electronics

MDPI

Article

A Study on an IoT-Based SCADA System for Photovoltaic Utility Plants

Sergio Ferlito [1], Salvatore Ippolito [2], Celestino Santagata [1], Paolo Schiattarella [2] and Girolamo Di Francia [1,*]

[1] ENEA, Italian National Agency for New Technologies, Energy and Sustainable Economic Development, P.le E. Fermi 1, Portici, 80055 Napoli, Italy; sergio.ferlito@enea.it (S.F.); celestino.santagata@teatek.it (C.S.)
[2] TeaTek, Consorzio Area, Via Maddaloni, snc, 80011 Acerra, Italy; salvatore.ippolito@teatek.it (S.I.); paolo.schiattarella@teatek.it (P.S.)
* Correspondence: girolamo.difrancia@enea.it

Abstract: Large-scale photovoltaic (PV) electricity production plants rely on reliable operation and maintenance (O&M) systems, often operated by means of supervisory control and data acquisition (SCADA) platforms aimed at limiting, as much as possible, the intrinsic volatility of this energy resource. The current trend is to develop SCADAs that achieve the finest possible control of the system components to efficiently and effectively cope with possible energy delivery problems. In this study, we investigated an innovative design of an IoT-based SCADA specifically tailored for large PV systems in which data transmission overheads are reduced by adopting lightweight protocols, and reliable data storage is achieved by means of hybrid solutions that allow the storage of historical data, enabling accurate performance analysis and predictive maintenance protocols. The proposed solution relies on an architecture where independent functional microservices handle specific tasks, ensuring scalability and fault tolerance. The technical approaches for IoT-SCADA connectivity are herein described in detail, comparing different possible technical choices. The proposed IoT-based SCADA is based on edge computing for latency reduction and to enhance real-time decision making, enabling scalability, and centralized management while leveraging cloud services. The resulting hybrid solutions that combine edge and cloud resources offer a balance between responsiveness and scalability. Finally, in the study, a blockchain solution was taken into account to certify energy data, ensuring traceability, security, and reliability in commercial transactions.

Keywords: SCADA; IoT; photovoltaic utility plant; blockchain; micro services; Kubernetes

Citation: Ferlito, S.; Ippolito, S.; Santagata, C.; Schiattarella, P.; Di Francia, G. A Study on an IoT-Based SCADA System for Photovoltaic Utility Plants. *Electronics* **2024**, *13*, 2065. https://doi.org/10.3390/electronics13112065

Academic Editor: Rui Castro

Received: 19 April 2024
Revised: 16 May 2024
Accepted: 24 May 2024
Published: 26 May 2024

1. Introduction

The control and management of any industrial or service process is generally based on a supervisory control and data acquisition (SCADA) system [1]. Its function is to acquire in real time the process data and transfer them all to a central, remote system where they are recorded and analyzed using, in general, a proper graphic interface so that the process can be in turn more finely tuned by means of specific management instructions. The rapid development of the Internet of Things and of the related data communication and management technologies is deeply changing, in any industrial sector, the SCADA architecture that more and more relies on artificial intelligence tools to extract the process-relevant information that is useful for improving management operations and reducing the human role to minimal supervising activities [2]. As far as the photovoltaic (PV) industry is concerned, it has been only very recently, in fact only in the last half decade, that industrial production has reached a well-defined standardization level. As a result, for large PV utilities, an increasing use of SCADA systems to improve the operation and management (O&M) process efficiency has been observed [3]. As a matter of fact, because of the continuous decrease in the fixed costs of photovoltaic system installation, those related to O&M are becoming increasingly relevant in determining the final cost of the

produced photovoltaic electricity, a trend that is expected to become more marked in the years to come [4,5]. A PV SCADA is therefore mainly conceived to analyze data coming from one or even more PV systems simultaneously, minimizing the O&M costs and at the same time maximizing the overall financial earnings. Monitoring a PV system involves tracking and analyzing the performance of the various system components to ensure it is optimally operating.

In this respect, machine learning (ML) methods are more and more usually employed in every aspect of modelling, optimization, and forecasting tasks related to PV plant operation [6–8]. In this respect, the huge amount of data readily available by means of an IoT-SCADA can be very useful. Up to now, commercially available PV SCADAs mostly rely on data produced by grid connection point, inverters, electric transformers, storage system (if any), strings electric data, local weather stations, and local radiation measuring equipment, and they use external data, mainly weather, for O&M analysis. It is worthwhile to stress that such a SCADA fully complies with the recommendations for the management of large PV systems as per the IEC 61724-1:2021 "Photovoltaic System Performance-Part 1: Monitoring" [9]. Nevertheless, the increasing need to improve the accuracy of PV utility energy forecasts and of the plant fault predictions has rapidly led to the development of the concept of an IoT-SCADA for photovoltaic systems. Voicu et al., in [10], clarified the essential differences between a classic SCADA and an IoT-SCADA for the photovoltaic case. Operatively, the IoT approach offers three key benefits. First, it enables the monitoring of the individual photovoltaic module, which is the basic energy generating unit of the PV plant. This is a very critical issue for a large PV system normally consisting of several tens thousands of interconnected modules since the fault of any of them can affect the performance of several modules; second, it allows for a better integration of on-site and external data (e.g., weather) to minimize energy-forecasting errors that can be a critical issue in terms of energy trading; finally, an IoT-SCADA architecture can be conceived to be more prompt for other data sources to be integrated. An IoT-SCADA designed to implement these three issues optimizes the O&M management through predictive maintenance, therefore maximizing the overall economic gain and the photovoltaic energy delivery reliability.

Although offering many benefits, an IoT-based SCADA has some obvious drawbacks, mainly related to the security aspects of such a solution type. The following taxonomy Table 1, provides a high-level overview of the benefits and challenges associated with integrating IoT with SCADA systems in the context of photovoltaic energy management. The pros are mainly related to the advancements in data processing, communication, and system scalability, while the cons mainly focus on the potential performance cost issues and security concerns related to this type of system. It is important to consider these factors when designing a SCADA solution for photovoltaic applications.

Table 1. Pros and Cons of IoT-based SCADA.

Feature	Pros	Cons
Data Acquisition	Real-time monitoring of performance metric	Additional sensors and data acquisition hardware needed
Remote Management	Ability to diagnose and troubleshoot issues remotely	Vulnerability to cyberattacks if not properly secured
Scalability	Easy integration of additional sensors and modules for pervasive monitoring	Increased complexity as the system scales
Alerting and Notification	Timely alerts for system faults, performance drops, or maintenance needs	Potential overload from excessive alerts

Table 1. *Cont.*

Feature	Pros	Cons
Data Analysis	Improved understanding of system behavior, having multiple sources of data parameters	Requires expertise to interpret and utilize data effectively and to handle the huge amount of data acquired
Security	Enhanced system security through features like encryption, access control, and intrusion detection	Requires ongoing maintenance and updates for security protocols and an high level expertise in the field
Cost Efficiency	Potential cost savings through preventive maintenance and optimized performance	High initial investment cost in terms for hardware, software, system setup, and training

Further details and/or useful suggestions about benefits or drawbacks about this type of SCADA solution can be found in [11–13]. A further issue that should be also considered in implementing an IoT-SCADA is the more complex mathematical framework that needs to be used for providing the analytical tools and methods necessary to extract insights from vast amounts of data made available by the technique in terms of data analysis, machine learning, signal processing, data optimization, and finally, security algorithms such as block-chain, as discussed in [14].

As is known, the IoT paradigm is structured in five different layers [15]: connectivity, information, knowledge, forecast, and autonomy. As discussed above, this work is focused on the connectivity layer. It details how the various parts of a large PV utility can be connected so that data produced from and flowing to the plant can be reliably used to obtain the information required for the status of the plant to be known in terms of both its performance and its external demands. Section 2 reports the relevant literature of the sector; in Section 3, the general structure of the PV IoT-SCADA is shown; Sections 4–6 describe the three basic modules a PV IoT-SCADA according to the approach proposed. Finally, in Section 7, the proposed general architecture is discussed, also highlighting the main drawbacks of an IoT-SCADA, especially regarding security, and finally, conclusions are presented in Section 8.

