energies

MDPI

Article

A Survey on IoT-Based Smart Electrical Systems: An Analysis of Standards, Security, and Applications

Chiara Matta [1], Sara Pinna [1], Samoel Ortu [1], Francesco Parodo [2], Daniele Giusto [1] and Matteo Anedda [1,*]

[1] Department of Electric and Electronic Engineering (DIEE), University of Cagliari (UniCA), 09124 Cagliari, Italy; c.matta20@studenti.unica.it (C.M.); s.pinna62@studenti.unica.it (S.P.); s.ortu26@studenti.unica.it (S.O.); ddgiusto@unica.it (D.G.)
[2] Dauvea srl, 09123 Cagliari, Italy; parodo@dauvea.it
* Correspondence: matteo.anedda@unica.it

Abstract

The rapid integration of Internet of Things (IoT) technologies is transforming electrical power systems into intelligent, interconnected, and data-driven infrastructures, enabling advanced monitoring, control, and optimization across the entire energy value chain. IoT-based smart electrical systems enable advanced monitoring, control, and optimization of energy generation, distribution, and consumption, while also introducing new challenges related to interoperability, security, scalability, and data management. Despite the growing body of literature, existing surveys typically address these challenges in isolation, focusing on individual technological or operational aspects and thus failing to capture their strong cross-dependencies in real-world deployments. This paper delivers a comprehensive survey that systematically analyzes and interrelates nine key dimensions that prior literature largely examines in separate silos: architectural models, communication protocols, reference standards, cybersecurity and privacy mechanisms, data processing paradigms (edge, fog, and cloud), interoperability solutions, energy management strategies, application scenarios, and future research directions. Unlike conventional reviews confined to single-layer or domain-specific perspectives, this survey adopts a holistic, cross-layer approach, explicitly linking architectural choices, protocol stacks, interoperability frameworks, and security mechanisms with application and energy management requirements.

Keywords: Internet of Things (IoT); smart electrical systems; communication standards; cybersecurity; interoperability; smart grid; edge computing; energy management systems

Academic Editors: Ferdinanda Ponci and Joao Ferreira

Received: 14 December 2025
Revised: 30 January 2026
Accepted: 9 February 2026
Published: 12 February 2026

1. Introduction

The rapid digital transformation of the energy sector [1] is reshaping the foundations, operations, and future trajectories of electrical systems worldwide. Traditional power infrastructures, once characterized by centralized generation, unidirectional flows, and limited observability, are increasingly giving way to a new paradigm defined by connectivity, automation, distributed intelligence, and pervasive sensing. At the heart of this shift lies the Internet of Things (IoT), a technological ecosystem enabling seamless interaction between physical electrical assets and digital systems [2]. Networks of interconnected sensors, actuators, gateways, and intelligent platforms empower these systems to gather high-resolution data, interpret dynamic conditions, and respond autonomously to real-time events—overcoming the rigidity and inefficiencies of legacy infrastructures. This omnidirectional sensing ushers in a new era for smart grids, where heterogeneous sensor networks

deliver comprehensive, real-time visibility across the energy infrastructure. Vibration and temperature sensors on electric motors, for instance, enable predictive maintenance by spotting early bearing wear or imbalance via spectral vibration analysis, averting costly downtime [3]. Likewise, current leakage detectors, overload monitors, and thermal imaging tools provide vigilant oversight of hazards like ground faults, phase imbalances, short circuits, and overheating—triggering alarms and automated responses such as circuit breaker activation or load shedding to prevent fires, shocks, or cascading failures [4]. This sensor-driven intelligence bolsters reliability while enabling proactive grid stewardship in IoT deployments.

This evolution toward IoT-based smart electrical systems stems from the mounting complexity of the energy landscape and the pressing need to weave in renewables, electrified mobility, storage, and demand-side flexibility. As decarbonization and resilience goals intensify, must embrace unprecedented decentralization and variability. Photovoltaic arrays, electric vehicles, home automation, industrial controls, building management, and advanced metering now fringe the grid [5], bringing fresh capabilities alongside novel challenges [6]. IoT serves as the vital substrate, harmonizing these elements through real-time monitoring, distributed control, and data-driven optimization across the energy value chain.

IoT adoption has since transcended early smart-home pilots permeating residential, commercial, industrial, and utility-scale realms [7]. Smart homes harness interconnected devices for optimized consumption and comfort; smart buildings deploy sensor networks and predictive controls to cut costs and emissions [8]. Industry 4.0/5.0 embeds IoT sensing into production for enhanced efficiency and sustainability. At grid level, IoT powers Smart Grids with bidirectional flows, adaptive control, and synergy among distributed resources [9]. With billions of devices set to anchor electrical infrastructures, IoT stands as indispensable to sustainable, intelligent energy futures. This progression has unfolded temporally and geographically: the 1990s pioneered ICT remote monitoring, the 2000s birthed Smart Grids for DER integration, and post-2010 saw full-scale IoT/AI deployment—via regulatory frameworks in Europe/USA and ubiquitous sensors/UHV tech in Japan/China. A recent exemplar from the state of the art underscores how IoT convergence in critical systems amplifies cybersecurity risks, calling for sophisticated data-driven defenses. In autonomous vehicles, ML classifiers (KNN, XGBoost) tuned by modified PSO achieve over 89% accuracy in detecting CAN intrusions [10]; similarly, hybrid deep models (CNN-DBN, Bi-LSTM-GRU) optimized via novel metaheuristics boost intrusion detection across IoT cyberattacks [11]. Yet despite its promise, IoT integration into electrical systems poses pressing challenges. Device, platform, and protocol proliferation breeds interoperability hurdles, especially where IT meets entrenched OT standards—demanding middleware to bridge data formats and paradigms, lest deployments fragment into inefficiency.

No less urgent are security imperatives amid the expanding IoT attack surface. Resource-constrained devices struggle with robust cryptography, exposing them to eavesdropping, man-in-the-middle, DoS, botnets, and disruptive intrusions that imperil energy operations [12]. As infrastructures digitize, safeguarding confidentiality, integrity, authenticity, and availability proves vital for reliability and public safety—yet nonuniform mechanisms across IoT technologies demand tailored, rigorous analysis for electrical contexts. Existing surveys on IoT-based smart electrical systems, while valuable, examine key dimensions—architectural models, communication protocols, standards, cybersecurity/privacy, data processing paradigms (edge/fog/cloud), energy management, and applications—in fragmented silos, obscuring cross-disciplinary optimization pathways. For instance, reviews focused on security [5] or protocols [13] neglect architectural shifts and interoperability, while energy-centric works [14] overlook holistic IT/OT convergence.

Quantitative analyses reveal that over 80% of recent surveys (2020–2025) address fewer than four dimensions, limiting their guidance for integrated deployments. This survey addresses these gaps through a systematic literature review detailed in Section 2. Unlike prior narrative reviews, we introduce novel cross-layer taxonomies (e.g., linking edge latency reductions to OT protocol mappings and cybersecurity mitigations) that reveal previously underexplored synergies, such as unified V2G/EMS frameworks for real-world IoT ecosystems. Section 9 quantifies our holistic scope against fragmented predecessors, positioning this work as the first comprehensive roadmap for practitioners and researchers navigating smart electrical transformations. This survey delivers exactly that across nine sections: state-of-the-art review (Section 3, grounded in Section 2's PRISMA workflow), IoT-based Smart Electrical Systems (Section 4), standards/protocols (Section 5), technologies/interoperability (Section 6), energy strategies (Section 7), use cases (Section 8), security (Section 9), and findings/future directions (Section 10)—weaving disparate threads previously siloed, unlike conventional reviews.

2. Research Methodology

To ensure a rigorous and comprehensive analysis of the state-of-the-art, this survey was conducted following a systematic literature review approach. The methodology employed for article selection and analysis is detailed below.

2.1. Database and Search Strategy

The systematic literature search and review process was conducted over a period of more than six months. The primary indexing engine utilized for this study was Google Scholar, chosen for its extensive coverage of academic literature across multiple disciplines. This allowed for the retrieval of documents from major authoritative repositories, including MDPI, IEEE Xplore and ScienceDirect, as well as other relevant academic sources.

The search strategy relied on a combination of keywords aimed at covering the intersection of Internet of Things (IoT) technologies and electrical power systems. The search strings were constructed using Boolean operators (AND, OR) to combine the following core terms:

- Core Domains: "Internet of Things" (IoT), "Smart Grid", "Internet of Energy" (IoE), "Smart Electrical Systems";
- Enabling Technologies & Protocols: "Communication Protocols", "Networks", "5G/6G", "Edge Computing", "Cloud Computing";
- Applications & Management: "Smart Home", "Smart Building", "Energy Storage Systems", "Energy Optimization", "Energy Management Systems" (EMS), "Demand Response";
- Cross-cutting Issues: "Cyber Security", "Privacy", "Data Protection", "Interoperability", "Blockchain".

2.2. Inclusion and Exclusion Criteria

To ensure the relevance and currency of the survey, the screening process was guided by the following criteria:

- Language: only full-text articles written in English were considered.
- Timeframe: a specific preference was given to articles published in the last 5 years (2020–2025) to capture the most recent technological advancements. However, foundational works and highly cited papers from the last 10 years (2015–2025) were also included to provide necessary context and theoretical background.
- Source Reliability: priority was assigned to peer-reviewed journals and conference proceedings from recognized publishers (e.g., MDPI, IEEE, ScienceDirect). Grey

literature and non-indexed sources were largely excluded unless representing official technical standards.

2.3. Selection Process (PRISMA)

The selection workflow adhered to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines. As illustrated in Figure 1, the initial search yielded about 1200 records. After removing duplicates and screening titles and abstracts for relevance, 900 records were retained for closer inspection. A substantial number (750) were excluded at this stage due to being outside the scope (e.g., purely theoretical IoT without grid application) or outside the selected timeframe.

Subsequently, 150 full-text articles were assessed for eligibility. During this phase, 50 articles were excluded primarily due to insufficient technical depth, lack of peer review, or a generic focus on IoT not specific to electrical systems. This rigorous filtering process resulted in a final core set of 100 high-quality studies that form the basis of this survey.

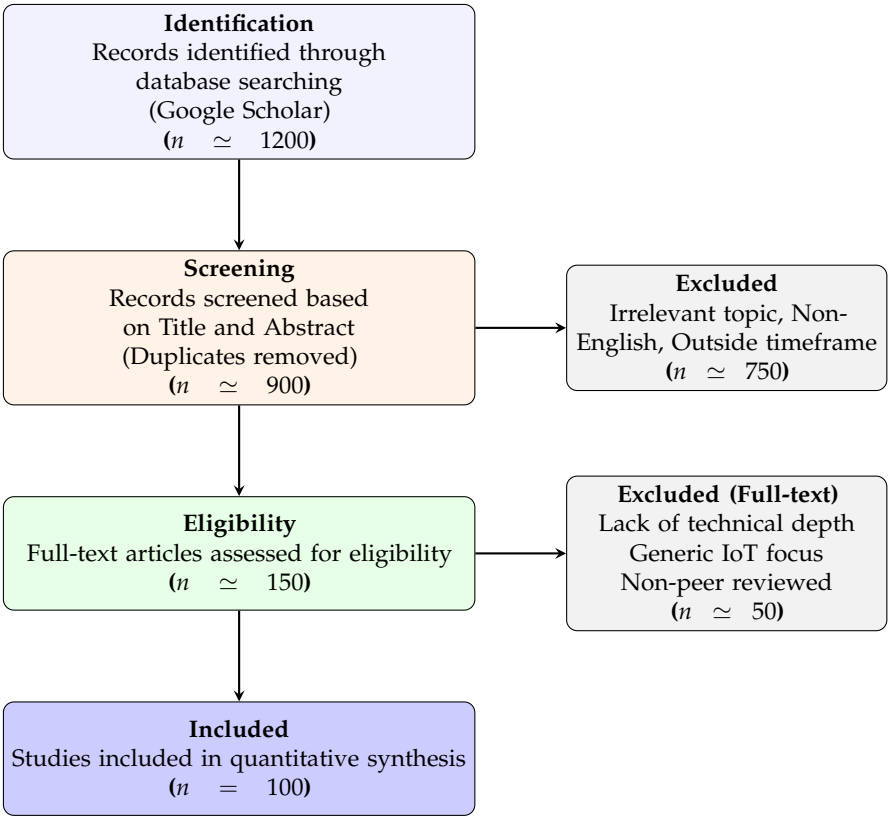

Figure 1. Flow diagram illustrating the selection methodology. From an initial pool of 1200 records, 100 high-quality studies were selected for the final review.

3. State of the Art

Drawing from the systematic literature review outlined in Section 2—which screened about 1200 records—this section synthesizes emergent trends in IoT-based smart electrical systems. Key findings reveal persistent silos in prior work: architectural shifts (e.g., edge computing), IT/OT interoperability challenges (e.g., middleware mapping), and cyber-security vulnerabilities (e.g., DDoS in expanded attack surfaces). These gaps underscore the need for a holistic, cross-dimensional analysis. The evolution of electrical systems represents a fundamental paradigm shift that has unfolded through distinct historical phases, marking the transition from traditional power grids to Smart Grids and, more recently, towards the Internet of Energy (IoE).

While the 1990s marked the first step towards automation with the introduction of ICT-based remote monitoring systems, the early 21st century saw the emergence of the Smart Grid concept, driven by the urgent need to integrate Distributed Energy Resources (DERs) to meet decarbonization goals. Since 2010, the sector has entered a new phase of "full deployment," characterized by the deep integration of the Internet of Things (IoT), Big Data, and Artificial Intelligence. This transition has been geographically diversified: while Europe and the United States focused on regulatory frameworks for renewable integration and demand response markets, countries like Japan and China prioritized the deployment of ubiquitous smart sensors and Ultra-High Voltage (UHV) technologies [15].

As illustrated in Figure 2, this trajectory underscores the transition from a centralized model to a distributed and interconnected one. Traditionally, the electrical grid was characterized by a centralized and unidirectional structure. It was designed primarily to transmit energy from large power plants to end consumers, with limited real-time monitoring capabilities and minimal integration of renewable sources [16]. However, the growing demand for energy, the need to reduce carbon emissions, and the integration of Distributed Energy Resources (DER) have necessitated the modernization of the infrastructure. The embedding of the Internet of Things (IoT) into power grids has transformed conventional infrastructures into Smart Grids, significantly improving efficiency, reliability, and sustainability through bidirectional monitoring and control [5]. A crucial aspect of this evolution concerns the data processing architecture. While early Smart Grid implementations relied heavily on Cloud Computing for data analysis, the vast volume of data generated by IoT devices and the need for low latency have exposed the limitations of a purely centralized approach [17].

Why is a shift from centralized Cloud to distributed Edge computing necessary? The primary driver is the need to handle the massive volume of data with the low latency required for grid stability.

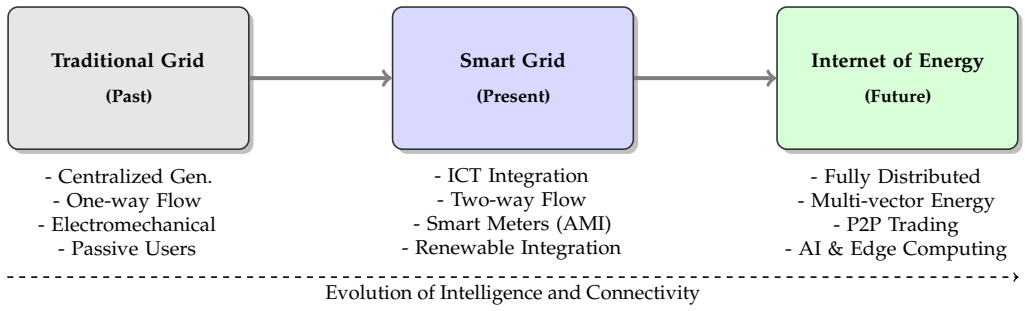

Figure 2. Evolutionary path from Traditional Grids to the Internet of Energy (IoE).

