period covered within the last decade. In addition, these hits were improved based on the following important categories: "architectures", "offloading procedures", and "security". These keywords were used to manually narrow down our selection to around 250 articles, of which 234 were included in this article. The articles omitted were those that did not contribute directly to our area of interest.
3. Furthermore, all survey articles found within this narrowed list were then culled and analyzed to establish the originality of the current article, for which we will now discuss these related survey articles.

Table 1. Summary of Related Surveys.

Survey Articles	Year	Highlights
Rigas et al. [31]	2014	• Survey on AI techniques to render EVs in SGs • Identify the commonalities and key differences in the approaches • Develop classification of key technologies • Develop benchmarks for state-of-the-art
Meloni et al. [23]	2018	• Analyze case studies based on distribution networks monitoring • State-of-the-art solutions • Demonstrate the performance of Cloud-IoT-based architectural solution for SE in SG
Gilbert et al. [32]	2019	• Systematic review on the research trend of actual implementations of edge and fog computing for SG applications • Investigate the challenges hindering adoption of fog and edge computing in SG
Ferrag et al. [33]	2020	• Comprehensive survey of existing cyber security solutions for fog-based SG SCADA systems • Overview of architecture and the concept of fog-based SG SCADA • Summarize informal and formal security analysis techniques • Provides taxonomy of attacks mitigated by privacy-preserving and authentication solutions
Rosero et al. [34]	2021	• Identify elements in existing works to define cloud-based architecture • Revise and run microgrid real-time simulation platforms • Presents scalable and autonomous cloud-based architecture for forecasting, consumption, etc using ML techniques
Feng et al. [35]	2021	• Comprehensive review of interdisciplinary research on EC applications in SG • In-depth analysis of EC is conducted from SG perspective • Systematically explores application scenarios of EC in SG • Assisted synergistic effect of the integration of EC and SG
Slama [5]	2021	• Investigate EC solutions for the SG • Comprehensive review on emerging issues of EC in SG • Extensively covers techniques to improve reader awareness on prosumer SG system
Mehmood et al. [6]	2021	• Comprehensive review of SG systems based on IoT and EC • Development in the rising technologies • Framework for EC-IoT based SG is examined • Requirements to implement EC-IoT SG system are outlined
Li et al. [36]	2021	• Introduce AI-based algorithms for multi-access EC for benchmark microgrid performance optimization • Present online dual-network-based action-dependent heuristic dynamic programming method • Apply optimal control strategy to a benchmark microgrid system
Hudson et al. [24]	2021	• Provide an overview for how EC and EI can supplement AMI applications • FL-based architecture to empower distributed data processing • Demonstrate the efficacy of the architecture using NILM
Wu et al. [37]	2021	• Comprehensive discussion on the key infrastructures • Systematic overview on how IoT drives the digitization of transactive EI • Discussion on how to implement digitization and decentralization of transactive EI such as AMI • Highlights challenges and future trends from cyber space point of view
Massaoudi et al. [38]	2021	• Thorough review on the state-of-the-art advances of DL in SG systems • Bibliometric analysis • Taxonomy of the trending DL algorithms • DL enabling technologies (FL, EI and distributed computing) in SG

EI has dominated the majority of the research undertaken thus far in terms of developing and constructing resilient SG infrastructures. This is due to the importance and sensitivity of the data generated by SG applications. Consequently, AI approaches that operate well with the edge computing paradigm need be studied thoroughly before they can be deployed in practical SG use cases. Thus, the authors in [31] conducted a detailed study of AI approaches that may be suited for the application of EI in SG. Specifically, they discussed the difficulties that often arise from using AI to jointly manage the distribution of electric vehicles (EVs) in SG networks.

In a related article, the authors in [23] analysed several case studies that are based on the concept of distribution network monitoring. They also introduced a cloud-IoT-based architecture solution for estimating SG state. Nonetheless, despite the benefits of SG network operation, there are a number of issues that require rapid research and development attention from both academia and industry. Towards this end, the authors in [32] reviewed the research trend of actual edge and fog computing solutions for SG applications. The limits of various computing paradigms were also investigated. It was noted that the evolution

of architectural solutions from cloud-based [23] to edge-based [32] and cyber-based [33] is certainly necessary on the electrical energy frontiers. Similarly, the authors in [33] presented a survey of research on some of the cyber security solutions for fog-based SG supervisory control and data acquisition (SCADA) systems. In addition, an introduction to the architecture and idea of fog-based SG SCADA was presented. This, however, was restricted to the cyber security challenges typically encountered by SCADA systems. They also examined current informal and formal security studies in the literature, as well as created a taxonomy of threats addressed by privacy-preserving and authentication methods. Similarly, the review presented in [34] examined modifications to microgrid real-time simulation with the help of ML. Their goal was to identify a scalable and autonomous cloud-based architecture that improves forecasting and consumption through the use of ML techniques.

Recently, edge computing has garnered considerable interest as a potential solution for mitigating some of the fundamental difficulties confronting SG. It achieves this by bringing computing operations executed in the remote Internet cloud closer to end users. According to some of the theoretical assumptions established in the literature, this concept promises to minimise data transmission time while simultaneously increasing bandwidth usage, among other advantages. The authors in [35] conducted a rigorous and comprehensive assessment of the multidisciplinary research of edge computing applications in SGs. They extensively investigated application possibilities available in the edge computing literature in SG. Similarly, the review in [5] explored edge computing solutions for SG. A detailed analysis of the growing difficulties and the implementation of edge computing in SG were also emphasized. The survey, however, was limited to prosumers in SG systems. Instead of focusing solely on edge computing and SG, the authors in [6] thoroughly analysed SG systems from an IoT and edge computing standpoint. They also emphasized the prerequisites for implementing edge computing-IoT-based SG systems.

From the foregoing, it is clear that the introduction of edge computing has the potential to greatly transform SG applications. Nevertheless, although edge computing has demonstrated remarkable performance in a variety of applications, it still faces significant limitations that restrict its potential to be used in real-time applications. Considering the potentials that surround the coordination of AI in real-time applications, researchers are now investigating its benefits in the context of edge computing [24,36–39]. For example, in Ref. [36], an introduction to AI-based methods for multi-access edge computing for benchmarking microgrid performance optimization was presented. In addition, their study offered an optimum control technique that was implemented on a benchmark microgrid system. In a different article, an outline of how edge computing and EI may be used together to improve AMI applications was presented [24]. In addition, a federated learning (FL)-based architecture for enabling distributed data processing in AMI was demonstrated. Because IoT is essential in delivering EI benefits, the authors in [37] undertook a comprehensive examination of how this notion encourages transactive EI digitization. Based on EI, they also performed a complete evaluation of certain existing critical infrastructure. They discussed how to adopt digitalization and decentralization of transactive EI such as AMI. To realize the benefits of SG deployment, DL supporting technologies such as FL, EI, and distributed computing were shown in an SG context.

Although the emergence of EI has been studied in a variety of business domains, the same cannot be said for the frontiers of electrical energy. To the best of our knowledge, the convergence of EI and SGs remains a budding research area with limited survey articles available on the subject matter. Consequently, the purpose of this article is to contribute by conducting an in-depth survey of key concepts in this area.

3. Overview of Edge Intelligence and Smart Grid

This section provides an overview of EI and SG and the necessity to deploy EI in the next-generation power grids. To begin, we will define EI by examining various elements of edge computing such as its characteristics, important enabling technologies, and its emerging advantages. Then, we will provide a general discussion of SGs.

3.1. Edge Intelligence

Edge intelligence (EI) refers to the combination of artificial intelligence (AI) with edge computing [40,41]. Thus, in order to comprehend EI, it is essential to consider separately the concept of edge computing and AI. On the one hand, edge computing describes the process of extending computing, storage, and communication resources from a centralized cloud server to the edge of a network [19,42]. The purpose of edge computing is to provide mobile applications with real-time access to the radio network while maintaining ultra-low latency and high bandwidth capabilities. On the other hand, we have witnessed a transformation in recent years due to the widespread use of AI in a number of application areas. Consequently, as a result of the rapid growth of both of these areas (edge computing and AI), researchers and developers are continuously looking for newer ways to investigate them jointly [20,22,25,41,43–45]. This convergence of interest in AI and edge computing has resulted in the emergence of EI. However, before delving into EI in detail, a brief explanation of edge computing and its associated computing paradigms will serve as a basis for comprehending the concept of EI.

3.1.1. Edge Computing

Edge computing refers to the process of relocating certain storage and computation resources out from the central data center and closer to the data source [46]. Rather than send raw data to the central cloud server for processing and analysis (as in cloud computing), such data are analyzed closer to the source of the data (network edge). Thus, only the outcomes of such edge computing operations, such as real-time business analytics, equipment repair projections, or other actionable responses are routed directly to the central cloud server for scrutiny and perhaps for other human interaction purposes. To have a better understanding of edge computing, it is necessary to emphasize other closely related concepts that are often mistaken for edge computing. These related concepts are discussed in the next subsection.

Concepts Closely Related to Edge Computing

Due to the fact that some aspects of edge computing overlap with other related computing paradigms such as fog computing, mobile edge computing, and cloudlet computing, as illustrated in Figure 2, some researchers have frequently used these paradigms interchangeably [19,35]. As a consequence, because they are not precisely the same, these different concepts may generate some misunderstanding among readers. By and large, these related paradigms were developed to address the issues inherent in cloud computing, such as latency, complexity, and security. However, there have been some misconceptions about how these various paradigms differ from one another.

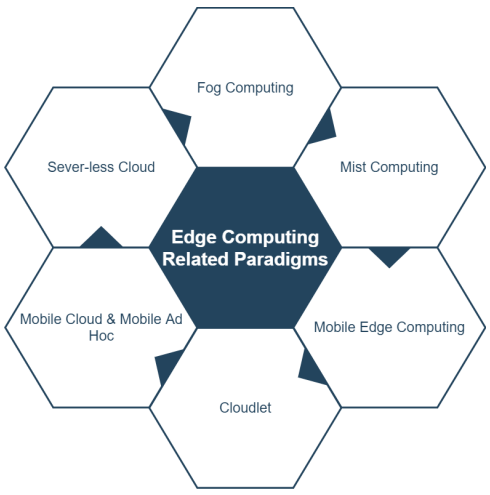

Figure 2. Different closely related concepts to the paradigm of edge computing.

Consequently, we present a brief discussion of how these paradigms might be characterized in terms of their relationship with cloud computing, applications, and the location of computational resources. Furthermore, we emphasize their advantages and disadvantages from a computing standpoint. These are discussed as follows:

(i) **Mobile Ad hoc:** Originally, a mobile ad hoc cloud was proposed as a potentially transformative solution to the issues inherent in the traditional cloud model. This concept consists of many mobile cloudlets (nearby mobile servers) that are utilized by mobile end users (i.e., smart phones, tablets, etc.) to offload intensive computational workloads in an ad hoc manner [47]. Additionally, it promises to accelerate the execution of computationally intensive operations and minimize the energy consumed by devices. Due to its self-configuration and self-maintenance characteristics, this paradigm has attracted significant interest in the frontiers of communication technologies over the last decades.
However, despite its advantages, mobile ad hoc networking has some significant issues, including the lack of an open network architecture, shared wireless medium, resource constraints, and a highly dynamic network topology [48]. Furthermore, due to the shared nature of the mobile ad hoc architecture, security is one of the most crucial challenges in this concept. Various articles have attempted to address these issues in a variety of ways. For example, the authors in [49] have proposed an enforced cooperative bait detection scheme (CBDS).

(ii) **Cloudlet:** Cloudlet, like other post-cloud computing concepts, may be viewed as an extension of the standard cloud. This paradigm is comprised of relatively small-scale mobility support clouds located near mobile end-users. It was created primarily to reduce the computation offloading latency across wide area networks (WANs). Existing work from around 2009 is included among the early work on cloudlet [50]. They have also established the cloudlet concept as a typical intermediate layer in a three-tier architecture. The architecture, as the name implies, is composed of three tiers: end-device, an edge cloud platform, and a centralized data center [51]. Fundamentally, cloudlet is used to alleviate pressure on the remote Internet cloud by shifting computation resources to mobile devices with minimal latency.
The key benefit of cloudlets is their capacity to support mobility. A typical cloudlet consists of a server and wireless access points that are linked together through a local area network (LAN) [52]. Given the distributed nature of these cloudlets, managing large numbers of cloudlets in an efficient and effective manner remains a significant difficulty. Furthermore, cloudlets suffer from a number of challenges, including network capacity and backhaul linkages, as a result of the rapid growth in the demand for multimedia services [53]. The authors in [54] provided a thorough survey of existing works entirely focused on cloudlet-based mobile computing. Whereas, in a separate article, a secured cloudlet-based recommendation system for EVs was presented [55].

(iii) **Fog Computing:** In comparison to other existing post-cloud computing paradigms, fog computing appears to be the most popular, along with edge computing. The authors of [16] conducted a thorough study on these emerging paradigms with focus on performance metrics. The ability of these two paradigms to support the introduction of new IoT applications such as smart cities, SGs, EVs, and wireless sensor and actuator networks is the primary reason for their increased popularity. Furthermore, they are both known for their essential feature of shifting from a centralized to a decentralized architecture in which computation services are performed close to end-users rather than in the cloud. For these reasons, most researchers have been using these paradigms interchangeably, despite the fact that they are not identical [24,56]. As with Zhang and Tao [57], we also distinguish these concepts for the sake of clarity. According to the OpenFog Consortium [58], these paradigms can be distinguished based on where the intelligence and computing power are executed.
For example, fog computing can enable computing, networking, storage, control, and acceleration anywhere from the cloud to end-devices (on the network side),

whereas edge computing may only be capable of performing these functions at the edge (end node side). In general, fog computing has been recognized as a form of edge computing. Cisco defines fog computing as a highly virtualized platform that provides computing, storage, and networking services between end devices and traditional cloud computing data centers, which are typically but not exclusively located at the network's edge [59]. The term "fog computing" is distinct due to the fact that, literally, we consider fog in the natural geological environment as being closer to people than clouds [53].

According to the literature, fog computing has been integrated into various business domains with the goal of addressing a variety of challenges. For example, the authors in [60] have provided a detailed classification of fog computing applications such as smart cities, augmented reality (AR), and virtual reality (VR) from a machine learning (ML) perspective, with the goal of facilitating decision-making. An investigation into how to deal with security and privacy issues was conducted in [61,62]. The authors of [63] proposed a fog computing-based framework for SG applications (microgrid to be specific). Hussain and Beg highlighted the importance of integrating fog computing as a supporting technology for real-time SG data analytics [64]. In summary, the devices used in the fog computing-based architecture are not programmed to conduct any computation functions, but instead to serve as the network's data acquisition component while the analysis of data is performed in the gateway. As a result, fog computing experiences significant challenges such as latency and inefficient bandwidth utilization [65].

(iv) **Mist Computing:** Mist computing can be thought of as a lightweight version of fog computing that is located very close to the network edge [66]. This paradigm serves as a bridge between the fog and IoT tiers, with the goal of bringing fog computing functions even closer to end users. As a result, the traditional fog computing architecture experiences less data transmission delay. Mist computing, such as fog computing, is often referred to as edge computing, which is not the case [66]. Mist computing occurs at the network's extreme edge, which is comprised of microcontrollers and sensors. In this instance, mist computing involves the use of microcomputers and microcontrollers to offer processed data as input to fog computing nodes and, ultimately, towards cloud computing services. This paradigm aims to reduce latency and traffic issues by allowing processed data at the network's edge to be transmitted to the cloud storage system via the network's fog nodes.

(v) **Mobile Edge Computing:** According to the European Telecommunications Standards Institute (ETSI), mobile edge computing (MEC) is a new platform that provides information technology (IT) and cloud computing capabilities within the radio access network (RAN) near mobile subscribers [18]. This paradigm was first realized in 2013 by IBM and Nokia Siemens. The authors in [51] have provided a detailed discussion of the evolution of this paradigm. Because of the benefits provided by MEC, the European fifth generation (5G) infrastructure public-private partnerships (PPP) have identified it as one of the next-generation 5G networks that will massively revolutionize mobile network intelligence. Reduced latency, improved energy efficiency for mobile devices, power saving mechanisms, support for context-awareness, and improved privacy and security for mobile applications are some of the primary benefits of MEC. These advantages stem from the critical role of this computing paradigm, which shifts data-intensive tasks to the edge and concurrently executes data processing near end-users rather than in a centralized cloud. As a result, there are fewer bottlenecks in the core, and heavy computational tasks are offloaded to the edge via network operators [51].

Table 2 summarizes the important distinctions between cloud, fog, and edge computing (all of which are the most prominent ideas considered for SG purposes).

Table 2. Comparison of Cloud, Fog, and Edge Computing.

Metrics	Cloud	Fog	Edge
Deployment	Centralized	Decentralized	Decentralized
Distance from end users	Huge	Small	Extremely small
Computational Power	Pervasive	Limited	Limited
Efficiency	Low	High	Extremely High
Latency	High	Low	Ultra-low
Processing Location	Core	Fog server	Edge server
Storage Capacity	Pervasive	Limited	Limited
Privacy and Security	Low	Low	High
Mobility support	No	Yes	Yes
Processing Capability	Pervasive	Limited	Limited

Essential Features of Edge Computing

Generally, edge computing can be characterized by the following features:

(i) **Computing and Networking:** Edge computing allows for advanced IT and network infrastructures to be shifted to the network's edge, thus allowing computing and storage to take place close to where data are generated.

(ii) **Storage:** In the edge computing framework, computing and storage devices such as cloudlets, fog nodes, or micro-data centers are deployed at the base station, which is located near the end-devices, to avoid obstructions and network failures. This has the potential to significantly contribute to the success of SG deployment because it promises to reduce data transmission delays while also improving QoS and quality of experience (QoE) for end users.

(iii) **Data Management:** It is noted that the centralized data management model used in cloud computing fails to keep up with the rate at which data in SGs are generated. Thus, several studies have recently been conducted to investigate the adoption of a decentralized data management framework. For example, the authors in [67] have used edge computing to present a secure and efficient data management system for mobile healthcare systems.

Key Enabling Technologies for Edge Computing

With an enormous number of IoT devices envisaged to be deployed in next-generation systems, relying solely on the concept of edge computing may prove to be ineffective in the long run. This is because despite the improvements demonstrated in recent years, edge computing still has significant limitations that prevent it from being pervasively deployed in real-time applications. These include issues linked to resource allocation, such as limited bandwidth utilization, CPU cycle frequency, radio frequency, and access jurisdiction, to name a few [22]. Thus, in this regard, we outline notable enabling technologies that possess the ability to address the aforementioned difficulties associated with edge computing.

(i) **Containerization:** It has been noted that the widespread deployment of edge computing has been constrained by limitations associated with the use of virtual machines (VMs) as well as the bandwidth utilization of wide area networks (WANs) [68]. As a result, the emergence of containerization as a viable solution among virtualization technologies has garnered considerable attention from researchers and developers alike. Containerization is one of the most widely used virtual technologies for addressing some of the issues that VMs encounter when deployed in cloud computing paradigms. Containers, like VMs, partition the resources of physical machines into numerous user-space instances. However, these containerized instances are isolated

and have a much smaller footprint than VMs. Consequently, large internet-based companies such as Google, Spotify, eBay, and Twitter, among others, have been experimenting with containerization technologies in order to scale their services efficiently. In terms of container technologies, Docker has emerged as the most popular and widely adopted solution for enabling edge computing. Many developers typically leverage Docker or Kubernetes, the two most widely used container technologies, to overcome some of the challenges inherent in latency-sensitive IoT applications. These technologies have been developed as a viable approach for developing an operating system tailored to these applications [69].

(ii) **Orchestration:** Orchestration is defined in [69] as a technology for managing interactions between virtualized components such as containers and for composing, managing, and terminating services. To meet the requirements of orchestration models, the authors in [70] expanded the definition of orchestration to include the management of services workload placement and processing via dynamic and intelligent resource configuration in order to meet services level agreements. Orchestration technologies are divided into two categories: service orchestration and infrastructure orchestration. Orchestration is a broad concept in the context of edge computing, consisting of numerous management efforts at various levels. Orchestration is critical in multi-tier edge computing to ensure efficient and reliable operation of all components [71]. Additionally, in edge computing, a typical orchestrator is used to manage resource allocation.

Although several works in the literature have used this technology to address a variety of problems, orchestration still faces issues with QoS estimation and matchmaking [72]. Consequently, the authors in [73] introduced an intelligent-based architecture for IoT-based applications that combines orchestration (used between the cloud and the edge) and AI techniques (which provides for the intelligence capability of an architecture). In a separate article, authors in [74] proposed an online orchestration framework for cross-edge service function chaining to improve cost-efficiency.

(iii) **Fifth-Generation (5G) Mobile Network:** Cellular communication technologies have advanced tremendously over the last decades. Specifically, over the last two decades, cellular networks have evolved significantly from third-generation (3G) to fifth-generation (5G) technologies, necessitated by the proliferation of IoT devices [45,75]. Initially, the goal of preceding technologies such as 3G and 4G was to develop high-speed wireless networks capable of supporting the transition from voice-centric to multimedia-centric traffic. However, by advancing upon its predecessors, 5G promises to outperform them by delivering remarkable benefits to mobile end users, such as enhanced Mobile Broadband (eMBB), ultra-reliable low-latency communications (URLLC), and massive machine type communications (mMTC). To fully realize the benefits of a variety of applications such as AR, VR, and smart environments, 5G has been consolidated to facilitate and enhance the communication infrastructure's overall performance. In 2020, 5G drew considerable attention from researchers as a promising wireless cellular network standard capable of meeting the stringent requirements of next-generation systems.