2. Literature Review

Classic SCADAs for photovoltaic applications were widely discussed in the recent review by Hazrat and coauthors in [16], mainly for plant management and optimization. Hoarca and Valcea examined instead, in [17], the essential parameters that characterize a classic SCADA for PV. The main parameters the work refers to are the system efficiency and its performance ratio, the two basic indicators that allow insight into the PV system's operation and management. Aghenta and Iqbal in their work [18] proposed the use of IoT devices and related methodologies to monitor the operating status of a photovoltaic system. The work refers, however, to small photovoltaic systems, and they show that, even in that limited case, IoT application has the advantage of making the plant management independent of any inverter control systems. The proposed methodology can be also generalized to large systems, and similar studies have been performed by one of the authors on PV systems connected to the grid [19,20]. The use of IoT systems serving simple SCADA systems has been very often proposed, especially for small photovoltaic systems. For example, Tran Thanh Son and coauthors showed a simple IoT-SCADA that relies for its operation on wireless power sensors using a set of small rooftop photovoltaic arrays in Vietnam as test site [21]. In [22], Quays and coauthors presented an IoT-SCADA for a mixed-generation small system composed of photovoltaic, wind, and batteries, where wireless sensors are used for real-time monitoring of current and voltage. Again, Aghenta and Iqbal in [23] examined in detail the basic structural elements of a generic IoT-SCADA in terms of usable IoT protocols, proposing and testing possible photovoltaic system hardware

configurations designed for small PV applications. In all cases, open-source solutions were preferred. It is worth noting that the literature never reports, however, IoT-SCADAs conceived for large utilities, which is one of the original contributions of this paper.

3. The General Structure of a PV IoT-SCADA

From the O&M point of view, a large photovoltaic utility can be considered as an industrial system with a large and even increasing number of elements to control. The system may be using multiple network data transfer protocols, different logics, and different functional domains, and it may rely on a considerable number of sensors: in the order of tens of thousands if each single PV module is to be continuously monitored. This is a quite peculiar structure of a PV-SCADA, leading to highly frequent bursts of data from multiple sources, flowing to and from the PV plant at rates mainly depending on the requirements of specific applications. Therefore, a PV IoT-SCADA has to be characterized by a modular and scalable structure that allows the plant to be fully controlled at the finest granularity level, but it also has to be designed to obtain a continuously refreshed simple digital representation of the plant status to allow a control room operator to easily check any one of the operating field devices. This calls for the adoption of an open, extensible, scalable, and adaptable architecture such as that provided by the development of a cloud application based on a microservice architecture [24,25].

In Figure 1, a schematic representation of the PV IoT-SCADA structure and of the operating modules on which it relies, as proposed in this paper, is shown.

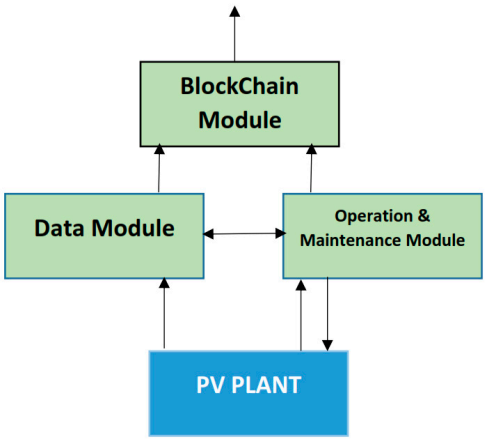

Figure 1. A schematic structure of the PV IoT SCADA investigated in this paper with the three basic operative modules: the data module, the operation and maintenance module, and the blockchain module.

It consists of three modules: The data module (DM) and the operation and maintenance module (OM) are mainly related to operations at the IoT-SCADA connectivity level, while the third module, the blockchain module (BM), is conceived to connect the PV plant to the external world mostly in terms of energy transactions management, with their relevance in terms of the IoT-SCADA status being related to providing feedbacks on plant operation (for instance, battery storage can be activated or not, according to the energy market requirements) and, eventually, to certifying plant operation status.

More in detail, the data module (DM) is devoted to the seamless integration of any IoT device and of any type of sensor deployed across the photovoltaic plant. The module acts as a central hub for collecting and processing data from these devices, easing the remote monitoring [26] and management of the plant in order to enhance its operational efficiency and reliability. It has to be designed and realized to support a wide range of IoT devices and transmission protocols, to perform real-time data collection and processing for immediate insights, and finally, to assure the most reliable and safe data transmission and storage to protect sensitive information.

The operation and maintenance module (OM) [27] is designed for the plant operations to actually meet the expected target performances, preventing faults and minimizing operation downtimes. It sets the plant operational parameters, such as the PV array configuration, the inverter settings, and the actuation of any other automatic operation that can be performed on the plant. It has to be characterized by the capacity for real-time monitoring of the plant's configuration changes and by a full integration with the hardware for automatic configuration update. Moreover, it is the module dedicated to providing information to forecast energy production in the short and long term and also to carry on the plant's predictive maintenance operations. The OM module may be equipped with a console and a centralized dashboard, where the real-time PV plant status and the collected plant performance metrics, coming from the PV equipment, are aggregated, analyzed, and compared to the set targets. The dashboard can alert system administrators to the occurrence of deviations, and it also provides contextual information and actionable insights the administrators can use to troubleshoot and face plant issues. The OM module focuses on analyzing the solar plant energy output and its efficiency in order to identify areas for operation improvement and, finally, to suggest recommendations for optimizing energy production. The module has to be characterized by comprehensive analytic tools for performance evaluation, by a tool for the immediate visualization and easy interpretation of performance metrics, by a tool for PV plant alerts for immediate notification of performance deviations, and finally, by a tool for historical data recording and analysis for trend identification and long-term planning, even using other PV plants as comparative benchmarks.

Finally, a blockchain module (BM) must also be conceived to implement blockchain technology for energy data certification, assuring the traceability, security, and reliability of the commercial transactions [28–30]. Its main functions are the certification of the energy data since the blockchain records in an immutable and transparent manner the production feeding into the grid and the external energy demand; data traceability since blockchain transactions trace production data along the entire supply chain, allowing the point source of the energy to be identified; security, as blockchain guarantees data integrity and transaction security, preventing fraud and tampering; and finally, it may provide real-time feedback on the external world energy market status on the PV plant operation [31,32]. The BM architecture is based on a private blockchain infrastructure derived from Ethereum, implementing a proof of authority (PoA) or similar consensus algorithm to ensure the security and efficiency of the network while maintaining "closed" write access to the registry [33,34]. In the following paragraphs, the three modules are more deeply discussed.

4. The Data Module

The IoT-SCADA operation relies on data [35–37] obtained by means of a number of different devices:

1. Wireless Sensors: Solar module sensors providing detailed data on voltage, current, temperature, or even module defects, if some continuously air- or ground-running monitoring equipment is made to operate in the plant, are generally based on wireless operation since wired connection could be very cumbersome to adopt in this case due to the very high number of objects to monitor. Air or grounded drones for plant surveillance may be also in general operating with this same protocol;
2. Local Weather Stations: These provide real-time data on factors like wind speed, solar irradiance, and ambient temperature, allowing for better prediction of energy generation and potential issues. They can operate both wireless and wired;
3. Other Connected Devices: Strings of modules, combiner boxes, inverters, and electric transformers as well as smart meters to monitor grid connection and power quality in real time are typically wire-connected. For large utility plants, the same occurs for plant surveillance cameras, sky cameras offering images with high temporal and spatial resolutions, and PV plant soiling monitoring equipment, which is now more

and more frequently used. Energy storage equipment is also to be considered in this category, although its use in large PV plants is still not usual;

4. Web Data: These are satellite data, mainly weather and solar forecasts, often obtained by means of dedicated REST API service, but are also economic and commercial data related to the energy market;
5. Energy Market Data: These are Blockchain data related to the commercial transactions being operated on a specific PV plant energy production. Such data may be considered to operatively affect the PV plant production.