Consequently, the architecture is shifting towards Edge and Fog Computing models. This decentralized approach allows data to be processed closer to the source (sensors and field devices), reducing latency and bandwidth consumption, and improving system resilience against network interruptions [18].

Traditional cloud-centric Smart Grid models, prevalent in pre-2020 literature , face scalability limits due to IoT-generated data volumes exceeding 10 TB daily in urban grids, necessitating low-latency processing. Recent studies advocate edge/fog paradigms, reporting latency reductions of up to 50% in real-time fault detection [19]. However, quantitative benchmarks remain sparse, with peer-reviewed validations limited to simulations rather than field deployments. This transition aligns with standards like IEC 61850 [20], yet integration with lightweight IoT protocols demands further empirical scrutiny.

Regarding the interoperability challenges and IT/OT gaps, legacy OT protocols (e.g., DNP3, IEC 61850) prioritize real-time determinism, clashing with IT/IoT standards

like MQTT, which favor flexibility but introduce overhead [13]. Middleware and gateways offer mapping solutions (e.g., IEC 61850 to JSON/MQTT), enabling bidirectional flows in AMI/DSM; nonetheless, surveys indicate fragmented adoption, with <30% of studies addressing cross-layer validation. Authoritative frameworks such as NIST SP 800-213 highlight unresolved semantic mismatches, amplifying deployment inefficiencies [20]. Moreover, concerning the security landscape, IoT proliferation expands the Smart Grid attack surface, with documented rises in DDoS, false data injection (FDI), and device tampering [21]. Peer-reviewed analyses report detection accuracies >89% via ML hybrids (e.g., CNN-BiLSTM), but energy-constrained nodes limit cryptographic feasibility [22]. Unlike siloed security reviews, holistic integration of physical-cyber defenses from design phases remains underexplored, per NIST guidelines.

Existing surveys on IoT-based smart electrical systems remain fragmented, addressing dimensions in isolation rather than through integrated frameworks—a limitation evident across recent peer-reviewed works. For instance, while refs. [5,22] offer valuable insights into cybersecurity and applications, they overlook architectures, protocols, and energy management, reducing their utility for cross-disciplinary deployments. Similarly, ref. [13] excels in protocol-interoperability analysis but neglects security and application contexts, while ref. [14] covers architectures and energy strategies yet ignores standards and holistic IT/OT convergence.

In contrast, this survey synthesizes nine interconnected dimensions—architectural models, communication protocols, reference standards, cybersecurity/privacy, data processing paradigms (edge/fog/cloud), energy management strategies, application scenarios, interoperability solutions, and future directions—via novel cross-layer taxonomies that explicitly link, for example, edge computing latencies to OT protocol mappings and security mitigations . Unlike prior works confined to silos (e.g., security-only in or protocol-focused in), our approach reveals optimization pathways obscured by fragmentation, such as unified V2G/EMS frameworks absent in 80% of reviewed studies. This comprehensive positioning equips researchers and practitioners with actionable intelligence for real-world IoT-driven electrical ecosystems.

4. Overview of IoT-Based Smart Electrical Systems

By integrating physical devices with digital intelligence, the IoT serves as the framework for autonomous and highly responsive electrical infrastructures. In smart grids, this integration transforms traditional unidirectional energy distribution into a dynamic network where energy and information flow bidirectionally [23]. The following sections offer an overview of the foundational concepts that underpin IoT technologies and the architectural frameworks that allow them to organize and manage their functionality effectively.

4.1. Foundational Concepts of IoT

IoT's architecture is based on an integrated ecosystem in which interaction occurs between the physical and digital worlds. The fundamental elements of this system are sensors, actuators, and connectivity. Sensors are devices capable of detecting and measuring physical properties by converting chemical-physical effects into useful informational signals. For smart electrical systems, these sensors are critical for monitoring real-time voltage, current, and frequency, enabling the grid to react to fluctuations instantly. The category of sensors ranges from simple RFID tags (Radio-Frequency IDentification), essential for the unique identification and tracking of objects [23], to active "smart sensors" that perform complex processing of primary data. Two functional macro-categories can be identified [24]:

- Passive Sensors: these respond to external stimuli from the observed object without requiring an internal power source for the sensing mechanism.

- Active Sensors: these emit energy to interact with the observed object and detect the resulting reflections or environmental variations.

Complementing sensors are actuators—devices that receive digital commands and execute corresponding physical actions. In the context of the smart grid, actuators play a decisive role in automated demand response, such as remotely disconnecting non-essential loads or switching power sources during an outage [25]. Sensors and actuators constitute the "Perception Layer" of the IoT architecture but with opposite operational functions: sensors are used for monitoring purposes, converting physical parameters into electrical signals, whereas actuators are responsible for operating within the surrounding environment [26].

Interconnectivity between these components is maintained through communication protocols that guarantee data exchange and interoperability. These include short-range technologies such as NFC, Bluetooth, and Zigbee; long-range solutions such as LoRaWAN; and Machine-to-Machine (M2M) communication paradigms that allow devices to autonomously exchange information. M2M is particularly vital for smart grids as it facilitates the direct interaction between smart meters and utility control centers without human intervention [14].

Finally, data processing is handled by various functional units through microcontrollers and microprocessors tasked with executing local algorithms. At a higher level, middleware acts as a software interface that abstracts hardware complexity by managing service composition, security, and privacy, relieving the programmer from detailed knowledge of the underlying technologies [23]. This abstraction is fundamental for the smart grid to ensure interoperability between heterogeneous legacy power systems and modern digital controllers [27]. Processing extends to gateways and cloud services, which aggregate data from sensors and provide the necessary infrastructure for advanced analysis and storage [25].

Table 1 provides a structured overview of the key architectural components, methodologies, and applications in Smart Electrical IoT systems.

Table 1. Summary of architectural elements, methodologies and functions in Smart Electrical IoT.

Element/Concept	Description and Methodology	Application in Smart Electrical Systems
Perception (Sensors)	Conversion of physical/chemical effects into informational signals [24].	Real-time monitoring of grid parameters like voltage, current, and phase [24].
Action (Actuators)	Execution of physical actions based on processed digital data [25,26].	Remote circuit breaking, load shedding, and automated switchgear operation [25].
Connectivity	Use of short-range (ZigBee) and long-range (LoRaWAN) protocols [14].	Reliable communication between Smart Meters and the Data Aggregation Point [14,26].
M2M Paradigm	Autonomous data exchange between devices without human intervention [14].	Automated meter reading (AMR) and self-healing grid protocols [14].
Abstraction Layer	Software middleware that hides hardware heterogeneity [23,27].	Integration of different brands of smart meters and legacy electrical equipment [27].
Strategic Management	High-level data analysis for performance and strategic decisions [27].	Definition of dynamic pricing models and profit analysis for utilities [27].
Edge/Cloud Units	Local (microcontrollers) and remote (cloud) processing units [25].	Fast local fault detection vs. long-term energy consumption analytics [25].

4.2. Architectural Layers

IoT systems facilitate the interconnection of a vast array of devices, necessitating robust mechanisms for managing high-volume data traffic and big data analytics. Accordingly, the proposed architecture must adhere to various principles such as scalability, quality

of service, and reliability. In electrical grids, reliability and low latency are paramount to prevent power failures during data congestion [27]. The traditional model includes three layers, illustrated in Figure 3, namely: (1) the Perception Layer, which consists of objects and sensors responsible for identifying elements in the environment and collecting data; (2) the Network Layer, responsible for transporting and preliminarily processing the information coming from the underlying layer; (3) the Application Layer, which provides services and applications based on the data collected and transmitted by the lower layers.

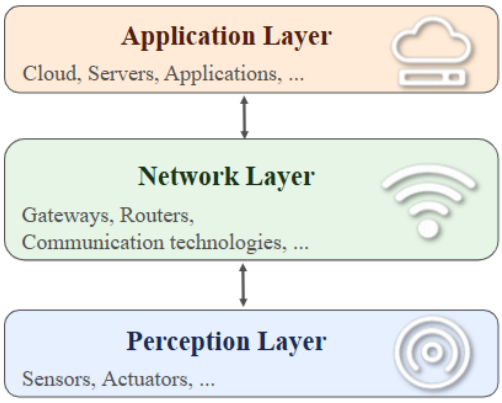

Figure 3. Three-Layer IoT Architecture.

By combining the TCP/IP model, the TMN model, and specific IoT characteristics, a new five-layer hybrid architecture is proposed, shown in Figure 4. The first level, the Object Layer, is responsible for sensing, collecting, and digitizing information through heterogeneous sensors and actuators, generating Big Data transmitted through secure channels. In smart grids, this layer includes Phasor Measurement Units (PMUs) and smart meters. The data is then passed to the Object Abstraction Layer, which handles transport and networking and, through the concept of abstraction, manages protocols, security, and quality of service.

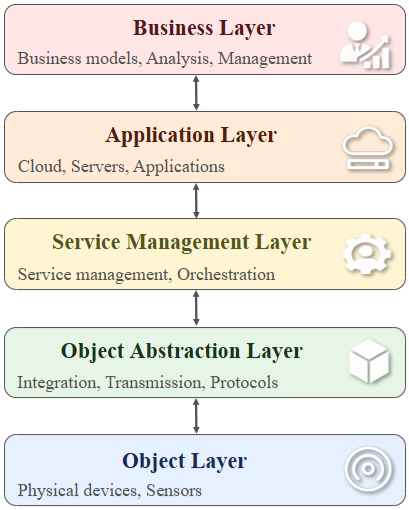

Figure 4. Five-Layer IoT Architecture.

The Service Management Layer analyzes, processes, and stores large volumes of data received. These data then move to the Application Layer, which provides specific services based on customer needs, such as real-time energy billing or fault detection. Finally, the Business Layer manages the entire IoT ecosystem, assessing performance, defining business and profit models, and supporting strategic decision-making through data analysis performed by the lower layers [27].

5. Communication Standards and Protocols

In IoT systems, the balance between consumption, coverage, latency, and reliability is largely determined by the choice of communication protocol, which operates across the three-level architecture: the perception layer, including sensors and actuators for data collection; the transmission layer, responsible for data transfer via appropriate protocols and channels; and the application layer, which processes and delivers the data to users. In the specific context of the smart grid, this architecture facilitates the bidirectional flow of information necessary for Advanced Metering Infrastructure (AMI) and Demand Side Management (DSM), connecting power generation, distribution, and consumption points. Specifically for smart electrical systems, the perception layer handles the precise measurement of electrical parameters, while the transmission layer must ensure that critical grid events, such as sudden voltage drops or equipment failures, are communicated with minimal delay to prevent cascading effects [28].

In the network layer, it is possible to distinguish short-range protocols such as Wi-Fi, Bluetooth, Zigbee, and Z-Wave, characterized by limited range but lower power consumption; and long-range protocols such as LoRaWAN, SigFox, and NB-IoT, which provide extended coverage up to kilometers while maintaining low energy demand. The former are therefore more suitable for domestic and industrial contexts, while the latter provide effective solutions for scenarios where device longevity and network scalability are important requirements [29].

5.1. Short-Range Standards

The choice of the short-range standard depends on the balance between consumption, network capacity, and application requirements.

Wi-Fi (IEEE 802.11) is the most widely used technology, characterized by high throughput and direct IP connectivity. Given its high consumption (100–350 mA according to [30]), it is suitable for applications requiring continuous power supply [31]. In a smart grid context, its high data rate capability makes it suitable for specific applications such as linking smart meters to in-home displays or facilitating video monitoring in substations where power is readily available. Furthermore, it is leveraged for Home Energy Management Systems (HEMS) that require high-frequency sampling of power quality data.

ZigBee (IEEE 802.15.4) is optimized for low-power and low-data-rate communication and is widely used in IoT scenarios due to its scalability and support for large mesh networks. This technology is dominant in home area networks (HAN) of smart grids due to its ability to integrate with monitoring and home control systems. A key advantage for electrical systems is its ability to create self-healing mesh networks, which ensures that even if one smart appliance or meter fails, the energy consumption data can still reach the central gateway through alternative nodes [32]. ZigBee is particularly effective for monitoring individual appliances and implementing demand response programs to reduce peak load.

Bluetooth (IEEE 802.15.1), particularly in the Low Energy (BLE) version, represents an intermediate option for personal and wearable devices. In a smart home environment, it enables the user to connect mobile devices to energy controllers for local monitoring of consumption data without requiring a complex network infrastructure [28].

Z-Wave, operating in sub-GHz bands, provides a stable signal and low latency with greater signal penetration and reduced interference compared to the 2.4 GHz bands [30]. For residential energy management, Z-Wave offers the advantage of not interfering with existing Wi-Fi networks while enabling reliable remote control of smart plugs and lighting, which is essential for automated energy-saving routines.

Table 2 compares the technical characteristics among the standards presented.

Table 2. Comparison of Short-Range Technologies.

Standard	Power Consumption	Data Rate	Topology
Wi-Fi	100–350 mA [30]	up to 300 Mbps [28] 9.6 Gbps	Star/Mesh [28]
ZigBee	≈100 mW [32]	250 kbps [28]	Mesh [28]
BLE	1–35 mA [30]	up to 2 Mbps [28]	Piconet/Scatternet [28]
Z-Wave	≈1 mW [32]	100–200 kbps [28]	Mesh [28]

5.2. Long-Range Standards

Long-range technologies represent a fundamental solution for large-scale, low-power applications. These technologies support the Neighborhood Area Network (NAN), aggregating data from multiple smart meters to data collection points for transmission to the utility. According to [28], approximately 86% of IoT devices connect using three LPWAN technologies: LoRaWAN, NB-IoT, and Sigfox. Table 3 compares the technical characteristics among the long-range standards presented.

From an energy efficiency perspective, Sigfox is often reported as the most power-efficient LPWAN technology, followed by LoRaWAN, whereas NB-IoT tends to be less energy-efficient due to its reliance on cellular infrastructure and more complex signaling procedures [31]. However, experimental data shows that while Sigfox is extremely energy-efficient, it can suffer from packet loss in dense urban environments due to its ultra-narrowband nature, which could be problematic for real-time grid monitoring [33].

Among LPWAN technologies, LoRaWAN is frequently evaluated for smart grid communications because of its scalability, energy efficiency, and extended coverage [28,31]. Specific applications, such as outage detection or management, are typically studied at the network or AMI level rather than being protocol-specific [28]. Conversely, NB-IoT is based on licensed frequencies and ensures greater reliability [28,31], making it highly suitable for utility metering in dense urban environments where interference is a major concern [34].

Table 3. Comparison of Long-Range Technologies for Smart Metering.

