frontiers in Communications and Networks

ORIGINAL RESEARCH
published: 24 June 2021
doi: 10.3389/frcmn.2021.689590

Smarter Grid in the 5G Era: A Framework Integrating Power Internet of Things With a Cyber Physical System

Yuanjie Liu[1], *Xiongping Yang*[2], *Wenkun Wen*[3] *and Minghua Xia*[1]*

[1]School of Electronics and Information Technology, Sun Yat-sen University, Guangzhou, China, [2]Strategy and Planning Department, China Southern Power Grid Co., Ltd., Guangzhou, China, [3]Guangzhou Techphant Co., Ltd., Guangzhou, China

As the energy infrastructure of smart cities, smart grid upgrades traditional power grid systems with state-of-the-art information and communication technologies. In particular, as the full deployment of the Internet of Things in the power grid (a.k.a. power Internet of Things or PIoT), the newly introduced information flow together with inherent energy flow makes it more efficient for power generation, transmission, distribution, and consumption. To further exploit the precious energy and the latest 5G technologies, this article boosts to add a value flow in the smart grid, mainly including the value created by innovative services and market mechanisms and the value added by the information flow. Specifically, by integrating PIoT with cyber-physical systems, this article sketches a conceptual framework of the cyber-physical power system (CPPS). The CPPS carries out holistic perception and ubiquitous connection of distributed energy sources and electrical facilities and builds up a smarter power grid with global information interaction, intelligent decision-making, and real-time agile control. Finally, for illustration purposes, we conduct a case study regarding an intelligent home management system.

Keywords: 5G, smart grid, power IoT, cyber-physical power system, energy flow, information flow, value flow

Edited by:
Uche Kennedy Chude-Okonkwo, University of Johannesburg, South Africa

Reviewed by:
Muhtahir Oloyede, University of Ilorin, Nigeria

Correspondence:
Minghua Xia
xiamingh@mail.sysu.edu.cn

Specialty section:
This article was submitted to IoT and Sensor Networks, a section of the journal Frontiers in Communications and Networks

Received: *01 April 2021*
Accepted: *31 May 2021*
Published: *24 June 2021*

Citation:
Liu Y, Yang X, Wen W and Xia M (2021) Smarter Grid in the 5G Era: A Framework Integrating Power Internet of Things With a Cyber Physical System. Front. Comms. Net 2:689590. doi: 10.3389/frcmn.2021.689590

1 INTRODUCTION

By integrating state-of-the-art information and communication technologies (ICTs) with legacy urban infrastructure facilities, it is envisaged that future cities will evolve into huge cyber-physical systems and finally a digital-physical twinning world. To this end, a smart grid is of the first and foremost importance. For instance, in the Texas power crisis that occurred in February 2021, the United States, a massive electricity generation failure in the state of Texas resulted in shortages of water, food, and heat, yielding more than 4.5 million homes and businesses being left without electricity in severe winter storms (Campbell, 2021).

According to the definition made by the American Electric Power Research Institute in 2011, a smart grid is an electricity network enabling a two-way flow of electricity and information (EPRI, 2011). Unlike traditional electric power grids with only a one-way electricity flow, the smart grid allows a two-way electricity flow between power grids and electricity customers. More importantly, integrating ICTs into power grids yields a novel two-way information flow and enables grids to have self-healing capabilities and electricity customers to become active participants.

Figure 1 shows the conceptual model of smart grid, proposed by the National Institute of Standards and Technology (NIST, 2014). It consists of seven domains and energy/information flows

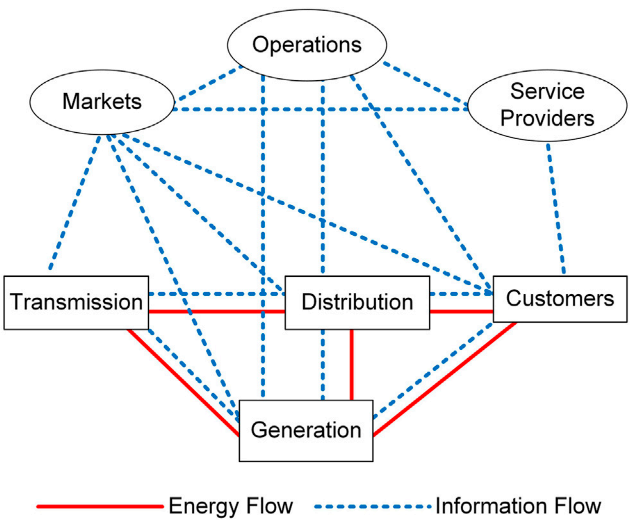

FIGURE 1 | Conceptual model of a smart grid.

among them. The four lower domains correspond to the physical facilities in traditional power grids, and they represent the power generation, transmission, distribution, and customers. Among them, there exists a legacy energy flow, as denoted by the solid red lines. The three upper domains are mainly related to information communication infrastructure and electricity services, including power markets, operations, and service providers. The information flow denoted by dashed blue lines among all seven domains allows their interaction, equipping the power grid with intelligence.

Integrating energy flow and information flow enables additional functionality of the smart grid. On the one hand, the power grid is the carrier of electricity. Complete physical facilities and grid architecture ensure energy flow and provide powerful and reliable electricity transmission and supply to meet optimal dispatch of electricity in a wide area. On the other hand, the information network is the soul of the smart grid. Characterized by informatization, automation, and interaction, the smart grid improves the quality of the power supply and provides diversified services for customers securely and efficiently. Unlike a traditional power grid, in a smart grid, the information network plays a more important role. Relying on advanced ICTs, the smart grid has a highly reliable and flexible communication infrastructure, to realize real-time information interaction, and to provide more reliable asset supervision, load management, peer-to-peer electricity trading, and other innovative electricity services.

As a typical application of 5G technology to machine-type communications, in recent years, the Internet of Things (IoT) was widely integrated into power grids, yielding the so-called power Internet of Things (PIoT) (Wang and Wang, 2018). In principle, the IoT provides interconnection for anyone and anything, which is no longer limited to devices or objects, but also applications and human behaviors, among others (Shafique et al., 2020). In a PIoT, various electrical premises and power facilities interconnect to provide efficient and secure electricity services. After PIoT interconnects physical facilities and makes traditional power grids to evolve into smart grids, the cyber-physical system (CPS) can improve the intelligence level of a smart grid, by interacting between physical facilities and the cyber world and controlling the physical process with the help of processed data and information (Gavriluta et al., 2020). In other words, PIoT implements the interconnection of the wide-area devices and performs data collection, storage, and aggregation, while the CPS performs data mining and information retrieval and makes effective, reliable, accurate, and real-time control of the physical process in the smart grid. From the perspective of the CPS, PIoT is a network infrastructure that provides the mapping from physical into cyber worlds.

To further explore the potential of PIoT, this article conducts a comprehensive overview of PIoT regarding architecture, enabling technologies, security, and privacy issues. Then, integrating PIoT with the CPS yields a cyber-physical power system (CPPS), making the current smart grid turn smarter. In particular, in addition to the energy flow and information flow, a new value flow is created, and the operation of the next-generation smarter grid is value driven. In brief, the CPPS carries out holistic perception and ubiquitous connection of distributed energy resources and electrical facilities to build up a smarter power grid with global information interaction, intelligent decision-making, and real-time agile control.

The remainder of this article is organized as follows. **Section 2** describes the PIoT architecture, enabling technologies, security, and privacy issues. **Section 3** sketches a cyber-physical power system for a future smarter grid, including a conceptual framework and the corresponding cloud-pipe-edge-end architecture. **Section 4** performs a case study of a home energy management system. Finally, **Section 5** concludes the article.

2 POWER INTERNET OF THINGS

For the intelligent development of power grid, in addition to building a sound power physical infrastructure, it is also necessary to realize the digitalization, informatization, automation, and interaction of a power grid.

As shown in **Figure 2**, PIoT is composed of the perception layer, network layer, platform layer, and application layer, which, respectively, focuses on data collection, transmission, management, and value creation. At the perception layer, all things are interconnected, and the state of a power grid is fully visualized; at the network layer, backbone network, distribution network, and terminal access network ensure the ubiquitous and all-time communication ability; at the platform layer, digital management makes power grid knowable and controllable; and at the application layer, power grid provides all kinds of services to create greater opportunities for all walks of life. Cyber security and privacy is an important issue throughout all layers in data-based PIoT. For reaching IoT's full potential in smart grid, we should fully consider the characteristics of the layers, and select appropriate facilities, devices, and communication technologies for various applications. We discuss the different layers and cyber security and privacy issue in the following.

