IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 11 August 2022, accepted 21 August 2022, date of publication 29 August 2022, date of current version 8 September 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3202914

SURVEY

Cyber-Security of Industrial Internet of Things in Electric Power Systems

HAMED SARJAN[1], AMIR AMELI[1], (Member, IEEE), AND MOHSEN GHAFOURI[2], (Member, IEEE)

[1]Department of Electrical Engineering, Lakehead University, Thunder Bay, ON P7B 5E1, Canada
[2]Concordia Institute for Information Systems Engineering (CIISE), Concordia University, Montreal, QC H3G 1M8, Canada

Corresponding author: Amir Ameli (aameli@lakeheadu.ca)

This work was supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) under Grant ALLRP-566258-21.

ABSTRACT Electric Power Systems (EPSs) are among the most critical infrastructures of any society, since they significantly impact other infrastructures. Recently, there has been a trend toward implementing modern technologies, such as Industrial Internet of Things (IIoT), in EPSs to enhance their real-time monitoring, control, situational awareness, and intelligence. This movement, however, has exposed EPSs to various cyber intrusions that originate from the IIoT ecosystem. Statistics show that 38% of reported attacks have been against power and water infrastructure, and so far at least 91% of power utilities have experienced a cyber-attack. The cyber-security problem is even more severe for IIoT applications in EPSs due to the vulnerabilities and resource limitations of such applications. Thus, based on the above statistics, it is necessary to investigate the vulnerabilities of IIoT-based applications in EPSs, identify probable attacks and their consequences, and develop intrusion prevention and detection approaches to secure IIoT systems. On this basis, this paper first elaborates on the applications of IIoT-based systems in EPSs, and evaluates their security challenges. Afterwards, it comprehensively reviews various cyber-attacks against IIoT-assisted EPSs, with a particular focus on attack entry points and adversarial methods. Finally, efforts to prevent cyber-intrusions against IIoT systems in EPSs are explained, and different attack detection techniques are discussed.

INDEX TERMS Cyber-attacks, cyber-security, electric power systems, industrial internet of things, intrusion detection systems.

I. TRANSFORMATION OF IoT TO IIoT

The concept of Internet of Things (IoT), which was introduced by Kevin Ashton in 1999, aims to connect anything at anytime in anyplace [1]. IoT is a novel paradigm shift in Information Technology (IT), in which billions of physical objects are connected to the internet and can share real-time data without needing human interference. Additionally, innovations affected by IoT, such as sophisticated automation and manufacturing technologies, exchange and administration of information, and smart and automatic processes and systems are becoming increasingly popular for businesses and organizations [2]. By 2020, IoT connected 12.4 billion things, and it is predicted that this number grows to 26.4 billion by 2026 [3].

The associate editor coordinating the review of this manuscript and approving it for publication was Zhouyang Ren.

The most important differences between conventional and IoT-based networks, in terms of their security, are as follows:

- The first and foremost distinction between traditional and IoT networks is related to the resourcefulness of end devices [4]. IoT networks often includes embedded devices, such as Radio-Frequency Identification (RFID) and sensor nodes, with resource constraints. They are often equipped with little memory, low computational power, little disc space, and minimal power consumption. Thus, IoT systems require lightweight safeguards to balance security with available resources [5]. However, the conventional networks consist of a variety of computers, servers, and devices. Thus, sophisticated and multi-factor security methods may support conventional networks without considering any resource limitations.
- In terms of security architecture, conventional networks use a combination of firewalls, Intrusion Detection

Systems (IDSs), Intrusion Prevention Systems (IPSs), and static network perimeter protection to secure the network. Additionally, end devices are protected by host-based security techniques, such as anti-virus and security/software patches. In contrast, host-based security strategies cannot be applied to IoT devices with resource restrictions [6]. In fact, IoT devices have numerous vulnerabilities, and the conventional defense methods are not able to protect these devices.

- The majority of IoT devices are connected to the network or gateway devices through slow and less-secure connections, such as 802.15.4, 802.11a/b/g/n/p, Long-Range Radio (LoRa), ZigBee, NB-IoT, and SigFox. As a result, IoT devices are susceptible to data leakage and other privacy concerns. For the conventional networks, however, end devices interact over secure and more rapid wired/wireless channels, such as fibre optics, DSL/ADSL, WiFi, 4G and LTE [5].
- Conventional-network devices utilize almost the same operating system and data format. However, there are diverse data contents and formats in IoT networks, due to the application-specific capabilities of devices and the absence of an operating system. Due to this diversity, development of a default security protocol that suits all sorts of IoT systems and devices is yet challenging [5].

Recently, IoT protocols and technology have been incorporated into industrial processes as well to address their ever-increasing complexity, and make them robust against service disruptions [7]. Industrial IoT (IIoT) is a term coined to describe the integration of intelligent electronics into manufacturing processes throughout a product's life cycle [8]. The IIoT, which provides industrial systems with connectivity and intelligence via sensing devices and actuators with ubiquitous networking and computing capabilities, is a key component of future industrial systems. For a faultless system, IIoT not only connects machines, but also has a human interface unit. It is expected that IIoT takes over the routine tasks of quality control, assembly, and administration in the near future [9].