Standard	Energy Efficiency	Latency	Reliability in Smart Grids
LoRaWAN	Ultra-low consumption [30,31]	NAN-compliant (1–15 s) [28]	High interference robustness (CSS modulation) [31,34]
NB-IoT	Coverage-dependent efficiency [31]	Fast response, near real-time [28,31]	Carrier-grade reliability (licensed spectrum) [31]
Sigfox	IoT energy benchmark [31]	Optimized for periodic, non-critical transmissions [28,31]	Congestion-sensitive in dense urban areas [34]

5.3. Application Layer Protocols

Application layer protocols manage IoT device communication, directly influencing efficiency. Message Queuing Telemetry Transport (MQTT) is a TCP-based publish/subscribe protocol designed for remote monitoring over fragile networks. In a smart grid scenario, smart meters act as publishers sending consumption data to the broker, which then routes information to utility billing systems [35]. MQTT's Quality of Service (QoS) levels are essential for control commands (e.g., disconnecting a load), where losing a packet is not an option [36].

In contrast, the Constrained Application Protocol (CoAP) is a UDP-based protocol designed to reduce overhead and energy consumption [36]. Technical evaluations show that CoAP reduces significantly the communication overhead compared to HTTP, allowing utilities to collect more frequent data points without draining the batteries of remote sensors.

From an energy perspective, transport is crucial: TCP (used by MQTT) requires persistent connections and delivery acknowledgments, increasing consumption. UDP (used by CoAP) allows lighter communications. However, security implementation remains a challenge; studies indicate that encryption (TLS for MQTT or DTLS for CoAP) can increase energy consumption, a factor that grid operators must consider when planning the 10–15 year lifecycle of smart meters.

In the case of MQTT-SN (the UDP-based version), clients can enter "sleep" mode, enabling significant energy savings. Total consumption between MQTT-SN and CoAP is very similar, with MQTT-SN being slightly more efficient due to lower client complexity [35]. Ultimately, the integration of these protocols enables the transition to smart grids, supporting advanced functions like outage management, fraud detection, and the integration of distributed renewable energy resources.

The technical specifications and the differences between these solutions are summarized in Table 4.

Table 4. Comparison of Application Protocols.

Protocol	Description	Focus Smart Grid / IoT
MQTT	TCP-based publish/subscribe protocol designed for high reliability and many-to-many communication [36].	Ideal for grid control commands where delivery must be guaranteed via QoS levels [36].
CoAP	UDP-based request/response protocol (RFC 7252) with low overhead and binary header [36].	Optimized for frequent periodic readings from battery-powered smart meters to save energy [36].
HTTP	Standard text-based client-server protocol using TCP, characterized by high overhead [29].	Used primarily for integration with existing web infrastructures and non-constrained back-end services.
MQTT-SN	UDP-based version of MQTT specifically for sensor networks, supports a "sleep" mode for clients [36].	Offers a balance between MQTT's logic and the low energy requirements of wireless sensor nodes [28].
Security	Cryptographic protocols providing authentication and data encryption (TLS for TCP, DTLS for UDP) [36].	Essential for Smart Grid security, although its energy impact must be considered over the meter lifecycle [28,36].
QoS Levels	Mechanisms in MQTT to ensure message delivery (0: At most once, 1: At least once, 2: Exactly once) [36].	Level 2 is crucial for critical grid operations like remote disconnection to avoid command duplication or loss [36].
Overhead	The ratio of control data to actual payload data in a communication packet [35].	Reduces unnecessary traffic, improving bandwidth efficiency in NAN/AMI networks [28,36].
Observing	A CoAP feature that allows a server to push updates to a client when a resource state changes [36].	Useful for "event-driven" monitoring, such as immediate notification of a voltage threshold violation [28].

After discussing short-range, long-range, and application-layer communication protocols, it is useful to summarize their characteristics in a single comparative overview. Table 5 presents a synthesis of the key protocols, highlighting their trade-offs in energy efficiency, latency, and typical use cases in Smart Electrical Systems. This allows for a quick comparison and aids in selecting the most suitable protocol for specific IoT applications.

Table 5. Synthesis of protocol performance and suitability for Smart Electrical Systems.

Protocol	Energy Eff.	Latency	Primary Characteristics and Use Cases
Wi-Fi	Low (100–350 mA [30])	Very Low	Power quality monitoring and high-frequency Home Energy Management System (HEMS) sampling [28].
ZigBee	High (1–10 mA [30])	Low	Self-healing mesh networks for demand response and home control [28].
Z-Wave	High (≈10 mW [30])	Low/Stable	Remote control of smart plugs and lighting with reduced interference [28].
LoRaWAN	Very High [31]	Medium	Wide-range monitoring and robust communication in urban areas [31,34].
NB-IoT	Medium [31]	Variable	Reliable utility metering in dense urban environments using licensed spectrum [31].
MQTT	Medium (TCP [36])	Low	Reliable control commands through QoS levels for grid assets [36].
CoAP	High (UDP [36])	Very Low	Frequent readings from battery-powered sensors with reduced overhead [36].

6. Technologies, Platforms, and Interoperability

The IoT ecosystem for energy management and building automation relies on a diverse array of platforms, protocols, and standards that facilitate integration and communication among heterogeneous devices [37,38]. These platforms constitute the critical infrastructure for Smart Homes, Smart Buildings, and Smart Grids, providing essential tools for consumption monitoring, automated management, and data security. Two primary architectural paradigms can be distinguished: commercial platforms, prioritizing high usability and vertical integration, and open-source or DIY (Do-It-Yourself) platforms, which emphasize flexibility, interoperability, and local data sovereignty. A taxonomy of these ecosystems, categorized by their architectural approach and target user base, is illustrated in Figure 5.

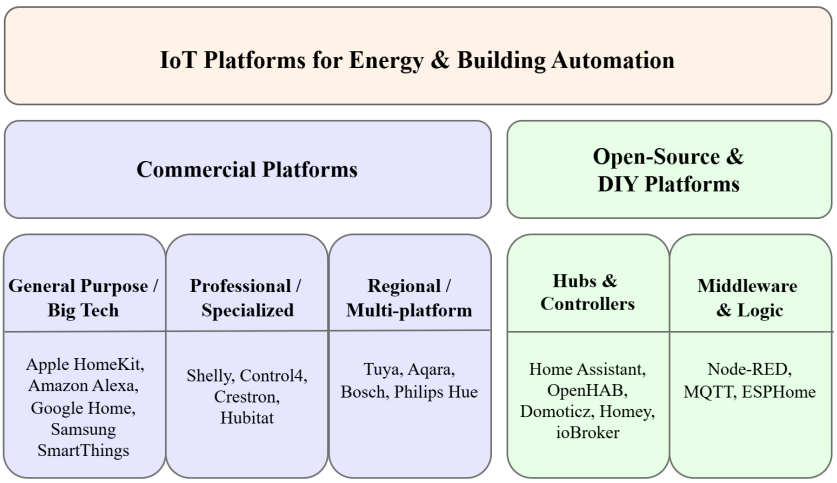

Figure 5. Landscape of IoT platforms for energy management and building automation. The diagram classifies solutions into Cloud-Centric (Commercial) and Local/Edge-Centric (Open-Source) architectures, highlighting key market players.

6.1. Commercial Platforms

Commercial IoT platforms currently dominate the market for smart device integration in both residential and professional settings. Predominantly cloud-centric, these architectures

prioritize user experience by offering "turnkey" environments where sensors, actuators, and digital services operate cohesively. Current market solutions fall into two distinct categories: general-purpose consumer ecosystems and specialized platforms for advanced automation and energy control. The first group includes widely adopted ecosystems such as Apple (HomeKit), Amazon (Alexa), Google (Home), and Samsung (SmartThings).

Functioning as centralized hubs, these systems enable device management via mobile applications or voice assistants. Their primary advantage lies in deep cloud service integration and the capability to execute automated routines that optimize comfort, safety, and energy efficiency [39]. However, from a research perspective, these ecosystems can operate effectively as 'black boxes.' They often restrict direct access to raw, granular sensor data, which may constrain their applicability in scenarios requiring precise demand-response mechanisms.

Despite their prevalence, these platforms face inherent structural constraints. Since device coordination occurs primarily on remote servers, they introduce challenges related to privacy, latency, and operational resilience, alongside the risk of vendor lock-in. While this closed model ensures stability, it limits the integration of third-party devices. Beyond consumer-grade solutions, the market includes professional platforms tailored for installers and advanced users. Solutions such as Shelly, Control4, Crestron, HomeSeer, Hubitat, Hornbach Smart Home, Cozify, Symcon, and Telldus offer a modular, configurable approach, frequently targeting HVAC, lighting, and energy control. Many of these systems support multiple communication protocols—including Zigbee, Z-Wave, Thread, Wi-Fi, and Bluetooth Low Energy (BLE)—and allow integration with third-party systems through APIs or dedicated gateways. While generally offering superior stability, their architectural structure can present challenges regarding scalability. The complexity of retrofitting and a tendency toward rigid configurations may render them comparatively less adaptable to the dynamic requirements of emerging Smart Grid standards.

In recent years, regional and multi-platform ecosystems such as a wide range of proprietary and vertical ecosystems has emerged, including Tuya Smart, Aqara Home, Bosch Smart Home, Philips Hue, Netatmo, Hive Home, Eve Systems, and IKEA Dirigera. These solutions are characterized by the adoption of interoperable protocols (Zigbee, Thread, Matter) and an increasing focus on energy efficiency and data security. The introduction of the Matter protocol has represented a major step forward toward the standardization of interoperability among heterogeneous ecosystems. Matter, together with the Thread network technology, enables secure and local communication between devices from different manufacturers (Apple, Google, Amazon, Samsung, IKEA), reducing market fragmentation and simplifying the user experience [40].

6.2. Open-Source and DIY Platforms

Conversely, open-source and DIY (Do-It-Yourself) platforms offer a flexible alternative for managing IoT systems. Driven by collaborative developer communities and open architectures, these solutions empower users to integrate multi-vendor devices and design highly personalized automations. Prominent platforms include Home Assistant, OpenHAB, Homey, Domoticz, ioBroker, Node-RED, Nymea, Homebridge, and ESPHome, which enable the creation of interoperable ecosystems based on open protocols such as MQTT, REST API, Modbus TCP, and CoAP [41].

A particularly notable example is Home Assistant, which allows local device management, energy monitoring, and the creation of complex automation scenarios through graphical interfaces or scripting. Similarly, OpenHAB and ioBroker offer modular architectures based on extensible components, facilitating the integration of Zigbee, Wi-Fi, and Modbus systems. Node-RED, developed by IBM, represents a low-code solution for automation flow creation, making it accessible even to non-expert users.

More recent open-source platforms adopt edge or fog-based architectures, moving part of the data processing closer to the devices to reduce latency, increase resilience, and improve privacy by design. This decentralized model allows greater data control and reduces dependency on cloud infrastructures, enhancing local interoperability and responsiveness in heterogeneous IoT environments [38]. A detailed synthesis of these architectural approaches, highlighting the key differences in interoperability and operational trade-offs between commercial and open-source models, is provided in Table 6.

At the research level, European initiatives such as INTER-IoT have proposed multi-layer interoperability frameworks — physical, syntactic, semantic, and organizational—to connect heterogeneous platforms in industrial and civil scenarios [42]. These frameworks represent a key step toward achieving technical convergence among diverse ecosystems and realizing a truly unified IoT infrastructure.

Table 6. Comparison of architectural approaches, interoperability, and trade-offs.

Approach	Key Concept	Interoperability	Trade-Offs
Commercial Platforms	Cloud-centric architectures; Integrated and user-friendly ecosystems aiming for a "turnkey" experience.	Adoption of standard protocols like Matter and Thread to improve cross-vendor compatibility.	Strengths: High usability, deep cloud integration, automated routines. Limitations: Privacy risks, latency, dependence on internet connection, vendor lock-in.
Open-Source & DIY Platforms	Open architectures prioritizing local control, flexibility, and collaborative development.	Universal bridging via open protocols (MQTT, REST API, Modbus TCP, CoAP).	Strengths: Data sovereignty, extreme customization, resilience (offline operation). Challenges: Higher technical complexity (setup & maintenance).
Edge/Fog Computing Trend	Decentralized model moving data processing closer to the devices (local intelligence).	Enhances local interoperability and responsiveness in heterogeneous environments.	**Strengths:** Reduced latency, improved *privacy by design* , greater operational resilience.

6.3. Strategies for Interoperability and Large-Scale Integration

To overcome interoperability limitations and enable large-scale IoT deployments across heterogeneous devices and vendors, compatibility must be addressed at multiple architectural levels. Rather than relying on a single technological choice, effective interoperability emerges from the coordinated adoption of communication standards, abstraction mechanisms, semantic alignment, and ecosystem-level governance.

- Adoption of Standardized Communication Protocols.
  The adoption of standardized communication protocols represents the first and most fundamental step toward reducing system integration complexity. Widely accepted protocols such as MQTT, CoAP, RESTful APIs, OPC UA, and AMQP provide common communication primitives that are independent of specific vendors or hardware implementations [43]. By converging toward shared standards, heterogeneous devices can exchange data using well-defined interaction models, potentially reducing integration effort by promoting shared interaction patterns and vendor-independent interfaces, although the realized benefit depends on legacy constraints, data-model alignment, and deployment scale [44]. In large-scale deployments, interoperability is further enhanced when manufacturers are encouraged to support at least one standardized protocol in parallel with proprietary solutions, or when protocol translation gateways are provided to ensure backward compatibility.

- Middleware and Integration Platforms.
  Middleware platforms play a central role in abstracting protocol heterogeneity by acting as intermediaries between devices and applications [45]. Through message brokers, integration frameworks, or cloud-based IoT platforms, middleware solutions decouple device-level communication from application logic, enabling devices to operate using their native protocols while exposing normalized interfaces to higher layers. This architectural separation can reduce tight coupling and simplify system evolution, enabling large-scale deployments to integrate heterogeneous devices without requiring changes at the application level.
- Data Format Standardization.
  Beyond communication protocols, interoperability critically depends on the standardization of data representations. Even when devices successfully exchange messages, inconsistent data formats can hinder effective integration and interpretation. The adoption of common data serialization formats such as JSON, Protocol Buffers, Apache Avro, or XML enables consistent data parsing and processing across platforms [46]. Defining canonical data models that capture shared semantics ensures that heterogeneous data sources can be interpreted uniformly, regardless of the originating device or protocol, thereby facilitating scalable analytics and control applications.
- API Gateway Architecture.
  API gateways provide a unifying architectural layer that consolidates access to heterogeneous IoT resources. By supporting protocol translation, data transformation, authentication, authorization, and rate limiting, API gateways can enable a consistent interaction model for applications operating over diverse device ecosystems [47]. This approach allows backend services to remain agnostic to device-specific protocols while enforcing centralized security and lifecycle management policies. As systems evolve, API versioning mechanisms further support long-term compatibility without disrupting existing integrations.
- Digital Twin Framework.
  Digital twin frameworks address interoperability by introducing a virtual abstraction of physical devices. Each physical asset is represented by a standardized digital counterpart that exposes uniform interfaces and behaviors, regardless of the underlying hardware or communication protocol [48]. Applications interact exclusively with digital twins rather than directly with devices, effectively isolating them from protocol heterogeneity. This abstraction not only simplifies integration but also enhances scalability, maintainability, and the ability to perform simulation, monitoring, and predictive analysis across large fleets of devices.
- Edge Computing and Protocol Converters.
  Edge computing architectures contribute to interoperability by localizing protocol conversion and data normalization close to the data source. Edge gateways collect information from devices using native protocols, translate it into standardized representations, and perform preprocessing before forwarding data to central systems [44]. This approach can reduce latency and bandwidth usage and improve resilience, particularly in geographically distributed deployments. Moreover, edge-based interoperability enables continued operation under limited or intermittent connectivity conditions.
- Semantic Interoperability.
  While syntactic compatibility ensures that data can be exchanged, semantic interoperability ensures that data is correctly understood. Semantic frameworks based on shared ontologies, standardized vocabularies, and metadata models enable consistent interpretation of data meaning across heterogeneous systems [48]. The use of schema

registries and standardized units of measurement, timestamps, and naming conventions further reduces ambiguity. This semantic alignment is particularly critical in large-scale applications, where data from diverse sources must be aggregated and analyzed coherently.