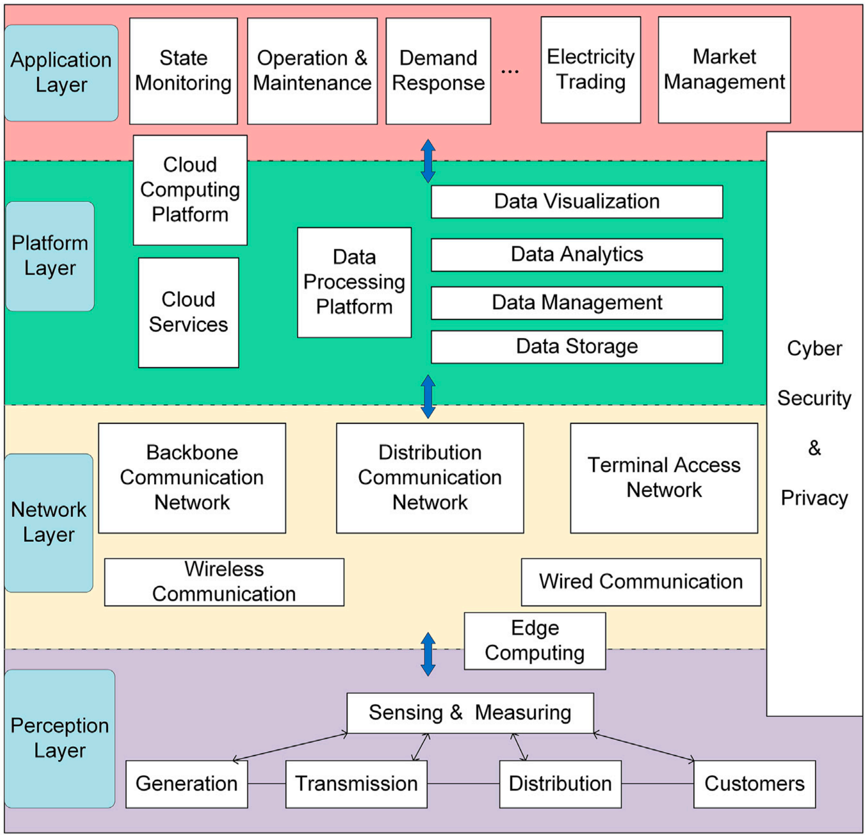

FIGURE 2 | Architecture of power IoT.

2.1 Perception Layer: Sensing and Measurement

The sensing and measurement facilities and devices in the smart grid include intelligent metering equipment, phasor measurement units (PMUs), various sensors, *etc.* They compose the perception layer and play a critical role in data collection. Sensing and measurement devices are deployed in the whole area of the power grid to realize the digitalization and visualization through the ubiquitous information network. Through smart meters, PMUs, and various sensing devices, the physical grid is intensively perceived in time and space and can be easily mapped into a digital logical grid.

2.1.1 Smart Meter–Based Advanced Metering Infrastructure

A smart meter is a kind of equipment that fundamentally changes the operation of power grid and promotes the intellectualization of a power grid. Smart meters enable two-way information flow and energy flow between the customer and supplier. In addition to performing the function of metering, smart meters can act as intelligent sensing devices and actuator in distribution network, participating in the distribution and management of energy (Alahakoon and Yu, 2016).

Advanced metering infrastructure (AMI) based on smart meters is the core infrastructure of the smart grid. AMI consists of three key components: smart meters, two-way communication links, and a data center for data aggregation, analysis, and processing. Smart meters collect the electric power data and transmit them to a data management system. After data analysis, the system makes decisions, such as billing, load forecasting, load management, and demand response. When customers deploy the distributed energy system, AMI allows customers to sell the excess electricity to the grid through the market. Hence, AMI can improve the quality of power supply and the service level by building a two-way interactive relationship of energy flow and information flow between public utilities and households.

With the increasing deployment of AMI, the amount of electric power data increases sharply such that the centralized architecture for AMI will not be sustainable. By contrast, the distributed architecture with an advanced computing technology such as edge and fog computing will provide more powerful performance (Olivares-Rojas et al., 2020). In the 5G and IoT era, the advanced distributed architecture, the ICT, and the security mechanism are the key to the intelligent functionality of AMI.

2.1.2 PMU-Based Wide-Area Measurement System

PMUs play a more important role in wide-area measurement systems and state estimation in transmission network. PMUs support synchronous data collection and calculation. They connect with multiple substations and upload data in real time, which are used for dynamic monitoring and management, system prediction, and protection of smart grid.

A wide-area measurement system has four key components: PMUs, phasor data concentrator (PDC), applications, and information network among PMUs and PDC. A PMU obtains synchronous measurement and transmits data to the PDC through the information network. The decision-making and control center make the corresponding predictive correction and protection measures based on these data and send the feedback signal for self-control. Compared to situational awareness of supervisory control and data acquisition (SCADA), the advanced PMU has a higher update frequency that can adapt to the highly dynamic operations of the smart grid (Gore and Valsan, 2018). Using PMUs for distributed state estimation benefits lower cost of data communication, sufficient redundancy and stability, and higher accuracy and efficiency. However, a distributed PMU network is vulnerable to hackers. And malicious manipulation of PMU data causes damage to power transmission and distribution, regardless of potential voltage instability or out of phase. Therefore, it is necessary to fully consider the information security of the PMU and evaluate the impact of distributed state estimation on a power grid (Cosovic et al., 2017).

2.1.3 Wireless Sensor Network

Considering the diversification and the explosive growth of electric power data and high demand for real-time interaction, the low scalability, low flexibility, and relatively high deployment cost of wired networks restrict the development of the smart grid, which promotes the application of wireless sensor networks. Sensor nodes in wireless sensor networks are responsible for measurement, data processing, storage, and communication. And they transmit information to sink nodes in a multi-hop way. Sink nodes have powerful computing and communication capabilities, and they connect to the management center. The management center makes decisions according to the acquired information of sensor networks. Wireless sensor networks are capable of self-organization, self-healing, adaptivity, and multi-hopping. They enhance the reliability of the power grid information network by allowing better monitoring of the system components, implement coordinated protection, and avoid and reduce the power grid fault (Chhaya et al., 2017).

The wireless sensor network plays a critical role in many fields of the smart grid, such as wireless automatic meter reading, remote system monitoring, and equipment fault diagnosis. However, wireless sensor networks are inherently limited to battery life, processing capability, and cache capacity. Therefore, it is imperative to ensure the performance of sensor nodes and extend the network life span under strictly resource-constrained conditions (Ogbodo et al., 2017).

2.2 Network Layer: Communication Technologies in a Smart Grid

To facilitate the interconnection and intercommunication of grid components, one must adopt an open and plug-and-play communication network architecture. It is also necessary to use universal standards and protocols to enable seamless communication among various devices. The network layer of PIoT has a ubiquitous communication capability around the clock and realizes the holographic perception of the power grid. To choose the most suitable communication technology and infrastructure for the smart grid, four key factors to be considered in practice consist of deployment duration, operation and management costs, communication performance, and environmental factors. In the following, the pros and cons of six typical communication technologies widely applied to the smart grid are sketched, including four wireless technologies and two wired technologies.

2.2.1 ZigBee

ZigBee is a low-power wireless communication technology based on the physical layer and medium access control layer of the IEEE 802.15.4 standard developed by the ZigBee Alliance (LAN/MAN Standards Committee, 2003). ZigBee is devoted for wireless devices that require a low data rate and ultralow power consumption. It is mainly applied in the fields of industrial control, home automation, building automation, energy management, personal health care, and consumer electronics.

The mesh topology of the ZigBee network is capable of self-healing and route repair. These features provide scalability, stability, and tolerance to node and link failures. These powerful network characteristics, as well as high anti-interference performance, have promoted the application of ZigBee in distribution network measurement, monitoring, and home energy management. For instance, integrating ZigBee-based smart devices with machine learning benefits intelligent home control with high robustness, stability, and efficiency for home's energy control and management (Zhang et al., 2019).

2.2.2 WLAN

Wireless local area network (WLAN) can provide high data rate communication with low latency, and perform point-to-point and point-to-multipoint communication within a limited coverage area such as home area network (HAN). In WLAN, Wi-Fi, a wireless network protocol based on the IEEE 802.11 standards, is widely used for local area networking of devices and Internet access.

WLAN is greatly affected by interference, such as the electromagnetic interference of high-voltage electrical equipment and the interference of other wireless signals. Moreover, WLAN is vulnerable because the transmission channel is open such that anyone within the range of a network with a wireless network interface controller can attempt to access it. However, with the advantages of easy deployment, flexible topology, and high scalability, WLAN can form a dynamic self-organizing and self-healing network. In practice, WLAN is suitable for applications with a high data rate and low-interference environment requirements, such as smart meters communication (Hlaing et al., 2017) and substation communication (Zheng et al., 2018).