This technology has been integrated into a variety of smart environments, including SGs [76], smart healthcare [77], and smart cities [78], each of which addresses a unique set of challenges. While 5G brings with it a slew of promising benefits, legacy computing paradigms may deny end users the opportunity to explore them. To this end, edge computing appears to be a viable solution for enabling the evolution of 5G by essentially pushing cloud functions to end users [79]. Specifically, the authors in [79] presented a taxonomy for edge computing in 5G, and emphasized critical aspects of its coordination, such as computational platforms, key attributes, 5G functions, and performance metrics. As a summary, a comprehensive investigation into MEC in 5G and IoT contexts can be accessed in [45].

Benefits of Edge Computing

Due to the complexity and diversity of the SG environment, stringent requirements have been established that cannot be met by existing cloud-based infrastructures. However, given the benefits of edge computing, which are discussed further below, it provides an ideal platform for ensuring that SG requirements are met adequately. These advantages are discussed under the following areas:

(i) **Reduced Latency:** The concept of edge computing has proven to be very beneficial for latency-sensitive applications because it aims to reduce data transmission times while also making the network structure easier to implement [80]. Edge computing has been identified as a suitable platform in this regard to ensure that the requirements emerging with SG applications such as wide area situational awareness (WASA), outage management, and substation automation are met appropriately as discussed in details in Section 3.2.3.

(ii) **Mobility enhancement:** An edge computing architecture typically consists of geographically distributed fog and edge devices distributed across the network for computational and storage purposes. Edge computing, as a result of this benefit, can provide mobility support to all mobile end-devices used in SGs.

(iii) **Ease of data processing:** Because of its ability to be deployed in close proximity to data sources, edge computing has the advantage of analyzing and extracting some useful insights from "big data". Furthermore, since the number of smart meters deployed in SGs is expected to grow at an exponential rate in the future, edge computing can help manage and analyze data generated by smart meters in a more effective and efficient manner.

(iv) **Location Awareness:** Unlike cloud computing, the edge computing paradigm can perform some computation functions on data based on its geographic location. Furthermore, this can be accomplished without the use of cloud services. Edge computing significantly performs better than traditional cloud computing in terms of location awareness, which will contribute to the success of WASA in SGs.

3.1.2. Artificial Intelligence

Artificial intelligence (AI) is envisioned in many different application areas and technologies as a means of imbuing physical machines with human-like intelligence. Given the critical role that human intelligence plays in the success of AI, as the definition implies, neuroscientists believe that biology can be viewed as an enabling ecosystem for emerging AI applications [81]. AI has thus gained prominence in many application areas as a result of the breakthroughs in other variants, such as in deep learning (DL) [38,40].

Deep Learning

To keep things simple, DL can be thought of as an enabling technology for ML [82]. Essentially, DL enables ML technologies to realize a wide variety of applications, thus further expanding the initial scope of AI [83]. Typically, DL is considered a subset of ML with the goal of implementing AI through the use of effective algorithms to extract critical insights from collected data for further prediction and decision-making. Recently, AI has been applied to a variety of IoT applications, including smart healthcare, SGs, and transportation, as a result of advancements in ICT, software engineering, and biotechnology. Additionally, these technologies have been extensively used in the SG environments, creating new requirements and challenges.

Several studies have been conducted recently on the transition of the centralized power grid to decentralized SGs through the use of edge computing. The rationale is to concentrate computation resources at the network's edge. As previously stated, edge computing alone may be unable to meet certain emerging requirements in complex and distributed environments, such as those found in SGs. As a result, the requirement to push AI to the network's edge has gained significant attention as a viable strategy for fully exploiting the potentials of edge computing. Thus, the fusion of these two terminologies (edge computing

and AI) has resulted in the emergence of "edge intelligence (EI)" [22,41,45]. Among the benefits that EI enables is a significant increase in the computational speed of IoT devices. Another advantage of EI is that it effectively reduces computational reliance on the Internet cloud by leveraging distributed edge resources on the network to improve the energy efficiency of different AI applications such as in smart healthcare, smart Internet of Vehicles (IoVs), smart cities, smart grids, and smart homes, among others. The development of EI is considered as a crucial step toward resolving some of the most severe challenges (i.e., limited resources and short battery life) encountered in global industrial applications [84].

AI for and on Edge Computing

There are typically two terminologies often associated with the use of AI within edge computing, namely, "AI for edge computing" and "AI on edge computing" [22]. To differentiate the two categories, "AI for edge computing" is defined as a research direction that is solely concerned with developing feasible approaches for solving constrained optimization problems in edge computing using efficient and effective AI techniques, whereas "AI on edge computing" is concerned with developing methods for effectively and efficiently executing AI models at the network's edge.

The integration of AI into advanced technologies such as IoT, edge computing, and wireless networks has been widely documented. Recent works have attempted to investigate the convergence of these technologies, specifically AI for edge computing [40,85,86]. In general, AI for edge computing can be viewed in four essential aspects: edge caching, edge training, edge inference, and edge offloading. To this effect, the authors in [43] conducted a comprehensive review of EI from a variety of perspectives, including caching, inference, training, and offloading. Moreover, in terms of providing a specific definition, the authors in [24] defined EI as "the deployment of computationally intensive intelligent models (predominantly ML, DL, and data analytics) at the edge of the network". In this regard, EI applications are expected to benefit from the advantages of edge computing, such as reduced latency and robust scalability [24]. Furthermore, in Ref. [87], a monitoring paradigm based on EI was proposed that enables the grid to offload workloads to the edge layer with the goal of reducing latency, data integration risks, and also providing disaster monitoring facilities for SGs.

To address security concerns in electric power systems, the authors in [88] used edge computing and image processing techniques to effectively and rapidly identify security risks. In another architecture proposed by Ghosh and Grolinger in [25], sensors were partitioned into groups based on their proximity to data sources in order to process data efficiently. The authors in [41] examined the history and motivations for deploying AI at the network's edge. Moreover, the motivation for deploying AI at the edge was described in [89] based on AI-based edge computing in accordance with edge computing architectures and technologies. In another article, Amin and Hossain conducted a thorough analysis of the cutting-edge artificial intelligence-based classification and prediction technique used for EI [44]. Their study's primary focus was on the issues confronting the smart healthcare ecosystem.

Fundamentally, the authors in [21] explored the general architecture of AI-of-Things (AIoT) by combining IoT, AI, and edge computing. In the AIoT, edge devices are empowered to conduct data analysis and make intelligent decisions independently of human intervention. Unlike a typical IoT architecture, which relies on the application layer to make decisions, the AIoT architecture enables an advanced end layer to perform small AI computational tasks or preprocess data produced by end devices. The authors of [26] examined deep EI in terms of FL, distributed computation, compression schemes, and conditional computation. Similarly, the authors of [21] concentrated on emerging technologies for AI models, particularly inference and training at the network edges. The authors of [90] proposed a new framework for automating wind turbine monitoring in SGs by using unmanned aerial vehicles (UAVs) as EI units.

3.1.3. Summary of the Discussion on Edge Intelligence

EI has the ability to significantly improve the overall network performance of IoT applications in terms of latency, efficiency, and mobility, among other metrics. This is demonstrated in [91], where the strategy they provided considerably enhanced the performance of the applications by achieving a speedup of 1.1–18.7 times the baseline methods under different network circumstances and settings. The authors decreased the average time required to complete a task in order to attain constant latency. Similarly, in Ref. [92], different edge caching, communication, and computation characteristics were studied towards decreasing the optimum latency of an end device, where each task to be offloaded by this device has a 10 ms latency requirement. In this sense, their suggested strategy reduced overall latency by roughly 2.5 ms when the maximum processing rate of the edge server approaches 38 GHz. In Ref. [93], vehicle mobility, distributed storage, and computation resources were leveraged to overcome the issue of constrained backhaul. Due to the restricted options for communication between the car and the relevant roadside unit, the cost performance increases when vehicle movement is minimal. Thus, by using reinforcement learning in [94] based on ultra-dense edge computing, the mobility management problem was solved by lowering latency and using handover cost as a penalty term for the offloading task. Due to the possibility of intelligently offloading computation-intensive activities to neighboring edge servers, the energy consumption of each network device is drastically reduced [95]. This section has discussed the most often suggested EI concepts in the literature with regard to edge computing, including their closely related concepts, features, enabling technologies, and benefits. A few key articles that have tackled security issues associated with the use of edge computing in SGs are summarized in Table 2. Furthermore, several developments revolve around the concept of transferring computation applications and services from the cloud to the edge. One of these developments is understanding how edge computing differs from established computing paradigms and its capacity to transcend the present limitations of these established paradigms. Another is identifying effective and efficient enabling technologies that will allow this concept to be realized. While EI may appear to be the right solution for the majority of the difficulties encountered in the IoT ecosystem (SGs in particular), edge computing still has significant constraints, including security and privacy, storage, and computing power. To address these problems, a number of research works have examined the convergence of effective AI technologies and enabling technologies, such as those indicated in Section 3.1.1.

3.2. Smart Grid: A General Overview

One of the most frequently used definitions of SG is the ability to integrate information, two-way, cyber-secure communication technologies, and computational intelligence across the vast bulk of the electricity supply chain (generation, transmission, distribution, and consumption) in order to achieve a system that is clean, safe, secured, reliable, resilient, efficient, and sustainable [1,2,96]. It is considered the next generation of power grids [12,97], and also one of the main subsets of smart cities powered by IoT [98]. The concept of SG was born out of the requirement for alternate solutions to the present difficulties confronting legacy power networks. Legacy grids were planned decades ago with a fundamentally different political, social, and technical context in mind than exists today [8], with a schematic of a typical legacy grid as shown in Figure 3. As a result, legacy grids have failed to meet the 21st century requirements of customers. These include, but are not limited to, the inclusion of RES, the conversion of centralized to distributed generation, and the replacement of digital meters with smart meters [9,99].

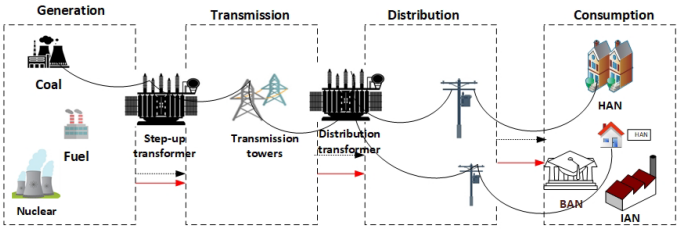

Figure 3. General representation of legacy power grids "Reprinted/adapted with permission from Ref. [3]. 2020, MDPI".

For example, in emerging economies such as South Africa, fossil fuels (coal, crude oil, and natural gas) continue to be the primary source of energy generation. However, oil reserves are presently considered to be dwindling, and according to a 2016 analysis on South Africa's power, gas, and water supply industries, around 85.7 percent of the country's electricity was noted to be generated by fossil fuels [100]. However, the amount of carbon dioxide emitted by these fossil fuels has resulted in worldwide climate change challenges. Thus, governments and electric utilities have sought effective and economical ways to deliver sustainable energy while still meeting the stringent expectations of customers [38]. To this effect, given Africa's abundance of RESs, a recent research on Africa's energy supply has examined strategies to maximize the use of these sources in order to mitigate global climate change while also contributing to the continent's socioeconomic development [101].

It is beyond question that the legacy grid has had a significant impact on the daily lives of customers since its establishment. Furthermore, it has existed for more than ten decades as a critical engine of global economic development and expansion [102]. However, there are significant issues arising from the exponential growth in power consumption and the increased penetration of renewable energy sources, both of which pose new difficulties to the flexibility of traditional systems. The power grid pattern is evolving as a result of improvements in ICTs, and older grids are being compelled to adapt to these new changes [3]. With governments now constrained by environmental and economic constraints, fundamental system planning and operation are constrained to rely on existing infrastructure with constricted operating and stability margins. Thus, recently, grids have undergone a substantial shift to the developing paradigm known as SG, which aims to serve as a promising ecosystem by delivering high reliability and efficient energy management via the integration of modern ICTs across traditional grid domains. According to Ref. [8], the first critical part of achieving this evolution to SGs, as well as its emerging advantages, is to have a clear vision of its objectives. Thus, in the next subsection, we shall discuss some of the emerging technologies required for the successful establishment of SGs. A general representation of a smart grid architecture is shown in Figure 4.

3.2.1. Key Enabling Technologies of Smart Grid

Traditional power grids present a significant problem in addressing the various and stringent expectations of customers in the IoT age including security, stability, QoS, flexibility, and scalability. SG development has emerged along with other technological improvements to address these concerns. This section discusses many of the most significant and popular technologies associated with the implementation of SGs, as presented below.

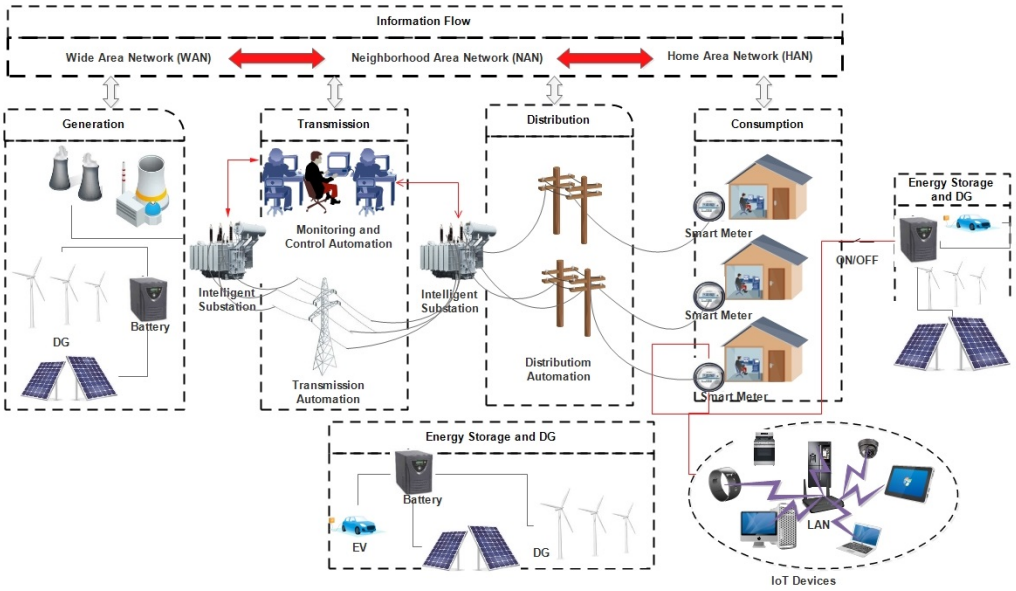

Figure 4. General smart grid architecture.

Advanced Metering Infrastructure

From a communication standpoint, advanced metering infrastructure (AMI) may be thought of as a paradigm that offers bidirectional communication infrastructure between end users (smart meters) and utility centers [3]. This application is widely recognized as the first step toward the development of SGs. AMI typically consists of smart meters, a communication network, and a data management system for the meters (MDMS). In this context, smart meters are primarily used to collect data on the energy consumed by all smart devices (IoT and mobile) connected to the home area network (HAN). Additionally, the acquired data are sent to the utility center's MDMS through access points, allowing for the issuance of control instructions and decision-making. AMI enables users to benefit from self-monitoring, self-healing in the event of a problem, and automated operating capabilities through the implementation of IoT in SGs. A further advantage of AMI is that it has the capability of facilitating interaction between solar household systems and the utility grid. However, in recent years, there has been an increase in the number of solar panels installed on rooftops, which has made managing the dynamic flow of electricity a significant issue for both power suppliers and customers [103]. In order to overcome this difficulty, a communication model of a solar home system and smart meter that is based on the IEC 61850 standard was developed in [103]. In addition, the end-to-end latency, also known as ETE delay, was employed as a performance parameter for the suggested communication architecture.

In general, AMI enables SGs to collect critical information from an end user's device and appliances while also managing their behavior [99]. In Ref. [75], an advanced version of AMI was demonstrated that enables SGs to achieve accurate real-time electricity price forecasting, localize real-time analysis of application services, optimize resource allocation schemes, improve the reading efficiency of metering systems, and reduce costs. The authors included edge computing and IoT devices into their framework. A knowledge-based usage strategy for optimizing the energy consumption and longevity of smart meters was presented in [104]. To increase operational flexibility, system performance, and ownership costs, authors in [105] suggested a scalable serverless SG architecture based on fog-edge computing virtualization.

Distributed Generation

Distributed generation (DG) is a general term that refers to the integration of distributed energy sources such as solar panels and wind turbines with the goal of reducing transmission and distribution losses, assisting the local power grid, and enhancing system

stability, efficiency, and environmental protection [99,106]. Despite the environmental issues created by fossil fuels over the last couple of decades, it is evident that these generating sources have shaped the power grid's frontiers. With fossil fuels depleting and becoming prohibitively expensive for the electricity sector, power providers and governments are refocusing their efforts on the integration of RESs into next-generation power grids. This becomes a reality since SGs can facilitate two-way electrical and information flows, hence enabling the power generating domain to become "smarter". The notion of DG technology is achieved in this regard. In order to make the most of this cutting-edge technology, a novel architecture of an edge computing gateway based on the IEC 61850 extensible messaging and presence protocol (XMPP) was developed in [107]. The goal of this architecture is to reduce decision latency between DERs while simultaneously enhancing the microgrids' level of stability.

Microgrid

A microgrid is a localized grouping of distributed energy generation, energy storage, and loads [99]. The authors in [108] defined a smart microgrid as a collection of all technologies, concepts, topologies, and approaches that enable silo hierarchies of generation, transmission, and distribution to be replaced by an end-to-end, spontaneously intelligent, fully integrated environment in which all stakeholders' business processes, objectives, and needs are supported by the efficient exchange of data, services, and transactions. Microgrids, in general, are a viable approach to deal with the problems that DG imposes on the macrogrid. They can run in two modes: normal operation and islanding mode. In normal functioning mode, a microgrid is supplied with electricity from the traditional power grid (macrogrid). In the islanding mode, microgrids are capable of decoupling from the macrogrid and operating autonomously, thus increasing reliability and power quality while minimizing investment costs, emissions, and power loss on the distribution network. A detailed discussion of the architecture and functionality of microgrids can be found in [106]. Despite the potential benefits of this paradigm, the distribution network protection system is confronted with new challenges as the demand for DG integration into microgrids grows, such as false tripping and protection blinding [109]. Protection blinding is a phenomenon that can occur in SG networks with integrated DG sources when overcurrent relays either delay or fail to trip off fault currents, resulting in an increase in fault current contribution to the main feeder. This can have severe effects on the entire network, including downtime and equipment failure. False tripping, on the other hand, happens when relays trip when there is no need for them to. The detailed review in [110] elaborates on many notable solutions available for addressing these challenges. Additionally, such unintentional islanding in the microgrid has become a major technical challenge, which can consequently have a significant impact on the power quality, security, voltage and frequency stability of SG networks [111,112]. In a general sense, these restrictions are brought about by the concept of power flowing in both directions within SGs. In recent years, there has been progress made in developing adequate protection strategies to solve the limitations imposed by DGs in the distribution network [113–115]. For instance, the authors of [116] developed an AI-based protection strategy that is comprised of two techniques, namely, a centralized controller and a zone controller. Communication among smart protection devices is enabled under a centralized controller technique to effectively isolate malfunctioning equipment from the overall network without affecting the grid's stability. In contrast, the zone controller technique, also known as the backup strategy, partitions the grid network into protection zones in order to autonomously choose and isolate the problematic zone from the network by making use of a protective device that is embedded inside the zone. These very sophisticated defensive gadgets come equipped with functions such as rapid reaction, sensitivity, selectivity, and dependability in their design. In Ref. [117], the authors offered a novel method for rapidly detecting islanding events in a microgrid. This method is based on the extraction of phase-space features and an adaptive ensemble classifier. In a similar vein, a rapid islanding approach that requires a minimum amount of processing burden was presented in [115] to intelligently detect

islanding occurrences. The detailed review in [112] provides readers with an in-depth look at the various methods of islanding detection. In addition, the authors classified these strategies as either central or local islanding, depending on their level of isolation. According to Ref. [111], remote islanding is achieved either via SCADA or power line communication systems, and their major purpose is to ensure communication between DG units and the utility. On the other hand, local islanding takes advantage of variations in system characteristics including voltage, frequency, current, and harmonic distortion in order to identify instances of islanding. It is anticipated that the above significant efforts and future solutions being put forward would make it possible for microgrids to island securely while also injecting electricity into an SG network via reliable and stable mechanisms.

Electric Vehicles

Recent advances in SGs, along with the integration of electric vehicles (EVs), have emerged as a viable alternative for reducing greenhouse gas emissions associated with fossil fuels. Following the realization of SGs, EVs may act as either energy storage systems or consumers, depending on the condition of the macrogrid. On the one hand, EVs utilize their stored energy to power the macrogrid during peak load periods. This technique is referred to as "vehicle to grid" (V2G). On the other side, EVs may function as consumers, drawing energy from the macrogrid to charge. This is referred to as "grid to vehicle" method (G2V). The authors in [118] have provided an overview of the state-of-the-art in EVs. They discussed this technology from a variety of perspectives, including current charging methods, RES integration, and the viability of smart V2G.