The advantages of IIoT, however, have been achieved at the expense of exposing industrial processes to cyber-attacks, since the increased number of interconnected networks and devices provide cyber-attackers with more number of access points. For this reason, IIoT providers have prioritized cyber-security as a top concern for IIoT adoption [2], [10]. Given that IIoT is a natural transition from IoT, it inherits some of the IoT's security problems. Additionally, IIoT applications have some other security needs that are unique when compared to IoT applications. These unique concerns mostly stem from the absence of human interactions and autonomous machine/device activities in IIoT applications. Major differences between IIoT and IoT can be categorized as follows:

- *Market focus:* IoT covers a variety of sectors, such as enterprises, healthcare, and the public sector. Thus, it tends to concentrate more on universal applications. In contrast, IIoT systems are focused on a smaller market, as they are only applied to industrial settings, such as power plants, oil and gas refineries, and manufacturing facilities [11].
- *Objectives:* IoT is usually deployed to improve productivity, health, and safety. IIoT, however, is usually less user-centric and concentrates more on increasing security and efficiency. Thus, in contrast to IoT, IIoT is an industrial process that is not utilized by general consumers in their individual lives [11].
- *End devices:* IoT and IIoT systems usually use different devices as they both have different focuses and objectives. IIoT devices are built to provide their users with data on equipment, and these devices are integrated with the existing equipment, instead of working alone. In contrast, IoT devices—such as smartphones, smartwatches, and smart thermostats—are often employed in the daily life, and can be used independently [12].
- *Risk of failure:* The risk of failure in IoT devices is relatively low as these devices are only applied on a small scale. Typically, IoT devices are not utilized for restorative practices that pose a threat when they fail. In contrast, failure of IIoT devices is more hazardous, since IIoT is linked to an industrial system [13].
- *Development needs:* IoT manufacturers aim to develop technologies to suit the user's daily life. Hence, IoT development concentrates more on improving the comfort of its users. In contrast, IIoT development usually emphasizes on creating new devices that efficiently improve the operation of its consumers [14].
- *Compatibility with legacy systems:* IoT devices don't have to be compatible with legacy systems. These devices are not designed with backward compatibility as they often work independently. In contrast, IIoT devices should be compatible with the legacy systems and equipment in manufacturing plants, since most IIoT devices assist the legacy systems in offering digital information and receiving IT system commands [14].
- *Environmental requirements:* IoT devices are usually designed to function in normal environments with a standard temperature and ecological pressure. IIoT devices, however, are made more durable and reliable, since they are primarily used in harsher environments, like factories, energy plants, and oil refineries. Thus, manufacturers of IIoT devices usually craft their products to tolerate extreme temperatures, humidity, and radio interference to ensure they provide reliable services [15].
- *Ecosystem architecture:* An IoT system consists of a public cloud, which is manageable by an operator. When an inquiry is received, it is examined and directed through a particular route that needs proprietary data unavailable for the inviting entity. Once the cloud-based IoT process ends, the outcomes are conveyed to the user through specific devices, such as smartphones [16]. In contrast, the architecture of the IIoT network is entirely different. An IIoT process is completed in a private cloud operated by a service provider. The data collected through an IIoT network is used to make an efficient decision, which is transmitted to the

Industrial Control System (ICS) via the organization's IT network [16].

• *Operation safety:* For the majority of IoT systems, the safety of operation is not a concern, as these systems do not usually handle industrialized processes. In IIoT ecosystem, however, situation is entirely different, since an inappropriate action of the IIoT system can render a process unstable or unsafe, and can endanger people's lives [17].

• *Operation reliability:* In an IoT system, operation reliability is essential, since people's decisions entirely depend on the result of IoT processes. Thus, an IoT system should be capable of identifying and detecting deliberate or incorrect acts by an approved individual. Additionally, an IoT network should be equipped with measures to detect any data manipulation and cyber-attacks [17]. In IIoT systems, this requirement is even more serious, since IIoT systems are often the components of ICSs in critical infrastructure [17]. Additionally, IIoT devices also need to last for a longer time, since industrial plants and equipment are built for larger time horizons. Therefore, IIoT devices need to function reliably for a longer time than typical IoT devices [17].

• *Communication media:* The architecture of an IoT ecosystem should match its communication media and protocols. As operations are consumer-oriented, the majority of IoT ecosystems utilize communication media such as Bluetooth, WI-FI, and cellular networks, as well as standard IT protocols. As a part of ICSs, an IIoT network offers wireless and wired communication links among the ICS servers, sensors, and Programmable Logic Controllers (PLCs) using ICS-oriented protocols. Communication latency in IIoT ecosystems is an important concern, since in such systems sensitive information must be shared almost simultaneously [12].

• *Cyber-security defense:* In both IoT and IIoT systems, cyber-risks are of significant concern, since the majority of endpoint devices in both systems can serve as attack entry points. As an IoT ecosystem deals with consumer-oriented end devices, their cyber-security is a fundamental problem, since this technology comes with cost limitations that prevent deployment of cyber-security measures. For an IIoT ecosystem, cyber-security risks are even higher, although investment resources for retrofitting and upgrading are easier to obtain. Thus, extra security measures are essential for IIoT systems [12].