2.2.3 Cellular Communication

Cellular communication has a long history of development, and almost everywhere, ubiquitous cellular communication systems and infrastructure already exist. With the characteristics of broadband, such as high data rate and wide-area coverage, cellular communication helps reduce investment in dedicated communication infrastructure, allows rapid deployment of applications, and provides low maintenance costs and high performance.

In the smart grid, cellular technologies suit wide-area intelligent applications such as automatic demand response and remote monitoring and control of distributed energy resources. However, cellular technologies need to be tailored and/or strengthened because cellular technologies such as LTE were designed originally for mobile communication. Therefore, it is necessary to fully consider the spectrum usage, data flow characteristics, security, energy efficiency, reliability, and congestion mechanism of cellular technologies. For instance, narrow-band IoT is promising for machine-type communications with a low power and data rate in a smart grid (Li et al., 2018).

2.2.4 WiMAX

WiMAX, a microwave access technology with global interoperability, is a communication technology developed by the IEEE 802.16 wireless broadband standard. It supports long-distance and broadband wireless communications, especially in rural and suburban areas. WiMAX is devoted to point-to-multipoint communications in fixed or mobile applications, allowing thousands of simultaneous users in wide-area coverage.

On the account of wide-area coverage, high data rate, low latency, and high scalability, WiMAX is suitable for smart grid applications such as wireless automatic meter reading and real-time pricing. In particular, WiMAX mesh networks can use multiple channels and rapidly identify outages and restore, thereby improving reliability and efficiency of smart grid operation (Eissa, 2018). However, WiMAX deployment costs and equipment are expensive, and the radio frequency that can be easily interfered by obstacles is very high. Therefore, it is imperative to select suitable geographic locations for WiMAX towers to meet higher quality of service (QoS) requirements (Tavasoli et al., 2016).

2.2.5 Power Line Communication

Power line communication (PLC) refers to a communication technology that exploits power lines to transmit data and media signals. PLC is divided into narrowband PLC and broadband PLC. The former works between 3 and 5 kHz frequency band with a low data rate, which is suitable for sensor measurement applications in the power grid. The latter works in 2–250 MHz with a data rate up to hundreds of Mbps, which is more inclined to media entertainment and Internet applications.

PLC is widely used in the monitoring, control, and automation of medium-voltage power grids and substations, mainly involving fault location, isolation, and recovery. PLC can exploit the existing distribution line as the transmission line and easily penetrate into every family, providing plug-and-play communication at a very low cost. However, the PLC communication system is vulnerable to high noise, poor communication channel condition, interference sensitivity, and low security such that it is not suitable for high-quality data transmission services. In practice, PLC is usually integrated with other communication technology, for example, wireless communication systems, for smart grid applications (d. M. B. A. Dib et al., 2018).

2.2.6 Fiber-Optic Communication

Fiber-optic communication refers to a communication method that uses optical fiber to transmit information, which performs great in high data rate, very low interference, reliability, security, and broadband. In the smart grid, it is mainly used in the backbone network between the wide area network (WAN) and the neighborhood area network (NAN), connecting the control center, substations, and public utilities, bringing extremely low latency, high data rate, and coverage of hundreds of kilometers, and being free from electromagnetic interference.

As fiber-optic communication suffers from poor scalability and high cost of deployment and maintenance, integrating fiber-optic communication with other technologies like wireless communications provides heterogeneous solutions for communications with strict latency and reliability requirements. For instance, with the integration of fiber-optic communication into a wireless sensor network, the collected information is transmitted to a data center through optical fibers to process front-end data in real time. Advanced optical fiber sensor network helps realize the real-time monitoring and control of the power system and improve the stability of the power system (Akerele et al., 2019).

To sum up, **Table 1** compares the performance of communication technologies described above. It is not hard to see that cellular communication, especially 5G technology, outperforms the others in terms of data rate, coverage, latency, and deployment cost.

2.3 Platform Layer

The platform layer of PIoT refers to a digital power grid platform that integrates physical grid architecture and information network infrastructure. The digital platform employs big data and artificial intelligence (AI) technologies to gather, store, manage, and analyze data. And it realizes the holographic perception and intelligent decision-making of the power grid. As shown in **Figure 2**, the components and functionalities of the digital grid platform include both cloud computing platform for cloud services and data processing platform for data storage, management, analysis, and visualization, as each detailed below.

Data at the platform layer come from various sources at the lower perception layer, including power grid state data, operation data, and external environmental data. The cloud computing platform provides electricity services and applications *via* a remote cloud computing server rather than an on-site server. Cloud services do not only benefit from decoupling applications and physical servers but also reduce costs on building infrastructure and maintaining local servers. Moreover, it provides scalable computing resources for data processing as per service and application requirements (Talaat et al., 2020).

The data storage module typically includes distributed file systems, distributed databases, relational database management

TABLE 1 | Comparison of typical communication technologies for a smart grid.

Technology	Standards	Data rate[a]	Distance covered	Latency	Cost	Scope
ZigBee	IEEE 802.15.4	Low	100 m	50 ms	Low	HAN
WLAN	IEEE 802.11ax	Very high	70 m	3 ms	Medium	HAN and NAN
	IEEE 802.11ac	High	70 m	10 ms	Low	HAN and NAN
	IEEE 802.11n	Medium	50 m	15 ms	Low	HAN
	IEEE 802.11g	Medium	50 m	15 ms	Low	HAN
Cellular	2G	Low	35 km	300 ms	Low	HAN and NAN
	3G	High		100 ms	Low	HAN, NAN, and WAN
	4G	High		10 ms	Low	HAN, NAN, and WAN
	5G	Very high		<1 ms	Medium	HAN, NAN, and WAN
WiMAX	IEEE 802.16	Medium	30 km	50 ms	High	NAN and WAN
PLC	\	High	1–5 km	5 ms	Medium	HAN and NAN
Fiber-optic	\	Very high	>100 km	3 μs/km	High	NAN and WAN

[a]*Data rate: low (<1 Mbps), medium (1–100 Mbps), high (100 Mbps-1 Gbps), and very high (>1 Gbps).*

systems, and distributed message queues, providing high-performance life-cycle data storage and access. The appropriate storage strategy is usually chosen according to data types and characteristics to ensure adequate storage capacity. The connections between different storage systems are crucial to data fusion, yielding an optimal amount of data and valuable information from them (Ding et al., 2019).

The data management module supports various functionalities of model management, data asset operation and maintenance, and metadata management. Data management refers to the effective use of hardware and software resources to systematically gather, manage, and extract useful information from big data of the smart grid to build up a unified public data model. The unified framework for data management is fundamental to data consistency, interoperability, granularity, and reusability (Gharaibeh et al., 2017).

The data analytics module refers to the process of a large number of diverse data, which can discover potentially useful data characteristics and relationships. It uses distributed computing and grid simulation technology to realize the whole process of power grid simulation, electrical calculation, spatial analysis, topology analysis, *etc*. Moreover, data are deeply analyzed using approaches, like deep learning and reinforcement learning, to enhance intelligent applications, grid operations, and customer insight (Syed et al., 2021).

The data visualization module uses graphics and image processing and computer vision to implement visual interpretation of data (Sanchez-Hidalgo and Cano, 2018). The visualization module effectively integrates the large-scale computing capabilities and human cognitive abilities to realize power grid simulation and panoramic visualization. It provides historical data query and inversion, self-served application intelligence, and multi-terminal mobile decision support, and supports the construction of digital power grid visualization applications.

After comprehensive data processing, the platform layer can fully explore the value and benefit in the data; ensure the safe, secured, and stable operation of the grid; provide value-added services; and create new value for various power businesses at the application layer.

2.4 Application Layer

The application layer is the highest in PIoT architecture from the perspective of client's end. Ready-to-use data from the platform layer create value only if they result in problem-solving solutions and achieve different application goals. The application layer needs to precisely match data with various affairs, closely link the data with the specific content of various transactions, and realizes the combination of data and smart grid applications. With graphic user interfaces, smart grid applications such as state monitoring and demand response are implemented through PIoT, allowing the smart grid to benefit from IoT and manipulate the physical power grid.

Many smart grid applications exist in this layer, with each having very different requirements. For example, the demand response application needs to respond to load changes timely and reliably, while the state monitoring application needs to collect small packet data from massive devices. Indeed, each smart grid application is the collaboration of all layers. Taking reading meters, for example, one obtains the customers' power consumption and load information, acting as sensors at the perception layer of PIoT. Then, the electric power data are sent through the network layer to the data center at the platform layer for data analysis. Then some corresponding strategies such as automatic billing and pricing are made at the application layer. In the 5G era, the smart grid can support more and more new application scenarios with ICTs. Equipped with AI and machine learning technologies, the application layer can efficiently handle the stochastic factors influencing the smart grid. For instance, the smart grid can provide a customized power plan through learning from customer behaviors such as daily electricity load profiles inferred from smart metering data (Wang et al., 2019). Meanwhile, a novel event classification can help smart grid operators to detect and classify local events that have a considerable impact on safety and operation. The work (Haddad et al., 2018) used artificial neural networks to distinguish different classes of events to maintain the quality and reliability of the smart grid with various impairments. In sum, the application layer is the value realization layer of the combination of energy flow and information flow through PIoT.