- Vendor Partnership and Certification Programs. Finally, interoperability at scale cannot be achieved solely through technical solutions but also requires organizational coordination. Vendor partnership and certification programs play a crucial role in fostering ecosystem-level compatibility by defining interoperability requirements, testing procedures, and compliance criteria. Certification schemes incentivize manufacturers to adopt common standards and provide assurance to system integrators regarding device compatibility. Industry consortiums and reference implementations further accelerate convergence toward interoperable solutions, reducing fragmentation and supporting sustainable large-scale adoption.

While several interoperability solutions are already mature and widely adopted at the protocol, middleware, and architectural levels, a fully uniform and seamless interoperability across heterogeneous IoT ecosystems remains challenging, particularly at scale. This limitation is not solely technical in nature, but also reflects the absence of a widely recognized and authoritative standardization body capable of coordinating and enforcing interoperability across multiple layers, including data models, semantics, and certification procedures. As a result, current solutions often remain fragmented, with partial standardization confined to specific domains, platforms, or vendor-driven ecosystems. Future research and industrial efforts should therefore focus not only on advancing semantic alignment and certification frameworks, but also on fostering stronger cross-industry governance mechanisms that can promote convergence toward truly interoperable, vendor-agnostic, and scalable IoT systems.

The above mentioned strategies summarized in Table 7 outline a comprehensive approach to mitigating protocol fragmentation and facilitating scalable integration.

Table 7. Interoperability strategies for large-scale IoT systems and their architectural roles.

Strategy	Interoperability Level	Primary Role
Standardized Communication Protocols	Syntactic/Transport	Reduce protocol fragmentation and enable cross-vendor communication
Middleware and Integration Platforms	Technical/Middleware	Abstract device heterogeneity and decouple devices from applications
Data Format Standardization	Data/Structural	Ensure consistent data representation and parsing across systems
API Gateway Architecture	Architectural	Provide unified access, security, and protocol translation
Digital Twin Framework	Logical/Application	Abstract physical devices through uniform virtual representations
Edge Computing and Protocol Converters	Physical/Network	Perform local protocol translation, reduce latency, and enhance resilience
Semantic Interoperability	Semantic	Align data meaning through shared ontologies and metadata models
Vendor Partnership and Certification	Organizational	Promote ecosystem convergence and validated interoperability

7. IoT-Enabled Integration of PV, Storage, and Grid Systems

The modern energy landscape is increasingly characterized by a high degree of heterogeneity, stemming from the integration of diverse energy resources. Prominent among these

are distributed renewable energy sources (RES), such as photovoltaic (PV) systems, various forms of energy storage—both stationary (batteries) and mobile (electric vehicles, EV)—and the traditional electrical grid infrastructure [49,50]. This transition towards more complex energy systems, often defined as the evolution towards the Internet of Energy (IoE) [51], necessitates advanced management and control mechanisms capable of harmonizing components with disparate technologies, communication protocols, and data formats [52,53]. The Internet of Things (IoT) serves as a pivotal enabling framework to orchestrate the interaction between these heterogeneous elements within Smart Energy Systems (SES), Smart Grids (SG), and Smart Cities [54,55]. The IoE, in particular, enables bidirectional flows of energy and information, fostering the deep integration of ICT technologies into the energy sector.

7.1. Heterogeneous Components in the IoE Ecosystem

Integration of IoT/IoE in the context of smart energy systems involves a wide range of heterogeneous components that must coexist and interact. Photovoltaic distributed generation (PV) represents an intrinsically stochastic renewable source, whose production depends on environmental factors, primarily solar irradiance and temperature [56]. Consequently, IoT systems are deployed to monitor these parameters in real-time, along with production and inverter status, to optimize yield and facilitate forecasting [53].

In the wind energy sector, Wind Energy Conversion Systems (WECS) are similarly evolving into intelligent nodes within the IoE. Modern induction generators, particularly Double Output Induction Generators (DOIG), leverage IoT to operate at variable speeds and optimize power extraction through Maximum Power Point Tracking (MPPT) [57]. IoT sensors continuously monitor critical parameters such as vibration, temperature, and wind speed, enabling predictive maintenance strategies that detect faults early and reduce downtime, thus enhancing the overall reliability of wind power generation.

In parallel, energy storage systems (ESS) include stationary batteries and electric vehicles (EVs) via Vehicle-to-Grid (V2G) or Vehicle-to-Home (V2H) technologies. These enable a bidirectional energy flow, allowing vehicles not only to charge but also to feed energy back into the grid, respectively [52,58]. These systems are recognized as fundamental components of smart grids and provide essential flexibility to balance generation and consumption. Management of these storage systems is conducted via Battery Management Systems (BMS), which are monitored via IoT to supervise critical parameters such as State of Charge (SoC), State of Health (SoH), and temperature, while actively managing charging and discharging cycles. Finally, the third heterogeneous component involves the interface with the electrical grid itself. This interface, which includes the traditional grid infrastructure, must be monitored and controlled in a much more granular way than in the past. The IoT/IoE fulfills this task through a series of connected devices such as smart meters, sensors (often organized in WSNs), smart actuators, EV charging stations, and other smart user devices.

A comparative summary of these heterogeneous components, highlighting their specific energy profiles and key IoT functions, is provided in Table 8.

Table 8. Comparison of Heterogeneous IoT-Enabled Energy Components.

Component	Energy Profile	Key IoT Functions	Critical Data Points
Photovoltaic (PV)	Stochastic (Source)	MPPT optimization, forecasting, inverter sync	Irradiance, Temp, DC/AC Voltage
Wind Turbines	Stochastic (Source)	Predictive maintenance, Pitch control, MPPT	Vibration, Wind speed, Gearbox temp
Storage (BESS)	Flexible (Buffer)	SoH estimation, charge/discharge scheduling	SoC, Cell Temp, Cycle count
EVs (V2G)	Mobile (Load/Source)	Smart charging, frequency regulation	Battery ID, Location, Plug-in time
Smart Grid	Base (Transport)	Fault detection, power quality monitoring	Voltage sags, Phase angle, Harmonics

7.2. Integration Architecture and Data/Energy Flows

The effective integration of heterogeneous physical systems (PV, storage, grid) requires a structured architectural framework. The scientific literature converges on multi-layer models (often 3 to 5 layers) that logically separate functions, from data collection to application services [59]. These architectures are designed to manage the duality of flows in smart grids: the physical flow of energy and the bidirectional digital flow of data and commands. A common representation of this architecture is summarized Figure 6 and detailed in Table 9.

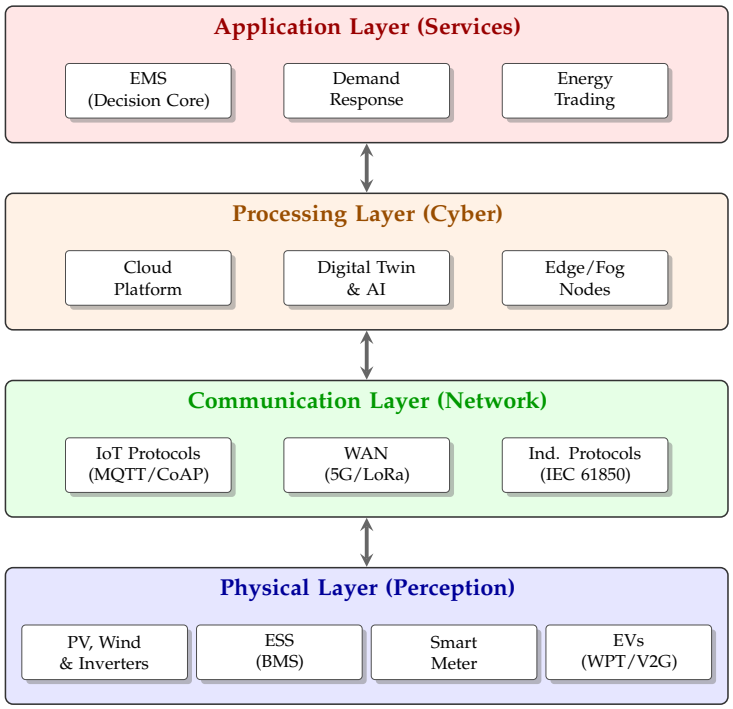

Figure 6. Layered architecture for IoT-enabled integration of heterogeneous energy components.

This layered architecture is designed to handle the vast volume, velocity, and variety (Big Data) of data generated by heterogeneous energy devices [53,59]. Processing is no longer confined to a centralized level (Cloud), but is increasingly distributed on Edge and Fog computing platforms. This hybrid approach is fundamental to ensure the low latency and high resilience necessary for real-time grid control functions [49,52]. Specialized software components such as middleware play a crucial role in abstracting the heterogeneity of hardware and protocols, thus facilitating integration and interoperability [20,55]. Within

this framework, the literature also proposes advanced concepts such as the Energy Router or Energy Hub, which are intelligent specialized nodes capable of actively managing multi-vector energy and information flows at a local level [50].

Table 9. Layered Architecture for IoT/IoE Integration: Functions and Technologies.

Layer	Main Function	Exemplary Technologies/Protocols
Application	Service provision, Decision making	EMS algorithms, Demand Response apps, dashboards
Processing	Data aggregation, AI analysis, Storage	Cloud platforms, Edge/Fog nodes, Digital Twins
Communication	Bi-directional data transport	MQTT, CoAP, 5G, LoRaWAN, IEC 61850 (OT)
Physical	Sensing and Actuation	Smart Meters, PMUs, Inverters, Environmental sensors

7.3. Communication, Interoperability, and Data Management Challenges

The integration of such complex systems introduces significant technological challenges, primarily concerning heterogeneity [53,56]. This heterogeneity manifests across multiple levels. The primary level is within the IoT domain itself, where numerous wireless network standards (such as Wi-Fi, Zigbee, LoRaWAN) and application protocols (such as MQTT, CoAP, XMPP) coexist, each with different profiles for power consumption, range, and reliability [54,58].

However, a critical dilemma arises: how can the gap be bridged between the flexible, data-centric world of Information Technology (IT)—characterized by open protocols and cloud connectivity—and the world of Operational Technology (OT), which prioritizes strict determinism and safety? This profound interoperability challenge lies in bridging the gap between the world of Information Technology (IT)—which includes IoT protocols, the cloud, and web APIs—and the world of Operational Technology (OT), which involves domain-specific protocols from the energy sector [20]. OT systems (like SCADA or industrial controllers) are designed for the control of critical physical equipment (inverters, relays, switches) and prioritize reliability, functional safety, and temporal determinism, rather than web connectivity.

Within this OT domain, interaction with Distributed Energy Resources (DERs) relies on established standards for substation automation and equipment management. Among these, the IEC 61850 standard is fundamental, as it defines not just a communication protocol, but an entire abstract data model to describe every component of the electrical grid (e.g., "Logical Nodes") [20]. This standard, along with legacy protocols like Modbus, uses communication paradigms (e.g., client-server, register polling, or real-time GOOSE messaging) that are intrinsically incompatible with the lightweight publish/subscribe protocols (like MQTT) or RESTful APIs of the IT world [20,58].

Addressing this IT/OT heterogeneity requires the development of middleware platforms or specialized gateways that act as "translators", as illustrated in Figure 7. These gateways must perform the complex task of mapping the rigid industrial data models (like those from IEC 61850) into interoperable and lightweight formats (like JSON) and, conversely, translating commands from the IoT world (e.g., an MQTT message) into actions compliant with OT protocols [20].

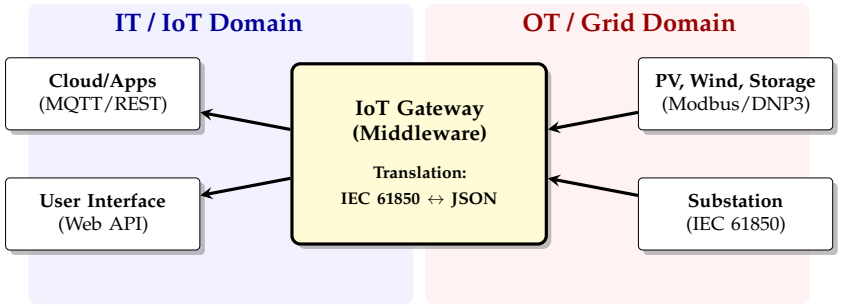

Figure 7. IT/OT interoperability scheme managed via Middleware Gateway.

Once this interoperability is established, further large-scale management challenges emerge. Scalability is a primary concern, given the need to manage potentially millions of interconnected devices [53,55]. This mass of devices generates a huge flow of data, posing the challenge of managing Big Data, characterized by the 5Vs (Volume, Velocity, Variety, Veracity, Value) [52,59]. Variety, in particular, is critical, as the system must normalize heterogeneous data (structured, semi-structured, unstructured) coming from both IoT sensors and OT systems [59].

Finally, the entire system must operate while respecting strict non-functional requirements. It is essential to ensure reliability and low latency for critical grid control functions [49,53], while balancing the power consumption of IoT devices (which are often battery-powered) [56]. Overcoming these challenges requires a holistic approach based on standardization and open architectures [50,56].

7.4. Intelligent Energy Management Systems (EMS)

The operational core of IoT/IoE integration resides in Energy Management Systems (EMS), which act as the decision-making "brain" that orchestrates the coordinated operation of the heterogeneous resources. Unlike specific application scenarios (such as Smart Homes, discussed in Section 7), the architectural role of the EMS is to act as the central convergence point for data streams coming from the Perception Layer and control commands directed to the Physical Layer.

The operation of these EMS, depicted in Figure 8, relies fundamentally on the IoT's ability to collect real-time data from sensors and to use forecasts (often generated by AI and Machine Learning) related to renewable production, consumption profiles, and energy prices [52,60]. As illustrated in the diagram, solid arrows represent the information flow (monitoring data and control signals) managed by the EMS, while dashed lines depict the physical energy exchange between the assets. Leveraging these inputs, the EMS must solve a complex optimization problem to decide how to allocate energy flows.

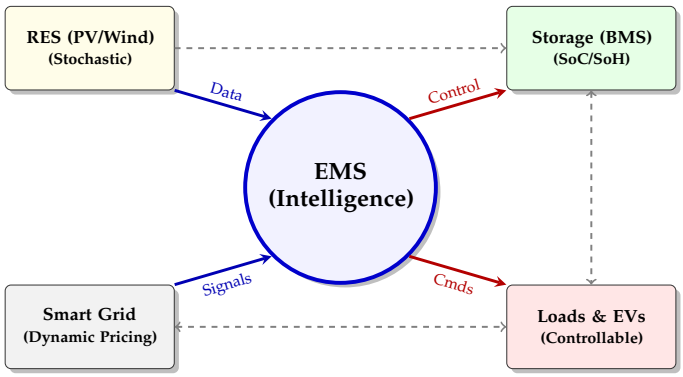

Figure 8. The central role of the EMS in orchestrating heterogeneous resources.