One of the major applications of IIoT networks is in EPSs, since these systems are undergoing a revolution to increase their efficiency, dependability, security, cost efficiency, resiliency, and sustainability [18]. IIoT systems can benefit the three main domains of EPSs—i.e., power generation, transmission, and distribution—by providing them with real-time feedback, and allowing them to better serve their consumers via more-advanced monitoring and control capabilities. Additionally, IIoT systems can facilitate faster adoption of renewable and sustainable energy solutions by dynamically controlling the demand and synchronizing it with the supply [19]. Thus, integration of IIoT systems in EPSs can bring about potential economic, social, and environmental benefits.

Cyber-security, however, is a growing challenge for EPSs, since it directly impacts their reliability and overall cost. Statistics reveals that, so far, (i) 91% of power generating companies have been the victims of cyber-attacks; (ii) cyber-attacks against electricity and water suppliers account for 38% of all identified threats; and (iii) 61% of oil and gas suppliers, which provide power generation companies with their required fuel, are not able to detect sophisticated cyber-attacks [20]. As these statistics demonstrate, EPSs are highly vulnerable to cyber attacks, and are attractive targets for adversaries. On the other hand, integration of IIoT in EPSs can intensify this problem due to the inherent vulnerabilities and resource limitations of IIoT systems. Therefore, it is crucial to investigate the cyber-security challenges of IIoT-based applications in EPSs, and take necessary measures to secure such systems.

The remainder of this paper is organized as follows: Section II elaborates on integration and applications of IIoT systems in EPSs; Section III explains major IIoT architectures for EPSs; cyber-security challenges and requirements of IIoT-based applications in EPSs are discussed in section IV; Section V reviews cyber-attacks against different layers of IIoT systems in EPSs; security enhancement measures for IIoT-aided applications are described in section VI; and the paper is concluded in Section VII.

II. IIoT SYSTEMS IN EPSs

IIoT networks in EPSs use smart devices to collect data from the grid through a cyber layer. This data is then used to operate the grid more efficiently, and to serve the customers better. Thus, connectivity and interoperability are two important features of IIoT networks, which lead to higher standard procedures and services. The following subsections elaborate on major applications of IIoT systems in EPSs, which are also shown in Fig. 1.

A. ELECTRIC POWER GENERATION

IIoT systems—which are a combination of cloud-based analytics, IT, and Operational Technology (OT) technologies—can be implemented for different applications in the power generation process to improve the operator's situational awareness using the real-time data coming from power plants. This enhanced situational awareness can improve the operation of power plants, facilitate integration of renewable energy, and enhance the timely/predictive maintenance of generating units. Some of the applications of IIoT systems in electric power generation are as follows.

1) OPTIMIZING FUEL MIX

The first application of IIoT systems is to optimize the fuel mix of different types of generating units. This task is of high importance, since there is a wide range of generating units in a power network, which are becoming increasingly diversified [21]. Thus, integration of IIoT systems in EPSs can

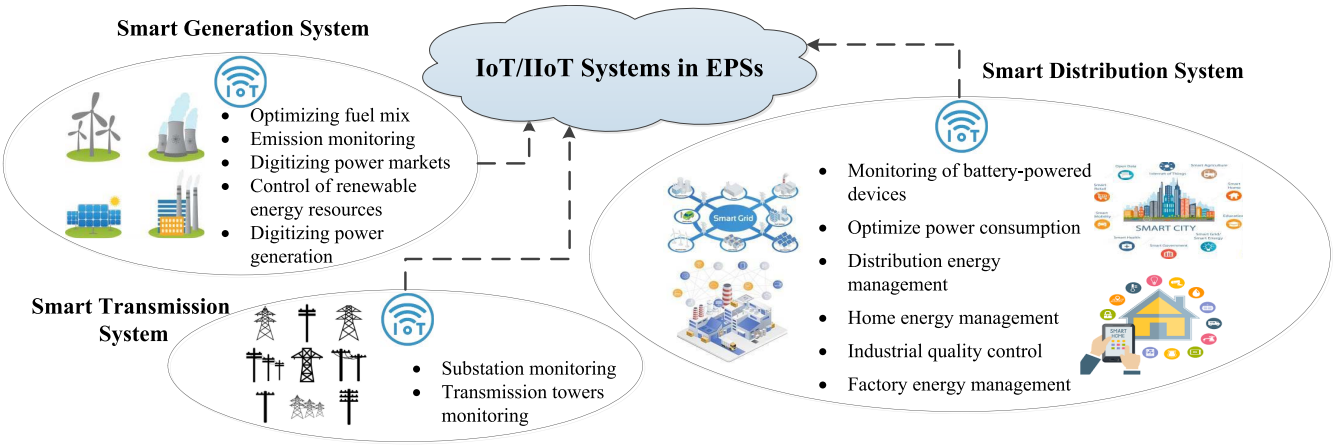


FIGURE 1. IIoT systems in EPSs.

maximize the efficiency of power generation by balancing the fuel mix. As a result, it is critical that operators have real-time data about all the assets in the network to analyze the supply and demand, and their reaction to the energy price [18]. On the other hand, energy providers are required to update and adjust their business models to take advantage of new IIoT applications' capabilities [22]. For instance, it is critical to use the insights gained by big data analytics to balance the fuel mix.