2.5 Security and Privacy

The value created by various applications depends heavily on the secure and reliable information flow. However, the large-scale and heterogeneous deployment of smart grid information networks has introduced many network access points. The destruction of any one of the links may directly affect the power generation and distribution of the entire power grid and cause huge economic losses to customers and utilities. For example, an attacker can extract important information such as keys from the memory of a smart meter and insert malicious code into the device to attack other parts of the power grid. In addition, information networks contain the private electricity consumption information of many customers, which discloses personal electricity consumption habits and privacy.

The reliability of the smart grid depends not only on the stable operation of energy grid components and facilities but also on the reliable communication of various intelligent terminal and measuring devices. Therefore, it is imperative to improve the reliability and effectiveness of communications while using more secured mechanisms and algorithms to resist and even avoid network attacks and/or data theft.

2.5.1 Security

Attacks on the power grid can usually be divided into three types (Saghezchi et al., 2017): 1) attacks on the data collection system, making the control center obtain false information and perform wrong operations; 2) attacks on the operation of the power market, disrupting pricing in the electricity market and making profits from it; and 3) attacks on the smart metering and demand-side response, destroying the balance of supply and demand by changing the load status. While the security issues of the PIoT are similar to those of the Internet, they still have particularities (Demir and Suri, 2017): 1) The edge node equipment have the same high-security requirements as the control center; 2) grid data need to be transmitted in time and accurately, which is totally different from the best-effort delivery on the Internet; and 3) the computing and communication capabilities of the grid nodes may be insufficient. Therefore, PIoT adopts lightweight and active data security mechanisms such as identity authentication and access control, intrusion detection, and other security mechanisms.

1 Authentication

Authentication is applied to verify device identity and data validity. Each trusted user has a unique identity and obtains data after being authenticated by both parties during the communication process. There are three main methods of identity authentication: shared key, public key infrastructure (PKI), and biological characteristics. Among them, the PKI is the basic security tool in most telecommunication networks and distributed systems. And it is also the first line of defense to ensure the security of the power grid.

Although the PKI is the most popular key management solution in telecommunication networks, the application of the PKI to the smart grid still faces several challenges, such as scalability, delay, and fault tolerance (Ancillotti et al., 2013). As the PKI requires a high computational cost and communication overhead, the work by Mahmood et al. (2016) proposed a lightweight message authentication scheme for the smart grid. Furthermore, Kumar et al. (2019 proposed a mutual authentication scheme, which requires less computational cost as it builds upon the elliptic curve cryptography, symmetric encryption, hash function, and message authentication code.

2 Access Control

Access control is a data protection mechanism that uses predefined strategies to limit authorized users to access constrained data resources. The commonly used access control method in telecommunication networks is role-based access control (RBAC), which defines different roles according to distinct tasks or functions and then allocates resources and operating permissions for these roles (Saxena et al., 2016).

Electric power data are multidimensional and multilevel. And an efficient aggregation of data and fine-grained data access control are the concerns of security and privacy issues in the smart grid. The work by Lang et al.(2018) proposed a mechanism that tightly aggregates multidimensional data and supports privacy protection and fine-grained access control, called MTA-PA. In the MTA-PA, the authors used homomorphic encryption technology to aggregate multidimensional data into ciphertext and key-policy attribute-based encryption (KP-ABE) to achieve fine-grained dimension-level access control. Moreover, as data in the smart grid were stored in a distributed way due to the cloud-edge computing infrastructure, it is necessary to develop an efficient access control scheme for edge computing infrastructure (Chaudhry et al., 2020).

3 Intrusion Detection

An intrusion detection system (IDS) ensures data security by identifying attacks and triggering appropriate countermeasures. There are three major schemes for intrusion detection technology in the network: signature-based, anomaly-based, and specification-based schemes.

Distributed smart grid network structure leads to the distributed intrusion detection system. The work by Zhang et al. (2011) proposed a hierarchical IDS solution in the power grid. This solution deploys intelligent analysis modules at each network layer, using support vector machines and artificial immune systems to detect and classify malicious data or possible network attacks. The work by Patel et al. (2017) showed that traditional intrusion detection systems based on signature and anomaly techniques are insufficient to protect the smart grid due to the ever-rapidly-evolving masquerades and cyber criminality. Hence, they proposed a collaborative IDS to provide excellent protection with a fully distributed management structure. With the development of machine learning and advanced information processing technologies, IDS will integrate more statistics and machine learning–based algorithms to enhance their efficiency in identifying the data that have different underlying distributions (Ahmed et al., 2019).

2.5.2 Privacy

In the smart grid, smart meters and other measuring instruments frequently collect detailed energy and state information.

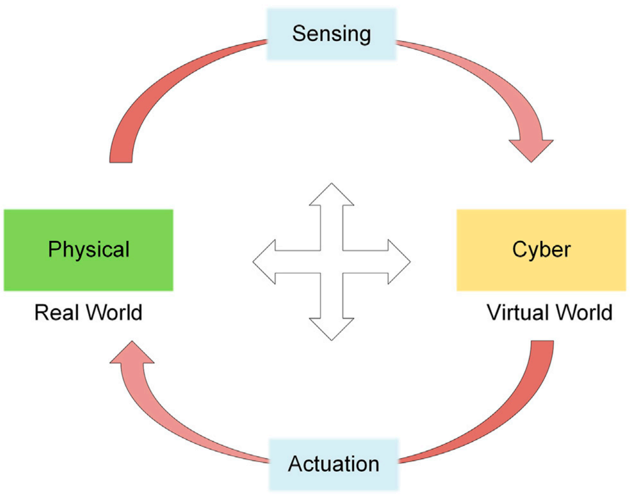

FIGURE 3 | CPS framework.

Although data accuracy is essential to power distribution, demand-side management, load control, and other services, these data may expose customer privacy such as personal energy use mode and power consumption.

To guarantee electricity services and applications while protecting customer privacy, lots of privacy preserving approaches have been proposed, which can be classified into two categories: cryptography-based and non–cryptography-based privacy preserving schemes (Liao et al., 2019).

The cryptography-based privacy preserving approaches in the smart grid are divided into two main categories: anonymization and data aggregation. An effective cryptography privacy preserving is to use an anonymous scheme such that the data are not easy to connect with the relevant customers. For example, each smart meter can be equipped with a key through a trusted third party to correspond to customer data (Ambrosin et al., 2016). Data aggregation is an important method for data management while preserving customer privacy, because it is hard to extract the electricity consumption information of a specific customer from aggregated data. Meanwhile, the aggregated data can be used for electricity applications such as dynamic pricing-based billing and demand response management (Gope and Sikdar, 2018).

A feasible non-cryptography solution is to divide electric power data into two parts: the low-frequency data and the high-frequency data. In this approach, the storage units are used to flatten high-frequency and fine-grained usage curve, and hide detailed energy usage information, which only shows a low-frequency shape for billing (Sun et al., 2018). Another popular non-cryptographic approach is physically unclonable function (PUF)-based approach. PUF devices have a unique physical feature, which is not only non-reproducible by the cryptographic primitives but also too hard or impossible to be cloned physically (Kaveh and Mosavi, 2020). This unique property makes PUF useful in the key generation, authentication and customer privacy protection.

In practice, privacy protection and information accessibility need to be balanced. The more information customers are willing to disclose, the more intelligent decisions the management system can make to improve the service level. However, easy access to information means more privacy leakage, thus obtaining a compromise between accessibility and privacy protection and determines the level of privacy protection to deal with different grid services.

3 CYBER-PHYSICAL POWER SYSTEM

Figure 3 illustrates a basic CPS framework. On the one hand, the physical system (i.e., the real world) perceives the environment and component states, collects and processes data, and sends them to the cyber system through the network. On the other hand, the cyber system (i.e., the virtual world) analyzes the data according to the system model and operating mechanism and sends instructions to the execution devices of the physical system to actuate physical entities.

The CPS embeds the sensing, communication, computing, and control abilities into the physical devices to realize the distributed sensing, reliable data transmission, and comprehensive information processing of the external environment and resources and implements the real-time control of physical entities through the feedback loop. It is a critical premise to reach the intelligent industrial production automation and make the industrial system evolve toward Industry 4.0 (Tao et al., 2019).