All these heterogeneous data have to be handled in an efficient way, allowing an easy and effective interoperation between different sensors. This also should take into account data from field devices that may take advantage of proprietary servers not always allowing access in a programmatic and/or open way. The communication protocols used for data collection [38] by the IoT-SCADA systems may generally fall into two main categories, namely the sensor-specific protocols and the network-specific protocols:

1. Sensor-specific protocols:
    - SDI-12: This low-power, low-cost protocol is commonly used for environmental sensors such as temperature, humidity, wind speed, and rainfall. It operates at layers 1 and 2 of the OSI model, focusing on reliable data transmission within a single physical link [39,40];
    - Proprietary protocols: Some sensors, especially monitoring/inspection cameras, utilize vendor-specific protocols for communication. These protocols can significantly depend on the manufacturer.
2. Network communication protocols:
    - Modbus: This widely adopted protocol is often used for sensors measuring electrical parameters such as current, voltage, and power. It can operate over various physical layers, including RS-485 and Ethernet (with TCP/IP) [41];
    - IEC 61850: This newer standard is gaining traction in PV systems due to its object-oriented approach and support for Ethernet communication. It can be used for a broader range of sensors, including those measuring electrical data, environmental conditions, and inverter performance [42].

In order to manage such an heterogeneous and heavy data payload, an industrial device/router, often called Smart Logger, must be installed in the PV plant in order to collect data from sources 1 to 3 (wireless sensor data, local weather data, and other connected devices data) and send them to the cloud IoT-SCADA through a 4G mobile network to be fused with web data and blockchain-processed [43–45]. In this respect, the best possible solution seems, at present, to be an industrial device/router equipped with RutOS, a Linux-based operating system, targeting embedded devices. The equipped OpenWrt tool, the base of RutOS, provides a fully writable filesystem with package management that allows customization of the device through the use of suitable packages for any required application. The Smart Logger is a versatile device that supports a wide range of network protocols. These include common protocols like TCP, UDP, IPv4, IPv6, and ICMP as well as application-level protocols like HTTP, HTTPS, SFTP, FTP, SMTP, and others (some details are listed in Table 2 highlighting the corresponding ISO/OSI level). It also supports protocols for managing network connections, such as DHCP, Telnet, SSH, and VPN protocols (PPP and PPPoE). Additionally, the Smart Logger can be programmed using various languages. This includes scripting languages like Busybox v.1.30.1 shell and Lua, compiled languages like C and C++, an interpreted one such as Python v.3.9.16, and even the bytecode-compiled Java (available through a package manager). This flexibility allows developers to tailor the Smart Logger to specific needs, especially in edge-computing scenarios where data pre-processing is crucial. In Figure 2, a draft of the conceived data module is shown.

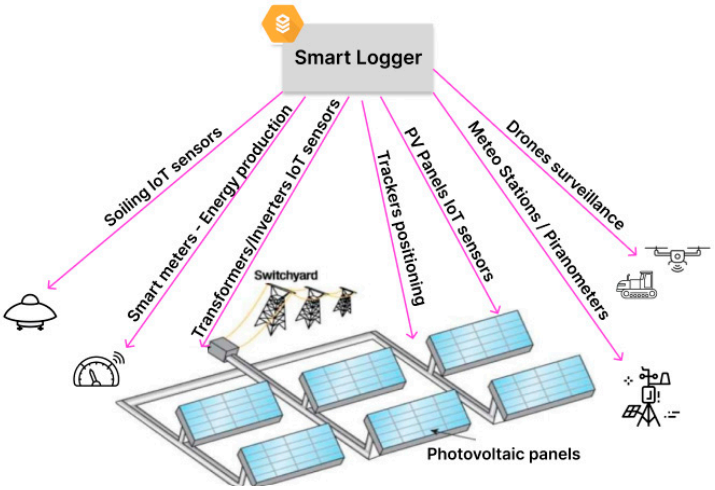

Figure 2. A schematic view of the data module. Data from the PV plant are collected for further processing by an industrial router, the Smart Logger.

Table 2. Protocols commonly used in PV system for data transmission to synchronize the local database with the remote one, grouped by their layer in ISO/OSI Model.

# OSI Layer	Protocol
7	MQTT, AMQP, WebSocket, HTTP/2, CoAP
3	6LoWPAN
2	LoRaWAN, NB-IoT, ZigBee, 6LoWPAN, SigFox, LTE, Wi-Fi
1	SigFox, LTE, Wi-Fi, LoRa

The Smart Logger main functions are as follows:

1. To collect all data and establish a common format for further transmission;
2. Define a common timestamp;
3. Resample and/or filter data to reduce the amount of data to be sent to the cloud;
4. Data quality assurance for anomaly detection or data normalization;
5. Local data storage to handle network failures, avoiding data loss with automatic synchronization with a centralized storage solution on the cloud.

Pre-processing/analysis of data at the edge [46] has the major benefits in reducing data transmission (mainly in in terms of data size) to optimize the transfer time required and to provide fast proactive alerts by employing machine learning (ML) methods on edge devices to detect anomalies.

Data transmission for PV plants located in commercial/residential or industrial environments is usually not of concern, and the protocols commonly adopted, acting at layer 1/2, are Wi-Fi or LTE, while in more isolated environments such as plants in desert regions, protocols like LoRaWAN or SigFox can be a valid solution. In Table 3, each protocol is discussed in terms of its specific features.

Table 3. Transmission protocols and features commonly adopted in data transmission by PV systems.

# OSI Layer	Protocol	Features
7	MQTT, AMQP, WebSocket, HTTP/2, CoAP	-Flexible and efficient for various data types; -Support real-time and non-real-time communication; -Secure options available (e.g., TLS with MQTT, AMQP).
3	6LoWPAN	-Enables IPv6 addressing and routing for resource-constrained devices in PV systems; -Low overhead compared to full IPv6 implementation.

Table 3. *Cont.*

# OSI Layer	Protocol	Features
2	LoRaWAN, NB-IoT, ZigBee, 6LoWPAN, SigFox, LTE, Wi-Fi	-Low power consumption, suitable for battery-powered sensors; -Offer varying ranges and data rates depending on the protocol; -Some offer security features (e.g., LoRaWAN, NB-IoT);
1	SigFox, LTE, Wi-Fi, LoRa	-Wide range of options with varying capabilities; -LTE and Wi-Fi offer high data rates for specific applications; -LoRa and SigFox offer long-range, low-power communication.

The choice of the optimal data transmission protocol can vary according to the specific condition, but limiting the analysis to layer 4 of ISO/OSI model, MQTT (message queue telemetry transport) is the most widely adopted choice, although the slightly less common alternative, AMQP (advanced message queuing protocol), could suit, too. MQTT is designed for lightweight communication [47] with resource-constrained devices, and it is commonly used in Internet of Things (IoT) applications, so it can be considered a de-facto standard. It prioritizes simplicity, low bandwidth usage, and efficient battery utilization. AMQP is designed for robust and reliable messaging in industrial applications, offering a richer feature set for complex message routing, security, and message guarantees. In a design of a PV IoT-SCADA where, as previously described, a device is devoted to data gathering, AMQP could be a better solution, while MQTT is to be preferred if the single specific sensor transmits data directly over the internet. AMQP also shows some advantages in terms of data transmission security [48]. In fact, MQTT supports the following:

- Basic Authentication: MQTT offers basic username and password authentication for identifying clients and restricting unauthorized access. This provides a rudimentary level of security but is susceptible to brute-force attacks and eavesdropping;
- TLS/SSL Encryption: While not part of the core MQTT specification, MQTT can be secured using transport layer security (TLS) or secure sockets layer (SSL) encryption. This encrypts data in transit, protecting it from eavesdropping on unsecured networks;
- While MQTT itself does not natively support M2M (machine-to-machine) OAuth2 authentication, it is possible to achieve this functionality using Auth0 or similar identity providers.

AMQP offers an even larger set of security features, as it supports the following:

- SASL (simple authentication and security layer): This provides various authentication mechanisms beyond basic username/password, including token-based and certificate-based authentication, offering stronger security;
- TLS/SSL Encryption: Like MQTT, AMQP can leverage TLS/SSL for data encryption in transit;
- Message Signing and Verification: AMQP allows digitally signing messages, ensuring message integrity, and preventing unauthorized modification during transmission;
- Access Control Lists (ACLs): These enable fine-grained control over user and application access to specific queues and exchanges, enhancing security by restricting unauthorized access to sensitive data.