2) EMISSION MONITORING OF POWER PLANTS

IIoT-based embedded systems can be used for monitoring harmful gas emissions from thermal power plants by measuring the Carbon Monoxide (CO) and Particulate Matter (PM) concentrations emitted by them [23]. Additionally, IIoT systems can control the condition of combustion and minimize the emission of Sulphur Dioxide (SO2) in power plants using combustion images [24]. In fact, it is critical to monitor the gases generated by thermal power plants in order to reduce their negative effects on the environment and diminish their health threats [25]. Such IIoT-based systems utilize a variety of sensors to determine the concentration levels of the gases in the atmosphere, and send the sensed information to the cloud computation center. If the measured data exceeds the emission requirements, the operator is notified to take appropriate actions and minimize hazardous emissions.

3) DIGITIZING POWER MARKETS

The power market is another important application for IIoT systems. So far, the volumetric tariffs have been used as a revenue model in conventional EPSs. In this model, people are the source of information, skills, and knowledge for the power market. This invaluable resource becomes inaccessible if current employees retire. In order to preserve the wisdom and expertise of senior employees, digital advancements must be made. For instance, new income streams must be developed for future EPSs to accurately evaluate and distribute investment costs and other activities [18]. Additionally, small-scale energy resources are not taken into account for market participation in the national or regional levels. Furthermore, conventional markets are unable to cope with renewable energy resources in real-time due to their stochastic nature [26]. Thus, a new IIoT-based information-driven infrastructure is needed to boost the productivity of power markets by considering new components, such as local energy generation units [27].

4) CONTROL OF RENEWABLE ENERGY RESOURCES

It is imperative to increase the penetration level of renewable energy resources in future EPSs. These sources of energy, however, are intermittent in nature, and are highly dependent on environmental factors; for instance, the speed and direction of the wind affect the generation of wind power plants, and solar irradiation impacts the output power of photovoltaic cells. To improve the efficiency of such resources and the reliability of the entire grid, IIoT systems can be used to ensure a constant supply of safe, economical, and reliable energy [28], [29], [30]. In fact, IIoT systems can use sensor measurements, a cloud computing platform, and enhanced load and weather models to accurately and efficiently control renewable energy resources [22].

5) DIGITIZING POWER GENERATION

To intelligently operate EPSs and effectively balance the demand and supply, it is crucial to collect real-time data from both transmission and distribution networks. To this aim, IIoT systems can be implemented, and the required data can be collected using smart meters, intelligent feeders, Phasor Measurement Units (PMUs), and micro PMUs [31]. This data can be processed for forecasting the load, estimating the states of the system, and controlling the EPS in a distributed manner. For instance, Digital Twin, built by General Electric, is an ensemble of physics-based methods and advanced data analytics that employs IIoT systems to model the present state of every asset in a digital power plant [18].

B. POWER TRANSMISSION

Existing transmission systems are faced with challenges, such as slow reaction to outages, high power losses, data theft, and poor monitoring of transmission lines and other components. Such challenges can be addressed by implementing IIoT systems for real-time monitoring of transmission networks [32].

As an example, an IIoT-based monitoring platform has been developed for substations in [33], and has been practically implemented in a petrochemical facility's local power substation in Texas, USA [33]. This platform monitors all critical parameters of substations, including voltage, frequency, power, circuit breaker status, and transformer temperatures, in steady-state and during transients. In this platform, high-resolution time-stamping and synchronization are provided using industrial-standard GPS, and high-speed and reliable data acquisition and processing are achieved using FPGA-embedded controllers. The controllers are equipped with predefined event triggering mechanisms with recording functions. When such events occur, the controller records the information and sends it to a control center through the IIoT platform. This data can be used to prevent future similar incidents.

Additionally, IIoT-aided systems have been used to prevent physical damages to transmission towers, e.g., caused by theft, natural catastrophes, hazardous constructions, and the growth of tree limbs beneath the wires. To monitor and prevent such damages, IIoT-enabled transmission towers use various sensors to detect early signs of potential risks, and prompt an immediate and appropriate action. Anti-theft fasteners, lean sensors, cameras, and vibration sensors are some components that can be used for this purpose. Every time a risk is detected by these components, a signal is sent to the control center to make appropriate decisions [34].

C. POWER DISTRIBUTION

Similar to transmission systems, distribution networks are faced with a number of challenges, including power outages, ineffective demand response, electricity theft, and inefficient integration of distributed energy resources. These challenges can be addressed by employing IIoT systems in different domains of distribution systems, as discussed below.