From an algorithmic perspective, the EMS acts as an optimizer that balances conflicting constraints—such as grid stability limits versus economic profit—in real-time. How can optimal decisions be made when both generation and demand are highly stochastic? For this reason, advanced artificial intelligence techniques, particularly Deep Reinforcement Learning (DRL), are gaining popularity. Unlike fixed rule-based approaches, DRL allows the EMS to learn an optimal control strategy through continuous interaction with the environment, adapting dynamically to uncertainty regardless of the specific domain (residential, industrial, or utility-scale) [61,62].

To summarize the optimization strategies discussed, Table 10 presents a comparative overview of the main approaches used in intelligent Energy Management Systems.

Table 10. Optimization approaches and algorithmic strategies in Intelligent EMS.

Approach	Methodology and Characteristics	Role in Smart Electrical Systems
Rule-based	Rely on fixed, predefined logic and heuristics; simpler to implement but less adaptable [61].	Used for basic operational routines and as a baseline for advanced control strategies.
AI-driven Forecasting	Leverages Machine Learning for renewable production and dynamic price forecasting [52,60].	Provides the stochastic inputs necessary for real-time energy flow allocation.
Deep Reinforcement Learning (DRL)	Enables agents to learn optimal control through continuous interaction with the environment [61].	Dynamically adapts to uncertainty in demand and generation regardless of the domain [62].
Multi-objective Optimization	Algorithms designed to balance conflicting constraints such as grid stability versus economic profit.	Acts as the central "brain," orchestrating heterogeneous resources and energy flows.

8. Application Domains and Use Cases

Building upon the architectural frameworks and intelligent management strategies detailed in Section 6, this section explores how these technologies are deployed in real-world scenarios. While the core infrastructure—comprising sensors, actuators, and AI-driven EMS—remains conceptually consistent, the operational objectives and scale vary significantly by domain. The application of IoT in the energy sector manifests primarily in four vertical markets: Smart Homes, Smart Buildings, Industry 4.0/5.0, and Smart Grids. Figure 9 illustrates these domains, highlighting how the generic IoE concepts translate into specific capabilities for each sector.

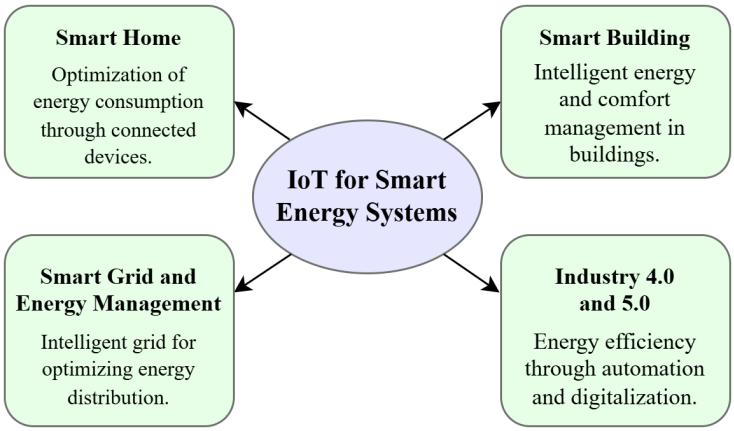

Figure 9. Primary application domains of IoT in the energy sector.

8.1. Smart Home

The residential sector contributes significantly to global energy consumption, making housing a critical focus for efficiency and demand management strategies [63]. The adoption of IoT in homes aims to transform the end-user from a passive consumer into a *prosumer*—an actor who not only consumes but also produces, stores, and manages energy. IoT provides the bidirectional visibility of energy flows necessary for the user to monitor consumption in real-time, coordinate distributed generation, and actively interact with the grid [64,65]. The primary goal is to effectively balance energy efficiency, reduced operational costs, and occupant comfort [61,66].

8.1.1. IoT Infrastructure: Connected Devices and Granular Monitoring

The IoT architecture in the domestic environment relies on the implementation of an interconnected network of devices that act as sensors and actuators for real-time data collection and exchange [63]. This network includes smart thermostats, smart plugs, connected appliances, and, crucially, smart meters [67]. Smart meters represent the fundamental sensing technology, providing electricity consumption data with high temporal granularity (often sub-hourly measurements), thereby enabling diagnostics and supporting advanced optimization strategies [63]. Monitoring can be further refined using plug-level power meters, which track the consumption of individual appliances, facilitating the identification of inefficiencies and waste [63].

8.1.2. Automated Consumption Management: SHEMS and Artificial Intelligence

Autonomous and optimized consumption management is the central task of Smart Home Energy Management Systems (SHEMS), which process data gathered from the IoT infrastructure to make real-time decisions regarding load control [61]. These systems leverage a wide range of inputs, spanning from the operational status of devices and environmental conditions (temperature, light, occupancy) to external information such as dynamic energy prices and weather forecasts [62,64].

Moving beyond the deterministic logic of early implementations, modern solutions integrate the Artificial Intelligence (AI) and Machine Learning (ML) techniques discussed in Section 7 [65,68]. Approaches based on DRL have proven particularly effective. They allow the system to learn optimal control policies through interaction with the environment and the maximization of a long-term reward, such as cost minimization or comfort maintenance [60,61]. These predictive control techniques form the basis of Load Scheduling strategies, which shift flexible loads (e.g., washing machines, electric vehicle charging) to off-peak periods or times with higher renewable energy availability [65,68].

8.1.3. Dynamic Integration with Distributed Energy Resources (PV and Storage)

IoT enables the prosumer model by seamlessly integrating Distributed Energy Resources (DERs) like domestic PV and storage systems [62,64]. By combining solar production forecasts with predicted consumption, the connected ecosystem coordinate energy usage in real-time. The Battery Management System (BMS), communicating via the IoT network, intelligently manages the ESS's charging and discharging cycles [60,65]. The control objective is to determine whether produced energy should be consumed immediately (self-consumption), stored for later use, or injected into the grid, thereby maximizing economic returns based on dynamic tariffs [64]. Advanced algorithms, such as Model Predictive Control (MPC), are often utilized to anticipate system evolution and optimally manage the ESS based on generation and load forecasts [62].

8.1.4. Benefits: Energy Savings and Personalized Comfort

The joint implementation of IoT devices and intelligent algorithms yields a quantifiable impact on residential energy performance. Comparative studies and reviews frequently report measurable reductions in household electricity consumption when adopting SHEMS, although the magnitude of the savings is highly scenario-dependent and varies across building types, occupant behavior, baseline efficiency, and automation scope [64,68]. It is important to note, however, that these figures often represent optimistic values observed in controlled evaluations (e.g., simulations, testbeds, or pilot studies); actual savings are heavily influenced by user behavior, the level of automation adopted, and the specific energy characteristics of the building [64,69].

A further distinguishing advantage of IoT is its ability to balance energy efficiency without compromising comfort. Occupancy and temperature sensors, combined with user interaction data, allow algorithms to learn personalized consumption profiles, ensuring that control strategies (e.g., for HVAC or lighting) adapt dynamically to the occupants' real needs [61,65]. This learning and personalization-based approach ensures a high level of perceived comfort, a key condition for the long-term adoption and sustainability of smart home technologies [60,65].

8.2. Smart Building

Smart Buildings represent one of the most significant applications of the IoT in the energy sector. By integrating networks of sensors, actuators, and distributed control systems, IoT enables real-time monitoring and intelligent management of energy consumption, occupant comfort, and environmental impact. Within Smart City ecosystems, buildings play a central role by supporting the convergence of energy efficiency, digitalization, and sustainability [69,70].

8.2.1. Intelligent Management and Energy Efficiency

The IoT infrastructure within modern buildings employs a distributed network of sensors collecting real-time data on temperature, humidity, air quality, lighting, and electrical consumption. These data are processed by centralized supervisory platforms—commonly known as Building Management Systems (BMS)—which coordinate the operation of subsystems such as HVAC, lighting, and security to maintain optimal indoor conditions [71]. By deploying the predictive control strategies (e.g., MPC) discussed in Section 6, the system automatically adapts behavior to varying occupancy profiles and environmental conditions Recent studies indicate that AI- and IoT-based HVAC control can reduce building energy use compared to conventional control strategies, while maintaining (and in some cases improving) thermal comfort and indoor air quality [72].

Concurrently, BMS increasingly integrate renewable energy sources and Battery Energy Storage Systems (BESS) to dynamically balance energy supply and demand. This capability supports peak load reduction and increased self-consumption, contributing to improved operational efficiency and grid interaction [70].

8.2.2. Sustainability and Smart Grid Integration

Adopting IoT technologies in building management delivers measurable improvements in energy efficiency, sustainability, and cost reduction. In a recent case study [73], IoT- and AI-enabled building energy management reported overall energy savings on the order of 20–30%, mainly driven by intelligent HVAC/lighting control, process automation, and predictive maintenance. Furthermore, Smart Buildings can interact bidirectionally with the Smart Grid, participating in demand response programs and providing flexibility services to improve grid stability and resilience. The convergence of IoT, AI, and building

automation thus represents a cornerstone of the ongoing urban transformation toward sustainable, resilient, and digitally integrated energy ecosystems [69]. In this regard, Digital Twin -based frameworks have recently emerged as powerful tools to link building operation and grid interaction, enabling predictive, personalized, and human-centric energy management [74].

8.3. Industry 4.0 and 5.0

In industrial environments, IoT adoption plays a central role in the digital transformation associated with the Industry 4.0 paradigm, which aims at the seamless interconnection of machines, processes, and human operators. The integration of smart sensors, cloud platforms, and data analytics algorithms enables more efficient energy management, reducing waste and optimizing production flows [75]. With the emergence of the Industry 5.0 concept, these objectives expand to include environmental sustainability, resilience, and human–machine collaboration as central pillars of a human-centric industrial ecosystem [76].

8.3.1. IoT and Energy Management in Industrial Processes

In modern manufacturing plants, IoT enables real-time monitoring of electrical and thermal consumption through distributed sensors and Supervisory Control and Data Acquisition (SCADA) systems. Industrial IoT (IIoT) platforms integrate machine learning techniques to detect anomalies, identify inefficiencies, and predict failures, thereby reducing downtime and overall energy consumption. Automation driven by energy data (energy-aware manufacturing) can reduce facility electricity consumption compared with traditional practices in evaluated settings, by enabling adaptive load control and energy-aware optimization [77]. Moreover, advanced energy management architectures leverage edge and cloud computing to process high-frequency sensor data, ensuring fast decision-making and robust cybersecurity [78].

8.3.2. Transition Toward Industry 5.0: Efficiency and Sustainability

The Industry 5.0 paradigm extends the efficiency-driven focus of Industry 4.0 by emphasizing collaboration between intelligent technologies and human operators, with increased attention to energy efficiency and sustainability. The integration of local renewable sources (e.g., photovoltaic, wind, and microturbine systems) and on-site energy storage allows greater operational flexibility and partial independence from the main grid [75]. Energy-aware manufacturing models employ predictive analytics and multi-objective optimization to plan production schedules based on energy availability and dynamic tariffs [76]. At the same time, digital twins and edge computing can enable real-time simulation and control of industrial processes, improving energy efficiency and reducing environmental impact [78]. Overall, the transition from Industry 4.0 to 5.0 reflects a shift from purely automated systems toward intelligent, sustainable, and human-centric industrial ecosystems, in which IoT, artificial intelligence, and digital twin technologies embed energy management across the entire production cycle. This transformation not only reduces costs and emissions but also supports the creation of an industrial framework where innovation, sustainability, and human values coexist in a dynamic balance [79].

8.4. Smart Grid and Energy Management

Smart grids and intelligent energy management systems represent an advanced evolution of energy infrastructures. Building upon the IoT integration discussed in Section 6, they enable distributed, automated, and data-driven energy management by supporting bidirectional communication between generation, distribution, and consumption. This paradigm transforms the traditional power grid into a dynamic, adaptive, and resilient ecosystem, capable of responding to variability and uncertainty at multiple scales. According to Kir-

mani et al. [5], the adoption of sensors, smart meters, actuators, and distributed control platforms may improve enhances efficiency, reliability, and sustainability by addressing key limitations of conventional grids.

8.4.1. Architecture and Operation

Smart Grid operation relies on IoT-enabled monitoring and control capabilities that support real-time visibility of grid conditions and adaptive decision-making. As discussed in Section 6, the combination of distributed sensing, edge-level processing, and centralized analytics enables dynamic pricing mechanisms, predictive maintenance of grid assets, and responsive demand-side management. These capabilities are fundamental to reducing peak loads, limiting energy losses, and improving overall grid resilience [5,80].

8.4.2. Integration and Flexibility

Smart Grids facilitate the integration of distributed renewable energy sources, energy storage systems, and local microgrids through advanced Energy Management Systems (EMS) that implement predictive and AI-based optimization strategies [81]. Microgrids, capable of operating either in islanded or grid-connected modes, enhance resilience and support supply continuity during faults or disruptions [80]. Flexibility services provided by distributed resources play a central role in modern grid operation. Vehicle-to-Grid (V2G) technologies allow electric vehicles to act as mobile energy storage units, supporting peak shaving and frequency regulation during demand peaks [82]. At a broader system level, Smart Energy Hubs enable the coordinated management of multi-vector energy resources—electricity, heat, and gas—supporting efficient and secure operation of complex energy infrastructures [83]. Overall, these application domains highlight how IoT-enabled energy management evolves from localized optimization to system-wide coordination, underscoring the need for interoperable, scalable, and data-driven solutions across all layers of modern energy ecosystems.

9. Security Challenges and Countermeasures

The Internet of Things ecosystem presents a complex landscape of security vulnerabilities that emerge across multiple architectural layers: at the perception layer, devices face threats from physical tampering and manipulation; the network layer is prone to routing attacks and interception, while the application layer struggles with authentication and data integrity challenges [84]. In the specific context of Smart Grids (SG), these vulnerabilities are amplified by the critical nature of the infrastructure, where cyber-attacks can lead to physical damage, blackouts, or energy theft [22].

9.1. Vulnerabilities and Threats

The diversity of IoT devices complicates security, since heterogeneity obstructs the adoption of unified protection strategies and creates weaknesses [85]. To better understand the risks in smart electrical systems, it is essential to categorize attacks based on their target and impact within the SG architecture [22]:

- Attacks on Availability: Denial of Service (DoS) and Distributed Denial of Service (DDoS) represent critical risks. In a Smart Grid, these can target communication links between Smart Meters and the Control Center, preventing the transmission of critical data and causing grid instability [22]. DDoS attacks are easy to deploy and particularly effective because IoT devices have limited computational and energy resources. From an energy perspective, there are ghost attacks on ZigBee nodes that deplete batteries without compromising security credentials, paving the way for subsequent DoS attempts. Closely linked are botnets, which exploit insecure devices

to orchestrate large-scale disruptions. In healthcare environments, such events can have severe consequences [84].

- Attacks on Integrity: False Data Injection (FDI) attacks are specifically dangerous for electrical systems. Adversaries can manipulate meter readings or price signals, leading to incorrect state estimation by the grid operator and potentially causing physical overflows or financial fraud [22].
- Attacks on Confidentiality: Among common threats, eavesdropping remains one of the most fundamental. Since a large portion of IoT traffic remains unencrypted, attackers can intercept sensitive information. In particular, Palo Alto Networks reported in 2020 that up to 98% of overall IoT traffic was transmitted without encryption, exposing personal and confidential data on the Internet [86]. In Smart Grids, this can reveal energy consumption patterns, compromising user privacy [22]. Even with encryption, metadata leakage may reveal user behaviors; for instance, fitness trackers can disclose activity levels simply through traffic analysis [87].