Another feature to be considered for an IoT-SCADA is the data serialization format that is critical for an efficient and interoperable data exchange. The most common solutions are JSON, Avro, and Protocol Buffers [49]. Table 4 provides a quick comparison of such data exchange formats.

Table 4. Comparison of JSON, Avro, and Protocol Buffers as data exchange formats.

Feature	JSON (JavaScript Object Notation)	Avro	Protocol Buffers (Protobuf)
Description	Key-value pairs representing data objects	Efficient binary format with schema evolution capabilities	Language-neutral, binary format known for its efficiency and performance
Structure	Easily readable by humans without additional tools	Schema-based, defines data structure before transmission	Schema-based, defines data structure before transmission
Readability	Larger file size due to text nature	Requires additional tools for interpretation if schema is unknown	Requires additional tools for interpretation if schema is unknown
Efficiency	Limited data validation and type checking	Smaller file size compared to JSON due to binary format	Extremely compact and efficient binary format
Data Validation	Limited support for schema changes	Schema enforces data validation and type safety	Schema enforces data validation and type safety
Schema Evolution	Simpler to implement, no schema definition required.	Supports schema evolution for backward and forward compatibility.	Supports schema evolution for backward and forward compatibility
Development Complexity	Widely supported by various programming languages and libraries	Requires defining Avro schemas, adding initial complexity	Requires defining Protobuf schemas, adding initial complexity
Language support	Human-readable, text-based format resembling JavaScript objects	Supported by most major programming languages	Supported by many programming languages, with potential for code generation in various languages

Although JSON is the most commonly employed data exchange format for an IoT-SCADA, a solution like Protobuf could be an optimal alternative mainly for its efficiency.

The last issue characterizing the data module is the data storage. The proposed architecture needs to fulfil the following requirements:

1. It must store data that are mainly *time-series data*, i.e., data that are collected and indexed over regular and/or irregular time intervals. This means each data point has two important components: the *data value* itself, which represents the actual measurement or observation being recorded, and *the timestamp*, which indicates the specific point in time at which the data value was captured;
2. The data must come from different sources with different sampling rates;
3. The principal data source is related to data from an MQTT broker;
4. It must have the capability to handle other data sources, such as weather forecasting providers; this is usually performed using the REST API service provided by the different providers;
5. It must handle the huge amount of data that also needs geo-referencing;
6. It must address the privacy concern for some sensitive fields;
7. It must have good scalability and availability;
8. It must avoid data explosion.

As already mentioned, the optimal storage solution is commonly described as a "hybrid storage solution" empowered with edge-computing functionalities. This means storing data at a finer granularity/sampling on the edge device available at the PV site and synchronizing data averaged automatically on the edge device with the data storage cloud solution. This approach reduces the amount of data to be sent over the internet, allows data safety in case of no cloud connectivity, and reduces the growth rate of data on remote servers receiving, in this way, only averaged data. In this scenario, although any database (DB) solution could be employed, solutions such as NoSQL DB, e.g., MongoDB, or time-series DB [50], developed exclusively to treat time-series data, such as InfluxDB, could be the optimal solutions able to fulfill all the requirements above [51].

5. The O&M Module

As discussed above, the O&M module is devoted to managing all the IoT-SCADA data flow [52]. It allows operators to monitor system performance in real time, visualize data by dashboards, and eventually to interact with the system (e.g., adjust settings, acknowledge automatic alerts, and send control commands).

The core software of SCADA provides the following functionalities/services:

1. Handling of data flow, alarms processing, and ML and providing access to data for the HMI and other applications;
2. Reporting for generating reports to analyze data trends and to identify potential issues and/or anomalies detection and to show real-time data;
3. Implementing various security measures like user authentication, authorization, data encryption, and network security protocols to protect against unauthorized access and cyberattacks;
4. System management to manage system configuration, user accounts, system backups, and system health monitoring to ensure smooth operation and timely response to potential issues;
5. Forecasting PV system power production using ML models gathering real-time data from remote systems as well as weather forecasts from commercial providers;
6. Detecting PV systems anomalies and/or obtain insight into plant conditions for predictive maintenance.

Currently, all functionalities listed above are not provided by open-source (OS) solutions, while many options are available to provide some of the functionalities listed above. For this reason, a new ad hoc software solution needs to be implemented by writing a proprietary code to encapsulate each service described above and integrating OS available solutions when useful. This module is characterized by a human–machine interface (HMI), a web front-end that will expose all functionalities by interacting with back-end services for each of the tasks listed above. For this architecture, a well-suited solution could be implemented using a micro-service architecture [53,54] deployed using Google Kubernetes [55]. Opposite to traditional monolithic applications that are self-contained pieces of software where all functionalities reside within a single codebase/project that can become cumbersome to scale as the application grows, a microservice-based architecture is a software development style that structures the application as a collection of small, independent services with the following characteristics [56]:

- *Loosely Coupled*: They communicate with each other through well-defined APIs (application programming interfaces) and rely minimally on shared resources;
- *Fine-grained*: Each service focuses on a single business capability or functionality;
- *Independently Deployable*: Services can be developed, deployed, and scaled independently without affecting other parts of the application.

Microservice-based architecture is therefore a more flexible and scalable alternative that is particularly valuable in the case of an IoT-SCADA, as it is characterized by specific advantages:

(1) *Agility and Speed*: Independent development and deployment cycles enable faster development and updates for individual services;
(2) *Scalability*: Services can be scaled independently based on their specific needs, optimizing resource utilization;
(3) *Resilience*: Failure in one service has minimal impact on others, enhancing overall system robustness;
(4) *Technology Heterogeneity*: Different services can leverage the most suitable programming languages and technologies;
(5) *Improved Maintainability*: Smaller codebases are easier to understand, test, and maintain compared to monolithic systems.

A PV IoT-SCADA can be realized using a microservice architecture, as each microservice can provide one definite service. For instance, a microservice can be assigned to provide weather forecasting data taken from an external provider, another could handle reads and writes of data from PV plants (data provided by the MQTT broker) to the central database, another the outputs of trained ML models that forecast power production of each plant, and so on. For the case in consideration, points 4 and 5 are extremely important, and probably, they cannot even be pursued using a monolithic solution.

On the other hand, microservice architecture also exhibits some drawbacks:

1. *Increased Complexity*: Managing a distributed system with multiple services requires more complex orchestration and communication mechanisms;
2. *Coordination Challenges*: All microservices need to talk each other and transfer data in a synchronized way, and this adds to the complexity and usually requires specific patterns as API gateway;
3. *Debugging and Troubleshooting*: Issues can arise from interactions between services, making debugging and troubleshooting more challenging;
4. *Testing Challenges*: Testing distributed services with complex interactions requires a more comprehensive testing strategy;
5. *Potentially Higher Infrastructure Costs*: Running and managing multiple independent services might incur higher infrastructure costs compared to a monolithic approach.

In the IoT-SCADA solution outlined above, since the MQTT broker [57–60] acts as the central collection point for the data generated by the monitored PV system, a deployment with an ad hoc integration cluster is by far the most efficient solution. At present, the Kubernetes operator is probably the best integration solution for a PV IoT-SCADA. Kubernetes (K8s) is an open-source system for automating the deployment, scaling, and management of containerized applications [61]. It groups containers, which are lightweight, self-contained units of software, into logical units called pods. Pods are managed by Kubernetes by means of a cluster of machines, ensuring efficient resource utilization and high availability.

Microservices integration within Kubernetes means the following:

- *Containerize Microservices*: Each microservice must be packaged in its own container image, including the necessary dependencies and runtime environment. This ensures isolation and portability across different environments. Docker is a widely used solution for this purpose;
- *Define Kubernetes Manifests*: This means creating YAML files, called manifests, for each microservice deployment. These manifests specify details like container image, resource requirements (CPU, memory), replicas (number of instances to run), and environment variables;
- *Deploy to Kubernetes Cluster*: A Kubernetes cluster needs to be configured using a solution based on virtual machines or physical servers.