In the traditional power grid, the physical system and the information system are relatively separated. Thus, it is hard to achieve refined and automated coordination of grid components. As many electrical devices, data collection devices, and computing devices interconnect through PIoT, the power grid has already had the main characteristics of the CPS to a certain extent. With the construction of grid automation systems, large-capacity transmission networks, ubiquitous sensor networks, and deep integration with the PIoT and power grid, the smart grid continues to evolve into a system with wide-area coordination and autonomous behavior, thus yielding the CPPS.

By integrating physical and cyber worlds, the CPPS enables the bidirectional real-time mapping and interaction between the physical and virtual digital systems. In other words, it is now allowed to reconstruct the objects, events, and human behaviors of the physical world in the digital world and, finally, to apply simulation models to optimize the physical performance in real worlds.

In the evolution of the smart grid, the gradual integration of the physical infrastructure and information system makes the smart grid smarter and smarter, with the following features:

- Heterogeneity and extreme complexity: The smart grid itself is a large-scale heterogeneous complex system. The components in the power grid have different protocols and standards, and the smart grid uses different technologies for the operation in various scenarios, yielding a heterogeneous and extremely complex system.

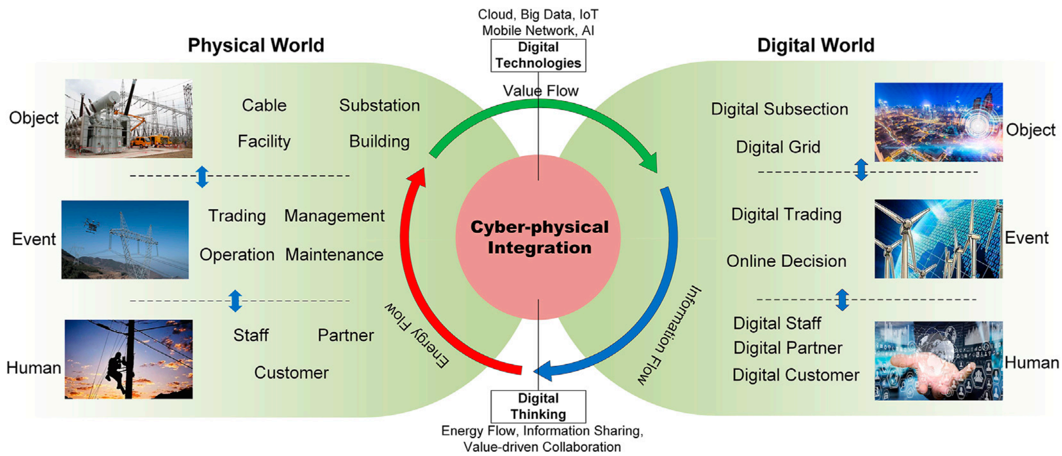

FIGURE 4 | Conceptual framework of the CPPS.

- Adaption and automation: The smart grid enables local control and global optimization through dynamic connections and interactions between physical and cyber systems. Thus, it can automatically and adaptively adjust grid parameters online through fault detection, state estimation, and control system.
- Real-time control: The stability of grid voltage, power, and frequency requires real-time feedback loops of sensing, transmission, and control. The long latency of information processing and asynchrony may lead to instability of the grid state and even destroy the power system.
- Deep integration of physical and digital worlds: Distributed intelligent component integrates with the central monitoring and control system to enable the cyber world to interact with the physical process so that the power grid has the ability of sensing, computing, communicating, and controlling.
- High safety and security: A secure and reliable operation of the smart grid is necessary to ensure people's productivity and living. Power supply interruption will seriously threaten production and personal safety. Therefore, the integration of cyber and physical systems can improve the reliability of the power system as the fundamental premise.

3.1 Conceptual Framework of the CPPS

Figure 4 illustrates the conceptual framework of the CPPS. The objects, events, and human behaviors in the physical world are mapped into the digital world through the information network using state-of-the-art ICTs, to provide a digital image for the complex processes of power generation, operation, management, and control. In the digital world, digital thinking is used to implement power system modeling, simulation, testing, and monitoring, to make efficient production scheduling and planning of smart grid. The core of the CPPS lies in the energy flow, information flow, and value flow and they represent the physical, information, and value dimensions in the CPPS, respectively.

1 Physical Dimension

It mainly involves the energy flow and the physical facilities as the carrier of energy flow. The smart grid aims to realize the generation, transmission, distribution, storage, and consumption of electric energy efficiently, and integrate large-scale distributed energy sources to build a power system with a two-way flow of electric energy.

2 Information Dimension

It takes data generated by an information network as a virtual entity, focusing on data collection, transmission, analysis, and processing. Information flow controls energy flow, conducting the planning and operation of the smart grid. Moreover, the information flow establishes a connection between energy flow and value flow, achieving the optimal value flow through the CPS control center.

3 Value Dimension

It mainly takes the profit and social benefit of energy flow and electrical applications as value entities, focusing on the value creation of smart grids. Driven by ICTs, the power industry creates innovations in business models and market mechanisms, to realize customer-centric value creation, data-centric value extraction, and technology-driven services innovations.

3.2 The Layered Architecture of the CPPS

Based on the aforementioned framework of the CPPS, we are now in the position to show the layered architecture for integrating smart grid with PIoT, and to analyze how the physical and cyber systems interact in the future smarter grid from the perspective of the CPS. In the context of the CPS, this subsection analyzes the key components, domains, and their interactions, to provide a deeper understanding on the integration of the smart grid, ICT, IoT, and CPS.

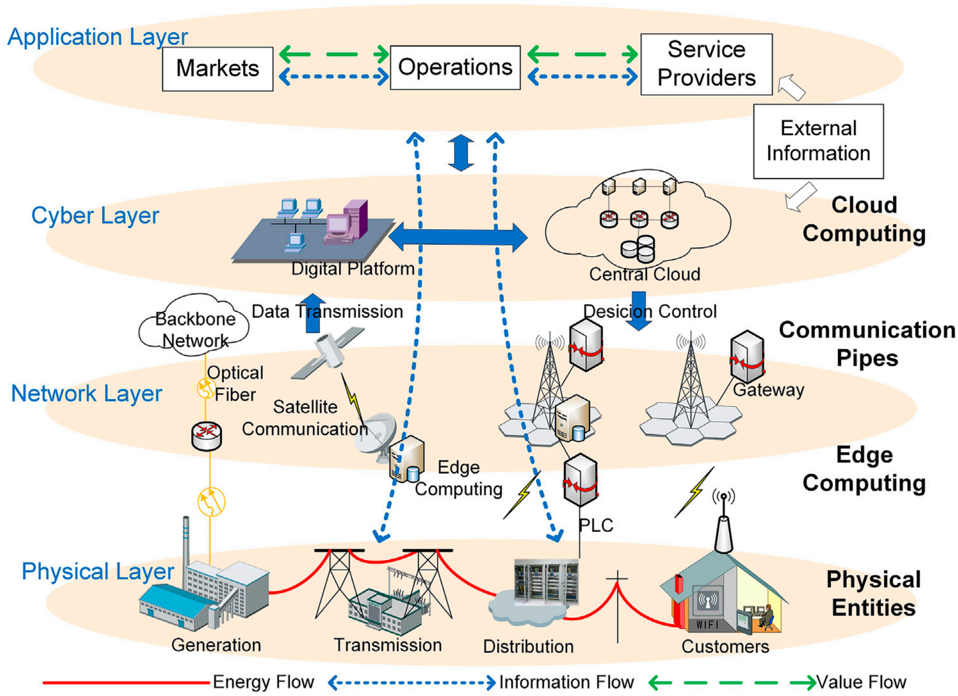

FIGURE 5 | Layered architecture and enabling technologies of the CPPS.

As shown in **Figure 5**, the CPPS architecture includes four layers: the physical layer, network layer, cyber layer, and application layer. The interaction of the four layers relies on the information flow across them. More specifically, the main functions of each layer are as follows:

- Physical layer (i.e., facilities layer) is the fundamental layer of the architecture, including various physical facilities and executors in the grid. It is deployed in a distributed manner, and the decision-making instructions are executed in this layer to achieve the required system functionality. Also, the enery flows in a two-way fashion within this layer among the power generation, transmission, distribution, and customers.
- Network layer (i.e., communication network layer) is the key of the architecture, which makes a bridge between the lower physical layer and the upper cyber layer. It describes the overall functions of the information network, namely, how the electrical facilities make the interaction between heterogeneous components and execute the control instructions of the upper layer.
- Cyber layer (i.e., decision-making layer) is the core of the architecture, which consists of a cloud computing–based central processing mechanism and distributed computing intelligence to optimize both computing and control strategies. This decision-making layer acts as the executive brain of the whole system and provides the human–computer interface with the upper layer to coordinate all the lower layers by designing and sending appropriate commands.
- Application layer (i.e., application, management, and control layer) includes service providers, markets, and operations between them, which is the highest level decision-maker. The decision-makers consider all issues from the perspectives of economy, society, and environment, taking market regulation, pricing, and incentive measures into account to conduct the power generation and consumption in the physical world. A dominant feature of this layer is that the optimal operations are performed based on the two-way information, and value flows between the markets and service providers.