Internet of Things

Recently, the term "energy internet" was coined to describe an innovative strategy for integrating IoT into SG applications. Thus, IoT-based SGs is another term that other researchers use interchangeably with energy internet [64,75,119]. According to Ref. [75], IoT-based SGs can be identified by a number of characteristics, including rapid interaction of services in power systems, efficient use of electric distribution systems, plug-and-play compatibility with a variety of terminal types, and comprehensive awareness of an SG's status.

In general, IoT has been widely recognized as an extension of the Internet that consists of interconnected and related things (sensors, smart meters, RFID, and global positioning systems, to name a few) that are capable of collecting and transmitting data over a network using wireless and mobile technologies with minimal human intervention [119]. IoT services are thus available regardless of time or location, which may result in more effective and efficient data transmission, monitoring, and administration of decentralized systems such as an SG. In Ref. [120], a comprehensive review of IoT applications in SGs is presented.

The authors in [121] examined the use of 5G and IoT to deliver disaster recovery services in SGs from a variety of angles, including cybersecurity, user privacy, and dependability. Similarly, the authors of [122] conducted a bibliometric analysis of IoT applications from a security standpoint. These authors approached their study by posing four fundamental questions: what is the current state of cybersecurity work in SGs; what is the future direction of cybersecurity in SGs; what are the existing cyber-threats posed to SGs; and finally, what are the available cybersecurity solutions used in IoT integrated SGs. Similarly, an innovative experimental prototype IoT system for energy management in smart buildings was built and is presented in [123]. The authors demonstrated a real-time location-based automated and networked energy control system across several smart buildings by merging smart location-based automated and networked energy control using smartphones and cloud computing concepts.

Artificial Intelligence for Smart Grids

Recent studies have utilized AI techniques to solve various challenges in SGs from different standpoints. EVs are one of the technologies growing in tandem with the development of SGs. They aim to act as a catalyst for the reduction of CO_2 emissions from

conventional power generation stations. To this effect, a study was conducted to determine how the deployment of AI approaches may be utilized to intelligently manage a network's distributed EVs [31]. Similarly, Serban and Lytras proposed an innovative method for constructing a theoretical framework with the goal of demonstrating how advanced AI might greatly increase the efficiency of the renewable energy sector in the European Union towards economic efficiency and sustainability. In another article, the authors suggested a conceptual model to handle significant issues encountered during the load forecasting process in SGs, such as long calculation time, huge data, data needs or restricted data, and extra back-propagation (BP) operations [124]. There, the authors used a DL algorithm to reduce the amount of processing time required to perform the load forecasting procedure. Additionally, they conducted a comprehensive evaluation that focused exclusively on studies published between 2015 and 2020, with some emphasis on DL techniques that may be effective for load forecasting in SGs. Similarly, the authors in [38] undertook a detailed evaluation from a wide viewpoint of the state-of-the-art developments in DL in SG systems. In the same light, in Ref. [125], ML technologies were linked to SG mobile applications in order to optimize consumer flexibility and increase energy savings. In Ref. [126], a FL-based AIoT system was presented to provide safe and efficient data sharing in SGs. Additionally, the authors leveraged edge-cloud computing in their suggested strategy to facilitate the effective sharing of private data within SGs.

Edge Computing

The future of edge computing in IoT applications (such as smart transportation, smart grids, and other similar ones) is currently undetermined. SG is only one of the IoT applications that is benefiting from the development of edge computing. SGs are faced with a variety of significant difficulties, and there are several studies in the literature that have sought to address some of these challenges through the use of edge computing. For example, in Ref. [127], the confluence of blockchain and edge computing was used to alleviate concerns about privacy and energy security in SGs. An edge computing architecture was developed by the authors of [128] in order to improve the real-time monitoring of smart grids. These authors additionally used heuristic techniques to optimize the performance of the suggested framework. The authors of [129] proposed EBDA, a lightweight approach for safeguarding data privacy during data aggregation in SG, which is built on edge-blockchain and is designed to be used on mobile devices. The authors in [130] designed a joint optimization problem that can be used to address both the computation offloading and caching difficulties in edge computing-based SG at the same time. A systematic study focused on the development of SG from the aspects of data analysis, edge computing, IoT, and context awareness is provided in [131]. Table 3 summarizes the critical security priority areas regarding the deployment of edge computing in the SGs.

Distributed Ledger Technology

Blockchain technology has advanced at a rapid pace in recent years, owing to the corresponding progress being made in the IoT domain. Blockchain technology can be considered a subclass of distributed ledger technology (DLT) due to its critical role in the digital cryptocurrency field. It has attracted substantial interest from the industry's high-tech leaders in recent years [19]. Security, transparency, and a decentralized architecture are among the benefits of this developing technology [28]. The authors in [29] suggested a decentralized blockchain-based architecture to address security concerns associated with the intelligent vehicle edge computing paradigm. In a separate effort, the authors in [86] proposed a broad framework for IoT scenarios using blockchain-based edge computing. They used an ML approach to ensure efficient resource allocation for edge computing. Additionally, the authors discussed the security and privacy concerns associated with edge computing-enabled IoT designs. Their generated smart contract demonstrates an exemplified way of integrating AI with blockchain. In Ref. [28], the authors used the Stackelberg game to optimize resource costs and also the resource demands on devices while offloading computation to an edge or cloud server. They studied the interaction

between the operator of an edge or cloud server and the collaborative mining network to achieve appropriate results.

Table 3. Summary of key security areas regarding the application of Edge Computing in SG.

Ref	Smart Grid Issue	Technique Used	Approach	Performance Metrics
[127]	Privacy protection and energy security	PBEM-SGN	Mathematical model	Gas and time cost
[132]	Spoofing, MIMT, DoS	Dynamic scheduling	Architecture and Simulation	Cumulative risk
[129]	Cyber attacks	PEO and EnPEO-DBN	Simulation	True positive rate and error rate
[27]	Security	Deep reinforcement learning	Evaluation	Processing time and rewards

3.2.2. Application Areas in Smart Grids

This section discusses briefly the primary applications that have emerged as a result of the development of SGs:

Substation Automation

Substations are critical components in the design and operation of electric power grids. In older power grids, the primary function of substations was to provide monitoring, control, and secure operation of the geographically distributed bulk of the power system via the network's different access points [133]. With the integration of ICTs across all domains of the power grid, SGs allow for a new technology called substation automation systems (SAS). This technology automates a variety of activities associated with traditional substation equipment, including monitoring, regulating, and protection. Additionally, SAS takes data from these devices and performs additional operations on them, providing comprehensive control and communication activities [134]. However, with the proliferation of smart IoT devices (smart sensors, smart meters, etc.), the distribution network has become readily accessible, thus posing significant information processing and analysis issues for distribution automation systems. In addition, many existing distribution automation and fault detection systems are largely dependent on centralized data processing systems, hence resulting in an increase in communication overhead and computational burden [135]. In this sense, edge computing has lately received a great deal of popularity as a potential solution to some of the challenges posed by this system. For example, in Ref. [136], a real-time detection system based on edge computing was designed to continuously monitor any security threats imposed by intruders that may be missed by a conventional substation monitoring system. Similarly, a distributed power distribution fault detection system based on edge computing was presented in [137]. Their proposed system aims, among other things, to enable prompt sensing and real-time reaction to distribution network failures, accelerate distribution fault processing speed, and reduce outage duration. To optimize the flexibility of the distribution automation system in the IoT era, the authors of [138] developed a microservice-based edge computing device for smart distribution transformers, which was able to improve the adaptability of a distribution automation system. Furthermore, a multilevel edge computing architecture was proposed in [139] to ensure that the stringent criteria of controlling distribution networks while minimizing continuous communication was addressed. An edge computing-based fault detecting system was also developed in [135] to monitor the condition of subterranean distribution wires. All of these options in general imply that substation automation in SG networks may be greatly enhanced, which will lead to increased performance and service delivery.

Home Energy Management System

Through the facilitation of two-way information and energy flows in SGs, consumers may be transitioned into prosumers. Consumers may now undertake DR programs autonomously through the integration of home energy management system (HEMS) applications into SGs (i.e., critical peak pricing, real-time pricing, day-ahead pricing, and incremental block rate pricing). The primary function of HEMS is to autonomously apply DR measures with the goal of lowering customers' power usage without compromising their QoE [140]. Additionally, HEMS is mainly concerned with monitoring the energy consumption of all electrical appliances used by consumers, where this equipment may be monitored and regulated autonomously in order to balance and optimize power supply and demand [141]. In recent years, small commercial RESs have become affordable, and as a result, customers now have the ability to install intelligent control systems in order to optimize the functioning of their own microgrids. For instance, during power outages on the utility grid, customers can access the autonomy feature of RESs to maintain normal operations on their end. However, these systems do not reach their full potential since, in most situations, they fail to establish full autonomy over all devices at the consumer's location. Reusing batteries has been recognized as one of the potential answers to this problem. In Ref. [142], batteries once used to power EVs have been repurposed to supply home DR services. Similarly, in Ref. [143], the authors presented a study on how the second-life batteries of EVs may be reused and re-energized to save grid costs and assure sustainable energy. Likewise in Ref. [144], the second-life batteries of EVs were examined for their reuse in smart buildings from an economic and aging perspective. Summarily, these studies strongly suggest the potential benefits of second life battery reuse towards enhancing the performance of HEMS as well as other application areas within SGs.

Wide-Area Situational Awareness

One of the critical concepts arising with the development of SGs is wide-area situational awareness (WASA) [145]. Notably, SGs include the extensive deployment of vital infrastructure in remote places with little or no human interaction. Effective and efficient monitoring of these infrastructures becomes difficult under this situation, and the grid's overall performance declines significantly. WASA has been realized by the combination of sophisticated technologies such as IoT into situational awareness, which enables the expansion of system monitoring at any time and from any location [146]. This paradigm aims to enable low latency and high throughput monitoring, archiving, reporting, and querying of the state of the power grid [147]. Additionally, WASA can aid power providers in responding quickly to network events, reducing the likelihood of catastrophic failures such as large-scale blackouts.

Overhead Transmission Line Monitoring

A typical power grid's fundamental components include domains for power generation, transmission, distribution, and consumption. Notably, normal transmission domain operation is regarded as a vital requirement for ensuring the secure and stable functioning of the whole power system. Recently, the idea of online monitoring technology for overhead transmission lines was introduced in conjunction with the deployment of SG to enhance transmission line protection and diagnostics [119].

Demand Response

Demand response (DR) has been generally acknowledged as a cost-effective and dependable method of developing policies and protocols for SG development with the goal of monitoring and managing end-user resources using sophisticated ICTs incorporated into next-generation power grids [148,149]. In simple words, DR may be seen as an upgraded version of the old idea of consumption demand, with the capability of adjusting loads in response to power system shortages and surpluses. Historically, time of use (ToU) and incentive programs were the most widely employed DR strategies beginning in the

1970's [140]. Facilitating the integration of new technologies such as 5G and IoT into disaster recovery will help maximize the benefits of this application while also improving the performance of its infrastructure [121].

Outage Management

Outage management is a cutting-edge technology that greatly contributes to distribution automation. This technology is primarily focused on detecting a problem as soon as it occurs (to avoid a catastrophic failure of the power system), as well as identifying the location of the fault and the protective devices (i.e., circuit breakers, relays, etc.) triggered by the fault [150]. The authors in [151] utilized data collected from various smart meters and fault indicators placed in SGs to provide an accurate and effective outage management strategy for SGs. They suggested a novel multi-hypothesis approach for determining the location of a feeder fault. A novel optimization-based home load control was presented in [149] to manage the operation times of responsive electrical appliances, identify multiple recommended operation hours for non-responsive appliances, and plan the charge and discharge cycles for plug-in hybrid electric vehicles (PHEV). The authors considered a variety of client preferences, including payment costs, disruption costs, and operational restrictions. The authors in [152] created a multi-agent system (MAS) for managing outages in a microgrid's electrical energy.

Plug-In Hybrid Electric Vehicles (PHEVs) Charging

The charging strategies for PHEVs may be grouped into four categories: uncontrolled, indirectly regulated, smart, and bidirectional charging [153]. This paradigm has recently emerged as a potential option for serving as a storage system in SG deployments with the goal of alleviating intermittency issues imposed by renewable energy sources and load demands. Practical application of PHEVs as energy storage systems continues to be a difficulty owing to their mobility as a mode of transportation, which may result in intermittency. To satisfy customers' real-time load needs, the authors in [154] provided an intelligent energy source selection approach that determines whether an energy source (macrogrid) or storage device (microgrid) should be deployed depending on the duration of power demand. Additionally, the authors used the particle swarm optimization (PSO) technique to minimize costs and emissions associated with grid-connected thermal producing sources. Due to the success of incentive policies, the development of this technology has gained significant attention in the research and academia space [155]. The number of EVs integrated into the utility grid is expected to increase dramatically in the near future. From an operational and management standpoint, this will pose technical challenges for the utility grid due to the technical limitations of the current grid to feed the increase in connected vehicles. Consequently, the development of an adequate technical and market operation framework is of great importance to address these challenges [156]. In addition, a variety of research and development initiatives have been made to solve these challenges; for instance, the authors of [157] offered an overview of PHEV charging systems in Spain. They underlined the necessity to standardize the charging connections used by different manufacturers of PHEVs so that PHEV owners may use any charging station. Furthermore, the authors advised for enhanced storage systems in isolated microgrid charging stations in order to increase charging efficiency, cycles, and modes owing to the negative demands on the main grid. This will necessitate more technological breakthroughs in battery design and management technologies. The authors of [158] undertook a simulation model research to examine the implications of large-scale PHEV charging on distribution networks from both a steady-state and dynamic operating standpoint. To improve the PHEV integration process, the following solutions were proposed: increasing the power factor of EV charging stations, installing large energy storage systems within charging stations, coordinating with local distribution generation to redirect power flow to charging stations, and providing adaptive controllers that can improve charging in response to fluctuating network load conditions. We note that other noteworthy PHEV charging solutions may be found in [159–162].

Asset Management

Many essential assets deployed in the SGs generation domain, including generating units and plant equipment, could be approaching the end of their stipulated service life. In this regard, scheduled maintenance and operation schedules should be executed on a regular basis to ensure that they last as long as envisaged. It is possible to describe asset management as a methodical procedure that ensures efficient and effective monitoring and maintenance of vital equipment(s) in a network [163]. With rapid advances in the development of smart sensors in SGs, new asset management-related elements may be integrated and explored. This is possible since SGs aim to provide ubiquitous monitoring across all of the grid domains via intelligent monitoring and control devices such as smart sensors and smart meters. An example of such a solution was proposed in [164] where a spectrum resource allocation scheme was proposed to extend the life of a battery-powered finite monitoring network. In Ref. [165], the issue of asset management in SG was resolved with the implementation of an intelligent grid management system (IGMS). Their method was described as an optimization technique in which the cost of assets was determined based on failure rate, loss, asset life estimation, outage, repair, and maintenance. The authors demonstrated that their approach can identify the frequency of maintenance and lower the overall cost of asset management. Similarly, the authors of [166] introduced a resource scheduling strategy based on the convergence of genetic algorithm and machine learning to forecast maintenance in a fog computing environment. In Ref. [167], an intelligent framework based on digital signal processing and pattern recognition algorithms was presented to efficiently monitor and analyze the condition of smart power transformers. These algorithms were utilized to automatically decrease the noise in sensor-collected signals, derive patterns from raw data, and detect the kind of transformer defects. These and many more solutions in published studies (such as in [154,167,168]) demonstrate that asset management can be improved upon in order to maximize the operating life of SGs.

3.2.3. Summary of the Discussion on Smart Grids

This section provides a summary of the discussion presented on SGs. Several components of SGs have been discussed, including their fundamental enablers and applications. From an application standpoint, it is indeed worth noting that the integration of IoT into power grids has been widely embraced, since it plays a critical part in this concept. Additionally, as noted in [134] , the bulk of these applications have a variety of demanding criteria. Given the need of edge computing to deliver ultra-low latency, it is a potential strategy for mitigating the limitations of SG networks. For example, because DERs are critical components of SG networks, it is critical that they interact with one another and that there should be some form of local intelligent computation among a widely dispersed set of DERs in order to minimize decision latency. It is possible to conduct this locally by leveraging the power of edge computing rather than executing these computations at a remote cloud center. As a result, communication latency between these components may be greatly decreased. In a similar vein, SGs are built on a multitude of different systems, all of which need to be constantly monitored and communicated with in order to guarantee the network's integrity and reliability. This may be accomplished by introducing new ideas such as asset management and WASA. However, the severity of the issue of latency must be taken into consideration, and the concept of edge computing can be leveraged. It is interesting to note that in [169], it was recommended that SG applications might be conducted over LTE base stations in order to provide low latency connection to smart meters with the goal of fulfilling the latency criteria that these applications demand. In addition, as presented in Table 3, a few studies have suggested the potential to address security and privacy issues connected with SGs based on the use of edge computing. Furthermore, we have discussed the possible benefits of edge computing in a number of SGs applications from the point of view of latency as noted in Section 3.2.1.

4. Architecture for Deploying Edge Intelligence in Smart Grids

In this section, an overview of an edge intelligence-based architecture suitable for SG applications is presented, which adopts the three-tier hierarchical architecture design similar to the general edge computing architecture, as depicted in Figure 5. Various studies in the literature have proposed different implementations of edge computing-based architectures with specialized application domains [51,67,73,170]. However, this section may be unable to cover all proposed designs in the literature due to the fact that each research has a unique purpose. We are only interested in research that focuses only on the application of edge computing and edge intelligence in SGs in this respect.

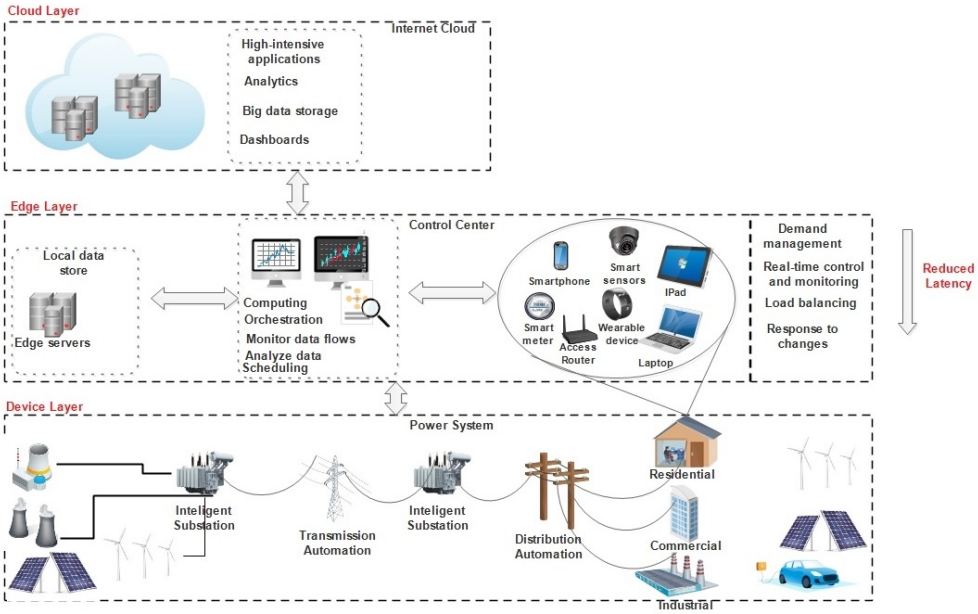

Figure 5. Generic edge computing architecture for smart grid.

4.1. General Edge Computing Architecture

According to Ref. [171], an architecture is a blueprint that defines the existing or future state of a "domain" constituted of components and their interconnections, the actions or activities performed by those components, and the rules or constraints governing those activities. Along with their concept, the authors developed three distinct reference designs from the standpoint of smart manufacturing. Thus, physical architecture (resources and components), functional architecture (functions and activity execution), and allocated architecture each have their own distinct characteristics (interconnection between the physical and functional architecture). Regardless of their origins or application areas, all extant architectures adhere to the general structural design of edge computing. Typically, as seen in the Figure 5, an edge computing architecture consists of three hierarchical layers: end-device, edge server, and core cloud. Several studies have been published in the literature seeking to integrate edge computing characteristics into SGs applications. On the edge servers, the FL method was employed to maximize the potential of edge intelligence in this architecture. This method enables AMI to do distributed data processing and make intelligent decisions.

The authors of [6] provided a high-level overview of an edge computing-IoT-based SG architecture that integrates edge computing and IoT to support an SG's network, computation, and memory management. The edge layer, which contains distributed edge nodes, gateways, and local servers, operates as an intermediate layer between cloud computing and the device layer in their proposed design. This layer is primarily responsible for filtering and preparing data generated by IoT devices (smart phones, smart meters, video cameras, and sensors) before it is communicated to the cloud. In Ref. [172], a universal three-tier edge computing system for efficient fault location in distribution grids was

presented. In Ref. [129], a novel architecture based on a three-layer basic design and utilizing edge computing and blockchain to safeguard data during SG aggregation was proposed. Similarly, edge computing and blockchain technology were used in [127] to address privacy and energy security concerns in SGs.