1) SMART GRIDS

Smart grids enjoy a bi-directional flow of information between consumers and suppliers, which can be used for system optimization and efficient energy distribution [35]. In smart grids, IoT/IIoT-related systems can be used for different purposes in energy generation, smart homes, transportation systems, and smart industry [35]. For example, consumers' energy demand patterns can be extracted by collecting data via an IoT platform. Another application of IIoT-based systems in smart grids is controlling and monitoring of battery-powered devices, thus distributing the energy more efficiently [36].

Additionally, IIoT-enabled loads, storage devices, and renewable generating units have enabled customers to generate a part or the entire of their required energy locally, and even to trade the surplus energy with the network. In this context, intelligent loads share their data—such as their demand, power consumption, and the time of use—to optimize their power consumption and cost. Energy storage devices, such as batteries and electric vehicles, are also used to deal with uncertainties and the intermittent nature of generating units, as well as to participate in demand response programs [22].

Moreover, in an IIoT-enabled smart grid, all assets connected to the grid can interact with each other to ensure that the distribution of energy is perfectly managed whenever and wherever it is required. In such a smart grid, the operator is notified before any acute problem occurs, thus an appropriate corrective or preventive action can be taken in advance. For example, exceeding the demand over the grid's capacity can be detected by real-time monitoring of loads and generating units. Thus, the energy consumption of flexible loads can be rescheduled to a time when demand is expected to be lower. Additionally, dynamic pricing models can be used to decrease the consumption or increase the generation during peak hours [37].

2) SMART LOAD MANAGEMENT

In general, electric energy consumption can be divided into four categories: residential, commercial, industrial, and transportation. The following discusses how IoT/IIoT can be used to manage the energy consumption in residential and industrial loads.

Residential loads include, but are not limited to, lighting, appliances, and water heaters, as well as Heating, Ventilation, and Air Conditioning (HVAC) systems. IoT systems can be used to manage energy consumption of the appliances and lighting systems. For instance, IoT/IIoT systems can notify customers when their energy consumption exceeds the standard level. Additionally, IoT/IIoT-based home energy management systems can monitor the energy usage to schedule and run some flexible loads, e.g. some appliances, during low-demand hours. This contributes significantly to the efficient use of electrical energy and reducing greenhouse gas emissions [36]. Moreover, given that HVAC energy consumption accounts for half of the total energy consumption in most buildings, IoT/IIoT-based HVAC management systems are critical for managing electric energy and its cost in buildings. For instance, such systems can determine unoccupied spaces in buildings, and manage the operation of the HVAC system in these spaces.

Industrial loads can be also managed by using IIoT-based systems. For instance, by monitoring each component and its consumption, the components that consume more energy than expected can be detected. Additionally, quality control can be performed by using an agile and flexible IIoT system that recognizes failures in real-time. These IIoT systems lead to a better management of components, detecting and fixing faults,

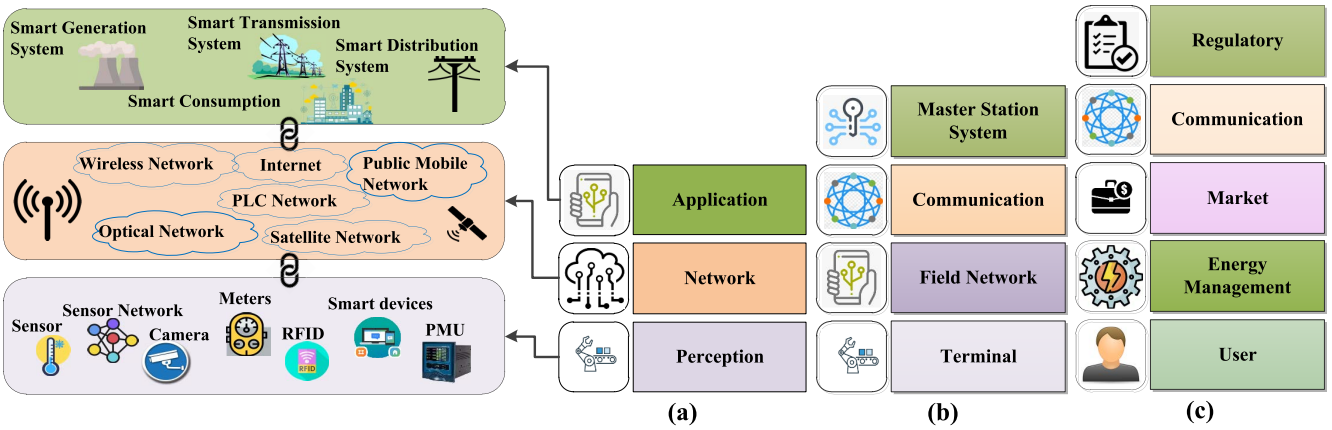


FIGURE 2. Common IIoT architectures for EPSs: a) basic three-layer, b) four-layer, and c) five-layer.

optimizing each component's consumption, and ultimately to the reduction of energy losses in smart factories [38].

III. ARCHITECTURE OF IIoT NETWORKS

IIoT architectures comprise several layers, each includes IIoT networking platforms, protocols, and standards. These layers are configured based on each application's requirements, e.g., scalability, flexibility, and interoperability, and allow multiple technologies to interact with each other. The disparate requirements of applications, result in diverse structures for IIoT systems, and barricades development of a standard design for all applications. The following subsections elaborate on various IIoT architectures in EPSs, which are shown in Fig. 2.