Figure 3 shows an example of such a solution provided by EMQX [62,63]. In this figure, the MQTT service is exposed to the outside clients (MQTT client in the figure) by a load balancer (in the figure, load balance distributes network traffic across multiple instances of an application running in a K8S cluster) using a Kubernetes cluster with three pods, the basic container unit in K8s. The solution depicted in Figure 3 is a K8s complete

solution with storage and monitoring services, the latter consisting of Prometeus [64] for monitoring and alerting tasks and Grafana for a graphical dashboard. The EMQX operator allows simplified deployment of EMQX cluster service and automated operations and maintenance for EMQX, including cluster upgrades, runtime data persistence, updating Kubernetes resources based on the status of EMQX, etc.

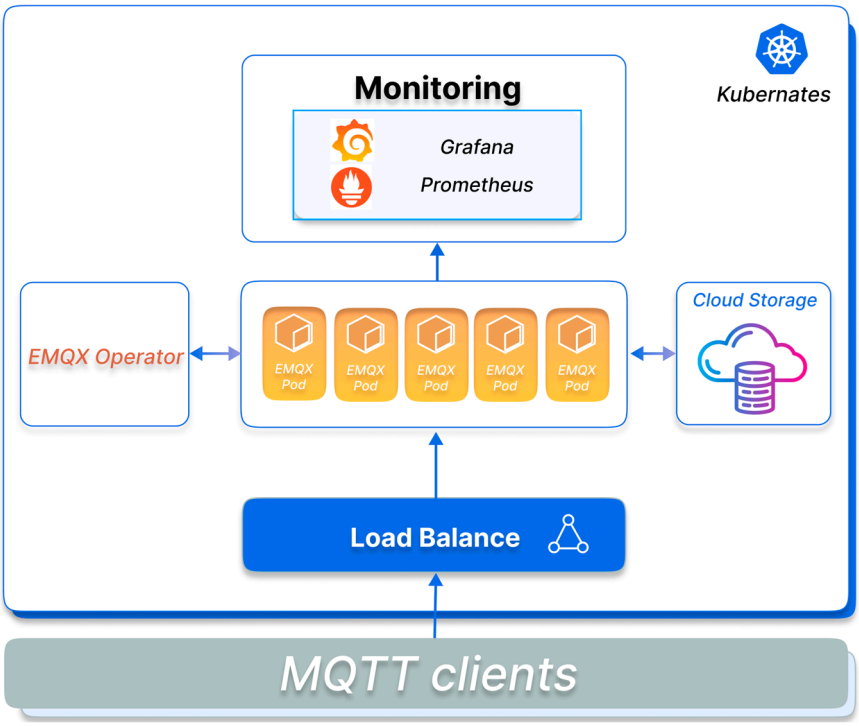

Figure 3. Integration of MQTT brokers by EMQX into K8s.

There are many benefits using Kubernetes for a microservice-based architecture:

1. *Simplified Deployment and Management*: It automates deployment, scaling, and rollback processes for all microservices through a single platform;
2. *Scalability and Availability*: It can easily scale individual microservices or the entire application up or down based on traffic and resource requirements. Kubernetes ensures high availability by automatically restarting failed pods and rescheduling them on healthy nodes;
3. *Resource Optimization*: Kubernetes efficiently allocates resources (CPU, memory) to pods based on their defined requirements, preventing over-provisioning and optimizing resource utilization;
4. *Service Discovery and Communication*: Built-in service discovery eliminates the need to manually manage IP addresses or service locations, simplifying communication between microservices.

By effectively utilizing Kubernetes, is then possible to gain significant advantages in managing and deploying a microservices architecture, promoting scalability, efficiency, and high availability for the whole solution.

6. BC Module

The blockchain module is designed to take into account scalability, efficiency, and compliance. It has to be modular and easily scalable so as to manage a high volume of transactions, even in the event of significant growth in the number connected devices. The distributed architecture and the use of sharding technologies make it possible to increase processing capacity and transaction speed without sacrificing security and decentralization of the system. The module architecture has be optimized to minimize costs and energy

consumption, and the use of efficient consensus algorithms and data aggregation technologies will reduce the number of transactions and network management costs. Furthermore, optimizing the transaction validation process and efficient data storage will improve the overall efficiency of the system. Finally, the module has to comply with current energy and privacy regulations and also to take into account data security and privacy requirements, ensuring the protection of sensitive information and respect for user rights. The module architecture is based on a private blockchain infrastructure derived from Ethereum [33], implementing a proof of authority (PoA) or similar consensus algorithm [34] to guarantee the security and efficiency of the network. The interaction between the blockchain module and data and O&M modules involves the exchange of files for various purposes. The data module and O&M module collect and process data from various sources, including sensors, weather stations, and other connected devices. These data may need to be processed by the blockchain module for certification and traceability purposes. The blockchain module thus receives files from both the modules through secure communication protocols such as MQTT or AMQP. The files exchanged between the modules may include data on energy production, efficiency, and other relevant factors that contribute to the overall performance of the PV plant. Once the blockchain module receives the files, it processes the data for certification and traceability purposes, and vice versa, when an energy request has to be performed, it is certified by means of the same BC module and sent to the O&M module for practical implementation. This involves recording the data in an immutable and transparent manner, ensuring the security and reliability of the commercial transactions related to the energy data. The blockchain module then provides certified and traced data back to the data module and O&M module for further analysis and optimization of energy production. The interaction between the blockchain module and the other modules is essential for the efficient and effective operation of the PV plant.

7. Discussion

7.1. General Design of the IoT-SCADA

Over the last 5–10 years, a plant for photovoltaic electricity production has become an industrial product characterized by well-defined technical and construction standards. The operation and management part of these structures presents peculiarities compared to any other electricity production plant, connected, in particular, to the high number of power generation units (the photovoltaic modules) and to the need to have frequent control of their electrical parameters as well as of the remaining components of the PV plant. Furthermore, monitoring must exhibit highly flexible characteristics to take into account the replacement of one or more components and the maintenance requests of the system. The solution proposed in this work is based on the addressing of the data produced by the PV plant to specific industrial routers where pre-processing operations are possible, essentially aimed at limiting the amount of data that must be transmitted to the cloud (or in any case to a dedicated server) and to make more readily available the data needed for machine learning applications. MQTT is suggested as the transmission protocol since it exhibits a series of operational advantages linked to its widespread use, which ensures a high reliability. The data produced must be appropriately serialized, preferably through JSON exchange format, and finally, for the storage part, although there are no specific requests except for the need to have NoSQL databases, the optimal choice could be to use a database that can effectively handle time-series data, e.g., DB such as InfluxDB. The data packaged in this way are transferred to the unit that manages and controls the system and also by the creation of a specific human–machine interface. The most effective technical solution proposed in this paper for this part of SCADA is the transmission of data upon activation of specific microservices managed by an orchestration system such as Kubernetes. In this work, the introduction to the SCADA of a data processing module that uses the blockchain protocol was also suggested. For large systems, security in the management of external transactions and requests from outside is an element of an increasing level of criticality as a result of the growing demand of photovoltaic energy volumes. In this work, the blockchain operative

Ethereum infrastructure was proposed, which now has high-reliability characteristics as an operational element of the blockchain that can be also used as an element of certification of the data produced by the system for internal control purposes.

7.2. IoT-Based SCADA Security Concerns

As previously stated, the overall design architecture so far illustrated aims to develop a comprehensive SCADA solution [65] that leverages many new technologies to optimize every choice in order to fully take advantage of the benefits of the technologies adopted. Table 5 summarizes some cyberattacks affecting microgrids and consequently IoT-SCADA systems.

Table 5. Common cyberattacks affecting renewables microgrids.