4.2. Edge Intelligence-Based Architectures for SGs

The authors of [24] presented an architectural paradigm for AMI systems that utilizes the combination of edge computing and edge intelligence. The architecture presented in this article is composed of multiple NANs. Each NAN is comprised of many HANs, each with its own AMI-edge, serving as a communication gateway between smart meters and cloud servers. Ref. [173] introduces another generic architecture, which is a three-tier IoT-edge-cloud architecture. The MEC network tier serves as an intermediate node between the smart device and cloud levels in their proposed design. To boost the speed and processing capabilities of resource-constrained smart devices at the bottom layer of the architecture, these devices offload computation-intensive tasks to neighboring edge nodes. By embracing industrial edge computing, the authors of [75] expanded this innovation to an advanced architecture with five levels (i.e., device, network, data, application, and cloud computing layers). The device layer is comprised of applications, security modules, networks, security operating systems, and control chips in the context of SG. Essentially, this layer is in charge of providing computation resources. In Ref. [172], the general edge computing architecture employs federated learning methods to alleviate communication burden between measurement nodes and the substation server.

The authors of [174] suggested a framework with two tiers that included edge computing, cloud computing, and, moreover, a deep reinforcement learning method was used to optimize their proposed architecture's communication, processing, and caching. Three distinct types of edge layers with various coverage areas were used at the edge layer to provide computing resources to constrained-resource devices in the service layer. A deep reinforcement learning approach based on edge computing was suggested in [27] to improve the security situational awareness of AMI. To control the power resources in SG systems, Ref. [175] presented a framework based on a mix of peer-to-peer (P2P) technology and edge computing. The authors in [12] exploited EI in SG systems to allow for effective defect detection with the purpose of increasing network performance and resource usage. In Ref. [20], a cost-effective edge-cloud integrated framework solution for identifying reinforcement learning for DR in smart buildings was proposed.

4.3. Summary and Comparison

This section has summarized the state-of-the-art research on EI-based SGs, with a particular emphasis on architectures. Figure 6 illustrates an architecture for SG applications based on EI. Similarly, as shown in Table 4, the majority of these designs were developed using a generic representation of edge computing architectures, the majority of which used DL to include intelligence characteristics.

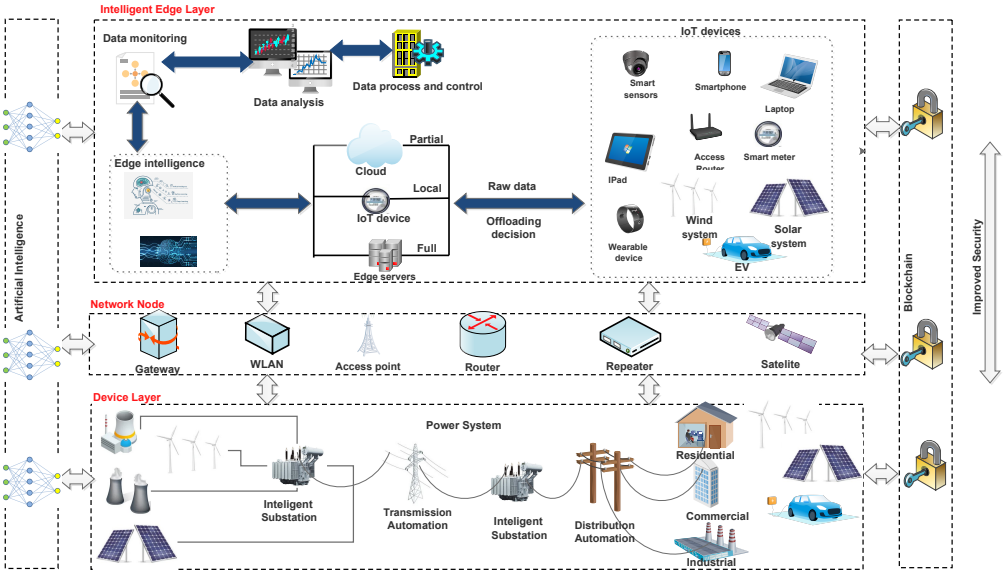

Figure 6. Edge intelligence-based architecture for smart grid.

Table 4. Different Edge Intelligence Architectures and their characteristics for SG applications.

Ref	Architecture Design	End User Devices	Type of Edge Server Devices	AI Algorithms Deployed at the Edge	Objectives	Pros	Cons
[6]	Three Layers: • Device • Edge • Cloud	• Smart phones • Video camera • Voltage sensors • Proximity sensors • Current sensors	Computers	–	Manage high volume of data from IoT devices in SGs	Compatibility between layers was considered Provision was made for security and management services	Provides a generic framework with no specific SG application use case Provides no software layers No interconnections between edge nodes
[24]	Three Layers: • Smart users • Edge • Central Cloud	• Smart meters	MDMS	Federated learning	Reduce overall communication cost, preserve user privacy and enhance situational awareness in AMI	Tailored for AMI Provides for interconnection of edge nodes	Provides no software layers Does not indicate security and management services
[75]	Five Layers: • Device • Network • Data • Application • Cloud	• Solar and wind farm • Airport, mall and town	Microgrid central controller	–	Enhancing the rapid response for user's requirement, intelligent scheduling, maintenance and rapid market responses	Provides details about hardware and software layers Provides for security and management services Adapted for power distribution surveillance systems	No provisioning for ML deployment at the edge
[172]	Three Layers: • Device • Edge • Cloud	• Sensor • Machine tool • Robot	Edge cloud Edge controller Edge gateway	–	Fault location in distribution grids	Provides details about the interconnection of devices at the edge layer It adapts the generic architecture for fault location application	No details of software layers No provisioning of security and management services
[174]	Three Layers: • Service • Edge • Cloud	• Power devices	Edge nodes	Deep reinforcement learning	Optimize communication, computing, and caching resources	It differentiates the service layer as a system consisting of users and power devices	No software layers No provision for security and management services
[27]	Three Layers: • Power terminal • Edge • Cloud	• Smart sensors • Microgrid facilities • Intelligent charging piles	Edge agents	Deep reinforcement learning	Enhance security situational awareness for SGs	Provides details about architecture's adaptation to security situational awareness in SG	Provides no details of software layers
[175]	Three Layers: • Smart grid • Edge • Cloud	• Smart meters • Distributed generators • Distributed energy storage systems • Smart electrical appliances	Edge nodes	P2P model, Alternating direction of method multipliers	Enhance energy resource management and penetration of renewable energy sources	Provides adaptation to SG applications	No provisioning of security and management services
[20]	Two Layers: • Edge • Cloud	• RTUs	RL agent	Reinforcement learning	Enable large-scale deployment in a cost-efficient manner	Provides details about the operations at edge and cloud	Does not differentiate between device and edge

5. Computation Offloading for Edge Intelligence in Smart Grids

Many IoT mobile devices are limited by their physical sizes, and they often encounter additional challenges due to their limited computational resources and battery life. Apart from their restricted capabilities, the majority of applications required by these mobile devices are computationally heavy and consume a lot of energy, putting a strain on these devices. With the proliferation of IoT mobile devices and the buzz around the use of EI in SG applications, these difficulties must be addressed.

To this effect, computation offloading has emerged as a realistic approach in recent years. Several researchers have used the words "cyber foraging" and "remote execution" interchangeably with computation offloading in the literature [176–179]. Nevertheless, computation offloading has been popularly defined as a strategy that entails splitting an application into discrete workloads and then offloading them from resource-constrained mobile devices to edge or cloud computing [22,89,180]. Additionally, it promises to minimize energy consumption and boost computation performance, which might result in decreased communication latency in edge computing systems [17,21].

It should be emphasized that the majority of applications that profit from computation offloading are those that utilize augmented, aided, or VR. Despite its enormous benefits, computation offloading in edge computing continues to face significant hurdles in terms of offloading decisions, computational resource allocation, and mobility management [17,83]. In general, computation offloading has been investigated in the context of edge computing and networking in [181]. Other papers in the literature have sought to address the aforementioned issues. Here, we review studies that have employed computation offloading in edge computing, classifying them into single- and multi-user cases. Additionally, we examined the responses to three critical problems highlighted by the computation offloading concept. As a result, the following factors are critical: (i) when to offload (precise time to offload the specified task); (ii) what to unload (offloaded workload selection); and (iii) where to offload (workload scheduling).

5.1. What Is Computation Offloading

To begin, computation offloading is a concept that entails using resilient infrastructures in order to augment the computational and storage capabilities of resource-constrained IoT and mobile devices [182]. According to Ref. [17], computation offloading may be used to effectively ensure users' QoS by offloading compute-intensive or latency-sensitive workloads to edge devices or neighboring edge servers. This strategy entails partitioning workloads into manageable subtasks, deciding on offloading strategies, and executing distributed tasks. This vision became a reality with the development of computing technologies during the last two decades. Task partitioning, offloading decisions, and distributed task execution are all critical components of computation offloading. Given the heterogeneity and distributed nature of edge devices, various considerations must be made prior to making any decision about computation offloading. These include performance optimization and energy consumption reduction. For instance, the authors of [180] used an offloading mechanism to reduce mobile users' power usage while allowing them to experiment with their own long-term offloading solutions. The article in [183] is one of the earliest publications to examine this idea. The authors created an agile prototype that enables the execution of a variety of mobile applications in this work. It is critical to highlight that, in edge computing, each device collaborates to offload their task locally, partially, or totally. A summary of key works on the subject of computation offloading is summarized in Table 5.

Table 5. Summary of key articles on computation offloading.

Reference	Architecture	Major Contributions on Computation Offloading
[180]	No	Offloading mechanism, interference, and energy consumption
[181]	No	Energy consumption, QoS guarantee, and QoE enhancement
[17]	Yes	Offloading decision, resource allocation, and mobility management
[184]	No	Optimal Offloading scheme, overall computation overhead, and computational efficiency
[182]	Yes	Task partitioning, allocation, and execution
[185]	No	Offloading decisions, caching enhancement, and reduce execution delay

5.2. Why Do We Need Computation Offloading

The literature highlights the importance of minimizing communication delays and enhancing the processing and storage capacities of limited-resource systems. Thus, the IoT and mobile devices to be deployed in next-generation networks are and will drive the need for edge computing computation offloading. To alleviate the load placed on such systems, it was recommended that some programs be moved and executed on an Internet cloud server for seamless operation [186]. Offloading to an Internet cloud, on the other hand, may not be the optimal solution in a diverse and dynamic environment such as SGs, where the bulk of applications require low latency. Rather than that, offloading to an edge server or edge device (in the event of an IoT device equipped with computation and storage resources) will be preferable. Offloading to the edge server (partial), the edge device (local), or both (complete), depending on the approach chosen, has demonstrated impressive benefits such as decreased energy usage, execution latency, and increased battery life of devices.

Several previous research works have concentrated on partitioning resource-intensive activities at the user's device in order to maximize QoE for users while also lowering execution costs and energy consumption [181,184,185]. The authors in [173] increased the capabilities of smart devices in terms of execution time, energy consumption, and payment cost by combining cloud computing with MEC in a computation offloading system. In Ref. [180], the long-term value of mobile users was maximized through the implementation of a model-free reinforcement learning offloading method. By obtaining a minimal execution delay of 42.83 percent and 33.28 percent in single user situations, respectively, and 11.71 percent in multi-user scenarios, the suggested optimum offloading scheme with caching enhancement strategy outperformed six alternative current systems. In Ref. [187], an integration model for computation offloading was developed with the goal of lowering the system's weighted total cost in terms of latency and energy usage. The authors in [188] chose a delayed online learning approach to account for changing latency during long-duration processing. It is clear from these publications that computation offloading is critical in the edge computing environment. As a result, SGs applications and services can significantly benefit from the use of this technology, which promises to lower latency, energy consumption, and device battery life, among other benefits.

5.3. Single-User Case

Splitting computation activities into sub-tasks is a critical aspect in enabling the offloading potential of computing models. The authors in [189] discussed strategies for efficiently partitioning a software application composed of a large number of components in cloud computing. These authors have taken into consideration the variability of cloud computing infrastructure. To increase the chance of success for the optimization problem defined in [190], the authors performed research on how a single-user task should be scheduled to both the edge and the Internet cloud. The research in [191] found the global optimum solution in the single-user situation with the goal of decreasing power consump-

tion during task offloading. In Ref. [192], a resource-efficient edge computing approach was suggested. The authors analyzed their approach in a single-user scenario, where each smart IoT device user on the network is provided with the potential to efficiently offload its resource-intensive activities to nearby local devices.

Certain fundamental concerns in conventional computing, such as network use, power consumption, memory utilization, and adaptive offloading cost, have been solved by the innovative distributed technique based on graph representation suggested in [193]. To save costs, the authors recommended that each device retain a similar graph consisting of components in its memory space, while simultaneously abstracting portions of components located in remote places. In Ref. [194], a ThinkAir framework was presented that enables a simpler migration of smartphone applications to the Internet cloud. According to the authors, the primary goals of their suggested architecture were to reduce the likelihood of wasting available resources and to improve the computing performance and efficiency of mobile devices. To prevent lengthy data transmission delays, Ref. [195] proposed a decentralized game theoretic technique that enables mobile devices to organize themselves automatically into mutually acceptable computation offloading decisions. Additionally, it was noted that the self-organizing capability of mobile devices will assist in reducing the amount of effort required of sophisticated data management systems.

5.4. Multi-User Case

In Ref. [187], the authors developed an advanced deep learning-based computational offloading technique for multilayer vehicular edge-cloud computing networks with the goal of determining near-optimal computation offloading decisions. Additionally, the synergy between computation offloading and resource allocation was articulated as a binary optimization problem in order to increase the network's time and energy efficiency. In this situation, computation activities might be offloaded locally (on the vehicle), partially (on the cloud server), or completely (on the vehicular edge computing). The authors in [186] proposed a solution for multi-user MEC systems based on spectral clustering computation under the premise that all users are supplied by a single edge server. However, if all users are permitted to offload duties concurrently, this may result in high inference owing to resource congestion. Considering a different approach, in Ref. [180], the authors presented an offloading strategy based on Q-learning that takes user mobility into account and also mitigates harsh inference caused by resource contention (which usually occurs when multiple mobile users offload workloads at the same edge server simultaneously). In this case, mobile users are permitted to maximize the amount of processed central processing unit (CPU) cycles within their respective time slots, resulting in decreased energy usage. Similarly, the authors in [196] established a unique online SBS peer offloading architecture to enhance the long-term system performance of small-cell base stations (SBSs) without exceeding their required energy consumption threshold. To solve the offloading decision-making difficulty in their suggested architecture, the authors used the Lyapunov drift-plus-penalty approach and also created an energy deficiency queue for each SBS placed on the network. Similarly, Ref. [188] presented an online-assisted cooperative offloading technique. Here, the authors considered a scenario in which computation offloading was structured according to the degree of trust that individuals had developed for one another. This would improve the effectiveness of cooperative offloading applications in MEC.

In comparison to earlier research, the solution in [184] considered that each computation task in their suggested model is atomic and cannot be partitioned. Additionally, each device is provided three computation strategies (i.e., locally, partly, or fully offloading) against which to choose when it comes to offloading its computation tasks. The connection between the mobile device and the edge server serves as a criterion for determining which of these offloading mechanisms to apply. Partial offloading, for example, refers to the offloading performed by the mobile device's CPU. Whereas partial offloading occurs at a MEC server attached to the macro base station, complete offloading occurs at the small cell associated with a mobile device. The proposition in [173] comprises a computation offloading technique based on queuing theory and the stochastic gradient descent (SGD)

algorithm to address the issue of resource consumption in smart devices. In a different approach, the authors in [197] conducted a research on management difficulties associated with computation offloading in heterogeneous networks with the goal of minimizing energy consumption and examining the influence of computation resource allocation on energy consumption and computation offloading. The authors in [198] reduced the weighted energy consumption of mobile devices by developing an optimization model to calculate a near-optimal offloading solution for each mobile device. Security and compression layers were also included in the optimization approach to safeguard and compress the data associated with compute activities before they were transmitted to servers.

5.5. Summary

Table 6 compares the AI and other strategies used to handle many of the main difficulties associated with computation offloading. Among these difficulties are judgments about offloading, resource allocation, and mobility management. As can be seen from the comparison table, the majority of articles sought to address one or two of these issues, but not all at the same time. Given the interconnected nature of these difficulties, future research that considers all three simultaneously from an SG viewpoint is essential. Additionally, the bulk of the research has framed offloading computing as an optimization problem.

Table 6. Application areas, techniques and other metrics associated with computation offloading (OD—offloading decision, RA—resource allocation, MM—mobility management).

Ref	Application Area	Technique	OD	RA	MM	Performance Metrics	Mathematical Tools	Accuracy
[187]	Vehicular	• Reinforcement learning • Distributed deep learning • Deep neural networks	Yes	Yes	No	• Reward ratio	Binary optimization	–
[199]	Multiuser interference environment	• BiJOR • ACS-CLPSO	Yes	Yes	No	• Average energy consumption • Average AN	Bilevel optimization	–
[180]	Wireless networks	• Q-Learning • BRI	Yes	No	No	• Performance ratio's bound • Average energy consumption • Multiple user offloading	Non-coorporative exact potential game	87.87%
[184]	Ultradense IoT networks	• Game-theoretic greedy	Yes	No	No	• Computation overhead • Running time • Energy consumption • Minimum processing time	MECO	79%, 83%, and 52%
[186]	MEC system	• Spectral clustering • Label propagation theory • Graph cut	No	Yes	No	• Running time • Local energy consumption • Transmission energy consumption	Constrained double-objective optimization	–
[185]	Mobile collaborative	• Cooperative call graph • Coalition formation game	Yes	No	No	• Average delay • Average caching hit probability • Average offloading probability	OOCS	42.83% and 33.28%
[173]	IoT	• Stochastic gradient descent • Queuing theory	No	Yes	No	• Execution time • Energy consumption • Payment cost	Nonlinear multiobjective optimization	–
[200]	Multi-channel wireless interference environment	• Heuristic • Nash Equilibrium	Yes	No	No	• No.of decision slots • Computation overhead • No.of beneficial cloud computing users	NP-hard	–

6. Cyber Security Challenges and Solutions in Edge Intelligence-Based Smart Grids

Edge computing is envisioned as one of the enabling technologies that will enable next-generation power grids (i.e., SGs) to reach their full potential. While SGs use modern ICT and computational intelligence, it is apparent that the majority of their critical services and applications are still delivered via cloud computing. Due to the shared background nature of such an architecture, it exposes end users' privacy and security, as well as the reliability of power grid infrastructure, to cyber attacks. In Ref. [201], an overview of the SGs' vulnerabilities (i.e., blackouts, communication protocols, customer privacy breaches, to name a few) is presented. Thus, the coordination of edge computing in SGs is indeed a pragmatic solution in light of these challenges.

It is worth noting that IoT smart devices play a significant role in the deployment of SGs. However, there are challenges that need to be addressed towards the deployment of IoT devices in SGs. These difficulties are mostly due to the extensive processing applications that these devices, despite their relatively small physical size, need. Edge computing combines developing technologies such as virtualization (Section 3) and computation offloading (Section 5) in order to relocate these jobs closer to edge devices (i.e., IoT devices or mobiles). Both of these technologies, as well as the edge computing paradigm, rely significantly on edge or cloud servers to operate properly. Prior to offloading, computation activities must be partitioned and offloaded to the edge or cloud server. Authentication should be addressed first during this stage. The buzz around the deployment of these servers in an environment densely packed with intelligent IoT devices creates security concerns for the edge computing paradigm. Various studies in the literature have presented a number of innovative techniques to address these concerns without compromising end-user QoS and QoE. For example, the authors in [202] have provided an overview of the security and privacy challenges raised by edge computing. Nevertheless, different from [202], in this section, we examine many critical security problems associated with the edge computing paradigm via the perspective of SGs. Additionally, we discuss blockchain, a novel technology that can aid in resolving security and privacy concerns in edge computing systems.

6.1. Security Challenges

6.1.1. Distributed Denial-of-Service (DDoS)

As explained in Section 3.2, the majority of applications, such as situational awareness and transmission line monitoring, need low latency. Additionally, attacks and threats against power grid infrastructure appear to be aimed at completely shutting down the grid. In this regard, SGs cannot afford communication delays, as this would result in massive data traffic on the network. To put it simply, a denial of service (DoS) attack denies authorized users access to shared services or resources [203]. DoS attacks manifest themselves in a variety of ways and may also be classified according to their influence on the afflicted system's safety-criticality. The authors in [204] suggested a distributed DoS attack detection technique based on DL. The authors also constructed a recurrent deep neural network to obtain the findings regarding the pattern from the sequence of network traffic and attack activities. The discussion in [205] included a comprehensive evaluation of DDoS statistical approaches. The authors of this article examined statistical techniques for tracking traffic arrivals at discrete time stamps. Several of the parameters discovered in this study that impact the overall effectiveness of DDoS detection systems include computational overhead, attack detection accuracy, and detection of the source or destination of an attack. Additionally, the growth of edge computing in SGs poses concerns about security and privacy. Typically, attacks against edge computing are the result of design flaws, improper setup, and implementation flaws [206]. Each layer in the edge computing architecture may encounter unique security challenges [207]. For instance, DDoS attacks, insecure systems and components, and a lack of data privacy protection are frequently encountered on edge servers, but malicious administrators may be viewed as a significant obstacle in edge administration. To show the robustness of their hierarchical software-defined perimeter (SDP) architecture, the authors in [202] utilized a DDoS attack as a performance metric. In Ref. [208], an intelligence-driven advanced persistent threats edge defense method was presented. Additionally, the authors employed a deep reinforcement learning method to address edge device response demands.