To put the CPPS into practice, there are four enabling ICTs; they are cloud computing, communication pipes, edge computing, and physical entities, with each detailed below.

1 Cloud Computing

The CPPS needs to analyze, process, and make decisions on big data, which poses new challenges to the computing and information processing capabilities. Cloud computing can meet the business requirements of massive data for networking, storage, and computing, and provide rich application services. With the support of virtualization technology, cloud computing can integrate the hardware and software resources distributed in different geographical locations to form a virtual platform with strong storage and computing capabilities. As cyber hardware is maintained at the cloud side, the electric power users only need to pay on demand and thus can largely reduce the local investment and operation costs on the hardware and software.

Cloud-based information infrastructure for smart grid has several merits, such as scalable resource provision and access convenience (Luo et al., 2016). Cloud computing can dynamically provide services to users on demand according to the different electricity application requirements in a distributed computing mode. Cloud can be accessed anytime and anywhere through the Internet; at the same time, many cyberattack-defending mechanisms for the specific power applications can be implemented to ensure security and fault tolerance (Guan et al., 2017).

2 Communication Pipes

Communication pipes refer to the data transmission channels between the physical layer and cyber layer, connecting user terminals, edge devices, and cloud computing resources, which represent the ubiquitous information network in the smart grid. In the CPPS, as various electricity services have different communication, computing, and cache requirements, deploying dedicated physical facilities for different types of applications is cost-intensive and may degrade interconnection and interoperability of the grid. Instead, communication pipes should integrate multiple communication methods to provide common communication services for different application scenarios.

5G network slicing provides distinct virtual networks and differentiated QoS guarantees under a shared physical infrastructure, which is a promising solution for the CPPS to efficiently handle different electricity services. Through the architecture based on virtualization and software-defined network, 5G network slicing realizes an end-to-end, multiservice ecosystem, in which users share the underlying physical infrastructure resources and use a virtualization method to efficiently meet requirements of various applications. However, the main difficulty in network slicing lies in how to efficiently use the physical network and computing infrastructure, and provide a reliable and secure connection and computation to the CPS (Liu et al., 2020). Machine learning is the potential to automate and optimize network slicing efficiently in a heterogeneous and dynamic environment (Sun et al., 2019).

3 Edge Computing

Edge computing is to deploy distributed intelligent agents at the edge of the network, which provides network, computing, storage, and application services near data sources. While cloud computing provides the computing resources needed by the smart grid, the remote central cloud is far away from data source, resulting in long-time latency. Using MEC to offload tasks to the local edge, many electricity applications and services will benefit from localized communication and data processing, thus dramatically decreasing service response latency, reducing the communication overhead and traffic load on the central network, and improving context awareness (Cosovic et al., 2017). It helps for peak-load shifting and balances the load with the demand in real time, to carry out the optimal electric power distribution.

MEC doubles the hardware resources and software applications at the end side, bridging the physical world and the cyber world. To some extent, MEC has certain computing and storage capacity at the local, avoiding the long-distance transmission of data. As computing capacities extend to the edge of the network, cooperative edge-cloud solutions help improve distributed intelligence and decision-making ability of the CPPS (Liu et al., 2019).

4 Physical Entities

Physical entities refer to various electrical and electronic equipment involved in the power grid. As the basic units of the power system, they are distributed throughout the power grid and perform distributed sensing and acting tasks. Through sensor technology, chip technology, and IoT, physical entities create a comprehensive network to enable the CPS and various stakeholders to interact closely. Physical entities can be connected to monitors or computers through the network, and provide a graphical interface for human–computer interaction. Through the device and network, customers have a deeper understanding on the electricity application and services, providing electrical staff with easier equipment control.

AI makes it possible for physical entities to learn from experience and environment, adjust to new inputs, and perform human-like tasks. As further development of distributed computing, physical entities may have certain computing capabilities and can apply for simple programs. Device-to-device (D2D) communication allows adjacent entities to establish direct communication links between them without a third-party base station, to share their connection, or directly communicate and exchange information. Therefore, the combination of D2D and AI provides communication and computing ability among local entities, which have potential to perform task completely at the device side without any servers. Decentralized federated learning techniques are promising solutions for these server-less applications (Savazzi et al., 2020).

4 CASE STUDY: AN INTELLIGENT HOME ENERGY MANAGEMENT SYSTEM

In a traditional home energy management system (HEMS), the efficiency of energy management and planning is very low due to inadequate energy consumption information collection and analysis, leading to high energy cost. By integrating PIoT and the CPPS, HEMS is equipped with much more powerful situation awareness ability and automatic control ability, turning to intelligent HEMS. Through advanced network infrastructure and machine learning–based big data analysis and control strategies, intelligent HEMS can improve the efficiency and provide innovative home energy management services, such as fine-grained consumption data collection, management for electric vehicles, precise load control, and customized energy management. Moreover, intelligent HEMS promotes comprehensive visibility, flexibility, and control of home assets and energy, and finally increases convenience and happiness of resident.

Figure 6 illustrates the architecture of integrating PIoT with the CPPS in an intelligent HEMS, which from the bottom-up

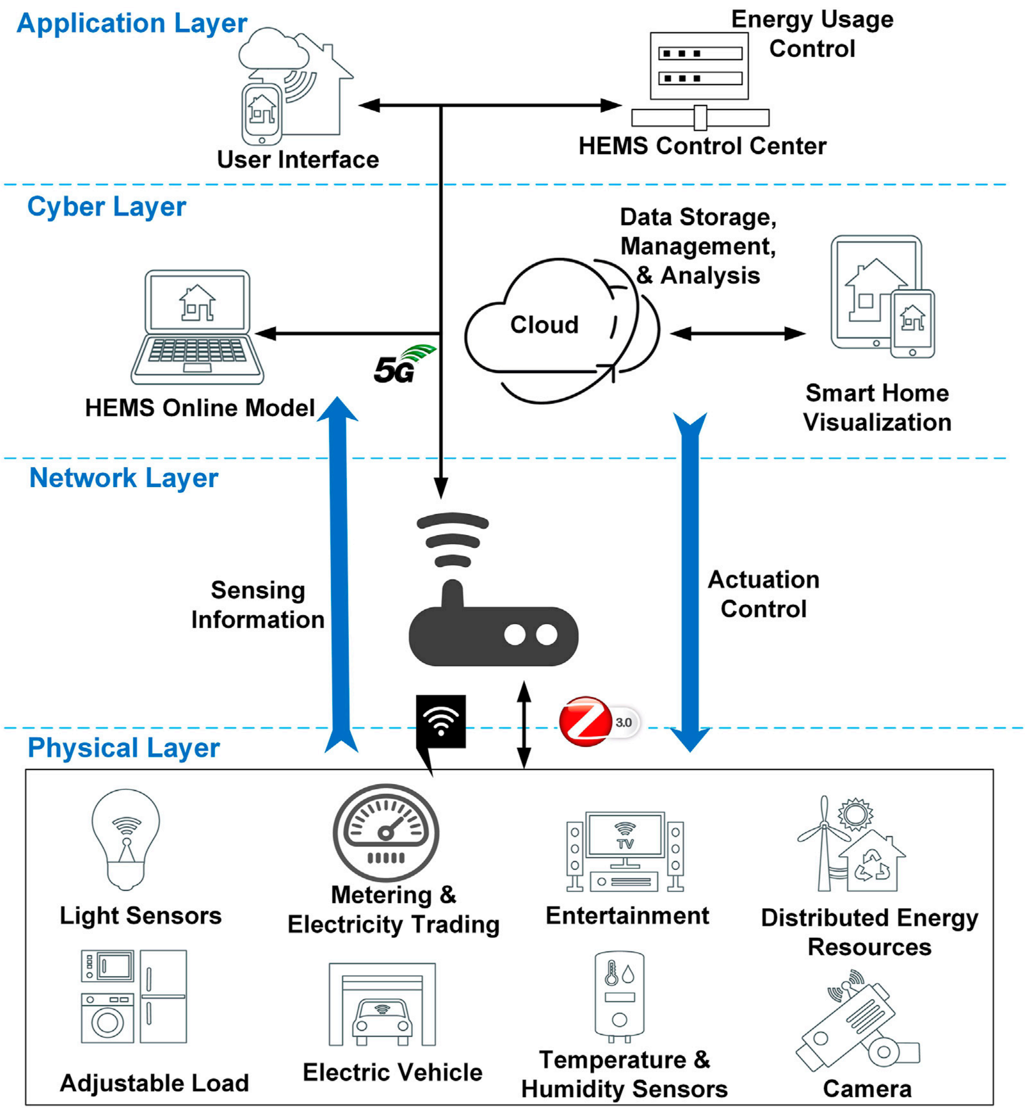

FIGURE 6 | Architecture of an intelligent home energy management system.

includes the physical layer, network layer, cyber layer, and application layer. The physical layer comprises all kinds of household electrical appliances, various sensors (e.g., temperature sensors, humidity sensors, and light sensors), data collection devices (e.g., smart meters and cameras), and electric actuators (e.g., light controllers and voltage/current controllers). Distributed energy resources, storage units, and electric vehicles enable the two-way energy flow between household consumers and power grid, which requires robust two-way information flow for interaction. The PIoT in the home area network provides interconnection for things, objects, and electricity applications, collecting household environment data, energy consumption data, and user behavior data.