Another major risk is the Man-in-the-Middle (MitM) attack, which exploits weak authentication mechanisms and often goes undetected by existing intrusion detection systems [85]. The cross-technology nature of IoT systems further increases the attack surface: WiFi devices can emulate ZigBee signals to launch effective protocol-based intrusions [88]. The scale of the problem is amplified by the rapid growth of IoT infrastructures. Fereidouni et al. [85] report that 16.6 billion IoT devices were connected globally in 2023, with forecasts suggesting that this number could exceed 40 billion by 2030.

Protocol-specific weaknesses also emerge. For example, in ZigBee, touchlink commissioning can be abused to reset devices and extract network keys. Bluetooth Low Energy (BLE) versions up to 4.1 rely on weak pairing, exposing them to eavesdropping and MitM attacks unless out-of-band pairing is used. In 6LoWPAN, routing exploits such as sinkhole attacks allow adversaries to manipulate large volumes of traffic [87]. In SG environments, these routing attacks can isolate entire sections of the grid from the monitoring system [22].

More sophisticated adversaries may resort to advanced persistent threats (APTs). MitM itself is often considered an APT due to its persistence [85]. An illustrative example is the fingerprint and timing-based snooping (FATS) attack, described in [89], where attackers infer user activities by analyzing encrypted smart home traffic patterns. Finally, several threats explicitly target energy availability. Battery depletion attacks accelerate energy loss; sleep deprivation attacks prevent low-power modes; and exhaustion attacks repeatedly drain network resources [84].

9.2. Security Protocols and Countermeasures

Securing IoT communications requires robust mechanisms to ensure confidentiality, integrity, and authentication despite device limitations. For Smart Grids, the National Institute of Standards and Technology (NIST) framework suggests a multi-layered defense strategy:

- Prevention: Use of robust encryption like AES and secure protocols (TLS/DTLS). To counter FDI attacks, message authentication codes (MAC) and digital signatures are vital for ensuring data source authenticity [22].
- Detection: Intrusion Detection Systems (IDS) must be adapted for SG traffic. Machine learning-based IDS are increasingly used to identify anomalies in energy consumption or communication flow that signal an ongoing attack [22].
- Mitigation and Recovery: Implementing automated response systems that can isolate compromised grid segments to prevent cascading failures [22].

The alignment between security goals, the specific threats faced by smart grids, and the corresponding countermeasures defined in the NIST framework is summarized in Table 11.

Table 11. Taxonomy of Security Threats and Countermeasures in Smart Grids.

Security Goal	Threats & Attacks	Countermeasures (NIST Framework)
Availability	Denial of Service (DoS/DDoS), Battery Depletion (Ghost Attacks), Jamming of communication links.	Machine Learning-based Intrusion Detection Systems (IDS), Automated isolation of compromised segments [22].
Integrity	False Data Injection (FDI) on meter readings, Routing attacks (Sinkhole), Replay attacks.	Message Authentication Codes (MAC), Digital Signatures, Blockchain for decentralized validation [22].
Confidentiality	Eavesdropping on unencrypted traffic, Traffic Analysis (metadata leakage), Man-in-the-Middle (MitM).	Lightweight Encryption (ECC for Smart Meters), Secure Protocols (TLS/DTLS), Low-latency VPNs (WireGuard) [22,90].

There are Virtual Private Networks (VPNs) and encryption frameworks such as TLS/SSL (and DTLS in constrained environments) that provide essential protections against interception and manipulation [91]. However, performance and energy costs vary. WireGuard offers much lower latency (52.44 ms) than OpenVPN (827.93 ms), making it attractive for latency-sensitive deployments, though it still faces DoS risks [90].

At the application layer, MQTT generally outperforms CoAP in energy-constrained scenarios. Several studies report that MQTT can achieve lower energy consumption and better reliability than CoAP in lossy network conditions, as well as higher efficiency during firmware update processes [87].

Regarding encryption algorithms, AES-CCM8 has been observed to provide slightly better energy efficiency compared to other AES modes in IoT environments. Lightweight authentication mechanisms, such as asynchronous OTP combined with pre-shared keys, also exhibit significantly lower processing overhead than traditional security protocols such as DTLS with large key sizes.

Cryptographic choices further impact gateway performance. In particular, elliptic curve cryptography (ECC) has been shown to outperform RSA in terms of energy consumption and computational efficiency, making it especially suitable for resource-constrained IoT gateways. Consequently, ECC is often recommended for Smart Meter applications, where limited processing power restricts the feasibility of complex cryptographic operations [22].

Finally, while TLS/DTLS remains central, their handshake procedures can be energy intensive. Pre-shared key (PSK) methods offer more efficient alternatives than certificate-based schemes, though elliptic-curve Diffie–Hellman (ECDHE) remains preferable when asymmetric security is unavoidable [90].

9.3. Privacy and Data Protection

Privacy protection in IoT systems extends beyond technical safeguards to include legal compliance design. The Privacy by Design principle requires integrating data protection at the earliest stages, shaping both system architecture and energy usage [92]. In smart electrical systems, privacy is a major concern as high-frequency meter data can reveal a resident's daily routine, used appliances, and even socio-economic status [22]. Compliance with regulations such as GDPR imposes technical and organizational measures that, while necessary, also increase computational and energy costs [86].

Technical solutions include differential privacy, which introduces noise for statistical anonymity at moderate energy cost; homomorphic encryption, which enables computation on encrypted data but with high overhead; and secure multi-party computation [93]. Furthermore, the use of blockchain technology is emerging as a solution for decentralized and tamper-proof energy trading, enhancing both security and privacy in peer-to-peer energy markets [22]. Emerging quantum technologies could theoretically transform IoT privacy protection [94], though their specialized hardware and energy requirements raise new concerns.

Privacy-preserving machine learning also represents a growing trend. Federated learning and secure aggregation allow model training without raw data exposure, but require additional computation and communication, increasing energy consumption. Recent approaches attempt to mitigate this by separating sensitive from non-sensitive data, applying heavier protections only where necessary with the aim to strike a balance between energy and privacy.

The reviewed sources shown in Table 12 provide a robust foundation for IoT privacy discourse, yet exhibit notable complementarities and limitations when contextualized within SES. Achaal et al. [22] and Anedda et al. [86] offer the strongest SES-specific contributions, with the former delivering a systematic analysis of privacy breaches via high-frequency metering data and the latter operationalizing GDPR-compliant architectures with quantified energy overheads. However, their cybersecurity orientation often subsumes privacy under broader threat models, lacking granular treatment of Privacy by Design principles. Shahid et al. [92] extends technical depth through differential privacy and homomorphic encryption analyses, but its healthcare provenance limits direct applicability to electrical metering profiles. Coiduras-Sanagustín et al. [93] contributes valuable user-centric design perspectives via systematic literature review, though its qualitative nature and erroneous DOI necessitate caution. Sharma et al. [94], while innovative in quantum-blockchain integration, remains exploratory, with immature technologies ill-suited for resource-constrained SES deployment. The corpus demonstrates source overlap on blockchain-enabled P2P energy trading and insufficient empirical benchmarking of privacy mechanisms' energy costs—a critical SES concern given constrained edge devices. Post-GDPR regulatory evolution (EU AI Act [95]) and NIST post-quantum cryptography standards remain unaddressed, representing temporal gaps given the manuscript's 2026 timeframe.

Despite advances in privacy-enhancing technologies (PETs), to the best of our knowledge, five substantive gaps persist for scalable SES deployment:

- Zero-Knowledge Proofs (ZKP) Maturity: while theoretically optimal for privacy-preserving energy trading (verifiable consumption without raw data exposure), ZKP implementations exhibit 3-5x computational overhead on typical ARM Cortex-M edge processors, lacking SES-specific benchmarks [96].
- Homomorphic Encryption Optimization: recent Cheon-Kim-Kim-Song (CKKS) schemes [97] reduce multiplicative depth overhead by 50% versus Paillier [98], yet no standardized SES profiles exist for AMI Advanced Metering Infrastructure (AMI) data structures, hindering practical adoption.
- Regulatory Harmonization: the EU AI Act [95] mandates risk classification for grid analytics AI models, requiring privacy impact assessments absent from current SES literature. Integration with NIS2 Directive for critical infrastructure adds compliance complexity.
- Edge-Centric Privacy: TinyML frameworks enable on-device anomaly detection (leakage/short-circuit) without cloud exfiltration, but remain vulnerable to side-

channel attacks and lack formal energy-privacy trade-off models for 10–15 year smart meter lifecycles.

- Quantum-Resistant Migration: NIST PQC standardization (2024) mandates Kyber/Dilithium adoption for long-term SES data at rest, yet IoT hardware acceleration trails by 2–3 years, creating a deployment window vulnerability.

A a research imperative, SES privacy frameworks mus prioritize hybrid PETs (ZKP + lightweight HE) with standardized energy-privacy metrics, validated through real-world AMI testbeds. User-centric dynamic consent mechanisms for prosumers, enabled via self-sovereign identity (SSI) on blockchain, represent the next architectural frontier absent from current literature.

Table 12. Critical Analysis of Privacy References.

Source	Strengths	Weaknesses/Limitations	Relevance for SES
Anedda et al. [86]	Concrete IoT best practices (GDPR compliance, energy costs); integrates Privacy by Design with SES architectures	More practical guidelines than empirical analysis; lacks quantum/federated learning comparison	Very High: SES/IoT contextualized, quantifies GDPR computational costs
Achaal et al. [22]	Comprehensive review of cyber-attacks (incl. privacy breaches via meter data), countermeasures; examples of routines inferred from consumption	Generic smart grid cybersecurity focus, less on privacy by design or quantum. Lacks quantitative energy overhead metrics	High: SES-specific, privacy from high-freq data. Overlaps with Anedda on P2P energy trading
Shahid et al. [92]	Detailed analysis of data protection in IoHT (similar to SES for sensitive data); covers differential privacy & homomorphic encryption	Healthcare context, not electrical; energy overhead underestimated for constrained devices	Medium: Valid analogies (personal data), but not meter data/grid-specific
Coiduras-Sanagustín et al. [93]	SLR on product design perspectives for IoT privacy; emphasizes user-centric & early-stage integration	Qualitative (SLR), lacks SES empirical data; incorrect DOI in text (fix needed)	Medium: Good for Privacy by Design, generic for electrical systems
Sharma et al. [94]	Quantum-blockchain fusion for Industry 4.0; quantifies data protection with low overhead	Theoretical/exploratory; quantum immature for SES deployment; energy concerns only mentioned	Low-Medium : Relevant for P2P energy markets, but speculative

10. Conclusions and Future Directions

This survey provides an integrated view of IoT technologies applied to smart electrical systems, highlighting how digitalization is deeply transforming the energy infrastructure. The analysis shows that:

- Evolution towards Smart Grid and Internet of Energy: the spread of sensors, actuators, distributed control platforms, and edge/fog computing enables real-time monitoring, automation, and optimization of energy flows [2,18].
- Communication Standards: both short-range technologies (Wi-Fi, ZigBee, BLE, Z-Wave) and long-range ones (LoRaWAN, NB-IoT, Sigfox) offer different trade-offs between power consumption, coverage, latency, and reliability [29,31]. No single standard is universally superior: the choice depends on the specific application context [32,99].
- Interoperability: the coexistence of IT/IoT and OT protocols requires the use of middleware and intelligent gateways. These tools must translate heterogeneous data models (e.g., from IEC 61850 to MQTT) and ensure consistent integration between

devices, platforms, and applications [20,40]. In this context, this survey specifically addressed the technical gap between IT and OT, analyzing middleware solutions capable of bridging legacy industrial protocols with modern IoT standards.

- Security and Privacy: the proliferation of IoT devices increases the attack surface, exposing the network to risks like DDoS and false data injection [21]. The limited computing resources of nodes make it difficult to implement advanced encryption protocols. Techniques such as lightweight cryptography, DTLS/TLS, differential privacy, federated learning, and quantum-resistant algorithms are promising but come with significant energy costs [94,100].
- Smart Applications: smart homes, smart buildings, Industry 4.0/5.0, and smart grids show measurable improvements in energy efficiency, automation, and resilience. The literature reports energy savings across a variety of residential and industrial deployments, although the magnitude of these gains is highly scenario-dependent and varies with baseline conditions, controllable load share, and operational constraints [68,77].
- Energy Management Systems (EMS): supported by advanced Artificial Intelligence techniques (such as Deep Reinforcement Learning), EMS act as the brain of smart energy systems, orchestrating heterogeneous resources like photovoltaics, storage systems, home loads, and electric vehicles [52,61].

The following Table 13 summarizes the comparison of the proposed work with existing surveys, highlighting the unique contributions and overlapping areas of study in the context of IoT-based smart electrical systems.

Table 13. Comparison of the Proposed Work with Existing Surveys.

KEY ASPECTS	[2]	[3]	[5]	[6]	[12]	[13]	[23]	[14]	[45]	[49]	[80]	[100]	Prop. Work
Architecture/Reference models	•	•	•	•	•	•	•	•	•	•	•	•	•
Comm. technologies & protocols	•	•	•	•	•	•	•	•	•	•	•	•	•
Interoperability IT/OT	•		•		•	•	•	•	•				•
Standards & frameworks	•		•		•		•	•	•	•	•	•	•
Security (threats & countermeasures)	•	•	•		•	•		•	•	•	•	•	•
Privacy	•					•					•	•	•
Edge/Fog/Cloud computing	•		•	•		•		•	•	•	•		•
Data management & Big Data analytics	•	•	•		•			•	•	•	•	•	•
AI/Machine Learning in smart energy										•			•
Energy management strategies	•	•	•		•				•	•	•		•
Applications/Use cases	•	•	•	•	•	•	•	•	•	•	•	•	•

As summarized in Table 13, the related literature often examines IoT-based smart electrical systems through partially disconnected perspectives. Foundational IoT surveys such as [14,23] consolidate generic architectures and enabling paradigms, but they are not tailored to the constraints of critical electrical infrastructures, where long device lifecycles, safety-critical requirements, and OT-driven standardization strongly influence design choices. Conversely, several domain-specific surveys provide in-depth coverage of individual functional layers: Refs. [3,13] emphasize communication requirements, QoS, and protocol-level considerations; Ref. [45] focuses on middleware/platform capabilities and adoption challenges; and security-oriented surveys such as [12,49,100] prioritize threats and countermeasures (and, in some cases, privacy aspects), often without a systematic cross-layer mapping to architectural and standardization and integration decisions. Although broader smart-grid/energy-domain surveys such as [2,5,6,80] cover a wider spectrum of technologies and applications, they often present standards, protocols, architectures, and use cases as parallel "silos", leaving key functional dependencies among these dimensions largely implicit. In contrast, our survey introduces a cross-layer synthesis that connects architectural/reference models, standards and communication protocols, IT/OT

interoperability mechanisms (including gateway/middleware-based translation across heterogeneous stacks), security and privacy requirements, edge–fog–cloud computing choices, and data/AI pipelines, thereby enabling readers to trace design decisions across layers toward implementable energy-management strategies and smart electrical applications.

Overall, the survey shows that IoT is now an essential element for building smart electrical systems. However, it also highlights that interoperability, security, and complexity management remain key challenges to address for creating truly scalable, reliable, and sustainable solutions.