6.1.2. Man-in-the-Middle

Man-in-the-Middle (MITM) refers to an attack in which a third party (intruder) intercepts communication between two parties without their knowledge, despite the fact that the data may be encrypted. It is frequently used for hacking purposes in LAN contexts [209]. In Ref. [210], authors established a way of protecting data from MITM attacks by using interlock protocols. To encrypt the process of exchanging information between

participants, the author used the Rivest–Shamir–Aldleman (RSA) method. An intrusion detection system model was also presented in [211] to identify, isolate, and reconfigure injected nodes on a wireless sensor network (WSN).

6.1.3. Physical Damage

Physical damage is one of the most often seen attacks in edge computing as a result of intruder manipulation. These attacks occur when an attacker acquires unauthorized access to an affected device and has the ability to re-configure the device in such a way that information is misdirected to certain applications [212].

6.1.4. Service or VM Manipulation

The emergence of SGs typically coincides with the widespread deployment of sensors across different network domains with the purpose of reducing catastrophic power grid breakdowns. However, irrespective of the benefits posed by these different sensors, attackers being able to manipulate sensing data may result in public fear. Furthermore, illegal access to vital information about citizens, healthcare systems, end-user data, and possibly personal identification information could cause widespread panic [213].

6.1.5. False Data Injection

Malware injection attacks entail acts designed to successfully and covertly inject false information into a computer system with the goal of exploiting the devices' vulnerabilities. Among these vulnerabilities include susceptibility to hardware Trojans, device cloning, less secure wireless protocols, and predictable access control credentials. The possible consequences for SGs resulting from malware injection attacks are service disruption and financial loss [201]. Edge devices and low-level edge servers are two of the most vulnerable components in the edge computing architecture to malware injection attacks. From the standpoint of edge computing, malware injection attacks may be classified as server-side (i.e., injections directed at edge servers) or device-side (i.e., injections directed at edge devices) [214].

6.2. Key Approaches to Solving Cyber Security Issues

Several approaches have been proposed recently to solve the security and privacy concerns associated with edge computing. The authors in [56] developed a taxonomy for current security solutions based on the layer of computing paradigm. Among the methods suggested by the authors for resolving security challenges at the sensing layer are permission, cryptography, image processing, and collision detection. In a separate article, the authors in [202] also provided a brief summary of the issues mentioned above. The solution in [215] introduced a novel authentication technique to reduce the threats posed by frequent data flow between smart devices and utility centers in Singapore. Additionally, the authors attempted to increase the efficiency of disaster recovery management by using their recommended method.

To address the security difficulties (MITM, sniffer, and location-based attacks) encountered by MEC during compute offloading, the authors in [202] suggested a software-defined perimeter (SDP) architecture to augment MEC. In Ref. [132], a polymorphic heterogeneous security architecture for edge-enabled SG was suggested. Additionally, they provided a feedback method to address issues resulting from hardware and software similarity, singleness, and SG static. This is referred to as a closed-loop feedback system. To accomplish the requisite security and scalability for IoT and edge computing integration, the potential of blockchain's peer-to-peer distributed ledger was carefully investigated from a variety of angles, including anonymity, integrity, and flexibility in [216]. The security situational awareness of SGs was analyzed using the suggested framework based on deep reinforcement learning algorithms and the multiagent deep deterministic policy gradient edge computing paradigm described in [27].

6.2.1. ML and DL Algorithms for Cybersecurity

As explained in further detail below, ML and DL algorithms are among the most extensively used strategies for mitigating the limits and constraints associated with traditional cybersecurity approaches. Recent research has demonstrated that these strategies may be utilized to identify any cyber attacks directed at the network of interest. Additionally, ML is regarded as a vital component of cybersecurity, since it can be used at both the attacker and defender sides. For example, the objective in [217] was to assess existing ML approaches (i.e., random forest, SVM, naive Bayes, decision trees, ANN, and deep belief networks) with the goal of demonstrating their capability for identifying cybersecurity risks. This investigation was conducted in the context of three primary threats: intrusion, spam, and malware detection.

Support Vector Machine

Support vector machine (SVM) has been identified as a suitable machine learning method for improving the performance of various cybersecurity applications. Presently, SVM's high resource consumption (in terms of time and space) restricts its usage, particularly in real-time applications. According to [218], SVM transforms data using kernels with the goal of discovering the best border between samples. The authors in [219] developed a model that combines multi-layer SVM and deep feature extraction to detect abnormal behavior in large-scale network traffic data in order to assure efficient security in distributed networks.

K-Nearest Neighbor

Essentially, the K-Nearest Neighbor (KNN) technique employs a distance function (such as Euclidean, Manhattan, or Minkowski) to determine the difference and similarity between two classes within a dataset [220]. In recent times, data have evolved in a variety of ways, which may not be feasible for other ML algorithms, but it is for KNNs because they make no prior assumptions about the data [221].

Decision Tree

The decision tree is a supervised learning method in which the labeled dataset is used to accurately predict the model's output. This ML approach is characterized as a supervised learning algorithm with a structure resembling a flowchart tree. Along with the multilayer perceptron processing technique, a decision tree was used in [222] to enhance the preprocessing of the large-scale cybersecurity dataset (UGR'16) in order to boost the performance of the anomaly detection model.

Deep Belief Network

A deep belief network comprises multiple layers, each of which may act as a restricted Boltzmann machine [217]. This approach may be helpful for applications involving large-scale datasets in the context of cybersecurity (high-dimensional data). In Ref. [223], the authors undertook a thorough study of the application of deep belief networks and other deep learning methods in cybersecurity. Similarly, the authors in [224] compared the overall performance of the deep belief network to that of a state-preserving extreme learning machine method using the NSL-KDD dataset for face recognition, pedestrian detection, and intrusion detection. In Ref. [225], a secured architecture was developed based on a deep neural network for detecting malicious detection attacks on SCADA systems by leveraging traffic and payload attributes as network performance metrics. A blockchain-based model of a healthcare system was used to identify intrusions in [226].

Recurrent Neural Networks

The recurrent neural network (RNN) can be characterized by its directed graph structure design composed of interconnected nodes. Additionally, RNN generates signals that travel in both directions and introduces loops into the network. In comparison to feedfor-

ward neural networks, RNNs are less extensively used in real-time applications for their highly computational nature. Nevertheless, RNN was utilized in [222] to improve the accuracy of intrusion detection systems based on the dataset used. In ref. [227], an innovative AI-based technique was developed to address false data injection attacks in direct current (DC) microgrids. To forecast the DC voltages and currents of RESs, these authors used a subtype of RNNs called the nonlinear auto-regressive exogenous model (NARX). NARX aims to improve network performance in terms of speed, accuracy, and learning potential as compared to standard RNNs [228].

Convolutional Neural Networks

Unlike some other deep learning algorithms, convolutional neural networks (CNNs) learn directly from raw input, eliminating the requirement for laborious data extraction prior to training the model. CNNs are often composed of convolutional, multiple hidden layers, pooling, and fully connected layers. CNN undoubtedly plays a critical role in the cybersecurity domain. Different methods based on CNN have been proposed to address a range of security and privacy concerns across a variety of commercial industries. For example, the CNN was used to develop a multiclass classification model for IoT networks in a novel anomaly-based intrusion detection methodology [229]. The authors in [230] employed this algorithm to detect cyber intrusions on industrial control systems with the goal of replicating a real-time industrial water treatment facility on a smaller scale. In Ref. [231], authors employed CNN to identify DoS attacks on IoT networks. A unique deep CNN system for malware detection was also suggested in [232], which also enables the network to be effectively implemented on a GPU. To identify intrusion attacks on industrial IoT networks, [233] suggested a multi-CNN fusion approach.

6.2.2. Blockchain for Cybersecurity

The authors in [234] undertook a thorough review of existing works published between 2013 and 2022 that focused only on cybersecurity measures for blockchain-based systems. Among the approaches are bitcoin (the first cryptocurrency to incorporate blockchain technology, launched in 2008), ethereum (which permits the use of smart contracts and was launched in 2015), and the hyperledger project (which comprises software developers designing and developing blockchain frameworks and platforms). Although blockchain technology was first associated with bitcoin, it has since expanded in terms of its potential for use in a range of applications. The discussion in [235] extended previous work on blockchain technology's cybersecurity issues. The authors investigated various remedies to blockchain's cybersecurity vulnerabilities. The web-based cybersecurity awareness campaign was implemented to help mitigate the danger of cybercrime in the process [235]. The proposed technique utilizes blockchain technology to essentially safeguard the application from any cyber attacks that may be imposed on it. To solve the cybersecurity issue in the healthcare sector, Ref. [226] presented a blockchain-based data transfer system with a categorization model.

6.3. Summary and Discussion

Both edge computing and the SG continue to have security flaws as a result of their extensive deployment of edge nodes and faulty smart meters, respectively. Additionally, attackers may infiltrate the edge data center and acquire illegal access to the system's control privileges, putting end users at risk. Several papers in the literature have sought to address these shortcomings by combining edge computing with blockchain technology, for which several efforts have been presented in this section and summarized in Table 7. EI solves important problems in SGs by combining edge computing and efficient AI technologies. Nevertheless, in spite of its various advantages, there are still unresolved research questions and new areas that can be investigated in the future, which will be discussed in the next section.

Table 7. Comparison of Different Cybersecurity Approaches.

Ref	Application Area	Cybersecurity Issue	Method	Contribution
[236]	IoT	Trust	Blockchain	• Devised trust computing to ensure reliability • New content model to encrypt hot data
[202]	LTE Networks	• DoS attacks • DDoS • MITM	SDP	• Implement SDP within LTE networks
[127]	Smart Grid	• Privacy protection • Energy security	Blockchain	• Guarantee user's validity • Novel solution for traceable energy governance
[230]	Industrial control systems	• Cyber attacks • Anomalies	CNN	• Successful use of 1D CNN • Comparison of different neural networks architectures
[237]	Smart Grid	Security	Blockchain	• Introduce blockchain-based mutual authentication and key agreement protocol

7. Research Challenges and Future Directions

Through the combination of edge computing and efficient AI technologies, edge intelligence delivers significant solutions to major difficulties faced by SGs. Despite its benefits, there are still unanswered research questions and prospective areas that can be explored in future studies and a few are discussed here.

7.1. Resource Management

Recently, the trend of facilitating edge computing has become prominent in most, if not all, IoT applications. There are still some issues with edge computing that need to be solved before it can be used to its full potential in IoT applications. One of the main problems in edge computing is successfully managing data processing at the edge in the shortest amount of time possible. There has been a significant number of papers published in the literature that have focused on the application of ML algorithms to handle data processing in edge computing. There is no doubt that ML algorithms will dramatically improve the performance of the edge computing paradigm in a variety of ways. However, ML techniques have several disadvantages that may result in performance reduction of edge computing applications in IoT-enabled infrastructures such as SGs. To this goal, we describe the issues inherent in edge computing's processing and computation management.

7.1.1. Communication and Big Data Processing at the Edge

From a processing and communication standpoint, the use of ML algorithms have considerably enhanced the overall performance of the edge computing paradigm in terms of latency, energy efficiency, and dependability. Since data would be completely outsourced to the edge, accuracy and flexibility will remain challenges in this architecture. Additionally, the majority of edge devices have little computational capabilities. To cope with the intermittent demands generated by distributed applications, edge computing architectures should be scalable and adaptable. The IoT and sensing devices are becoming increasingly prevalent, as are the data they generate. This places the Internet cloud in a new communication and energy predicament. DL has recently been demonstrated to be a useful approach to tackle many problems in many different applications, however its slow computing speed

creates problems with processing and communication. This makes it difficult to deploy in a variety of different and time-critical edge computing applications.

7.1.2. Load Balancing

Load balancing may be accomplished in edge computing by effectively and efficiently offloading an end user's workload to many edge data centers, therefore dramatically reducing intra-data center migration. Given the heterogeneity of data generated by IoT devices in SGs, which manifests itself in a number of ways (i.e., volume, variety, velocity, etc.), load distribution across edge data centers may need to be changed to account for the diversity of end-user workload. Additionally, SGs have emerged as a result of the inclusion of mobile networks such as 5G, which include mobile devices that regularly switch locations. In this way, traditional load balancing solutions are becoming increasingly difficult as load circumstances change [238]. To address this issue, a new load balancing mechanism that takes into consideration the mobility of edge computing may need to be developed in the future.

To address the resource management difficulties described above, the convergence of 5G ultra-dense and edge computing [40] may be investigated further in order to meet the network's computation and communication needs.

7.2. Advanced AI Technologies

Despite the benefits of AI applications, it is worth noting that some AI technologies continue to face difficulties in their deployment in the complex edge intelligence environment [239]. Recent studies have examined approaches to enhance the performance of AI techniques. There are limited studies in the literature that demonstrate how to make AI systems more adaptive, allowing them to fully use their human intelligence side, as the definition states.

7.3. Intelligent Computation Offloading

Computation offloading is a critical feature arising with the edge computing paradigm, allowing for the partitioning of resource-intensive computation workloads into manageable subtasks for onward transfer to resource-rich edge clouds or edge servers. Computation offloading in edge computing involves more than simply splitting and offloading activities to a nearby edge cloud or edge server; it is also about determining how to offload, when to offload, and what to offload. Several previous studies assumed that the solutions to one or more of the aforementioned essential problems were already known. With those three issues in mind, a full analysis and detailed architecture demonstrating the process of compute offloading in edge computing can be examined further. Additionally, while it is apparent that the application of AI to edge computing is gaining momentum everyday, there are few, if any, papers in the literature that have committed to completely exploiting AI technologies from a compute offloading viewpoint. Given the complexity of intelligent offloading, a number of aspects must be considered in order to achieve the purpose of this novel concept.

7.4. Secured and Robust Situational Awareness Framework for Smart Grid

Situational awareness is one of the critical applications that will emerge as a result of SG implementation. This application is defined by a low tolerance for data transmission delays and by its crucial role in the "big data" age of power grids. Notably, the widespread IoT devices and massive number of intelligent terminals accessing SG provide massive amounts and types of data, which may be both a "curse" and a "blessing" for next-generation power grids. From a technological standpoint, information retrieved from these data may be used to identify unique scenarios for future decision-making and monitoring of power grid domains, considerably improving the production and general functioning of SG infrastructure. In order to ensure the security and robustness of an SGs' situational awareness, there are a few factors to consider, noted as follows:

- SG's control system must work consistently and be responsive to any real-time dangers detected in such an environment. However, cloud-based SG architectures struggle to meet the requirements for swiftly responding to real-time threats without degrading end-user QoS.
- Due to sensitivity of data acquired from SGs and IoT devices such as smart meters, and sensors, SGs must have an uncompromising level of security, as they can be vulnerable to cyber assaults.
- Due to the variability of power terminals and the diversity of communication protocols, SGs have faced a number of interconversion and interoperability issues. Additionally, there are issues with establishing and deploying diverse networks, administering and sustaining networks. This complicates the efficient and effective utilization of a large number of various terminals in SGs.

Thus, future research might examine the establishment of a secure and resilient situational awareness for the deployment of SGs through the use of cutting-edge technologies such as edge computing, AI, and blockchain synergy as a possible solution to the aforementioned difficulties.

7.5. Privacy Concerns

Current research indicates that edge computing will potentially transform how we approach the SG paradigm. However, given the sensitivity of the data acquired in SG, privacy and security continue to be the most difficult concerns in this paradigm today. Additionally, the majority of edge computing applications support location awareness, which may contribute to the worry about privacy in SGs by requiring end-device location information prior to conducting computation operations. To ensure the safety of end users in SGs and the infrastructure's reliability, a privacy preservation strategy that takes into consideration the latency needs of SGs can be devised. To address the issue of privacy in SGs, an encryption method should be developed that takes inference and other cyber threats into consideration. A future research might examine the use of distributed ledger technologies, such as blockchain, to enhance the security of location privacy in edge computing-aided SG.

7.6. Facilitation of Two-Way Communication

In comparison to traditional power grids, SG aims to enable the bidirectional flow of electricity and information across grid domains with the goal of improving the grid's overall performance in terms of latency, energy efficiency, to name a few. To accomplish this, AMI is intended to deploy a considerable number of smart meters, allowing for regular acquisition of power consumption data from all the smart electrical gadgets installed within the consumer's premises. Additionally, this enables customers to maintain a sustained communication channel with power suppliers prior to implementing additional power management orders and making grid operating choices. Because consumers' premises are exposed to both cyber and physical attacks, this compromises both their privacy and the stability of electricity systems. In this regard, the SGs infrastructure has a new problem in terms of guaranteeing adequate security for these devices. The AMI system may be used to investigate the potential synergies between emerging AI and blockchain technologies.

7.7. Access Control Mechanisms

Despite the benefits of SGs' decentralized structure, monitoring and controlling geographically distributed devices under this new paradigm is a difficult task. Additionally, the access control techniques employed in SGs must be adaptable and sensitive to any emergency circumstance that may occur on the network, ensuring that the appropriate persons have the appropriate credentials.

7.8. Trust

The operation and advancement of SGs as a whole are significantly reliant on sensed data and control commands, often used to perform the majority, if not all, of their functions. In this sense, these data, as well as communicated commands, should not be taken at face value, but rather verified and permitted prior to implementation in SGs. Additionally, because SG is a complex and diverse paradigm, identifying malware injection attacks in real time becomes a significant difficulty, much more so when we rely on algorithms originally created for the sole goal of detecting defects [201].

7.9. Practical Implications of Research Directions

Following the above challenges and future research directions, we highlight a summary of the practical implications of EI in SGs based on our present survey as follows:

1. A decrease in latency: The use of edge computing can make it possible to drastically cut down on the amount of time spent transmitting data within different SG elements. This will contribute to the real-time monitoring of frequency and voltage characteristics within the grid, hence eliminating power factor penalties.
2. Privacy of transmitted data: While there is a significant risk of data leakage and other security issues associated with SGs, it has become abundantly evident that edge intelligence may help limit these kinds of problems to a significant degree. This is something that can be accomplished by performing computations, storing data, and processing them locally, as well as having the capacity to identify abnormalities using machine learning algorithms.
3. Capabilities to engage in transactive energy: The edge intelligence present in SGs has the potential to facilitate the easier integration of microgrids, which in turn makes it possible for prosumers and energy providers to engage in economic transactions. This will further guarantee that there is a fair balance of demand and supply within the network, which will ultimately result in the grid becoming more stable and reliable.
4. Increased dependability as a result of regular power status reports: Edge intelligence will make real-time transmission of network parameters possible, which will improve both the analysis of and the response to grid outages.
5. Decentralized voltage control: Due to the incorporation of microgrids in SGs, there is a larger potential for voltage instability throughout the grid. Edge intelligence provides a decentralized framework for monitoring these oscillations and promptly implementing mitigation techniques to reduce their consequences.
6. Asset management and planning: Because of the ever-increasing growth in the production, acquisition, and incorporation of renewable energy into the grid, there is a growing demand for asset management and planning that accounts for expansion within the grid. Edge intelligence provides a platform for the real-time documenting of such assets, as well as the analysis of their influence on the growth of the grid and the potential for future projections about the expansion and deployment of new assets.

8. Conclusions

EI has demonstrated significant potential as an enabling technology in a variety of enterprises. It may be regarded a realistic strategy for rapidly deploying the possible applications and services associated with SGs. This article has discussed EI-based SGs in detail, with an emphasis on architectures, computation offloading, and cybersecurity concerns and solutions. Separately, the ideas of EI and SGs were examined to gain a fundamental knowledge of each. A three-layer hierarchical design structure was proposed to study an EI-based architecture appropriate for SG implementation purposes. This structure begins at the first (i.e., lowest) level (edge devices), which comprises the IoT-based smart devices used across all SG domains (i.e., generation, transportation, distribution, and consumption). The second layer (edge node) is responsible for providing some of the computation resources transferred from the Internet cloud. Then, on the third tier (fog node-server layer), data analysis and reduction are performed, as well as control responses.

In summary, these layers constitute an ordered and decentralized architecture for deploying EI in SGs. While this design has demonstrated amazing benefits, security and privacy issues continue to be an underlying concern. Thus, we have conducted a survey of some of the most cutting-edge studies on cybersecurity solutions. As evidenced by the literature, blockchain technology has been considered as a viable solution. Summarily, this article will be of interest to the budding researcher who may be curious in becoming acquainted with the state-of-the-art principles necessary for comprehending the use of EI in SG systems.