A. THREE-LAYER IIoT ARCHITECTURE

A typical IIoT architecture includes at least three layers: perception, network, and application layers, which are illustrated in Fig. 2-(a). Generally, the top layer of a three-layer IIoT architecture is associated with applications, the middle layer corresponds to the network requirements and communication process, and the lowest layer is for hardware and physical devices. This architecture is the most basic one, which gives insights into the essential layers to make the system work. In fact, other more-complicated architectures can be also simplified to a three-layer architecture. The three-layer design for IIoT-assisted EPSs has been suggested in [39], [40], and [32].

The perception layer senses and collects data by installing and networking various sensors in EPSs. This layer comprises IIoT devices—e.g., remote terminal units, information gathering devices, smart meters, and intelligent electronic equipment—deployed in different domains of EPSs. This layer receives information from IIoT devices and transfers it to the network layer. The perception layer is divided into two sub-layers: (i) perception control and (ii) communication extension. The former controls the physical layer by acquiring data and analyzing IIoT devices, whereas the latter links IIoT devices with the network layer through a communication module [41].

The network layer embraces the communication system—which is assisted by numerous telecommunication networks as well as the Internet—to transfer the information acquired by IIoT devices at the perception layer to the application layer via the telecommunication networks. The core network, which can be the Internet, oversees the routing, information transmission, and control functions. The IIoT management and information centers are also in this layer [41].

The application layer is a combination of IIoT technologies and industrial practices/expertise to enable a wide range of IIoT-assisted EPS applications. This layer is responsible for processing information that is received from the network layer and using it for real-time monitoring, controlling, and debugging of IIoT devices. Information sharing and security are two important services in the application layer [41].

B. FOUR-LAYER IIoT ARCHITECTURE

A four-layer architecture for IIoT-aided applications in EPSs consists of terminal, field network, communication, and master station system layers, as shown in Fig. 2-(b). The terminal and field network layers in this architecture form the perception layer of the three-layer IIoT structure; the remote communication layer corresponds to the network layer; and the master station system layer is equivalent to the application layer. This architecture is the most common one for EPSs, which can be used for various applications, such as (i) power plant operation (e.g., for monitoring of pollutant and gas discharge, and controlling generation equipment), (ii) state monitoring for transmission lines (e.g., ambient condition, ice covering, temperature, sag), (iii) substation equipment operation and control (e.g., state monitoring of substation equipment and environment safety), (iv) power distribution automation, and (v) consumption management (e.g., in advanced metering infrastructure and smart homes) [42].

C. FIVE-LAYER IIoT ARCHITECTURES

A five-layer architecture (Fig. 2-(c)), which consists of user, energy management, market, communication, and regulatory layers, is proposed in [43] for Transactive Energy Systems

(TESs). The user layer consists of applications that benefit from the IIoT structure. The energy management layer optimizes the system operation to control congestions, improve the reliability, reduce system failures, and minimize frequency and voltage deviations. This layer also ensures maintaining a dynamic balance between supply and demand in EPSs. Information related to the energy demand is collected and stored in the market layer, which leverages either local or cloud infrastructure to facilitate energy transactions. The communication layer is used to transfer the data from the market layer to the regulatory layer through wired and/or wireless communication media. The highest layer is responsible for regulatory and governance processes, in which the rules and procedures required for transparent and smooth energy transactions are determined. In this architecture, user, energy management, and regulatory layers together are equivalent to the application layer of the three-layer architecture. Similarly, the communication and market layers correspond to the network and perception layers of the three-layer architecture, respectively.

IV. CYBER-SECURITY OF IIoT SYSTEMS

The purpose of cyber-security is to protect IIoT assets and privacy, and to reduce security risks that emanate from the cyber layer. New cyber-security technologies are constantly emerging to make systems more secure. However, developing cyber-security techniques for IIoT-based applications in EPSs is challenging, since (i) a variety of devices, applications, communication media, and protocols are used in IIoT networks, and (ii) the physical capabilities of devices and the volume of information shared by them are limited. The major security requirements of IIoT-based systems are as follows.

A. DEVICE SECURITY

The term device security refers to preventing a device (e.g., a PMU or an actuator in EPSs) from being maliciously used to conduct attacks, e.g., from participating in Denial of Service (DoS) attacks, eavesdropping on network traffic, or compromising other devices on the same network. This type of security is applicable to all IIoT devices in EPSs. One of the most important effects of security problems, such as DoS attacks against IIoT devices, is negatively affecting the availability of the network. Term availability in IIoT networks refers to both hardware and software. Hardware availability means the existence of all devices all the time, whereas software availability is the ability to provide service anywhere and anytime [44]. To secure an IIoT system and prevent unwanted malicious actions, a main step is to ensure that all devices are secure and trustworthy [45]. Trust management techniques are divided into two main categories: deterministic and non-deterministic trust. Deterministic trust encompasses policy- and certificate-based mechanisms, whereas non-deterministic trust includes recommendation-, and prediction-based ones [46]. Policy-based mechanisms use a set of policies to identify trust. In certificate-based approaches, trust is determined by using public or private keys and digital signatures. Recommendation-based systems utilize prior information to define trust. However, if there is no prior information, prediction-based methods can be used [46].