The evolution of IoT-based smart electrical systems is expected to accelerate in the coming years, driven by the increasing penetration of distributed energy resources, electric vehicles, and data-intensive applications. One of the most prominent trends concerns the growing adoption of edge and fog computing paradigms, which aim to reduce latency, enhance scalability, and improve resilience by enabling localized data processing and control closer to the physical infrastructure. In parallel, the integration of artificial intelligence and machine learning techniques, including deep learning and reinforcement learning, is anticipated to play a central role in predictive maintenance, adaptive energy management, and demand response optimization.

Addressing challenges such as data management, trustworthiness, AI explainability, and regulatory compliance will require multidisciplinary research efforts, combining advances in communication technologies, artificial intelligence, cybersecurity, and energy systems engineering, ultimately paving the way toward resilient, secure, and sustainable IoT-enabled smart electrical systems.

Beyond the general challenges outlined above, a more detailed analysis reveals a set of structural limitations that continue to hinder the large-scale deployment of IoT-based smart electrical systems. In accordance with current research trends and technological trajectories, the following open research gaps are identified in a concise form, highlighting critical weaknesses of existing solutions and outlining promising directions for future investigation:

- Scalable IT/OT Security
    - Problem: Existing security frameworks, including NIST-based guidelines and ECC-based cryptographic schemes [22], as well as VPN-based architectures [90], were not conceived to scale across the billions of heterogeneous devices expected by 2030 [85].
    - Research Gap: Absence of autonomous and zero-touch security mechanisms capable of dynamically managing trust and mitigating threats in massive-scale, heterogeneous IT/OT ecosystems.
- Real-time AI at the Edge
    - Problem: Advanced Artificial Intelligence and Deep Reinforcement Learning (DRL) models for energy management [61] frequently exceed the computational, memory, and energy constraints of most IoT nodes [90,100].
    - Research Gap: Lack of ultra-lightweight, edge-native AI models (e.g., TinyML) capable of supporting real-time decision-making under stringent latency, energy, and privacy constraints.
- Standard Harmonization
    - Problem: Emerging protocols such as Matter and MQTT [40] improve interoperability at the communication level but fail to address integration at the semantic and information-model levels.
    - Research Gap: Absence of a unified semantic framework or a universal ontology [48] enabling true cross-vendor and cross-domain interoperability in large-scale IoE ecosystems.

As shown in Table 14, despite these advancements, several open challenges remain. Interoperability across heterogeneous devices, platforms, and standards continues to represent a critical issue, particularly in large-scale deployments involving multiple vendors and legacy systems. While international standards provide partial solutions, achieving seamless integration between IT and operational technology OT domains remains an open research problem. Security and privacy also constitute major concerns, as the increased attack surface introduced by IoT devices exposes smart electrical systems to cyber–physical threats, data breaches, and service disruptions. Developing lightweight yet robust security mechanisms that can operate under the resource constraints of IoT nodes is still a challenging task.

Table 14. Summary of Open Research Gaps and Proposed Future Solutions.

Key Aspect	Current Limitations	Open Research Gap	Proposed Missing Solution
Scalable IT/OT Security	Manual trust management and high overhead in networks with billions of nodes [85].	Absence of autonomous and scalable security orchestration for large-scale IT/OT environments.	Self-adaptive zero-trust architectures and distributed identity systems for automated trust.
Real-time AI at the Edge	High energy cost of local AI execution and dependence on cloud infrastructures [90,100].	Lack of ultra-lightweight AI models for real-time decision-making on constrained edge nodes.	TinyML-based frameworks and hardware–software co-design for edge-native real-time processing.
Standard Harmonization	Protocol-level compatibility with persistent semantic fragmentation [48].	Absence of a unified semantic framework for cross-domain interoperability between IT and OT.	Universal semantic middleware and shared ontologies supporting cross-vendor integration.

Author Contributions: Conceptualization, M.A., D.G. and F.P.; methodology, M.A. and C.M.; software, C.M., S.P. and S.O.; validation, M.A. and D.G.; formal analysis, C.M., S.P. and S.O.; investigation, C.M., S.P. and S.O.; resources, F.P.; data curation, C.M., S.P. and S.O.; writing—original draft preparation, C.M., S.P. and S.O.; writing—review and editing, M.A., D.G. and F.P.; visualization, C.M., S.P. and S.O.; supervision, M.A., D.G. and F.P.; project administration, M.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article. The data presented in this study are available within the article (see tables and figures).

Conflicts of Interest: Author Francesco Parodo was employed by the company Dauvea srl. 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. Nazari, Z.; Musilek, P. Impact of Digital Transformation on the Energy Sector: A Review. *Algorithms* **2023**, *16*, 211. [CrossRef]
2. Motlagh, N.H.; Mohammadrezaei, M.; Hunt, J.; Zakeri, B. Internet of Things (IoT) and the Energy Sector. *Energies* **2020**, *13*, 494. [CrossRef]
3. Fadel, E.; Gungor, V.; Nassef, L.; Akkari, N.; Malik, M.A.; Almasri, S.; Akyildiz, I.F. A survey on wireless sensor networks for smart grid. *Comput. Commun.* **2015**, *71*, 22–33. [CrossRef]
4. Rivas, A.; Posso, G. Faults in Smart Grid Systems: Monitoring, Detection and Classification. *Energy Rep.* **2020**, *6*, 2090–2099. [CrossRef]
5. Kirmani, S.; Mazid, A.; Khan, I.A.; Abid, M. A Survey on IoT-Enabled Smart Grids: Technologies, Architectures, Applications, and Challenges. *Sustainability* **2023**, *15*, 717. [CrossRef]
6. Sharma, K.; Malik, A.; Batra, I.; Sanwar Hosen, A.S.M.; Latif Sarker, M.A.; Han, D.S. Technologies Behind the Smart Grid and Internet of Things: A System Survey. *Comput. Mater. Contin.* **2023**, *75*, 5049–5072. [CrossRef]

7. Durrani, A.M.; Asar, A.U.; Aziz, A.; Khan, W.; Yousaf, M.Z.; Farooq, U.; Altayeb, M.; Geremew, M.S. AI-driven optimization of energy consumption and demand response in smart homes. *Energy Explor. Exploit.* **2025**. [CrossRef]
8. Luthander, R.; Widén, J.; Nilsson, D.; Palm, J. Photovoltaic self-consumption in buildings: A review. *Appl. Energy* **2015**, *142*, 80–94. [CrossRef]
9. Tanwar, S.; Tyagi, S.; Kumar, S. The Role of Internet of Things and Smart Grid for the Development of a Smart City. In *Proceedings of the Intelligent Communication and Computational Technologies*; Hu, Y.C., Tiwari, S., Mishra, K.K., Trivedi, M.C., Eds.; Springer : Singapore, 2018; pp. 23–33.
10. Dakic, P.; Zivkovic, M.; Jovanovic, L.; Bacanin, N.; Antonijevic, M.; Kaljevic, J.; Simic, V. Intrusion detection using metaheuristic optimization within IoT/IIoT systems and software of autonomous vehicles. *Sci. Rep.* **2024**, *14*, 22884. [CrossRef] [PubMed]
11. Sagu, A.; Gill, N.S.; Gulia, P.; Singh, P.K.; Hong, W.C. Design of Metaheuristic Optimization Algorithms for Deep Learning Model for Secure IoT Environment. *Sustainability* **2023**, *15*, 2204. [CrossRef]
12. Bouslimani, M.; Benbouzid-Si Tayeb, F.; Amirat, Y.; Benbouzid, M. Cyber-Physical Security in Smart Grids: A Comprehensive Guide to Key Research Areas, Threats, and Countermeasures. *Appl. Sci.* **2025**, *15*, 12367. [CrossRef]
13. Tightiz, L.; Yang, H. A Comprehensive Review on IoT Protocols' Features in Smart Grid Communication. *Energies* **2020**, *13*, 2762. [CrossRef]
14. Goyal, K.K.; Garg, A.; Rastogi, A.; Singhal, S. A literature survey on Internet of Things (IoT). *Int. J. Adv. Netw. Appl.* **2018**, *9*, 3663–3668.
15. Xu, N.; Tang, Z.; Si, C.; Bian, J.; Mu, C. A Review of Smart Grid Evolution and Reinforcement Learning: Applications, Challenges and Future Directions. *Energies* **2025**, *18*, 1837. [CrossRef]
16. Wei, T.; Li, H.; Miao, J. Integration and Development Path of Smart Grid Technology: Technology-Driven, Policy Framework and Application Challenges. *Processes* **2025**, *13*, 2428. [CrossRef]
17. Akram, J.; Tahir, A.; Munawar, H.S.; Akram, A.; Kouzani, A.Z.; Mahmud, M.A.P. Cloud- and Fog-Integrated Smart Grid Model for Efficient Resource Utilisation. *Sensors* **2021**, *21*, 7846. [CrossRef]
18. Andriulo, F.C.; Fiore, M.; Mongiello, M.; Traversa, E.; Zizzo, V. Edge Computing and Cloud Computing for Internet of Things: A Review. *Informatics* **2024**, *11*, 71. [CrossRef]
19. Yadav, H.; Srivastava, L.; Sethi, S.S.; Bandopadhyay, A.; Swain, S.; Sharma, N. Fog Enabled Multi Tier Resource Orchestration for IoT Applications. In Proceedings of the 2025 International Conference on Engineering Innovations and Technologies (ICoEIT), Bhopal, India, 4–5 July 2025; pp. 976–981. [CrossRef]
20. Cavalieri, S.; Cantali, G.; Susinna, A. Integration of IoT Technologies into the Smart Grid. *Sensors* **2022**, *22*, 2475. [CrossRef] [PubMed]
21. Alomari, M.A.; Al-Andoli, M.N.; Ghaleb, M.; Thabit, R.; Alkawsi, G.; Alsayaydeh, J.A.J.; Gaid, A.S.A. Security of Smart Grid: Cybersecurity Issues, Potential Cyberattacks, Major Incidents, and Future Directions. *Energies* **2025**, *18*, 141. [CrossRef]
22. Achaal, B.; Adda, M.; Berger, M.; Ibrahim, H.; Awde, A. Study of smart grid cyber-security, examining architectures, communication networks, cyber-attacks, countermeasure techniques, and challenges. *Cybersecurity* **2024**, *7*, 10. [CrossRef] [PubMed]
23. Atzori, L.; Iera, A.; Morabito, G. The internet of things: A survey. *Comput. Netw.* **2010**, *54*, 2787–2805. [CrossRef]
24. Khujamatov, K.; Lazarev, A.; Akhmedov, N. Intelligent IoT Sensors: Types, Functions and Classification. In Proceedings of the 2021 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan, 3–5 November 2021; pp. 1–6. [CrossRef]
25. Ashfaq, M.; Nur, S. IoT Sensor Networks-Orchestrating Connectivity, Efficiency, and Intelligence Across Diverse Domains. *Int. J. Innov. Res. Comput. Sci. Technol.* **2024**, *12*, 154–161. [CrossRef]
26. Kazeem, O.O.; Akintade, O.O.; Kehinde, L.O.; Akintade, O.; Kehinde, L. Comparative study of communication interfaces for sensors and actuators in the cloud of internet of things. *Int. J. Internet Things* **2017**, *6*, 9–13.
27. Navani, D.; Jain, S.; Nehra, M.S. The Internet of Things (IoT): A Study of Architectural Elements. In Proceedings of the 2017 13th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS), Jaipur, India, 4–7 December 2017; pp. 473–478. [CrossRef]
28. Mahmood, A.; Javaid, N.; Razzaq, S. A review of wireless communications for smart grid. *Renew. Sustain. Energy Rev.* **2015**, *41*, 248–260. [CrossRef]
29. Gerodimos, A.; Maglaras, L.; Ferrag, M.A.; Ayres, N.; Kantzavelou, I. IoT: Communication protocols and security threats. *Internet Things Cyber-Phys. Syst.* **2023**, *3*, 1–13. [CrossRef]
30. Singh, D.K.; Sobti, R. Wireless Communication Technologies for Internet of Things and Precision Agriculture: A Review. In Proceedings of the 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC), Solan, India, 7–9 October 2021; pp. 765–769. [CrossRef]
31. Kadusic, E.; Ruland, C.; Hadzajlic, N.; Zivic, N. The factors for choosing among NB-IoT, LoRaWAN, and Sigfox radio communication technologies for IoT networking. In Proceedings of the 2022 International Conference on Connected Systems & Intelligence (CSI), Trivandrum, India, 31 August–2 September 2022; pp. 1–5. [CrossRef]