Author Contributions: Conceptualization, D.N.M. and A.J.O.; Funding acquisition, A.M.A.-M.; Investigation, D.N.M.; Methodology, D.N.M.; Project administration, A.J.O. and A.M.A.-M.; Supervision, A.J.O. and A.M.A.-M.; Writing—original draft, D.N.M.; Writing—review & editing, A.J.O. and A.M.A.-M. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Council for Scientific and Industrial Research (CSIR) and The APC was funded by project number 05400 054AT KR3EEMG.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

List of Abbreviations

Acronym	Meaning
3G	Third Generation
4G	Fourth Generation
5G	Fifth Generation
ACS-CLPSO	Ant Colony System-Comprehensive Learning Particle Swarm Optimizer
ADMM	Alternating Direction of Method Multipliers
AI	Artificial Intelligence
AIoT	Artificial Intelligence of Things
AMI	Advanced Metering Infrastructure
ANN	Artificial Neural Network
AR	Augmented Reality
BiJOR	Bilevel Optimization Approach
BP	Back-Propagation
BRI	Better Response with Inertia
CBDS	Cooperative Bait Detection Scheme
CNN	Convolutional Neural Network
CO_2	Carbon diOxide
CPU	Central Processing Unit
DC	Direct Current
DDoS	Distributed Denial of Service
DG	Distributed Generation
DG	Distributed Generaion
DL	Distributed Learning
DLT	Distributed Ledger Technology
DoS	Denial of Service
DR	Demand Response
DSM	Demand Side Management
EC	Edge Computing

EI	Edge Intelligence
eMBB	Enhanced Mobile Broadband
EnPEO-DBN	Ensemble Population External Optimization-Based Deep Belief Network
ETSI	European Telecommunications Standards Institute
EVs	Electric Vehicles
FL	Federated Learning
G2V	Grid to Vehicle
HAN	Home Area Networks
HEMS	Home Energy Management Systems
IBM	International Business Machines
ICT	Information and Communication Technology
IoT	Internet of Things
IoVs	Internet of Vehicles
IT	Information Technology
K-NN	K-Nearest Neighbor
LAN	Local Area Networks
MAS	Multi-Agent System
MDMS	Meter Data Management System
MEC	Mobile Edge Computing
MECO	Mobile Edge Computation Offloading
MITM	Man-in-the-Middle
ML	Machine Learning
MM	Mobility Management
mMTC	Massive Machine Type Communications
NANs	Neighborhood Area Network
NILM	Non-Intrusive Load Monitoring
OD	Offloading Decision
OOCS	Optimal Offloading with Caching-Enhancement Scheme
OOCS	Optimal Offloading with Caching-Enhancement Scheme
P2P	Peer-to-Peer
PEO	Population External Optimization
PHEV	Plug-in Hybrid Electric Vehicles
PPP	Public Private Partnerships
PSO	Particle Swarm Optimization
PSO	Particle Swarm Optimization
QoE	Quality of Experience
QoS	Quality of Service
RA	Resource Allocation
RES	Renewable Energy Source
RFID	Radio Frequency Identification
RNN	Recurrent Neural Network
RTUs	Remote Terminal Units
SAS	Substation Automation Systems
SBSs	Small-Cell Base Stations
SCADA	Supervisory Control and Data Acquisition
SDP	Software Defined Perimeter
SGD	Stochastic Gradient Descent
SGs	Smart Grids
SVM	Support Vector Machine
UAVs	Unmanned Aerial Vehicles
uRLLC	Ultra-Reliable Low-Latency Communications
V2G	Vehicle to Grid
VMs	Virtual Machines
VR	Virtual Reality
WANs	Wide Area Networks
WASA	Wide Area Situational Awareness
WSN	Wireless Sensor Network

References

1. Mishra, J.; Sheetlani, J.; Reddy, K.H.K.; Roy, D.S. A novel edge-supported cost-efficient resource management approach for smart grid system. In *Progress in Computing, Analytics and Networking*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 369–380.
2. Yao, J.; Li, Z.; Li, Y.; Bai, J.; Wang, J.; Lin, P. Cost-efficient tasks scheduling for smart grid communication network with edge computing system. In Proceedings of the 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), Tangier, Morocco, 24–28 June 2019; pp. 272–277.
3. Molokomme, D.N.; Chabalala, C.S.; Bokoro, P.N. A review of cognitive radio smart grid communication infrastructure systems. *Energies* **2020**, *13*, 3245. [CrossRef]
4. Kabalci, E.; Kabalci, Y. *Smart Grids and Their Communication Systems*; Springer: Berlin/Heidelberg, Germany, 2019.
5. 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, 101514.
6. Mehmood, M.Y.; Oad, A.; Abrar, M.; Munir, H.M.; Hasan, S.F.; Muqeet, H.; Golilarz, N.A. Edge computing for IoT-enabled smart grid. *Secur. Commun. Netw.* **2021**, *2021*, 5524025. [CrossRef]
7. U.S. Department of Energy. Available online: https://www.energy.gov/oe/office-electricity (accessed on 24 April 2022).
8. Strategic National Smart Grid Vision for the South African Electricity Supply Industry. Available online: https://www.ee.co.za/wp-content/uploads/2017/12/Smart-Grid-Vision-Document-2017.pdf (accessed on 22 January 2022).
9. Onumanyi, A.J.; Isaac, S.J.; Kruger, C.P.; Abu-Mahfouz, A.M. Transactive energy: State-of-the-art in control strategies, architectures, and simulators. *IEEE Access* **2021**, *9*, 131552–131573. [CrossRef]
10. Gungor, V.C.; Sahin, D.; Kocak, T.; Ergut, S.; Buccella, C.; Cecati, C.; Hancke, G.P. Smart grid technologies: Communication technologies and standards. *IEEE Trans. Ind. Inform.* **2011**, *7*, 529–539. [CrossRef]
11. Bera, S.; Misra, S.; Rodrigues, J.J. Cloud computing applications for smart grid: A survey. *IEEE Trans. Parallel Distrib. Syst.* **2014**, *26*, 1477–1494. [CrossRef]
12. Li, Q.; Deng, Y.; Sun, W.; Li, W. Communication and Computation Resource Allocation and Offloading for Edge Intelligence Enabled Fault Detection System in Smart Grid. In Proceedings of the 2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Tempe, AZ, USA, 11–13 November 2020; pp. 1–7.
13. Zhao, S.; Li, F.; Li, H.; Lu, R.; Ren, S.; Bao, H.; Lin, J.H.; Han, S. Smart and practical privacy-preserving data aggregation for fog-based smart grids. *IEEE Trans. Inf. Forensics Secur.* **2020**, *16*, 521–536. [CrossRef]
14. Jiang, D.; Zhang, Y.; Song, H.; Wang, W. Intelligent optimization-based energy-efficient networking in cloud services for multimedia big data. In Proceedings of the 2018 IEEE 37th International Performance Computing and Communications Conference (IPCCC), Orlando, FL, USA, 17–19 November 2018; pp. 1–6.
15. Goyal, S.; Bhushan, S.; Kumar, Y.; Rana, A.u.H.S.; Bhutta, M.R.; Ijaz, M.F.; Son, Y. An optimized framework for energy-resource allocation in a cloud environment based on the whale optimization algorithm. *Sensors* **2021**, *21*, 1583. [CrossRef]
16. Aslanpour, M.S.; Gill, S.S.; Toosi, A.N. Performance evaluation metrics for cloud, fog and edge computing: A review, taxonomy, benchmarks and standards for future research. *Internet Things* **2020**, *12*, 100273. [CrossRef]
17. Mach, P.; Becvar, Z. Mobile edge computing: A survey on architecture and computation offloading. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 1628–1656. [CrossRef]
18. Mao, Y.; You, C.; Zhang, J.; Huang, K.; Letaief, K.B. A survey on mobile edge computing: The communication perspective. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 2322–2358. [CrossRef]
19. Yang, R.; Yu, F.R.; Si, P.; Yang, Z.; Zhang, Y. Integrated blockchain and edge computing systems: A survey, some research issues and challenges. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1508–1532. [CrossRef]
20. Zhang, X.; Biagioni, D.; Cai, M.; Graf, P.; Rahman, S. An edge-cloud integrated solution for buildings demand response using reinforcement learning. *IEEE Trans. Smart Grid* **2020**, *12*, 420–431. [CrossRef]
21. Chang, Z.; Liu, S.; Xiong, X.; Cai, Z.; Tu, G. A survey of recent advances in edge-computing-powered artificial intelligence of things. *IEEE Internet Things J.* **2021**, *8*, 13849–13875. [CrossRef]
22. Deng, S.; Zhao, H.; Fang, W.; Yin, J.; Dustdar, S.; Zomaya, A.Y. Edge intelligence: The confluence of edge computing and artificial intelligence. *IEEE Internet Things J.* **2020**, *7*, 7457–7469. [CrossRef]
23. Meloni, A.; Pegoraro, P.A.; Atzori, L.; Benigni, A.; Sulis, S. Cloud-based IoT solution for state estimation in smart grids: Exploiting virtualization and edge-intelligence technologies. *Comput. Netw.* **2018**, *130*, 156–165. [CrossRef]
24. Hudson, N.; Hossain, M.J.; Hosseinzadeh, M.; Khamfroush, H.; Rahnamay-Naeini, M.; Ghani, N. A framework for edge intelligent smart distribution grids via federated learning. In Proceedings of the 2021 International Conference on Computer Communications and Networks (ICCCN), Athens, Greece, 19–22 July 2021; pp. 1–9.
25. Ghosh, A.M.; Grolinger, K. Edge-cloud computing for Internet of Things data analytics: Embedding intelligence in the edge with deep learning. *IEEE Trans. Ind. Inform.* **2020**, *17*, 2191–2200.
26. Lodhi, A.H.; Akgün, B.; Özkasap, Ö. State-of-the-art techniques in deep edge intelligence. *arXiv* **2020**, arXiv:2008.00824.
27. Lei, W.; Wen, H.; Wu, J.; Hou, W. MADDPG-based security situational awareness for smart grid with intelligent edge. *Appl. Sci.* **2021**, *11*, 3101. [CrossRef]
28. Guo, S.; Dai, Y.; Guo, S.; Qiu, X.; Qi, F. Blockchain meets edge computing: Stackelberg game and double auction based task offloading for mobile blockchain. *IEEE Trans. Veh. Technol.* **2020**, *69*, 5549–5561. [CrossRef]

29. Islam, S.; Badsha, S.; Sengupta, S.; La, H.; Khalil, I.; Atiquzzaman, M. Blockchain-enabled intelligent vehicular edge computing. *IEEE Netw.* **2021**, *35*, 125–131. [CrossRef]
30. Zhuang, P.; Zamir, T.; Liang, H. Blockchain for cybersecurity in smart grid: A comprehensive survey. *IEEE Trans. Ind. Inform.* **2020**, *17*, 3–19. [CrossRef]
31. Rigas, E.S.; Ramchurn, S.D.; Bassiliades, N. Managing electric vehicles in the smart grid using artificial intelligence: A survey. *IEEE Trans. Intell. Transp. Syst.* **2014**, *16*, 1619–1635. [CrossRef]
32. Gilbert, G.M.; Naiman, S.; Kimaro, H.; Bagile, B. A critical review of edge and fog computing for smart grid applications. In Proceedings of the International Conference on Social Implications of Computers in Developing Countries, Dar es Salaam, Tanzania, 1–3 May 2019 ; Springer: Berlin/Heidelberg, Germany, 2019; pp. 763–775.
33. Ferrag, M.A.; Babaghayou, M.; Yazici, M.A. Cyber security for fog-based smart grid SCADA systems: Solutions and challenges. *J. Inf. Secur. Appl.* **2020**, *52*, 102500. [CrossRef]
34. Rosero, D.; Díaz, N.; Trujillo, C. Cloud and machine learning experiments applied to the energy management in a microgrid cluster. *Appl. Energy* **2021**, *304*, 117770. [CrossRef]
35. Feng, C.; Wang, Y.; Chen, Q.; Ding, Y.; Strbac, G.; Kang, C. Smart grid encounters edge computing: Opportunities and applications. *Adv. Appl. Energy* **2021**, *1*, 100006. [CrossRef]
36. Li, T.; Yang, J.; Cui, D. Artificial-intelligence-based algorithms in multi-access edge computing for the performance optimization control of a benchmark microgrid. *Phys. Commun.* **2021**, *44*, 101240. [CrossRef]
37. Wu, Y.; Wu, Y.; Guerrero, J.M.; Vasquez, J.C. Digitalization and decentralization driving transactive energy Internet: Key technologies and infrastructures. *Int. J. Electr. Power Energy Syst.* **2021**, *126*, 106593. [CrossRef]
38. Massaoudi, M.; Abu-Rub, H.; Refaat, S.S.; Chihi, I.; Oueslati, F.S. Deep learning in smart grid technology: A review of recent advancements and future prospects. *IEEE Access* **2021**, *9*, 54558–54578. [CrossRef]
39. Wu, Y.; Wu, Y.; Guerrero, J.M.; Vasquez, J.C. Decentralized transactive energy community in edge grid with positive buildings and interactive electric vehicles. *Int. J. Electr. Power Energy Syst.* **2022**, *135*, 107510. [CrossRef]
40. Yu, S.; Chen, X.; Zhou, Z.; Gong, X.; Wu, D. When deep reinforcement learning meets federated learning: Intelligent multitimescale resource management for multiaccess edge computing in 5G ultradense network. *IEEE Internet Things J.* **2020**, *8*, 2238–2251. [CrossRef]
41. Zhou, Z.; Chen, X.; Li, E.; Zeng, L.; Luo, K.; Zhang, J. Edge intelligence: Paving the last mile of artificial intelligence with edge computing. *Proc. IEEE* **2019**, *107*, 1738–1762. [CrossRef]
42. Muniswamaiah, M.; Agerwala, T.; Tappert, C.C. A Survey on Cloudlets, Mobile Edge, and Fog Computing. In Proceedings of the 2021 8th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2021 7th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), Washington, DC, USA, 26–28 June 2021; pp. 139–142.
43. Xu, D.; Li, T.; Li, Y.; Su, X.; Tarkoma, S.; Jiang, T.; Crowcroft, J.; Hui, P. Edge Intelligence: Empowering Intelligence to the Edge of Network. *Proc. IEEE* **2021**, *109*, 1778–1837. [CrossRef]
44. Amin, S.U.; Hossain, M.S. Edge intelligence and Internet of Things in healthcare: A survey. *IEEE Access* **2020**, *9*, 45–59. [CrossRef]
45. Liu, Y.; Peng, M.; Shou, G.; Chen, Y.; Chen, S. Toward edge intelligence: Multiaccess edge computing for 5G and internet of things. *IEEE Internet Things J.* **2020**, *7*, 6722–6747. [CrossRef]
46. Khan, W.Z.; Ahmed, E.; Hakak, S.; Yaqoob, I.; Ahmed, A. Edge computing: A survey. *Future Gener. Comput. Syst.* **2019**, *97*, 219–235. [CrossRef]
47. Van Le, D.; Tham, C.K. A deep reinforcement learning based offloading scheme in ad-hoc mobile clouds. In Proceedings of the IEEE INFOCOM 2018-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Honolulu, HI, USA, 15–19 April 2018; pp. 760–765.
48. Yang, H.; Luo, H.; Ye, F.; Lu, S.; Zhang, L. Security in mobile ad hoc networks: Challenges and solutions. *IEEE Wirel. Commun.* **2004**, *11*, 38–47. [CrossRef]
49. Khalaf, O.I.; Ajesh, F.; Hamad, A.A.; Nguyen, G.N.; Le, D.N. Efficient dual-cooperative bait detection scheme for collaborative attackers on mobile ad-hoc networks. *IEEE Access* **2020**, *8*, 227962–227969. [CrossRef]
50. Satyanarayanan, M.; Bahl, P.; Caceres, R.; Davies, N. The case for vm-based cloudlets in mobile computing. *IEEE Pervasive Comput.* **2009**, *8*, 14–23. [CrossRef]
51. Taleb, T.; Samdanis, K.; Mada, B.; Flinck, H.; Dutta, S.; Sabella, D. On multi-access edge computing: A survey of the emerging 5G network edge cloud architecture and orchestration. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 1657–1681. [CrossRef]
52. Yahuza, M.; Idris, M.Y.I.B.; Wahab, A.W.B.A.; Ho, A.T.; Khan, S.; Musa, S.N.B.; Taha, A.Z.B. Systematic review on security and privacy requirements in edge computing: State of the art and future research opportunities. *IEEE Access* **2020**, *8*, 76541–76567. [CrossRef]
53. Wang, S.; Zhang, X.; Zhang, Y.; Wang, L.; Yang, J.; Wang, W. A survey on mobile edge networks: Convergence of computing, caching and communications. *IEEE Access* **2017**, *5*, 6757–6779. [CrossRef]
54. Pang, Z.; Sun, L.; Wang, Z.; Tian, E.; Yang, S. A survey of cloudlet based mobile computing. In Proceedings of the 2015 International Conference on Cloud Computing and Big Data (CCBD), Shanghai, China, 4–6 November 2015; pp. 268–275.
55. Teimoori, Z.; Yassine, A.; Hossain, M.S. A Secure Cloudlet-based Charging Station Recommendation for Electric Vehicles Empowered by Federated Learning. *IEEE Trans. Ind. Inform.* **2022**, *18*, 6464–6473. [CrossRef]
56. Puthal, D.; Mohanty, S.P.; Bhavake, S.A.; Morgan, G.; Ranjan, R. Fog computing security challenges and future directions [energy and security]. *IEEE Consum. Electron. Mag.* **2019**, *8*, 92–96. [CrossRef]

57. Zhang, J.; Tao, D. Empowering things with intelligence: A survey of the progress, challenges, and opportunities in artificial intelligence of things. *IEEE Internet Things J.* **2020**, *8*, 7789–7817. [CrossRef]
58. openfog. OpenFog Reference Architecture for Fog Computing. Available online: https://www.iiconsortium.org/pdf/OpenFog_Reference_Architecture_2_09_17.pdf (accessed on 19 February 2022).
59. Bonomi, F.; Milito, R.; Zhu, J.; Addepalli, S. Fog computing and its role in the internet of things. In Proceedings of the Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, Helsinki, Finland, 17 August 2012; pp. 13–16.
60. Guevara, J.C.; Torres, R.d.S.; da Fonseca, N.L. On the classification of fog computing applications: A machine learning perspective. *J. Netw. Comput. Appl.* **2020**, *159*, 102596. [CrossRef]
61. Khan, S.; Parkinson, S.; Qin, Y. Fog computing security: A review of current applications and security solutions. *J. Cloud Comput.* **2017**, *6*, 1–22. [CrossRef]
62. Zhang, P.; Zhou, M.; Fortino, G. Security and trust issues in fog computing: A survey. *Future Gener. Comput. Syst.* **2018**, *88*, 16–27. [CrossRef]
63. Barik, R.K.; Gudey, S.K.; Reddy, G.G.; Pant, M.; Dubey, H.; Mankodiya, K.; Kumar, V. FogGrid: Leveraging fog computing for enhanced smart grid network. In Proceedings of the 2017 14th IEEE India Council International Conference (INDICON), Roorkee, India, 15–17 December 2017; pp. 1–6.
64. Hussain, M.; Beg, M. Fog computing for internet of things (IoT)-aided smart grid architectures. *Big Data Cogn. Comput.* **2019**, *3*, 8. [CrossRef]
65. Preden, J.S.; Tammemäe, K.; Jantsch, A.; Leier, M.; Riid, A.; Calis, E. The benefits of self-awareness and attention in fog and mist computing. *Computer* **2015**, *48*, 37–45. [CrossRef]
66. Galambos, P. Cloud, fog, and mist computing: Advanced robot applications. *IEEE Syst. Man Cybern. Mag.* **2020**, *6*, 41–45. [CrossRef]
67. Li, X.; Huang, X.; Li, C.; Yu, R.; Shu, L. EdgeCare: Leveraging edge computing for collaborative data management in mobile healthcare systems. *IEEE Access* **2019**, *7*, 22011–22025. [CrossRef]
68. Babirye, S.; Serugunda, J.; Okello, D.; Mwanje, S. Resource-Aware Workload Orchestration for Edge Computing. In Proceedings of the 2020 28th Telecommunications Forum (TELFOR), Belgrade, Serbia, 24–25 November 2020; pp. 1–4.
69. Okwuide, J.; Haavisto, J.; Harjula, E.; Ahmad, I.; Ylianttila, M. SDN Enhanced Resource Orchestration for Industrial IoT in Containerized Edge Applications. *IEEE Access* **2020**, *8*, 2169–3536.
70. Guim, F.; Metsch, T.; Moustafa, H.; Verrall, T.; Carrera, D.; Cadendelli, N.; Chen, J.; Doria, D.; Ghadie, C. Autonomous Lifecyle Management for Resource-efficient Workload Orchestration for Green Edge Computing. *IEEE Trans. Green Commun. Netw.* **2021**, *6*, 571–582. [CrossRef]
71. Sonmez, C.; Ozgovde, A.; Ersoy, C. Fuzzy workload orchestration for edge computing. *IEEE Trans. Netw. Serv. Manag.* **2019**, *16*, 769–782. [CrossRef]
72. Ndiaye, M.; Abu-Mahfouz, A.M.; Hancke, G.P.; Silva, B. Exploring control-message quenching in SDN-based management of 6LowPANs. In Proceedings of the 2019 IEEE 17th International Conference on Industrial Informatics (INDIN), Helsinki-Espoo, Finland, 22–25 July 2019; Volume 1, pp. 890–983.
73. Wu, Y. Cloud-edge orchestration for the Internet of Things: Architecture and AI-powered data processing. *IEEE Internet Things J.* **2020**, *8*, 12792–12805. [CrossRef]
74. Zhou, Z.; Wu, Q.; Chen, X. Online orchestration of cross-edge service function chaining for cost-efficient edge computing. *IEEE J. Sel. Areas Commun.* **2019**, *37*, 1866–1880. [CrossRef]
75. Chen, S.; Wen, H.; Wu, J.; Lei, W.; Hou, W.; Liu, W.; Xu, A.; Jiang, Y. Internet of things based smart grids supported by intelligent edge computing. *IEEE Access* **2019**, *7*, 74089–74102. [CrossRef]
76. 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]
77. Ning, Z.; Dong, P.; Wang, X.; Hu, X.; Guo, L.; Hu, B.; Guo, Y.; Qiu, T.; Kwok, R.Y. Mobile edge computing enabled 5G health monitoring for Internet of medical things: A decentralized game theoretic approach. *IEEE J. Sel. Areas Commun.* **2020**, *39*, 463–478. [CrossRef]
78. Gohar, A.; Nencioni, G. The role of 5G technologies in a smart city: The case for intelligent transportation system. *Sustainability* **2021**, *13*, 5188. [CrossRef]
79. Hassan, N.; Yau, K.L.A.; Wu, C. Edge computing in 5G: A review. *IEEE Access* **2019**, *7*, 127276–127289. [CrossRef]
80. Shi, W.; Cao, J.; Zhang, Q.; Li, Y.; Xu, L. Edge computing: Vision and challenges. *IEEE Internet Things J.* **2016**, *3*, 637–646. [CrossRef]
81. Krichmar, J.L.; Severa, W.; Khan, M.S.; Olds, J.L. Making BREAD: Biomimetic strategies for artificial intelligence now and in the future. *Front. Neurosci.* **2019**, *13*, 666. [CrossRef]
82. Olowononi, F.O.; Rawat, D.B.; Liu, C. Resilient machine learning for networked cyber physical systems: A survey for machine learning security to securing machine learning for cps. *IEEE Commun. Surv. Tutor.* **2020**, *23*, 524–552. [CrossRef]
83. Ji, H.; Alfarraj, O.; Tolba, A. Artificial intelligence-empowered edge of vehicles: Architecture, enabling technologies, and applications. *IEEE Access* **2020**, *8*, 61020–61034. [CrossRef]
84. Sodhro, A.H.; Pirbhulal, S.; De Albuquerque, V.H.C. Artificial intelligence-driven mechanism for edge computing-based industrial applications. *IEEE Trans. Ind. Inform.* **2019**, *15*, 4235–4243. [CrossRef]