The data generated in the physical layer are transmitted to the network layer using Wi-Fi, ZigBee, and other short-distance communication technologies. Then, the network layer forwards the environment and energy data to the upper cyber layer using long-distance 5G communication technologies, where cloud computing provides data storage, management, and analysis. It is noted that the hybrid communication network can provide seamless two-way data transmission, to provide mutual real-time interaction between physical measurement systems and digital control systems. Each intelligent HEMS allows to update local AI models for efficient energy management and to customize local energy management plans, making adaption to distinct living habits of different families. Furthermore, the data can reuse anytime and anywhere to build up home energy management visualization. The application layer comprises user interfaces and a control center to provide various advanced energy management applications and services.

On the other hand, the layered architecture integrating PIoT with the CPPS implements intelligent home energy management through four steps. At first, the environment and energy data are sensed and aggregated by the local home area network. Then, the data are sent to a remote cloud computing center operated by a HEMS service provider for data processing and fusion. Afterward, the CPPS analyzes the data and optimizes the HEMS model or generates control parameter and instructions. Finally, the control center delivers control instructions to actuators to perform energy management for optimal energy consumption cost and user satisfaction.

5 CONCLUSION

This article integrated the power Internet of Things (PIoT) with the cyber-physical system, yielding a cyber-physical power system (CPPS) for the next-generation smart grid. First, we presented a brief overview of the architecture and enabling technologies of PIoT. Then, the PIoT was integrated into the CPPS and allowed a mapping from the physical world into the cyber world, followed by a case study of an intelligent home energy management system. Unlike the traditional smart grid focusing on the two-way energy and information flows, the dominant feature of the CPPS is its two-way value flow, mainly including the value created by innovative services and market mechanisms and the value added by the information flow. We look forward that the CPPS sheds new light on the design and development of a smarter grid.

DATA AVAILABILITY STATEMENT

The original contributions presented in the study are included in the article/Supplementary Material; further inquiries can be directed to the corresponding author.

AUTHOR CONTRIBUTIONS

YL carried out the investigations, codesigned the CPPS architecture, and drafted the article. XY codesigned the CPPS architecture. WW developed the use case. MX led the project and conceived the idea of this article. They are all involved in the revisions of the article.

REFERENCES

Ahmed, S., Lee, Y., Hyun, S.-H., and Koo, I. (2019). Unsupervised Machine Learning-Based Detection of covert Data Integrity Assault in Smart Grid Networks Utilizing Isolation forest. *IEEE Trans.Inform.Forensic Secur.* 14, 2765–2777. doi:10.1109/TIFS.2019.2902822

Akerele, M., Al-Anbagi, I., and Erol-Kantarci, M. (2019). A Fiber-Wireless Sensor Networks QoS Mechanism for Smart Grid Applications. *IEEE Access* 7, 37601–37610. doi:10.1109/ACCESS.2019.2906751

Alahakoon, D., and Yu, X. (2016). Smart Electricity Meter Data Intelligence for Future Energy Systems: A Survey. *IEEE Trans. Ind. Inf.* 12, 425–436. doi:10.1109/TII.2015.2414355

Ambrosin, M., Hosseini, H., Mandal, K., Conti, M., and Poovendran, R. (2016). "Despicable Me(ter): Anonymous and fine-grained Metering Data Reporting with Dishonest Meters," in 2016 IEEE Conference on Communications and Network Security (CNS), 163–171. doi:10.1109/CNS.2016.7860482

Ancillotti, E., Bruno, R., and Conti, M. (2013). The Role of Communication Systems in Smart Grids: Architectures, Technical Solutions and Research Challenges. *Comp. Commun.* 36, 1665–1697. doi:10.1016/j.comcom.2013.09.004

Campbell, R. J. (2021). *Power Outages in Texas. CRS Report No. IN11608*. URL: https://crsreports.congress.gov/product/pdf/IN/IN11608

Chaudhry, S. A., Alhakami, H., Baz, A., and Al-Turjman, F. (2020). Securing Demand Response Management: A Certificate-Based Access Control in Smart Grid Edge Computing Infrastructure. *IEEE Access* 8, 101235–101243. doi:10.1109/ACCESS.2020.2996093

Chhaya, L., Sharma, P., Bhagwatikar, G., and Kumar, A. (2017). Wireless Sensor Network Based Smart Grid Communications: Cyber Attacks, Intrusion Detection System and Topology Control. *Electronics* 6, 5. doi:10.3390/electronics6010005

Cosovic, M., Tsitsimelis, A., Vukobratovic, D., Matamoros, J., and Anton-Haro, C. (2017). 5G mobile Cellular Networks: Enabling Distributed State Estimation for Smart Grids. *IEEE Commun. Mag.* 55, 62–69. doi:10.1109/mcom.2017.1700155

Demir, K., and Suri, N. (2017). "Serecp: A Secure and Reliable Communication Platform for the Smart Grid," in *Pacific Rim International Symposium on Dependable Computing (PRDC)* (IEEE), 175–184. doi:10.1109/PRDC.2017.31

Dib, L. d. M. B. A., Fernandes, V., de L. Filomeno, M., Ribeiro, M. V., and Ribeiro, M. V. (2018). Hybrid PLC/wireless Communication for Smart Grids and Internet of Things Applications. *IEEE Internet Things J.* 5, 655–667. doi:10.1109/jiot.2017.2764747

Ding, W., Jing, X., Yan, Z., and Yang, L. T. (2019). A Survey on Data Fusion in Internet of Things: Towards Secure and Privacy-Preserving Fusion. *Inf. Fusion* 51, 129–144. doi:10.1016/j.inffus.2018.12.001

Eissa, M. M. (2018). New protection Principle for Smart Grid with Renewable Energy Sources Integration Using Wimax Centralized Scheduling Technology. *Int. J. Electr. Power Energ. Syst.* 97, 372–384. doi:10.1016/j.ijepes.2017.11.014

EPRI (2011). *Estimating the Costs and Benefits of the Smart Grid*. Palo Alto, CA: Tech. rep (Electric Power Research Institute).

Gavriluta, C., Boudinet, C., Kupzog, F., Gomez-Exposito, A., and Caire, R. (2020). Cyber-physical Framework for Emulating Distributed Control Systems in Smart Grids. *Int. J. Electr. Power Energ. Syst.* 114, 105375. doi:10.1016/j.ijepes.2019.06.033

Gharaibeh, A., Salahuddin, M. A., Hussini, S. J., Khreishah, A., Khalil, I., Guizani, M., et al. (2017). Smart Cities: A Survey on Data Management, Security, and Enabling Technologies. *IEEE Commun. Surv. Tutorials* 19, 2456–2501. doi:10.1109/COMST.2017.2736886

Gope, P., and Sikdar, B. (2018). An Efficient Data Aggregation Scheme for Privacy-Friendly Dynamic Pricing-Based Billing and Demand-Response Management in Smart Grids. *IEEE Internet Things J.* 5, 3126–3135. doi:10.1109/JIOT.2018.2833863

Gore, R. N., and Valsan, S. P. (2018). "Wireless Communication Technologies for Smart Grid (WAMS) Deployment," in IEEE International Conference on Industrial Technology (ICIT), 1326–1331. doi:10.1109/ICIT.2018.8352370

Guan, Z., Li, J., Wu, L., Zhang, Y., Wu, J., and Du, X. (2017). Achieving Efficient and Secure Data Acquisition for Cloud-Supported Internet of Things in Smart Grid. *IEEE Internet Things J.* 4, 1934–1944. doi:10.1109/JIOT.2017.2690522

Haddad, R. J., Guha, B., Kalaani, Y., and El-Shahat, A. (2018). Smart Distributed Generation Systems Using Artificial Neural Network-Based Event Classification. *IEEE Power Energ. Technol. Syst. J.* 5, 18–26. doi:10.1109/JPETS.2018.2805894

Hlaing, W., Thepphaeng, S., Nontaboot, V., Tangsunantham, N., Sangsuwan, T., and Pira, C. (2017). "Implementation of Wifi-Based Single Phase Smart Meter for Internet of Things (IoT)," in *International Electrical Engineering Congress (iEECON)*, 1–4. doi:10.1109/IEECON.2017.8075793

Kaveh, M., and Mosavi, M. R. (2020). A Lightweight Mutual Authentication for Smart Grid Neighborhood Area Network Communications Based on Physically Unclonable Function. *IEEE Syst. J.* 14, 4535–4544. doi:10.1109/JSYST.2019.2963235

Kumar, P., Gurtov, A., Sain, M., Martin, A., and Ha, P. H. (2019). Lightweight Authentication and Key Agreement for Smart Metering in Smart Energy

Networks. *IEEE Trans. Smart Grid* 10, 4349–4359. doi:10.1109/TSG.2018.2857558

LAN/MAN Standards Committee (2003). *Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)*. New York: IEEE Computer Society.