Attack Type	Target	Impact	How Mitigate
False Data Injection (FDI) [66–68]	SCADA systems, sensors	Manipulate energy production, mislead operators	Data integrity check, anomaly detection
Main-in-the-middle	Network communication	Alter data between devices	Use encryption
Denial-of-Service (DoS)	Control systems	Overloads systems that become unresponsive	Implement intrusion detection and prevention systems (IDS/IPS)
Malware	Inverters, controllers	Steal data or disable devices	Keep software updated, patch vulnerabilities
Under-Load Tap Changing (ULTC) Transformers [69]	Targeting specific equipment	Disrupt power flow, Cause outages	Monitor critical equipment, segment network

In this paper, blockchain is mainly described as a technology to assure data integrity for energy data transactions from the PV plant. However, its adoption as a basic tool of the IoT-SCADA also has potential benefits for mitigating cyber-attacks for its intrinsic features:

- Immutability: Data stored on a blockchain cannot be altered after it is added, making it tamper-proof and reducing the risk of false data injection;
- Transparency: All participants on the network can see the data, promoting trust and accountability;
- Decentralization: There is no single point of failure, making it harder for attackers to take down the entire system.

Nonetheless, introducing blockchain for every data transmission introduces complexity and latency in data transmission that need to be carefully considered for data analytics operations [70,71].

8. Conclusions

In the context of large photovoltaic utilities, the adoption of the IoT paradigm is a necessity linked to the peculiar structure of the plants. In this research work, the fundamental components for establishing the connecting layer of an IoT-based supervisory control and data acquisition (SCADA) system specifically tailored for the operation and management optimization of large photovoltaic (PV) plants are discussed. The proposed SCADA design architecture, as outlined in the paper, represents a preliminary concept directly focused on handling the ongoing operational challenges faced by large PV utilities, mainly in terms of real-time monitoring, fault detection, and predictive maintenance. One crucial aspect is data efficiency. The IoT-SCADA was designed in order to minimize the data transmitted from the monitored PV plants while still capturing essential information to effectively

implement the steps of knowledge extraction and development of forecasting algorithms. This selective data transmission ensures efficient utilization of network resources. Additionally, the proposed design is functional for the development of new tailored forecasting algorithms for PV power production. These algorithms leverage historical data, real-time measurements from PV plants, and meteorological data from weather service providers to predict energy generation, equipment operation, and potential issues (predictive maintenance). However, the proposed solution also has potential downsides, a major one being related to data security: Any breach in the system could allow hackers to manipulate the plant's operations or monitoring. Additionally, the reliance on constant connectivity raises concerns about what happens during outages, a problem that is further amplified by the expected huge amount of data that could easily come with IoT-based SCADA. In this respect, edge data processing and/or data storage, as outlined in previous sections, is suggested as a possible reliable solution. Future work will include the in-field testing and validation of the actual implementation of the proposed SCADA system as an O&M tool in a 5 MW PV grid-connected utility plant located in the Apulia region, mainly in terms of evaluating the reliability, security, and efficiency of the proposed design.

Author Contributions: Conceptualization, S.F., S.I., C.S., P.S. and G.D.F.; introduction, G.D.F. and S.F.; literature review, G.D.F. and S.F.; paragraphs 3 and 7 original draft preparation, S.I., C.S. and P.S.; paragraphs 4 and 5 and Section 7.2, S.F.; funding acquisition, G.D.F. All authors have read and agreed to the published version of the manuscript.

Funding: This research received partial funding from Ministero per lo Sviluppo Economico, Fondo per la Crescita Sostenibile, under the framework "Accordi per l'innovazione di cui al D.M. 31 Dicembre 2021 e DD 18 Marzo 2022" under project MARTA, n.: F/310193/01-02/X56.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: Authors Salvatore Ippolito and Paolo Schiattarella were employed by the company TeaTek, Consorzio Area, Via Maddaloni, snc, 80011 Acerra, Italy. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. Yadav, G.; Paul, K. Architecture and Security of SCADA Systems: A Review. *Int. J. Crit. Infrastruct. Prot.* **2021**, *34*, 100433. [CrossRef]
2. Peter, O.; Pradhan, A.; Mbohwa, C. Industrial Internet of Things (IIoT): Opportunities, Challenges, and Requirements in Manufacturing Businesses in Emerging Economies. *Procedia Comput. Sci.* **2023**, *217*, 856–865. [CrossRef]
3. Ho, J.Y.; O'Sullivan, E. Standardisation Framework to Enable Complex Technological Innovations: The Case of Photovoltaic Technology. *J. Eng. Technol. Manag.* **2018**, *50*, 2–23. [CrossRef]
4. Vartiainen, E.; Masson, G.; Breyer, C.; Moser, D.; Román Medina, E. Impact of Weighted Average Cost of Capital, Capital Expenditure, and Other Parameters on Future Utility-Scale PV Levelised Cost of Electricity. *Prog. Photovolt. Res. Appl.* **2020**, *28*, 439–453. [CrossRef]
5. PV Monitoring Technologies Market Size, Share | 2024 to 2031. Available online: https://www.businessresearchinsights.com/market-reports/pv-monitoring-technologies-market-103080 (accessed on 28 March 2024).
6. Takruri, M.; Farhat, M.; Barambones, O.; Ramos-Hernanz, J.A.; Turkieh, M.J.; Badawi, M.; AlZoubi, H.; Sakur, M.A. Maximum Power Point Tracking of PV System Based on Machine Learning. *Energies* **2020**, *13*, 692. [CrossRef]
7. Talayero, A.P.; Melero, J.J.; Llombart, A.; Yürüşen, N.Y. Machine Learning Models for the Estimation of the Production of Large Utility-Scale Photovoltaic Plants. *Sol. Energy* **2023**, *254*, 88–101. [CrossRef]
8. Yalçin, T.; Paradell Solà, P.; Stefanidou-Voziki, P.; Domínguez-García, J.L.; Demirdelen, T. Exploiting Digitalization of Solar PV Plants Using Machine Learning: Digital Twin Concept for Operation. *Energies* **2023**, *16*, 5044. [CrossRef]
9. *IEC 61724-1:2021*; Photovoltaic System Performance—Part 1: Monitoring. IEC Webstore: Geneva, Switzerland, 2021. Available online: https://webstore.iec.ch/publication/65561 (accessed on 28 March 2024).
10. Voicu, V.; Petreus, D.; Cebuc, E.; Etz, R. Industrial IoT (IIOT) Architecture for Remote Solar Plant Monitoring. In Proceedings of the 2022 21st RoEduNet Conference: Networking in Education and Research (RoEduNet), Sovata, Romania, 15–16 September 2022. [CrossRef]
11. 8 Benefits of Adopting Internet of Things (IoT) in SCADA System. Available online: https://www.biz4intellia.com/blog/8-benefits-of-adopting-internet-of-things-(IoT)-in-scada-system/ (accessed on 9 May 2024).