B. DATA SECURITY

Data security means protecting the confidentiality, integrity, and/or availability of IIoT data. This type of security is applicable to all devices, no matter if they send, receive or store data. IIoT devices in EPSs monitor the physical environments and transmit the collected data through the network. However, this transmitted data is exposed to different security threats like eavesdropping and altering. To secure data in the context of IIoT, the confidentiality and integrity of the data must be preserved [45]. Data confidentiality is the process of hiding private information from unauthorized objects. Standard encryption mechanisms cannot be implemented directly for improving the confidentiality of data in IIoT systems, since some IIoT devices have limited resources [47]. Data integrity ensures that the received data has not been altered or modified during transmission. Integrity involves maintaining the consistency, accuracy, and trustworthiness of data. Several cryptographic hash algorithms (e.g. MD5 [48] and SH1 [49]) are used to ensure data integrity. However, most of these mechanisms cannot be implemented in IIoT systems, since IIoT devices are inherently resource-constrained [50]. Availability means that the data remains available to authorized users at all times. If an attacker compromises the availability of data, the users are prevented from accessing crucial information, or the system is brought to a halt. The most important intrusion that can target the availability of data is a DoS attack.

C. COMMUNICATION SECURITY

Connectivity is a critical component of any IIoT network. To address this need, several different protocols (e.g., Bluetooth, WiFi, Zigbee, Z-Wave) may be utilized within a single IIoT system to account for environmental limitations and increase the reliability of IIoT communications. Choosing the right communication protocol and medium depends on (i) the configuration of the physical system, e.g., a high distance between devices obliges using long-range communication protocols; (ii) IIoT tasks, e.g., real-time applications require higher connectivity capabilities; and (iii) computing resources of devices, e.g., power-constrained devices may require low-power communication protocols such as Bluetooth Low Energy (BLE), ZigBee and LTE-M. In order to address the communication needs of IIoT systems in EPSs, standardization groups such as the IEEE and the Internet Engineering Task Force (IETF) have developed IoT/IIoT-specific communication protocols, such as IEEE 802.15.4e, 6LoWPAN, and LoRa [51], [52]. On the other hand, to establish a secure communication between IIoT devices, an authentication process is required to authorize only the legitimate devices to access the systems or their information. Access control is a security feature that verifies

the permission granted to users and systems to perform operations on other systems and resources [53]. Authentication is the process of validating a user's identity using login and other information—such as password, PIN and digital certificates [46]—and is required to secure the communication between two or group of parties. Authentication ensures that only authorized users access IIoT devices and achieves non-repudiation in communications. When a new device is connected to the network, it should authenticate itself before exchanging data. The authentication can be verified using lightweight cryptographic algorithms, physical primitives, or biometric identification [53].

D. INDIVIDUALS' PRIVACY

Privacy includes the concealment of personal information and the ability to control what can be done with this type of information [54]. Data privacy must be addressed during data collection, transmission, and storage. Several practical solutions—such as anonymization, pseudo-random number generators, block ciphers, and stream ciphers [46]—have been proposed to deal with individuals' privacy, which is important in some of IIoT applications, such as power markets. Privacy preservation preferences impact expansion of IIoT systems in the future, since concerns about privacy and potential hazards of data leakages might slow down the adoption of IIoT technologies.

V. TAXONOMY OF CYBER-ATTACKS AGAINST IIoT SYSTEMS IN EPSs

Generally, attacks can exploit the vulnerabilities of IIoT systems in EPSs for modification, interception, or interruption of data. These vulnerabilities are mainly due to the lack of physical security, inadequate authentication, improper data protection, insufficient access control, weak programming practices, and insufficient audit mechanisms [55], [56]. The vulnerabilities of IIoT systems stem from various layers (i.e., perception, application, and network layers), and result in different types of attacks against each layer (Fig. 3). The following subsections enumerate the major families of attacks against IIoT systems in EPSs.

A. ATTACKS AGAINST THE PERCEPTION/PHYSICAL LAYER

Edge nodes—such as sensors and smart controllers—are parts of the perception layer, which interact with the physical environment. In most IIoT applications of EPSs, edge nodes are easy to reach, as they are mostly unattended and some of them run on a limited battery [57]. Operation of IIoT devices in insecure areas makes them attractive targets for cyber-attackers. Additionally, IoT-based authentication procedures may be challenging for some IIoT devices, which makes them vulnerable to cyber-attacks. Moreover, there is a lack of standardized privacy policies for proper access control management [58], and users sometimes ignore to update the default credentials following the initial installation [55]. Therefore, access control protocols used for IIoT devices are vulnerable [59]. Furthermore, there is a lack of standard