85. Shirazi, S.N.; Gouglidis, A.; Farshad, A.; Hutchison, D. The extended cloud: Review and analysis of mobile edge computing and fog from a security and resilience perspective. *IEEE J. Sel. Areas Commun.* **2017**, *35*, 2586–2595. [CrossRef]
86. He, Y.; Wang, Y.; Qiu, C.; Lin, Q.; Li, J.; Ming, Z. Blockchain-based edge computing resource allocation in IoT: A deep reinforcement learning approach. *IEEE Internet Things J.* **2020**, *8*, 2226–2237. [CrossRef]
87. Gunaratne, N.G.T.; Abdollahian, M.; Huda, S.; Ali, M.; Frontino, G. An edge tier task offloading to identify sources of variance shifts in smart grid using a hybrid of wrapper and filter approaches. *IEEE Trans. Green Commun. Netw.* **2021**, *6*, 329–340. [CrossRef]
88. Zhu, Z.; Tian, Y.; Li, F.; Yang, H.; Ma, Z.; Rong, G. Research on edge intelligence-based security analysis method for power operation system. In Proceedings of the 2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), New York, NY, USA, 1–3 August 2020; pp. 258–263.
89. Huh, J.H.; Seo, Y.S. Understanding edge computing: Engineering evolution with artificial intelligence. *IEEE Access* **2019**, *7*, 164229–164245. [CrossRef]
90. Chung, H.M.; Maharjan, S.; Zhang, Y.; Eliassen, F.; Yuan, T. Edge Intelligence Empowered UAV s for Automated Wind Farm Monitoring in Smart Grids. In Proceedings of the GLOBECOM 2020–2020 IEEE Global Communications Conference, Taipei, Taiwan, 7–11 December 2020; pp. 1–6.
91. Huang, Z.; Dong, F.; Shen, D.; Zhang, J.; Wang, H.; Cai, G.; He, Q. Enabling Low Latency Edge Intelligence based on Multi-exit DNNs in the Wild. In Proceedings of the 2021 IEEE 41st International Conference on Distributed Computing Systems (ICDCS), Washington DC, USA, 7–10 July 2021; pp. 729–739.
92. Van Huynh, D.; Khosravirad, S.R.; Masaracchia, A.; Dobre, O.A.; Duong, T.Q. Edge Intelligence-based Ultra-Reliable and Low-Latency Communications for Digital Twin-enabled Metaverse. *IEEE Wirel. Commun. Lett.* **2022**, *11*, 1733–1737. [CrossRef]
93. Hu, R.Q. Mobility-aware edge caching and computing in vehicle networks: A deep reinforcement learning. *IEEE Trans. Veh. Technol.* **2018**, *67*, 10190–10203.
94. Zhang, H.; Wang, R.; Liu, J. Mobility Management for Ultra-Dense Edge Computing: A Reinforcement Learning Approach. In Proceedings of the 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall), Honolulu, HI, USA, 22–25 September 2019; pp. 1–5.
95. Dai, Y.; Zhang, K.; Maharjan, S.; Zhang, Y. Edge intelligence for energy-efficient computation offloading and resource allocation in 5G beyond. *IEEE Trans. Veh. Technol.* **2020**, *69*, 12175–12186. [CrossRef]
96. Baumeister, T. *Literature Review on Smart Grid Cyber Security*; Collaborative Software Development Laboratory at the University of Hawaii: Honolulu, HI, USA , 2010; Volume 650.
97. Kuzlu, M.; Pipattanasompom, M.; Rahman, S. A comprehensive review of smart grid related standards and protocols. In Proceedings of the 2017 5th International Istanbul Smart Grid and Cities Congress and Fair (ICSG), Istanbul, Turkey, 19–21 April 2017; pp. 12–16. doi: 10.1109/SGCF.2017.7947600. [CrossRef]
98. Liu, Y.; Yang, C.; Jiang, L.; Xie, S.; Zhang, Y. Intelligent edge computing for IoT-based energy management in smart cities. *IEEE Netw.* **2019**, *33*, 111–117. [CrossRef]
99. Fang, X.; Misra, S.; Xue, G.; Yang, D. Smart grid: The new and improved power grid: A survey. *IEEE Commun. Surv. Tutor.* **2011**, *14*, 944–980. [CrossRef]
100. Electricity, Gas and Water Supply Industry. 2016. Available online: https://http://www.statssa.gov.za/publications/Report-41-01-02/Report-41-01-022016.pdf (accessed on 05 February 2022).
101. Ibrahim, I.D.; Hamam, Y.; Alayli, Y.; Jamiru, T.; Sadiku, E.R.; Kupolati, W.K.; Ndambuki, J.M.; Eze, A.A. A review on Africa energy supply through renewable energy production: Nigeria, Cameroon, Ghana and South Africa as a case study. *Energy Strategy Rev.* **2021**, *38*, 100740. [CrossRef]
102. Kulkarni, S.; Gu, Q.; Myers, E.; Polepeddi, L.; Lipták, S.; Beyah, R.; Divan, D. Enabling a decentralized smart grid using autonomous edge control devices. *IEEE Internet Things J.* **2019**, *6*, 7406–7419. [CrossRef]
103. Hussain, S.S.; Tak, A.; Ustun, T.S.; Ali, I. Communication modeling of solar home system and smart meter in smart grids. *IEEE Access* **2018**, *6*, 16985–16996. [CrossRef]
104. Siddiqui, I.F.; Lee, S.U.J.; Abbas, A.; Bashir, A.K. Optimizing lifespan and energy consumption by smart meters in green-cloud-based smart grids. *IEEE Access* **2017**, *5*, 20934–20945. [CrossRef]
105. Albayati, A.; Abdullah, N.F.; Abu-Samah, A.; Mutlag, A.H.; Nordin, R. A serverless advanced metering infrastructure based on fog-edge computing for a smart grid: A comparison study for energy sector in Iraq. *Energies* **2020**, *13*, 5460. [CrossRef]
106. Yoldaş, Y.; Önen, A.; Muyeen, S.; Vasilakos, A.V.; Alan, I. Enhancing smart grid with microgrids: Challenges and opportunities. *Renew. Sustain. Energy Rev.* **2017**, *72*, 205–214. [CrossRef]
107. Liu, C.H.; Gu, J.C. Modeling and integrating PV stations into IEC 61850 XMPP intelligent edge computing gateway. *Energies* **2019**, *12*, 1442. [CrossRef]
108. Farhangi, H. The path of the smart grid. *IEEE Power Energy Mag.* **2009**, *8*, 18–28. [CrossRef]
109. Senarathna, T.; Hemapala, K.U. Review of adaptive protection methods for microgrids. *AIMS Energy* **2019**, *7*, 557–578. [CrossRef]
110. Usama, M.; Mokhlis, H.; Moghavvemi, M.; Mansor, N.N.; Alotaibi, M.A.; Muhammad, M.A.; Bajwa, A.A. A comprehensive review on protection strategies to mitigate the impact of renewable energy sources on interconnected distribution networks. *IEEE Access* **2021**, *9*, 35740–35765. [CrossRef]

111. Mahat, P.; Chen, Z.; Bak-Jensen, B. Review on islanding operation of distribution system with distributed generation. In Proceedings of the 2011 IEEE Power and Energy Society General Meeting, Detroit, MI, USA, 24–28 July 2011; pp. 1–8.
112. Khamis, A.; Shareef, H.; Bizkevelci, E.; Khatib, T. A review of islanding detection techniques for renewable distributed generation systems. *Renew. Sustain. Energy Rev.* **2013**, *28*, 483–493. [CrossRef]
113. Norshahrani, M.; Mokhlis, H.; Abu Bakar, A.H.; Jamian, J.J.; Sukumar, S. Progress on protection strategies to mitigate the impact of renewable distributed generation on distribution systems. *Energies* **2017**, *10*, 1864. [CrossRef]
114. AsghariGovar, S.; Pourghasem, P.; Seyedi, H. High impedance fault protection scheme for smart grids based on WPT and ELM considering evolving and cross-country faults. *Int. J. Electr. Power Energy Syst.* **2019**, *107*, 412–421. [CrossRef]
115. Menezes, T.S.; Fernandes, R.A.; Coury, D.V. Intelligent islanding detection with grid topology adaptation and minimum non-detection zone. *Electr. Power Syst. Res.* **2020**, *187*, 106470. [CrossRef]
116. Bakkar, M.; Bogarra, S.; Córcoles, F.; Aboelhassan, A.; Wang, S.; Iglesias, J. Artificial Intelligence-Based Protection for Smart Grids. *Energies* **2022**, *15*, 4933. [CrossRef]
117. Khamis, A.; Xu, Y.; Dong, Z.Y.; Zhang, R. Faster detection of microgrid islanding events using an adaptive ensemble classifier. *IEEE Trans. Smart Grid* **2016**, *9*, 1889–1899. [CrossRef]
118. Mwasilu, F.; Justo, J.J.; Kim, E.K.; Do, T.D.; Jung, J.W. Electric vehicles and smart grid interaction: A review on vehicle to grid and renewable energy sources integration. *Renew. Sustain. Energy Rev.* **2014**, *34*, 501–516. [CrossRef]
119. Jiang, A.; Yuan, H.; Li, D.; Tian, J. Key technologies of ubiquitous power Internet of Things-aided smart grid. *J. Renew. Sustain. Energy* **2019**, *11*, 062702. [CrossRef]
120. Reka, S.S.; Dragicevic, T. Future effectual role of energy delivery: A comprehensive review of Internet of Things and smart grid. *Renew. Sustain. Energy Rev.* **2018**, *91*, 90–108. [CrossRef]
121. 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]
122. 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]
123. Pan, J.; Jain, R.; Paul, S.; Vu, T.; Saifullah, A.; Sha, M. An internet of things framework for smart energy in buildings: designs, prototype, and experiments. *IEEE Internet Things J.* **2015**, *2*, 527–537. [CrossRef]
124. Akhtaruzzaman, M.; Hasan, M.K.; Kabir, S.R.; Abdullah, S.N.H.S.; Sadeq, M.J.; Hossain, E. HSIC bottleneck based distributed deep learning model for load forecasting in smart grid with a comprehensive survey. *IEEE Access* **2020**, *8*, 222977–223008. [CrossRef]
125. Chadoulos, S.; Koutsopoulos, I.; Polyzos, G.C. Mobile apps meet the smart energy grid: A survey on consumer engagement and machine learning applications. *IEEE Access* **2020**, *8*, 219632–219655. [CrossRef]
126. Su, Z.; Wang, Y.; Luan, T.H.; Zhang, N.; Li, F.; Chen, T.; Cao, H. Secure and Efficient Federated Learning for Smart Grid With Edge-Cloud Collaboration. *IEEE Trans. Ind. Inform.* **2021**, *18*, 1333–1344. [CrossRef]
127. Gai, K.; Wu, Y.; Zhu, L.; Xu, L.; Zhang, Y. Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks. *IEEE Internet Things J.* **2019**, *6*, 7992–8004. [CrossRef]
128. Huang, Y.; Lu, Y.; Wang, F.; Fan, X.; Liu, J.; Leung, V.C. An edge computing framework for real-time monitoring in smart grid. In Proceedings of the 2018 IEEE International Conference on Industrial Internet (ICII), Seattle, WA, USA, 21–23 October 2018; pp. 99–108.
129. Lu, W.; Ren, Z.; Xu, J.; Chen, S. Edge blockchain assisted lightweight privacy-preserving data aggregation for smart grid. *IEEE Trans. Netw. Serv. Manag.* **2021**, *18*, 1246–1259. [CrossRef]
130. Zhou, H.; Zhang, Z.; Li, D.; Su, Z. Joint Optimization of Computing Offloading and Service Caching in Edge Computing-based Smart Grid. *IEEE Trans. Cloud Comput.* **2022**, *2022*, 1–11 . [CrossRef]
131. Aranda, J.A.S.; dos Santos Costa, R.; de Vargas, V.W.; da Silva Pereira, P.R.; Barbosa, J.L.V.; Vianna, M.P. Context-aware Edge Computing and Internet of Things in Smart Grids: A systematic mapping study. *Comput. Electr. Eng.* **2022**, *99*, 107826. [CrossRef]
132. Wang, Z.; Jiang, D.; Wang, F.; Lv, Z.; Nowak, R. A polymorphic heterogeneous security architecture for edge-enabled smart grids. *Sustain. Cities Soc.* **2021**, *67*, 102661. [CrossRef]
133. Fan, J.; du Toit, W.; Backscheider, P. Distribution substation automation in smart grid. *Prot. Control. J.* **2009**, *9*, 65–68 .
134. Gungor, V.C.; Sahin, D.; Kocak, T.; Ergut, S.; Buccella, C.; Cecati, C.; Hancke, G.P. A survey on smart grid potential applications and communication requirements. *IEEE Trans. Ind. Inform.* **2012**, *9*, 28–42. [CrossRef]
135. Peng, N.; Liu, X.; Liang, R.; Tang, Z.; Ren, X.; Hu, Y.; Li, G. Edge Computing Based Fault Sensing of the Distribution Cables Based on Time-domain Analysis of Grounding Line Current Signals. *IEEE Trans. Power Deliv.* **2022**, *2022*, 1–13 . [CrossRef]
136. Du, Y.; Zhang, Z.; Li, Y.; Li, H.; He, G.; Zhang, Z.; Zhao, Y. A new type of substation real-time detection system based on edge computing and RAFT consensus algorithm. In Proceedings of the 2021 6th Asia Conference on Power and Electrical Engineering (ACPEE), Chongqing, China, 8–11 April 2021; pp. 451–455.
137. Huo, W.; Liu, F.; Wang, L.; Jin, Y.; Wang, L. Research on distributed power distribution fault detection based on edge computing. *IEEE Access* **2019**, *8*, 24643–24652. [CrossRef]
138. Cen, B.; Hu, C.; Cai, Z.; Wu, Z.; Zhang, Y.; Liu, J.; Su, Z. A configuration method of computing resources for microservice-based edge computing apparatus in smart distribution transformer area. *Int. J. Electr. Powe Energy Syst.* **2022**, *138*, 107935. [CrossRef]

139. Zhang, S.; Liu, Y.; Cai, Y.; Dong, S.; Xu, C.; Fang, R. A Multilevel Edge Computing Architecture and Edge Generation Method of Distribution Networks. In Proceedings of the 2020 IEEE Power & Energy Society General Meeting (PESGM), Virtual Event, 3–6 August 2020; pp. 1–5.
140. Shakeri, M.; Shayestegan, M.; Abunima, H.; Reza, S.S.; Akhtaruzzaman, M.; Alamoud, A.; Sopian, K.; Amin, N. An intelligent system architecture in home energy management systems (HEMS) for efficient demand response in smart grid. *Energy Build.* **2017**, *138*, 154–164. [CrossRef]
141. Bouhafs, F.; Mackay, M.; Merabti, M. Links to the future: Communication requirements and challenges in the smart grid. *IEEE Power Energy Mag.* **2011**, *10*, 24–32. [CrossRef]
142. Saez-de Ibarra, A.; Martinez-Laserna, E.; Koch-Ciobotaru, C.; Rodriguez, P.; Stroe, D.I.; Swierczynski, M. Second life battery energy storage system for residential demand response service. In Proceedings of the 2015 IEEE International Conference on Industrial Technology (ICIT), Seville, Spain, 17–19 March 2015; pp. 2941–2948.
143. Elkind, E. *Reuse and Repower: How to Save Money and Clean the Grid with Second-Life Electric Vehicle Batteries*; UC Berkeley, Berkeley Law; University of California: Berkeley, CA, USA, 2014; pp. 1–31 .
144. Casals, L.C.; Barbero, M.; Corchero, C. Reused second life batteries for aggregated demand response services. *J. Clean. Prod.* **2019**, *212*, 99–108. [CrossRef]
145. Alcaraz, C.; Lopez, J. WASAM: A dynamic wide-area situational awareness model for critical domains in Smart Grids. *Future Gener. Comput. Syst.* **2014**, *30*, 146–154. [CrossRef]
146. Law, Y.W.; Palaniswami, M.; Kounga, G.; Lo, A. WAKE: Key management scheme for wide-area measurement systems in smart grid. *IEEE Commun. Mag.* **2013**, *51*, 34–41. [CrossRef]
147. Basu, C.; Agrawal, A.; Hazra, J.; Kumar, A.; Seetharam, D.P.; Béland, J.; Guillon, S.; Kamwa, I.; Lafond, C. Understanding events for wide-area situational awareness. In Proceedings of the ISGT 2014, Washington, DC, USA 19–22 February 2014; pp. 1–5.
148. Bahrami, S.; Sheikhi, A. From demand response in smart grid toward integrated demand response in smart energy hub. *IEEE Trans. Smart Grid* **2015**, *7*, 650–658. [CrossRef]
149. Rastegar, M.; Fotuhi-Firuzabad, M. Outage management in residential demand response programs. *IEEE Trans. Smart Grid* **2014**, *6*, 1453–1462. [CrossRef]
150. He, Y.; Jenkins, N.; Wu, J. Smart metering for outage management of electric power distribution networks. *Energy Procedia* **2016**, *103*, 159–164. [CrossRef]
151. Jiang, Y.; Liu, C.C.; Diedesch, M.; Lee, E.; Srivastava, A.K. Outage management of distribution systems incorporating information from smart meters. *IEEE Trans. Power Syst.* **2015**, *31*, 4144–4154. [CrossRef]
152. Raju, L.; Morais, A.A.; Rathnakumar, R.; Ponnivalavan, S.; Thavam, L. Micro-grid grid outage management using multi-agent systems. In Proceedings of the 2017 Second International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM), Tindivanam, India, 3–4 February 2017; pp. 363–368.
153. Kong, P.Y.; Karagiannidis, G.K. Charging schemes for plug-in hybrid electric vehicles in smart grid: A survey. *IEEE Access* **2016**, *4*, 6846–6875. [CrossRef]
154. Debnath, U.K.; Ahmad, I.; Habibi, D. Gridable vehicles and second life batteries for generation side asset management in the Smart Grid. *Int. J. Electr. Power Energy Syst.* **2016**, *82*, 114–123. [CrossRef]
155. Gomez-Quiles, C.; Asencio-Cortes, G.; Gastalver-Rubio, A.; Martinez-Alvarez, F.; Troncoso, A.; Manresa, J.; Riquelme, J.C.; Riquelme-Santos, J.M. A novel ensemble method for electric vehicle power consumption forecasting: Application to the Spanish system. *IEEE Access* **2019**, *7*, 120840–120856. [CrossRef]
156. Lopes, J.A.P.; Soares, F.J.; Almeida, P.M.R. Integration of electric vehicles in the electric power system. *Proc. IEEE* **2010**, *99*, 168–183. [CrossRef]
157. Martínez-Lao, J.; Montoya, F.G.; Montoya, M.G.; Manzano-Agugliaro, F. Electric vehicles in Spain: An overview of charging systems. *Renew. Sustain. Energy Rev.* **2017**, *77*, 970–983. [CrossRef]
158. Chen, Y.; Oudalov, A.; Wang, J. Integration of electric vehicle charging system into distribution network. In Proceedings of the 8th International Conference on Power Electronics-ECCE Asia, Jeju, Korea, 30 May–3 June 2011; pp. 593–598.
159. Eltoumi, F.M.; Becherif, M.; Djerdir, A.; Ramadan, H.S. The key issues of electric vehicle charging via hybrid power sources: Techno-economic viability, analysis, and recommendations. *Renew. Sustain. Energy Rev.* **2021**, *138*, 110534. [CrossRef]
160. Ashfaq, M.; Butt, O.; Selvaraj, J.; Rahim, N. Assessment of electric vehicle charging infrastructure and its impact on the electric grid: A review. *Int. J. Green Energy* **2021**, *18*, 657–686. [CrossRef]
161. Lee, Z.J.; Chang, D.; Jin, C.; Lee, G.S.; Lee, R.; Lee, T.; Low, S.H. Large-scale adaptive electric vehicle charging. In Proceedings of the 2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Aalborg, Denmark, 29–31 October 2018; pp. 1–7.
162. Hutchinson, S.; Baran, M.; Lukic, S. Power supply for an electric vehicle charging system for a large parking deck. In Proceedings of the 2009 IEEE Industry Applications Society Annual Meeting, Houston, TX, USA, 4–8 October 2009; pp. 1–4.
163. Jung, C.M.; Ray, P.; Salkuti, S.R. Asset management and maintenance: A smart grid perspective. *Int. J. Electr. Comput. Eng. (2088-8708)* **2019**, *9*, *3391–3398* . [CrossRef]
164. Ahmed, S.; Lee, Y.D.; Hyun, S.H.; Koo, I. A cognitive radio-based energy-efficient system for power transmission line monitoring in smart grids. *J. Sens.* **2017**, *2017*, 3862375. [CrossRef]
165. Hanai, M.; Kojima, H.; Hayakawa, N.; Shinoda, K.; Okubo, H. Integration of asset management and smart grid with intelligent grid management system. *IEEE Trans. Dielectr. Electr. Insul.* **2013**, *20*, 2195–2202. [CrossRef]