12. SCADA vs. IoT: Which Meets Your Data Processing Needs? Available online: https://www.faircom.com/learn/blog/scada-vs-iot-which-is-better-for-your-operations (accessed on 9 May 2024).
13. Using the Internet of Things in a SCADA System: Practical Guide. Available online: https://webbylab.com/blog/iot-and-scada/ (accessed on 9 May 2024).
14. Mathematics and Data Structures in Blockchain and Ethereum. Available online: https://www.researchgate.net/publication/340418164_Mathematics_and_Data_Structures_in_Blockchain_and_Ethereum (accessed on 12 May 2024).
15. Digitization Maturity Levels and Roadmap—ROI-EFESO Management Consulting. Available online: https://www.roi-international.com/management-consulting/competences/increased-efficiency-through-digitisation-industry-40/digitization-maturity-levels (accessed on 9 May 2024).
16. Hazrat, S.F. Review of SCADA Systems for Photovoltaic Power Plants. *Int. J. Creat. Res. Thoughts* **2021**, *6*, 1565–1572.
17. Hoarca, I.C. Energy Management for a Photovoltaic Power Plant Based on SCADA System. In Proceedings of the 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Pitesti, Romania, 1–3 July 2021. [CrossRef]
18. Aghenta, L.O.; Iqbal, M.T. Development of an IoT Based Open Source SCADA System for PV System Monitoring. In Proceedings of the 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), Edmonton, AB, Canada, 5–8 May 2019. [CrossRef]
19. Baig, M.J.A.; Iqbal, M.T.; Jamil, M.; Khan, J. A Low-Cost, Open-Source Peer-to-Peer Energy Trading System for a Remote Community Using the Internet-of-Things, Blockchain, and Hypertext Transfer Protocol. *Energies* **2022**, *15*, 4862. [CrossRef]
20. Ahsan, L.; Baig, M.J.A.; Iqbal, M.T. Low-Cost, Open-Source, Emoncms-Based SCADA System for a Large Grid-Connected PV System. *Sensors* **2022**, *22*, 6733. [CrossRef]
21. Tran, T.S.; Vu, M.P.; Pham, M.H.; Dang, H.A.; Nguyen, D.T.; Nguyen, D.Q.; Tran, A.T.; Ma, T.T.H.; Nguyen, P.H. Study on IoT Based SCADA System for Rooftop Solar Power Systems in Vietnam. *Int. J. Renew. Energy Res.* **2023**, *13*, 1212–1222. [CrossRef]
22. Qays, M.O.; Ahmed, M.M.; Parvez Mahmud, M.A.; Abu-Siada, A.; Muyeen, S.M.; Hossain, M.L.; Yasmin, F.; Rahman, M.M. Monitoring of Renewable Energy Systems by IoT-Aided SCADA System. *Energy Sci. Eng.* **2022**, *10*, 1874–1885. [CrossRef]
23. Aghenta, L.O.; Iqbal, M.T.; Aghenta, L.O.; Iqbal, M.T. Design and Implementation of a Low-Cost, Open Source IoT-Based SCADA System Using ESP32 with OLED, ThingsBoard and MQTT Protocol. *AIMS Electron. Electr. Eng.* **2020**, *4*, 57–86. [CrossRef]
24. Dugyala, R.; Reddy, N.H.; Kumar, S. Implementation of SCADA Through Cloud Based IoT Devices–Initial Design Steps. In Proceedings of the IEEE International Conference Image Information Processing, Shimla, India, 15–17 November 2019; pp. 367–372. [CrossRef]
25. Jiang, L.; Li, W.; Fu, B.; Wang, J. Microservice Placement Method of SCADA Service in Collaborative Cloud-Edge Computing System. In Proceedings of the 2021 International Conference on Power System Technology: Carbon Neutrality and New Type of Power System (POWERCON), Haikou, China, 8–9 December 2021; pp. 1838–1842. [CrossRef]
26. Pasandideh, M.; Tito, S.R.; Apperley, M.; Atkins, M. Design and Implementation of a Simple Low-Cost and Real-Time Solar Power Monitoring System. In Proceedings of the 5th IEEE International Conference on DC Microgrids (ICDCM), Auckland, New Zealand, 15–17 November 2023. [CrossRef]
27. Livera, A.; Paphitis, G.; Pikolos, L.; Papadopoulos, I.; Montes-Romero, J.; Lopez-Lorente, J.; Makrides, G.; Sutterlueti, J.; Georghiou, G.E. Intelligent Cloud-Based Monitoring and Control Digital Twin for Photovoltaic Power Plants. In Proceedings of the 2022 IEEE 49th Photovoltaics Specialists Conference (PVSC), Philadelphia, PA, USA, 5–10 June 2022; pp. 267–274. [CrossRef]
28. Boumaiza, A.; Sanfilippo, A. Solar PV Energy Trading Market Blockchain-Based: Agent-Models Community. In Proceedings of the IEEE International Conference on Industrial Technology, Shanghai, China, 22–25 August 2022. [CrossRef]
29. Ahn, B.; Bere, G.; Ahmad, S.; Choi, J.; Kim, T.; Park, S.W. Blockchain-Enabled Security Module for Transforming Conventional Inverters toward Firmware Security-Enhanced Smart Inverters. In Proceedings of the 2021 IEEE Energy Conversion Congress and Exposition (ECCE), Vancouver, BC, Canada, 10–14 October 2021; pp. 1307–1312. [CrossRef]
30. Hadi, A.A.; Bere, G.; Ahn, B.; Kim, T. Smart Contract-Defined Secondary Control and Co- Simulation for Smart Solar Inverters Using Blockchain Technology. In Proceedings of the 2020 IEEE CyberPELS (CyberPELS), Miami, FL, USA, 13 October 2020. [CrossRef]
31. Zhang, Q.; Xu, T.; Wang, D.; Liu, Z.; Cheng, C.; Zheng, S.; Wang, G. Study of Traceability System of Renewable Energy Power Trading Based on Blockchain Technology. In Proceedings of the 2022 International Conference on Blockchain Technology and Information Security (ICBCTIS), Huaihua, China, 15–17 July 2022; pp. 171–176. [CrossRef]
32. Duan, T.; Li, D.; Guo, Q.; Wang, H.; Bai, D. Research and Application of Renewable Energy Power Consumption Certificate Based on Blockchain. In Proceedings of the 2021 International Conference on E-Commerce and E-Management (ICECEM), Dalian, China, 24–26 September 2021; pp. 147–152. [CrossRef]
33. Rosa-Bilbao, J.; Boubeta-Puig, J. Ethereum Blockchain Platform. In *Distributed Computing to Blockchain Architecture, Technology, and Applications*; Academic Press: Cambridge, MA, USA, 2023; pp. 267–282. [CrossRef]
34. Nalini, K.M.; Preetha, S.; Manjunath, P.; Raunak Prasad, P. Deploy a Private Blockchain Network with a Power of Authority (PoA) Consensus Model Using GoEtherium in Amazon EC2. In Proceedings of the 7th IEEE International Conference on Computational Systems and Information Technology for Sustainable Solutions (CSITSS), Bangalore, India, 2–4 November 2023. [CrossRef]
35. Adigüzel, E.; Gürkan, K.; Ersoy, A. Design and Development of Data Acquisition System (DAS) for Panel Characterization in PV Energy Systems. *Measurement* **2023**, *221*, 113425. [CrossRef]