32. Danbatta, S.J.; Varol, A. Comparison of Zigbee, Z-Wave, Wi-Fi, and Bluetooth Wireless Technologies Used in Home Automation. In Proceedings of the 2019 7th International Symposium on Digital Forensics and Security (ISDFS), Barcelos, Portugal, 10–12 June 2019; pp. 1–5. [CrossRef]
33. Prieto González, L.; Fensel, A.; Gómez Berbís, J.M.; Popa, A.; de Amescua Seco, A. A Survey on Energy Efficiency in Smart Homes and Smart Grids. *Energies* **2021**, *14*, 7273. [CrossRef]
34. Garlisi, D.; Pagano, A.; Giuliano, F.; Croce, D.; Tinnirello, I. Interference Analysis of LoRaWAN and Sigfox in Large-Scale Urban IoT Networks. *IEEE Access* **2025**, *13*, 44836–44848. [CrossRef]
35. Martí, M.; Garcia-Rubio, C.; Campo, C. Performance Evaluation of CoAP and MQTT_SN in an IoT Environment. *Proceedings* **2019**, *31*, 49. [CrossRef]
36. Seoane, V.; Garcia-Rubio, C.; Almenares, F.; Campo, C. Performance evaluation of CoAP and MQTT with security support for IoT environments. *Comput. Netw.* **2021**, *197*, 108338. [CrossRef]
37. Karnouskos, S.; Leitão, P.; Ribeiro, L.; Colombo, A.W. Industrial Agents as a Key Enabler for Realizing Industrial Cyber-Physical Systems: Multiagent Systems Entering Industry 4.0. *IEEE Ind. Electron. Mag.* **2020**, *14*, 18–32. [CrossRef]
38. Azad, T.; Newton, M.A.H.; Trevathan, J.; Sattar, A. IoT Edge Network Interoperability. *Comput. Commun.* **2025**, *236*, 108125. [CrossRef]
39. Vardakis, G.; Hatzivasilis, G.; Koutsaki, E.; Papadakis, N. Review of Smart-Home Security Using the Internet of Things. *Electronics* **2024**, *13*, 3343. [CrossRef]
40. Madadi-Barough, S.; Ruiz-Blanco, P.; Lin, J.; Vidal, R.; Gomez, C. Matter: IoT Interoperability for Smart Homes. *IEEE Commun. Mag.* **2025**, *63*, 106–112. [CrossRef]
41. Hannou, F.Z.; Lefrançois, M.; Jouvelot, P.; Charpenay, V.; Zimmermann, A. A Survey on IoT Programming Platforms: A Business-Domain Expert Perspective. *ACM Comput. Surv.* **2024**, *57*, 1–37. [CrossRef]
42. European Commission. INTER-IoT: Interoperability of Heterogeneous IoT Platforms. Horizon 2020 Project ID 687283. 2021. Available online: https://cordis.europa.eu/project/id/687283 (accessed on 26 October 2015).
43. Silva, D.; Carvalho, L.I.; Soares, J.; Sofia, R.C. A Performance Analysis of Internet of Things Networking Protocols: Evaluating MQTT, CoAP, OPC UA. *Appl. Sci.* **2021**, *11*, 4879. [CrossRef]
44. Viel, F.; Augusto Silva, L.; Leithardt, V.R.Q.; De Paz Santana, J.F.; Celeste Ghizoni Teive, R.; Albenes Zeferino, C. An Efficient Interface for the Integration of IoT Devices with Smart Grids. *Sensors* **2020**, *20*, 2849. [CrossRef]
45. Alfalouji, Q.; Schranz, T.; Kümpel, A.; Schraven, M.; Storek, T.; Gross, S.; Monti, A.; Müller, D.; Schweiger, G. IoT Middleware Platforms for Smart Energy Systems: An Empirical Expert Survey. *Buildings* **2022**, *12*, 526. [CrossRef]
46. Luis, Á.; Casares, P.; Cuadrado-Gallego, J.J.; Patricio, M.A. PSON: A Serialization Format for IoT Sensor Networks. *Sensors* **2021**, *21*, 4559. [CrossRef]
47. Ai, Y.; Zhu, Y.; Jiang, Y.; Deng, Y. MIGS: A Modular Edge Gateway with Instance-Based Isolation for Heterogeneous Industrial IoT Interoperability. *Sensors* **2026**, *26*, 314. [CrossRef]
48. Karabulut, E.; Pileggi, S.F.; Groth, P.; Degeler, V. Ontologies in digital twins: A systematic literature review. *Future Gener. Comput. Syst.* **2024**, *153*, 442–456. [CrossRef]
49. Goudarzi, A.; Ghayoor, F.; Waseem, M.; Fahad, S.; Traore, I. A Survey on IoT-Enabled Smart Grids: Emerging, Applications, Challenges, and Outlook. *Energies* **2022**, *15*, 6984. [CrossRef]
50. Ghiasi, M.; Wang, Z.; Mehrandezh, M.; Jalilian, S.; Ghadimi, N. Evolution of smart grids towards the Internet of energy: Concept and essential components for deep decarbonisation. *IET Smart Grid* **2023**, *6*, 86–102. [CrossRef]
51. Ahmad, S.; Jha, S.; Abdeljaber, H.A.; Rahmani, M.K.I.; Waris, M.M.; Singh, A.; Yaseen, M. An Integration of IoT, IoC, and IoE towards Building a Green Society. *Sci. Program.* **2022**, *2022*, 5206. [CrossRef]
52. Mishra, P.; Singh, G. Energy Management Systems in Sustainable Smart Cities Based on the Internet of Energy: A Technical Review. *Energies* **2023**, *16*, 6903. [CrossRef]
53. Ahmad, T.; Zhang, D. Using the internet of things in smart energy systems and networks. *Sustain. Cities Soc.* **2021**, *68*, 102783. [CrossRef]
54. Abir, S.A.A.; Anwar, A.; Choi, J.; Kayes, A. IoT-enabled smart energy grid: Applications and challenges. *IEEE Access* **2021**, *9*, 50961–50981. [CrossRef]
55. Arasteh, H.; Hosseinnezhad, V.; Loia, V.; Tommasetti, A.; Troisi, O.; Shafie-khah, M.; Siano, P. IoT-based smart cities: A survey. In Proceedings of the 2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC), Florence, Italy, 7–10 June 2016; pp. 1–6. [CrossRef]
56. Orumwense, E.F.; Abo-Al-Ez, K. Internet of Things for smart energy systems: A review on its applications, challenges and future trends. *AIMS Electron. Electr. Eng.* **2023**, *7*, 50–74. [CrossRef]
57. Ioannides, M.G.; Stamelos, A.P.; Papazis, S.A.; Stamataki, E.E.; Stamatakis, M.E. Internet of Things-Based Control of Induction Machines: Specifics of Electric Drives and Wind Energy Conversion Systems. *Energies* **2024**, *17*, 645. [CrossRef]

58. Pal, R.; Chavhan, S.; Gupta, D.; Khanna, A.; Padmanaban, S.; Khan, B.; Rodrigues, J.J.C. A comprehensive review on IoT-based infrastructure for smart grid applications. *IET Renew. Power Gener.* **2021**, *15*, 3761–3776. [CrossRef]
59. Al-Ali, A.; Gupta, R.; Zualkernan, I.; Das, S.K. Role of IoT technologies in big data management systems: A review and Smart Grid case study. *Pervasive Mob. Comput.* **2024**, *100*, 101905. [CrossRef]
60. Ajadalu, S.O. Optimizing Energy Efficiency in Smart Home Automation through Reinforcement Learning and IoT. *Asian J. Res. Comput. Sci.* **2024**, *17*, 9–24. [CrossRef]
61. Amer, A.A.; Shaban, K.; Massoud, A.M. DRL-HEMS: Deep Reinforcement Learning Agent for Demand Response in Home Energy Management Systems Considering Customers and Operators Perspectives. *IEEE Trans. Smart Grid* **2022**, *14*, 239–250. [CrossRef]
62. Lee, S.; Choi, D.H. Energy Management of Smart Home with Home Appliances, Energy Storage System and Electric Vehicle: A Hierarchical Deep Reinforcement Learning Approach. *Sensors* **2020**, *20*, 2157. [CrossRef] [PubMed]
63. Bindushree G.T. IoT-based Energy Management in Smart Homes: A Literature Review. *World J. Adv. Res. Rev.* **2022**, *16*, 1392–1400. [CrossRef]
64. Rao, C.K.; Sahoo, S.K.; Yanine, F.F. A comprehensive review of smart energy management systems for photovoltaic power generation utilizing the internet of things. *Unconv. Resour.* **2025**, *7*, 100197. [CrossRef]
65. Yu, L.; Xie, W.; Xie, D.; Zou, Y.; Zhang, D.; Sun, Z.; Zhang, L.; Zhang, Y.; Jiang, T. Deep Reinforcement Learning for Smart Home Energy Management. *IEEE Internet Things J.* **2019**, *7*, 2751–2762. [CrossRef]
66. Kumar, M.; Pandey, K.M. The Impact of IoT on Smart Home Energy Management. *Int. J. Soft Comput. Eng. (IJSCE)* **2023**, *13*, 7–11. [CrossRef]
67. Badar, A.Q.H.; Anvari-Moghaddam, A. Smart Home Energy Management System—A Review. *Adv. Build. Energy Res.* **2022**, *16*, 118–143. [CrossRef]
68. Saroha, P.; Singh, G.; Lilhore, U.K.; Simaiya, S.; Khan, M.; Alroobaea, R.; Alsafyani, M.; Alsufyani, H. Dynamic appliance scheduling and energy management in smart homes using adaptive reinforcement learning techniques. *Sci. Rep.* **2025**, *15*, 24594. [CrossRef]
69. Poyyamozhi, M.; Murugesan, B.; Rajamanickam, N.; Shorfuzzaman, M.; Aboelmagd, Y. IoT–A Promising Solution to Energy Management in Smart Buildings: A Systematic Review, Applications, Barriers, and Future Scope. *Buildings* **2024**, *14*, 3446. [CrossRef]
70. Costa, R.; Silva, R.; Faia, R.; Gomes, L.; Faria, P.; Vale, Z. Empowering energy management in smart buildings: A comprehensive study on distributed energy storage systems for sustainable consumption. *Energy Build.* **2024**, *324*, 114953. [CrossRef]
71. Bae, Y.; Bhattacharya, S.; Cui, B.; Lee, S.; Li, Y.; Zhang, L.; Im, P.; Adetola, V.; Vrabie, D.; Leach, M.; et al. Sensor impacts on building and HVAC controls: A critical review for building energy performance. *Adv. Appl. Energy* **2021**, *4*, 100068. [CrossRef]
72. Mischos, S.; Dalagdi, E.; Vrakas, D. Intelligent energy management systems: A review. *Artif. Intell. Rev.* **2023**, *56*, 11635–11674. [CrossRef]
73. Rojek, I.; Mikołajewski, D.; Mroziński, A.; Macko, M.; Bednarek, T.; Tyburek, K. Internet of Things Applications for Energy Management in Buildings Using Artificial Intelligence—A Case Study. *Energies* **2025**, *18*, 1706. [CrossRef]
74. Marcello, A.; Rossi, C.; Pagliari, D.; Passerone, R.; Tosi, D. Digital Twin Framework for Personalized Building Management in Ambient Assisted Living. In *Proceedings of the 2024 IEEE World Forum on Internet of Things (WF-IoT)*; IEEE: New York, NY, USA, 2024; pp. 883–888. [CrossRef]
75. Nemomsa, S.K.; Dejene, N.D.; Efa, D.A.; Negari, D.T.; Ifa, D.A.; Kumar, D.H. Clean Energy Demand in Industry 4.0: Trends, Challenges, and Opportunities. *Results Eng.* **2025**, *28*, 107260. [CrossRef]
76. Rame, R.; Purwanto, P.; Sudarno, S. Industry 5.0 and Sustainability: An Overview of Emerging Trends and Challenges for a Green Future. *Innov. Green Dev.* **2024**, *3*, 100173. [CrossRef]
77. Wyrzykowska, B.; Szczepaniuk, H.; Szczepaniuk, E.K.; Rytko, A.; Kacprzak, M. Intelligent Energy Management Systems in Industry 5.0: Cybersecurity Applications in Examples. *Energies* **2024**, *17*, 5871. [CrossRef]
78. Mazhar, T.; Khan, S.; Shahzad, T.; Khan, M.A.; Rehman, A.U.; Hamam, H. Integration of Smart Grid with Industry 5.0: Applications, Challenges and Solutions. *Meas. Energy* **2025**, *5*, 100031. [CrossRef]
79. Introna, V.; Santolamazza, A.; Cesarotti, V. Integrating Industry 4.0 and 5.0 Innovations for Enhanced Energy Management Systems. *Energies* **2024**, *17*, 1222. [CrossRef]
80. Ethirajan, V.; Mangaiyarkarasi, S.P. An In-Depth Survey of Latest Progress in Smart Grids: Paving the Way for a Sustainable Future through Renewable Energy Resources. *J. Electr. Syst. Inf. Technol.* **2025**, *12*, 195. [CrossRef]
81. Khan, M.R.; Haider, Z.M.; Malik, F.H.; Alghamdi, F.; Arif, M.; Qureshi, S. A Comprehensive Review of Microgrid Energy Management Strategies Considering Electric Vehicles, Energy Storage Systems, and AI Techniques. *Processes* **2024**, *12*, 270. [CrossRef]
82. Sultan, V.; Aryal, A.; Chang, H.; Kral, J. Integration of EVs into the Smart Grid: A Systematic Literature Review. *Energy Inform.* **2022**, *5*, 65. [CrossRef]

83. El-Afifi, M.I.; Sedhom, B.E.; Padmanaban, S.; Abdelaziz, A.Y.; Elsaid, M.; Mitolo, M. A Review of IoT-Enabled Smart Energy Hub Systems: Rising, Applications, Challenges, and Future Prospects. *Renew. Energy Focus* **2024**, *51*, 100634. [CrossRef]
84. Madanian, S.; Chinbat, T.; Subasinghage, M.; Airehrour, D.; Hassandoust, F.; Yongchareon, S. Health IoT Threats: Survey of Risks and Vulnerabilities. *Future Internet* **2024**, *16*, 389. [CrossRef]
85. Fereidouni, H.; Fadeitcheva, O.; Zalai, M. IoT and Man-in-the-Middle Attacks. *Secur. Priv.* **2025**, *8*, e70016. [CrossRef]
86. Anedda, M.; Floris, A.; Girau, R.; Fadda, M.; Ruiu, P.; Farina, M.; Bonu, A.; Giusto, D.D. Privacy and Security Best Practices for IoT Solutions. *IEEE Access* **2023**, *11*, 129156–129172. [CrossRef]
87. Meneghello, F.; Calore, M.; Zucchetto, D.; Polese, M.; Zanella, A. IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices. *IEEE Internet Things J.* **2019**, *6*, 8182–8201. [CrossRef]
88. Zhang, X.; Yu, S.; Zhou, H.; Huang, P.; Guo, L.; Li, M. Signal Emulation Attack and Defense for Smart Home IoT. *IEEE Trans. Dependable Secur. Comput.* **2023**, *20*, 2040–2057. [CrossRef]
89. Nassiri Abrishamchi, M.A.; Zainal, A.; Ghaleb, F.A.; Qasem, S.N.; Albarrak, A.M. Smart Home Privacy Protection Methods against a Passive Wireless Snooping Side-Channel Attack. *Sensors* **2022**, *22*, 8564. [CrossRef] [PubMed]
90. Pandey, S.; Agrahari, Y.K.; Verma, S. Secure Data Communication Protocols for IoT Systems: Ensuring Reliable Cloud Integration. *Res. Gate* **2025**. [CrossRef]
91. Gentile, A.F.; Macrì, D.; Greco, E.; Fazio, P. IoT IP Overlay Network Security Performance Analysis with Open Source Infrastructure Deployment. *J. Cybersecur. Priv.* **2024**, *4*, 629–649. [CrossRef]
92. Shahid, J.; Ahmad, R.; Kiani, A.K.; Ahmad, T.; Saeed, S.; Almuhaideb, A.M. Data Protection and Privacy of the Internet of Healthcare Things (IoHTs). *Appl. Sci.* **2022**, *12*, 1927. [CrossRef]
93. Coiduras-Sanagustín, A.; Manchado-Pérez, E.; García-Hernández, C. Understanding perspectives for product design on personal data privacy in internet of things (IoT): A systematic literature review (SLR). *Heliyon* **2024**, *10*, e30357. [CrossRef] [PubMed]
94. Sharma, A.K.; Peelam, M.S.; Chauasia, B.K.; Chamola, V. QIoTChain: Quantum IoT-blockchain fusion for advanced data protection in Industry 4.0. *IET Blockchain* **2024**,*4*, 252–262. [CrossRef]
95. van Kolfschooten, H.; van Oirschot, J. The EU Artificial Intelligence Act (2024): Implications for healthcare. *Health Policy* **2024**, *149*, 105152. [CrossRef]
96. Pop, C.D.; Antal, M.; Cioara, T.; Anghel, I.; Salomie, I. Blockchain and Demand Response: Zero-Knowledge Proofs for Energy Transactions Privacy. *Sensors* **2020**, *20*, 5678. [CrossRef] [PubMed]
97. Wang, J.; Xia, Z.; Chen, Y.; Hu, C.; Yu, F. Intrusion detection framework based on homomorphic encryption in AMI network. *Front. Phys.* **2022**, *10*, 1102892. [CrossRef]
98. Paillier, P. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. In *Proceedings of the Advances in Cryptology—EUROCRYPT '99*; Stern, J., Ed.; Springer: Berlin/Heidelberg, Germany, 1999; pp. 223–238.
99. Stanco, G.; Botta, A.; Frattini, F.; Giordano, U.; Ventre, G. On the performance of IoT LPWAN technologies: The case of Sigfox, LoRaWAN and NB-IoT. In Proceedings of the ICC 2022—IEEE International Conference on Communications, Seoul, Republic of Korea, 16–20 May 2022; pp. 2096–2101. [CrossRef]
100. Sun, P.; Shen, S.; Wan, Y.; Wu, Z.; Fang, Z.; Gao, X.Z. A Survey of IoT Privacy Security: Architecture, Technology, Challenges, and Trends. *IEEE Internet Things J.* **2024**, *11*, 34567–34591. [CrossRef]