166. Teoh, Y.K.; Gill, S.S.; Parlikad, A.K. IoT and fog computing based predictive maintenance model for effective asset management in industry 4.0 using machine learning. *IEEE Internet Things J.* **2021**, *2021*, 1–8 . [CrossRef]
167. Ma, H.; Saha, T.K.; Ekanayake, C.; Martin, D. Smart transformer for smart grid—intelligent framework and techniques for power transformer asset management. *IEEE Trans. Smart Grid* **2015**, *6*, 1026–1034. [CrossRef]
168. Cheng, M.; Zeng, Y.; Niu, R.; Chen, Y. Study on the model of advanced asset management in smart grid. In Proceedings of the 2011 4th International Conference on Electric Utility Deregulation and Restructuring and Power Technologies (DRPT), Weihai, China, 6–9 July 2011; pp. 781–785.
169. Trajano, A.F.; de Sousa, A.A.M.; Rodrigues, E.B.; de Souza, J.N.; de Castro Callado, A.; Coutinho, E.F. Leveraging mobile edge computing on smart grids using LTE cellular networks. In Proceedings of the 2019 IEEE Symposium on Computers and Communications (ISCC), Barcelona, Spain, 29 June–3 July 2019; pp. 1–7.
170. Zhang, X.; Wang, Y.; Lu, S.; Liu, L.; Shi, W.; et al. OpenEI: An open framework for edge intelligence. In Proceedings of the 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), Dallas, TX, USA, 7–10 July 2019; pp. 1840–1851.
171. Moghaddam, M.; Cadavid, M.N.; Kenley, C.R.; Deshmukh, A.V. Reference architectures for smart manufacturing: A critical review. *J. Manuf. Syst.* **2018**, *49*, 215–225. [CrossRef]
172. Peng, N.; Liang, R.; Wang, G.; Sun, P.; Chen, C.; Hou, T. Edge Computing-Based Fault Location in Distribution Networks by Using Asynchronous Transient Amplitudes at Limited Nodes. *IEEE Trans. Smart Grid* **2020**, *12*, 574–588. [CrossRef]
173. Sufyan, F.; Banerjee, A. Computation offloading for distributed mobile edge computing network: A multiobjective approach. *IEEE Access* **2020**, *8*, 149915–149930. [CrossRef]
174. Xi, L.; Wang, Y.; Wang, Y.; Wang, Z.; Wang, X.; Chen, Y. Deep Reinforcement Learning-Based Service-Oriented Resource Allocation in Smart Grids. *IEEE Access* **2021**, *9*, 77637–77648. [CrossRef]
175. Hou, W.; Jiang, Y.; Lei, W.; Xu, A.; Wen, H.; Chen, S. A P2P network based edge computing smart grid model for efficient resources coordination. *Peer-Peer Netw. Appl.* **2020**, *13*, 1026–1037. [CrossRef]
176. Patil, P.; Hakiri, A.; Gokhale, A. Cyber foraging and offloading framework for internet of things. In Proceedings of the 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), Atlanta, GA, USA, 10–14 June 2016; Volume 1, pp. 359–368.
177. Li, B.; Pei, Y.; Wu, H.; Shen, B. Heuristics to allocate high-performance cloudlets for computation offloading in mobile ad hoc clouds. *J. Supercomput.* **2015**, *71*, 3009–3036. [CrossRef]
178. Wolski, R.; Gurun, S.; Krintz, C.; Nurmi, D. Using bandwidth data to make computation offloading decisions. In Proceedings of the 2008 IEEE International Symposium on Parallel and Distributed Processing, Miami, FL, USA , 14–18 April 2008; pp. 1–8.
179. Akherfi, K.; Gerndt, M.; Harroud, H. Mobile cloud computing for computation offloading: Issues and challenges. *Appl. Comput. Inform.* **2018**, *14*, 1–16. [CrossRef]
180. Dinh, T.Q.; La, Q.D.; Quek, T.Q.; Shin, H. Learning for computation offloading in mobile edge computing. *IEEE Trans. Commun.* **2018**, *66*, 6353–6367. [CrossRef]
181. Jiang, C.; Cheng, X.; Gao, H.; Zhou, X.; Wan, J. Toward computation offloading in edge computing: A survey. *IEEE Access* **2019**, *7*, 131543–131558. [CrossRef]
182. Lin, L.; Liao, X.; Jin, H.; Li, P. Computation offloading toward edge computing. *Proc. IEEE* **2019**, *107*, 1584–1607. [CrossRef]
183. Noble, B.D.; Satyanarayanan, M.; Narayanan, D.; Tilton, J.E.; Flinn, J.; Walker, K.R. Agile application-aware adaptation for mobility. *ACM SIGOPS Oper. Syst. Rev.* **1997**, *31*, 276–287. [CrossRef]
184. Guo, H.; Liu, J.; Zhang, J.; Sun, W.; Kato, N. Mobile-edge computation offloading for ultradense IoT networks. *IEEE Internet Things J.* **2018**, *5*, 4977–4988. [CrossRef]
185. Yu, S.; Langar, R.; Fu, X.; Wang, L.; Han, Z. Computation offloading with data caching enhancement for mobile edge computing. *IEEE Trans. Veh. Technol.* **2018**, *67*, 11098–11112. [CrossRef]
186. Dong, L.; Satpute, M.N.; Shan, J.; Liu, B.; Yu, Y.; Yan, T. Computation offloading for mobile-edge computing with multi-user. In Proceedings of the 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), Dallas, TX, USA, 7–10 July 2019; pp. 841–850.
187. Khayyat, M.; Elgendy, I.A.; Muthanna, A.; Alshahrani, A.S.; Alharbi, S.; Koucheryavy, A. Advanced deep learning-based computational offloading for multilevel vehicular edge-cloud computing networks. *IEEE Access* **2020**, *8*, 137052–137062. [CrossRef]
188. Li, Y.; Wang, X.; Gan, X.; Jin, H.; Fu, L.; Wang, X. Learning-aided computation offloading for trusted collaborative mobile edge computing. *IEEE Trans. Mob. Comput.* **2019**, *19*, 2833–2849. [CrossRef]
189. Verbelen, T.; Stevens, T.; De Turck, F.; Dhoedt, B. Graph partitioning algorithms for optimizing software deployment in mobile cloud computing. *Future Gener. Comput. Syst.* **2013**, *29*, 451–459. [CrossRef]
190. Zhao, T.; Zhou, S.; Guo, X.; Niu, Z. Tasks scheduling and resource allocation in heterogeneous cloud for delay-bounded mobile edge computing. In Proceedings of the 2017 IEEE International Conference on Communications (ICC), Paris, France, 21–25 May 2017; pp. 1–7.
191. Sardellitti, S.; Scutari, G.; Barbarossa, S. Joint optimization of radio and computational resources for multicell mobile-edge computing. *IEEE Trans. Signal Inf. Process. Netw.* **2015**, *1*, 89–103. [CrossRef]
192. Chen, X.; Shi, Q.; Yang, L.; Xu, J. ThriftyEdge: Resource-efficient edge computing for intelligent IoT applications. *IEEE Netw.* **2018**, *32*, 61–65. [CrossRef]

193. Abebe, E.; Ryan, C. Adaptive application offloading using distributed abstract class graphs in mobile environments. *J. Syst. Softw.* **2012**, *85*, 2755–2769. [CrossRef]
194. Kosta, S.; Aucinas, A.; Hui, P.; Mortier, R.; Zhang, X. Thinkair: Dynamic resource allocation and parallel execution in the cloud for mobile code offloading. In Proceedings of the 2012 Proceedings IEEE Infocom, Orlando, FL, USA, 25–30 March 2012; pp. 945–953.
195. Chen, X. Decentralized computation offloading game for mobile cloud computing. *IEEE Trans. Parallel Distrib. Syst.* **2014**, *26*, 974–983. [CrossRef]
196. Chen, L.; Zhou, S.; Xu, J. Computation peer offloading for energy-constrained mobile edge computing in small-cell networks. *IEEE/ACM Trans. Netw.* **2018**, *26*, 1619–1632. [CrossRef]
197. Li, S.; Tao, Y.; Qin, X.; Liu, L.; Zhang, Z.; Zhang, P. Energy-aware mobile edge computation offloading for IoT over heterogenous networks. *IEEE Access* **2019**, *7*, 13092–13105. [CrossRef]
198. Elgendy, I.A.; Zhang, W.Z.; Zeng, Y.; He, H.; Tian, Y.C.; Yang, Y. Efficient and secure multi-user multi-task computation offloading for mobile-edge computing in mobile IoT networks. *IEEE Trans. Netw. Serv. Manag.* **2020**, *17*, 2410–2422. [CrossRef]
199. Huang, P.Q.; Wang, Y.; Wang, K.; Liu, Z.Z. A bilevel optimization approach for joint offloading decision and resource allocation in cooperative mobile edge computing. *IEEE Trans. Cybern.* **2019**, *50*, 4228–4241. [CrossRef]
200. Chen, X.; Jiao, L.; Li, W.; Fu, X. Efficient multi-user computation offloading for mobile-edge cloud computing. *IEEE/ACM Trans. Netw.* **2015**, *24*, 2795–2808. [CrossRef]
201. Humayed, A.; Lin, J.; Li, F.; Luo, B. Cyber-physical systems security: A survey. *IEEE Internet Things J.* **2017**, *4*, 1802–1831. [CrossRef]
202. Singh, J.; Bello, Y.; Hussein, A.R.; Erbad, A.; Mohamed, A. Hierarchical security paradigm for iot multiaccess edge computing. *IEEE Internet Things J.* **2020**, *8*, 5794–5805. [CrossRef]
203. Gligor, V.D. A note on denial-of-service in operating systems. *IEEE Trans. Softw. Eng.* **1984**, *SE-10*, 320–324. [CrossRef]
204. Yuan, X.; Li, C.; Li, X. DeepDefense: Identifying DDoS attack via deep learning. In Proceedings of the 2017 IEEE International Conference on Smart Computing (SMARTCOMP), Hong Kong, China, 29–31 May 2017; pp. 1–8.
205. Nooribakhsh, M.; Mollamotalebi, M. A review on statistical approaches for anomaly detection in DDoS attacks. *Inf. Secur. J. Glob. Perspect.* **2020**, *29*, 118–133. [CrossRef]
206. Bhat, S.A.; Sofi, I.B.; Chi, C.Y. edge computing and its convergence with blockchain in 5G and beyond: security, challenges, and opportunities. *IEEE Access* **2020**, *8*, 205340–205373. [CrossRef]
207. Li, X.; Chen, T.; Cheng, Q.; Ma, S.; Ma, J. Smart applications in edge computing: Overview on authentication and data security. *IEEE Internet Things J.* **2020**, *8*, 4063–4080. [CrossRef]
208. Li, H.; Wu, J.; Xu, H.; Li, G.; Guizani, M. Explainable Intelligence-Driven Defense Mechanism against Advanced Persistent Threats: A Joint Edge Game and AI Approach. *IEEE Trans. Dependable Secur. Comput.* **2021**, *19*, 757–775. [CrossRef]
209. Nayak, G.N.; Samaddar, S.G. Different flavours of man-in-the-middle attack, consequences and feasible solutions. In Proceedings of the 2010 3rd International Conference on Computer Science and Information Technology, Chengdu, China, 9–11 July 2010; Volume 5, pp. 491–495.
210. Rahim, R. Man-in-the-middle-attack prevention using interlock protocol method. *ARPN J. Eng. Appl. Sci* **2017**, *12*, 6483–6487.
211. Mohapatra, H.; Rath, S.; Panda, S.; Kumar, R. Handling of man-in-the-middle attack in wsn through intrusion detection system. *Int. J.* **2020**, *8*, 1503–1510. [CrossRef]
212. Ranaweera, P.; Jurcut, A.D.; Liyanage, M. Survey on multi-access edge computing security and privacy. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 1078–1124. [CrossRef]
213. Chen, D.; Wawrzynski, P.; Lv, Z. Cyber security in smart cities: A review of deep learning-based applications and case studies. *Sustain. Cities Soc.* **2021**, *66*, 102655. [CrossRef]
214. Xiao, Y.; Jia, Y.; Liu, C.; Cheng, X.; Yu, J.; Lv, W. Edge computing security: State of the art and challenges. *Proc. IEEE* **2019**, *107*, 1608–1631. [CrossRef]
215. Chaudhry, S.A.; Alhakami, H.; Baz, A.; Al-Turjman, F. Securing demand response management: A certificate-based access control in smart grid edge computing infrastructure. *IEEE Access* **2020**, *8*, 101235–101243. [CrossRef]
216. Nyamtiga, B.W.; Sicato, J.C.S.; Rathore, S.; Sung, Y.; Park, J.H. Blockchain-based secure storage management with edge computing for IoT. *Electronics* **2019**, *8*, 828. [CrossRef]
217. Shaukat, K.; Luo, S.; Varadharajan, V.; Hameed, I.A.; Chen, S.; Liu, D.; Li, J. Performance comparison and current challenges of using machine learning techniques in cybersecurity. *Energies* **2020**, *13*, 2509. [CrossRef]
218. Javed, A.R.; Usman, M.; Rehman, S.U.; Khan, M.U.; Haghighi, M.S. Anomaly detection in automated vehicles using multistage attention-based convolutional neural network. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 4291–4300. [CrossRef]
219. Marir, N.; Wang, H.; Feng, G.; Li, B.; Jia, M. Distributed abnormal behavior detection approach based on deep belief network and ensemble SVM using spark. *IEEE Access* **2018**, *6*, 59657–59671. [CrossRef]
220. Xin, Y.; Kong, L.; Liu, Z.; Chen, Y.; Li, Y.; Zhu, H.; Gao, M.; Hou, H.; Wang, C. Machine learning and deep learning methods for cybersecurity. *IEEE Access* **2018**, *6*, 35365–35381. [CrossRef]
221. Sheatsley, R.; Durbin, M.; Lintereur, A.; Mcdaniel, P. Improving Radioactive Material Localization by Leveraging Cyber-Security Model Optimizations. *IEEE Sens. J.* **2021**, *21*, 9994–10006. [CrossRef]
222. Larriva-Novo, X.; Vega-Barbas, M.; Villagrá, V.A.; Rivera, D.; Álvarez-Campana, M.; Berrocal, J. Efficient distributed preprocessing model for machine learning-based anomaly detection over large-scale cybersecurity datasets. *Appl. Sci.* **2020**, *10*, 3430. [CrossRef]

223. Podder, P.; Bharati, S.; Mondal, M.; Paul, P.K.; Kose, U. Artificial neural network for cybersecurity: A comprehensive review. *arXiv* **2021**, arXiv:2107.01185.
224. Mathai, K.J.; et al. Performance comparison of intrusion detection system between deep belief network (DBN) algorithm and state preserving extreme learning machine (SPELM) algorithm. In Proceedings of the 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), Coimbatore, India, 20–22 February 2019; pp. 1–7.
225. Huda, S.; Yearwood, J.; Hassan, M.M.; Almogren, A. Securing the operations in SCADA-IoT platform based industrial control system using ensemble of deep belief networks. *Appl. Soft Comput.* **2018**, *71*, 66–77. [CrossRef]
226. Nguyen, G.N.; Le Viet, N.H.; Elhoseny, M.; Shankar, K.; Gupta, B.; Abd El-Latif, A.A. Secure blockchain enabled Cyber–physical systems in healthcare using deep belief network with ResNet model. *J. Parallel Distrib. Comput.* **2021**, *153*, 150–160. [CrossRef]
227. Habibi, M.R.; Baghaee, H.R.; Dragičević, T.; Blaabjerg, F. Detection of false data injection cyber-attacks in DC microgrids based on recurrent neural networks. *IEEE J. Emerg. Sel. Top. Power Electron.* **2020**, *9*, 5294–5310. [CrossRef]
228. Lin, T.N.; Giles, C.L.; Horne, B.G.; Kung, S.Y. A delay damage model selection algorithm for NARX neural networks. *IEEE Trans. Signal Process.* **1997**, *45*, 2719–2730.
229. Ullah, I.; Mahmoud, Q.H. Design and development of a deep learning-based model for anomaly detection in IoT networks. *IEEE Access* **2021**, *9*, 103906–103926. [CrossRef]
230. Kravchik, M.; Shabtai, A. Detecting cyber attacks in industrial control systems using convolutional neural networks. In Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy, Toronto, ON, Canada, 15–19 October 2018; pp. 72–83.
231. Susilo, B.; Sari, R.F. Intrusion detection in IoT networks using deep learning algorithm. *Information* **2020**, *11*, 279. [CrossRef]
232. McLaughlin, N.; Martinez del Rincon, J.; Kang, B.; Yerima, S.; Miller, P.; Sezer, S.; Safaei, Y.; Trickel, E.; Zhao, Z.; Doupé, A.; et al. Deep android malware detection. In Proceedings of the Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy, Scottsdale, AZ, USA, 22–24 March 2017; pp. 301–308.
233. Li, Y.; Xu, Y.; Liu, Z.; Hou, H.; Zheng, Y.; Xin, Y.; Zhao, Y.; Cui, L. Robust detection for network intrusion of industrial IoT based on multi-CNN fusion. *Measurement* **2020**, *154*, 107450. [CrossRef]
234. Gimenez-Aguilar, M.; de Fuentes, J.M.; Gonzalez-Manzano, L.; Arroyo, D. Achieving cybersecurity in blockchain-based systems: A survey. *Future Gener. Comput. Syst.* **2021**, *124*, 91–118. [CrossRef]
235. Razaque, A.; Al Ajlan, A.; Melaoune, N.; Alotaibi, M.; Alotaibi, B.; Dias, I.; Oad, A.; Hariri, S.; Zhao, C. Avoidance of cybersecurity threats with the deployment of a web-based blockchain-enabled cybersecurity awareness system. *Appl. Sci.* **2021**, *11*, 7880. [CrossRef]
236. Zhang, L.; Zou, Y.; Wang, W.; Jin, Z.; Su, Y.; Chen, H. Resource allocation and trust computing for blockchain-enabled edge computing system. *Comput. Secur.* **2021**, *105*, 102249. [CrossRef]
237. Wang, J.; Wu, L.; Choo, K.K.R.; He, D. Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure. *IEEE Trans. Ind. Inform.* **2019**, *16*, 1984–1992. [CrossRef]
238. Zhao, Y.; Wang, W.; Li, Y.; Meixner, C.C.; Tornatore, M.; Zhang, J. Edge computing and networking: A survey on infrastructures and applications. *IEEE Access* **2019**, *7*, 101213–101230. [CrossRef]
239. Xue, M.; Yuan, C.; Wu, H.; Zhang, Y.; Liu, W. Machine learning security: Threats, countermeasures, and evaluations. *IEEE Access* **2020**, *8*, 74720–74742. [CrossRef]