36. Zhu, Y.; Xu, X.; Yan, Z.; Lu, J. Data Acquisition, Power Forecasting and Coordinated Dispatch of Power Systems with Distributed PV Power Generation. *Electr. J.* **2022**, *35*, 107133. [CrossRef]
37. Narayanan, L.K.; Subbiah, P.; Rengaraj Alias Muralidharan, R.; Baskaran, A.P.; Srinivasan, V.; Baskaran, A.P.; Victor, P.; Ramachandran, H. A Survey on AI- and ML-Based Demand Forecast Analysis of Power Using IoT-Based SCADA. In *Smart Energy and Electric Power Systems: Current Trends and New Intelligent Perspectives*; Elsevier: Amsterdam, The Netherlands, 2023; pp. 65–78. [CrossRef]
38. Rao, C.K.; Sahoo, S.K.; Yanine, F.F. A Literature Review on an IoT-Based Intelligent Smart Energy Management Systems for PV Power Generation. *Hybrid Adv.* **2024**, *5*, 100136. [CrossRef]
39. SDI-12 Support Group. Available online: http://www.sdi-12.org/ (accessed on 9 May 2024).
40. ISO/OSI Model | Request PDF. Available online: https://www.researchgate.net/publication/327177854_ISOOSI_model (accessed on 9 May 2024).
41. Belliardi, R.; Neubert, R. Modbus Protocol*. In *Industrial Communication Technology Handbook*; CRC Press: Boca Raton, FL, USA, 2017; pp. 10–11. [CrossRef]
42. Huang, Z.; Gao, L.; Yang, Y.; Kong, X.; Lin, J. IEC 61850 Standards and Configuration Technology. In *IEC 61850-Based Smart Substations: Principles, Testing, Operation and Maintenance*; Academic Press: Cambridge, MA, USA, 2019; pp. 25–62. [CrossRef]
43. Baodi, D.; Kai, C.; Meng, C.; Ying, Z.; Zhuandi, H.; Xiaoyun, Q. Design and Application of Regional Multi-Energy Complementary Distributed Energy Management and Control Platform Based on Big Data. In Proceedings of the 2020 IEEE/IAS Industrial and Commercial Power System Asia (I and CPS Asia), Weihai, China, 13–15 July 2020; pp. 121–126. [CrossRef]
44. Sudjana, O.; Septanto, H. Data Acquisition and Visualization for Solar Power Battery Using IoT Open Source Stack Solution. In Proceedings of the 2nd International Conference on Sustainable Engineering and Creative Computing (ICSECC), Cikarang, Indonesia, 16–17 December 2020; pp. 177–181. [CrossRef]
45. Yang, M.; Zhou, G. Design and Implementation of Photovoltaic Power Generation Management System Based on NB-IoT. In Proceedings of the 2021 IEEE International Conference on Information Communication and Software Engineering (ICICSE), Chengdu, China, 19–21 March 2021; pp. 255–259. [CrossRef]
46. Petersen, B.; Bindner, H.; You, S.; Poulsen, B. Smart Grid Serialization Comparison: Comparision of Serialization for Distributed Control in the Context of the Internet of Things. In Proceedings of the 2017 Computing Conference, London, UK, 18–20 July 2017; pp. 1339–1346. [CrossRef]
47. Uy, N.Q.; Nam, V.H. A Comparison of AMQP and MQTT Protocols for Internet of Things. In Proceedings of the 2019 6th NAFOSTED Conference on Information and Computer Science (NICS), Hanoi, Vietnam, 12–13 December 2019; pp. 292–297. [CrossRef]
48. Kotak, J.; Shah, A.; Shah, A.; Rajdev, P. A Comparative Analysis on Security of MQTT Brokers. In Proceedings of the 2nd Smart Cities Symposium (SCS 2019), Zallaq, Bahrain, 24–26 March 2019. [CrossRef]
49. Alshuwair, S.A. Edge Computing Applications for Smart Grid and Distributed Systems. In Proceedings of the 2022 Saudi Arabia Smart Grid Conference (SASG), Riyadh, Saudi Arabia, 12–14 December 2022. [CrossRef]
50. Tripathi, P.; Miraz, M.H.; Joshi, S. Comparative Analysis of MongoDB and InfluxDB for Time Series Data Management in IoT Environments: A Study on Performance, Scalability, and Concurrency. In Proceedings of the 2023 International Conference on Computing, Networking, Telecommunications and Engineering Sciences Applications (CoNTESA), Zagreb, Croatia, 14–15 December 2023; pp. 39–42. [CrossRef]
51. Ahmad, K.; Ansari, M. Hands-On InfluxDB. In *NoSQL: Database for Storage and Retrieval of Data in Cloud*; Chapman and Hall/CRC Press: Boca Raton, FL, USA, 2017; pp. 341–354. [CrossRef]
52. Radia, M.A.A.; Nimr, M.K.E.; Atlam, A.S. IoT-Based Wireless Data Acquisition and Control System for Photovoltaic Module Performance Analysis. In *e-Prime-Advances in Electrical Engineering, Electronics and Energy*; Elsevier: Amsterdam, The Netherlands, 2023; Volume 6, p. 100348. [CrossRef]
53. Paul, G.A.; Jagnani, Y.; Supraja, P. Improving Fault Tolerance and Tackling Broker Failure in MQTT through Blockchain. In Proceedings of the 2023 3rd International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), Bhilai, India, 5–6 January 2023. [CrossRef]
54. Nieman, K.; Sajal, S. A Comparative Analysis on Load Balancing and GRPC Microservices in Kubernetes. In Proceedings of the 2023 Intermountain Engineering, Technology and Computing (IETC), Provo, UT, USA, 12–13 May 2023; pp. 322–327. [CrossRef]
55. Poniszewska-Marańda, A.; Czechowska, E. Kubernetes Cluster for Automating Software Production Environment. *Sensors* **2021**, *21*, 1910. [CrossRef] [PubMed]
56. Larsson, M. *Microservices with Spring Boot And Spring Cloud—Build Resilient and Scalable Microservices Using Spring Cloud, Istio, and Kubernetes*; Packt Publishing: Birmingham, UK, 2021.
57. Suwardi Ansyah, A.S.; Arifin, M.; Alfan, M.B.; Suriawan, M.V.; Farhansyah, N.H.; Shiddiqi, A.M.; Studiawan, H. MQTT Broker Performance Comparison between AWS, Microsoft Azure and Google Cloud Platform. In Proceedings of the IEEE International Conference on Recent Trends in Electronics and Communication: Upcoming Technologies for Smart Systems (ICRTEC), Mysore, India, 10–11 February 2023. [CrossRef]
58. Mellit, A.; Benghanem, M.; Kalogirou, S.; Massi Pavan, A. An Embedded System for Remote Monitoring and Fault Diagnosis of Photovoltaic Arrays Using Machine Learning and the Internet of Things. *Renew Energy* **2023**, *208*, 399–408. [CrossRef]
59. Welcome to the OpenWrt Project. Available online: https://openwrt.org/ (accessed on 28 March 2024).

60. What Is Pub/Sub? | Cloud Pub/Sub Documentation | Google Cloud. Available online: https://cloud.google.com/pubsub/docs/overview?hl=en (accessed on 28 March 2024).
61. Senjab, K.; Abbas, S.; Ahmed, N.; ur Rehman Khan, A. A Survey of Kubernetes Scheduling Algorithms. *J. Cloud Comput.* **2023**, *12*, 87. [CrossRef]
62. Dizdarevi'c, J.; Michalke, M.; Jukan, A. Engineering and Experimentally Benchmarking Open Source MQTT Broker Implementations. *arXiv* **2023**, arXiv:2305.13893.
63. Ramyasri, G.; Ramana Murthy, G.; Itapu, S.; Mohan Krishna, S. Data Transmission Using Secure Hybrid Techniques for Smart Energy Metering Devices. In *e-Prime-Advances in Electrical Engineering, Electronics and Energy*; Elsevier: Amsterdam, The Netherlands, 2023; Volume 4, p. 100134. [CrossRef]
64. Yudha Erian Saputra, M.; Noprianto; Noor Arief, S.; Nur Wijayaningrum, V.; Syaifudin, Y.W. Real-Time Server Monitoring and Notification System with Prometheus, Grafana, and Telegram Integration. In Proceedings of the 2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS), Manama, Bahrain, 28–29 January 2024; pp. 1808–1813. [CrossRef]
65. Aghaei, M. Autonomous Monitoring and Analysis of Photovoltaic Systems. *Energies* **2022**, *15*, 5011. [CrossRef]
66. Naderi, E.; Asrari, A. Stealthy False Data Injection Cyberattack Targeting under Load Tap Changing Transformers in Smart Power Grid Causing Abnormal Voltage Profile. In Proceedings of the 2024 3rd International Conference on Power, Control and Computing Technologies (ICPC2T), Raipur, India, 18–20 January 2024; pp. 145–150. [CrossRef]
67. Naderi, E.; Asrari, A.; Ramos, B. Moving Target Defense Strategy to Protect a PV/Wind Lab-Scale Microgrid Against False Data Injection Cyberattacks: Experimental Validation. In Proceedings of the 2023 IEEE Power & Energy Society General Meeting (PESGM), Orlando, FL, USA, 16–20 July 2023. [CrossRef]
68. Naderi, E.; Asrari, A. Experimental Validation of a Remedial Action via Hardware-in-the-Loop System Against Cyberattacks Targeting a Lab-Scale PV/Wind Microgrid. *IEEE Trans. Smart Grid* **2023**, *14*, 4060–4072. [CrossRef]
69. Naderi, E.; Asrari, A. Detection of False Data Injection Cyberattacks: Experimental Validation on a Lab-Scale Microgrid. In Proceedings of the 2022 IEEE Green Energy and Smart Systems (IGESSC), Long Beach, CA, USA, 7–8 November 2022. [CrossRef]
70. Abdul-Jabbar, S.S.; Farhan, A.K.; Ghani, R.F. Data Analytics and Blockchain: A Review. *IRAQI J. Comput. Commun. Control. Syst. Eng.* **2023**, *23*, 23–34. [CrossRef]
71. Blockchain Database: A Comprehensive Guide | MongoDB. Available online: https://www.mongodb.com/resources/basics/databases/blockchain-database (accessed on 10 May 2024).