Lang, B., Wang, J., and Cao, Z. (2018). Multidimensional Data Tight Aggregation and fine-grained Access Control in Smart Grid. *J. Inf. Security Appl.* 40, 156–165. doi:10.1016/j.jisa.2018.03.008

Li, Y., Cheng, X., Cao, Y., Wang, D., and Yang, L. (2018). Smart Choice for the Smart Grid: Narrowband Internet of Things (NB-IoT). *IEEE Internet Things J.* 5, 1505–1515. doi:10.1109/jiot.2017.2781251

Liao, X., Srinivasan, P., Formby, D., and Beyah, R. A. (2019). Di-prida: Differentially Private Distributed Load Balancing Control for the Smart Grid. *IEEE Trans. Dependable Secure Comput.* 16, 1026–1039. doi:10.1109/TDSC.2017.2717826

Liu, B., Zhang, Y., Zhang, G., and Zheng, P. (2019). Edge-cloud Orchestration Driven Industrial Smart Product-Service Systems Solution Design Based on CPS and IIoT. *Adv. Eng. Inform.* 42, 100984. doi:10.1016/j.aei.2019.100984

Liu, Q., Han, T., and Ansari, N. (2020). Learning-assisted Secure End-To-End Network Slicing for Cyber-Physical Systems. *IEEE Netw.* 34, 37–43. doi:10.1109/MNET.011.1900303

Luo, F., Zhao, J., Dong, Z. Y., Chen, Y., Xu, Y., Zhang, X., et al. (2016). Cloud-based Information Infrastructure for Next-Generation Power Grid: Conception, Architecture, and Applications. *IEEE Trans. Smart Grid* 7, 1896–1912. doi:10.1109/TSG.2015.2452293

Mahmood, K., Ashraf Chaudhry, S., Naqvi, H., Shon, T., and Farooq Ahmad, H. (2016). A Lightweight Message Authentication Scheme for Smart Grid Communications in Power Sector. *Comput. Electr. Eng.* 52, 114–124. doi:10.1016/j.compeleceng.2016.02.017

NIST (2014). *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0*. Gaithersburg, MD: Tech. rep. (NIST).

Ogbodo, E. U., Dorrell, D., and Abu-Mahfouz, A. M. (2017). Cognitive Radio Based Sensor Network in Smart Grid: Architectures, Applications and Communication Technologies. *IEEE Access* 5, 19084–19098. doi:10.1109/ACCESS.2017.2749415

Olivares-Rojas, J. C., Reyes-Archundia, E., Gutiérrez-Gnecchi, J. A., González-Murueta, J. W., and Cerda-Jacobo, J. (2020). A Multi-Tier Architecture for Data Analytics in Smart Metering Systems. *Simulation Model. Pract. Theor.* 102, 102024. doi:10.1016/j.simpat.2019.102024

Patel, A., Alhussian, H., Pedersen, J. M., Bounabat, B., Júnior, J. C., and Katsikas, S. (2017). A Nifty Collaborative Intrusion Detection and Prevention Architecture for Smart Grid Ecosystems. *Comput. Security* 64, 92–109. doi:10.1016/j.cose.2016.07.002

Saghezchi, F. B., Mantas, G., Ribeiro, J., Al-Rawi, M., Mumtaz, S., and Rodriguez, J. (2017). Towards a Secure Network Architecture for Smart Grids in 5G Era. In International Wireless Communications and Mobile Computing Conference (IWCMC). 121–126. doi:10.1109/IWCMC.2017.7986273

Sanchez-Hidalgo, M.-A., and Cano, M.-D. (2018). A Survey on Visual Data Representation for Smart Grids Control and Monitoring. *Sustainable Energ. Grids Networks* 16, 351–369. doi:10.1016/j.segan.2018.09.007

Savazzi, S., Nicoli, M., and Rampa, V. (2020). Federated Learning with Cooperating Devices: A Consensus Approach for Massive IoT Networks. *IEEE Internet Things J.* 7, 4641–4654. doi:10.1109/JIOT.2020.2964162

Saxena, N., Choi, B. J., and Lu, R. (2016). Authentication and Authorization Scheme for Various User Roles and Devices in Smart Grid. *IEEE Trans.Inform.Forensic Secur.* 11, 907–921. doi:10.1109/TIFS.2015.2512525

Shafique, K., Khawaja, B. A., Sabir, F., Qazi, S., and Mustaqim, M. (2020). Internet of Things (IoT) for Next-Generation Smart Systems: A Review of Current Challenges, Future Trends and Prospects for Emerging 5G-IoT Scenarios. *IEEE Access* 8, 23022–23040. doi:10.1109/ACCESS.2020.2970118

Sun, Y., Lampe, L., and Wong, V. W. S. (2018). Smart Meter Privacy: Exploiting the Potential of Household Energy Storage Units. *IEEE Internet Things J.* 5, 69–78. doi:10.1109/JIOT.2017.2771370

Sun, Y., Peng, M., Zhou, Y., Huang, Y., and Mao, S. (2019). Application of Machine Learning in Wireless Networks: Key Techniques and Open Issues. *IEEE Commun. Surv. Tutorials* 21, 3072–3108. doi:10.1109/COMST.2019.2924243

Syed, D., Zainab, A., Ghrayeb, A., Refaat, S. S., Abu-Rub, H., and Bouhali, O. (2021). Smart Grid Big Data Analytics: Survey of Technologies, Techniques, and Applications. *IEEE Access* 9, 59564–59585. doi:10.1109/ACCESS.2020.3041178

Talaat, M., Alsayyari, A. S., Alblawi, A., and Hatata, A. Y. (2020). Hybrid-cloud-based Data Processing for Power System Monitoring in Smart Grids. *Sust. Cities Soc.* 55, 102049. doi:10.1016/j.scs.2020.102049

Tao, F., Qi, Q., Wang, L., and Nee, A. Y. C. (2019). Digital Twins and Cyber-Physical Systems toward Smart Manufacturing and Industry 4.0: Correlation and Comparison. *Engineering* 5, 653–661. doi:10.1016/j.eng.2019.01.014

Tavasoli, M., Yaghmaee, M. H., and Mohajerzadeh, A. H. (2016). "Optimal Placement of Data Aggregators in Smart Grid on Hybrid Wireless and Wired Communication," in *IEEE Smart Energy Grid Engineering (SEGE)*, 332–336. doi:10.1109/SEGE.2016.7589547

Wang, Q., and Wang, Y. G. (2018). "Research on Power Internet of Things Architecture for Smart Grid Demand," in 2018 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2), 1–9. doi:10.1109/EI2.2018.8582132

Wang, Y., Chen, Q., Gan, D., Yang, J., Kirschen, D. S., and Kang, C. (2019). Deep Learning-Based Socio-Demographic Information Identification from Smart Meter Data. *IEEE Trans. Smart Grid* 10, 2593–2602. doi:10.1109/TSG.2018.2805723

Zhang, J.-L., Zhu, Q.-H., and Yang, X.-Q. (2019). "Design of Intelligent home Control System Based on Machine Learning," in International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS), 498–503. doi:10.1109/ICITBS.2019.00126

Zhang, Y., Wang, L., Sun, W., Green II, R. C., and Alam, M. (2011). Green IIDistributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids. *IEEE Trans. Smart Grid* 2, 796–808. doi:10.1109/tsg.2011.2159818

Zheng, Z., Qiao, L., Wang, L., Cui, W., and Guo, J. (2018). "Discussion and Testing of 802.11ah Wireless Communication in Intelligent Substation," in IEEE International Conference on Energy Internet (ICEI), 208–212. doi:10.1109/ICEI.2018.00045

Conflict of Interest: XY was employed by the company China Southern Power Grid Co., Ltd. WW was employed by the company Guangzhou Techphant Co., Ltd.

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.