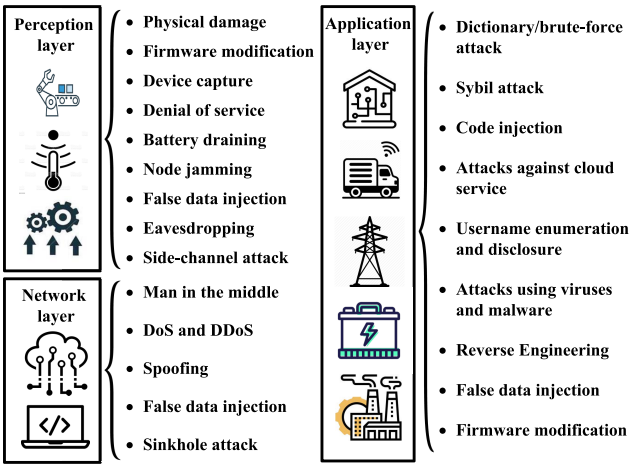


FIGURE 3. Taxonomy of cyber-attacks against layers of IIoT-aided EPSs.

programming practices for IIoT systems due to the abundance and variety of devices. Firmware with known vulnerabilities is an example of weak programming practices in the perception layer [55]. Hence, the aforementioned vulnerabilities can be exploited by adversaries to attack the hardware, firmware, and communication links of devices in the physical/perception layer. The following attacks can be launched against various components of this layer.

1) PHYSICAL DAMAGE

Unattended IIoT devices and nodes are subject to physical damages, such as storage removal, firmware manipulation, tampering attacks, or information extraction using open communication ports [60]. IIoT devices are often able to communicate and change settings through the communication systems, as well as through the physical layer. An attacker with access to the input/output ports of an IIoT object can change the parameters of devices and cause unwanted operations. Moreover, using these ports, cyber-attacks can take the control of devices, manipulate their firmware, and inject codes that cause them to act maliciously or even to be destroyed [61]. The change of firmware might also include a downgrade to previous versions, where known vulnerabilities exist. In such a condition, an adversary can benefit from the known vulnerabilities and take the control of devices. Attackers can also learn the specification and sensitive information of an IIoT system using unattended devices. For instance, attackers can remove the storage of a device to extract its data and also learn about the connections of devices in the network to plan for the next stages of an attack, or gather information about other devices that communicate with the targeted device.

2) FIRMWARE MODIFICATION ATTACKS IN PERCEPTION LAYER

With physical access to a device, an attacker can replace the default firmware of the device with a malicious one [55]. This intrusion gives attackers the full control of the device,

if they are present physically close to it or remotely through the communication system. In the latter case, the attack can be categorized as a threat to the network layer.

3) DEVICE CAPTURE/NODE REPLICATION ATTACKS

An attacker can perform a device capture/node replication attack, in which a malicious node is added to an existing network by adapting the ID number of a legitimate node in the system [62]. With the malicious node camouflaged, the attacker can perform malicious activities, such as rerouting or dumping packets. Hence, this type of attack can compromise the functionality of the entire IIoT-based system [58]. Due to the lack of sufficient auditing, this type of attack would not be identified easily and the operators will not notice that a legitimate node has been removed in the first place, since the power consumption remains almost unchanged. It should be mentioned that even though the malicious node has the identity of a benign node, there would be a slight imbalance in energy consumption, which can be detected if there is continuous audit of power consumption throughout the system.

4) DoS ATTACKS IN PHYSICAL LAYER

DoS attacks can occur in the form of firmware, physical, or network damages. In the case of firmware damage, the attack can be categorized as a threat against the application layer, whereas a loss of communication results in an attack on the network layer. DoS attacks negatively impact service availability, and occur by disabling the IIoT system from performing its duties. It typically happens because of (i) a flood of requests over the service host, resulting in a full buffer in the ports of devices (i.e., routers, or servers); (ii) physical removal of a device; and (iii) interrupting the communication between devices when data transfer is required. DoS attacks are categorized as either temporary or permanent. Devices with low/no security update mechanisms may be vulnerable to malicious firmware updates, and can be used as a bot for sending floods of requests to the network to clog services. A destructive update can also disable nodes or result in their malfunction, possibly when the update targets specific parts of the memory [63]. A Distributed DoS (DDoS) is an attack in which many nodes participate in sending clogging requests, whereas a DoS is initiated from a single device within the network.

5) BATTERY DRAINING ATTACKS

One of the most important factors for designing an IIoT device is its battery size, which directly impacts the size, portability, and cost-effectiveness of the device. Reliance of some IIoT devices on batteries makes them vulnerable to battery draining attacks. In this type of attack, an adversary sends a large number of packets to the target device to make it run its authentication mechanism, so resulting in the depletion of its battery [57]. As a result, the life of the node ends, and the system does not perform correctly. In another type of battery draining attack, the hostile node sends only as many queries to the victim node as are required to keep the target node awake and drain its battery. In this attack, however, the energy consumption of the victim device is not increased significantly in order to keep the attack stealthy [64].

6) NODE JAMMING ATTACKS

This attack happens when an adversary obscures network connection by interfering signals, such as jamming radio frequency signals. This type of attack disrupts the availability of IIoT systems, since target nodes and devices can no longer be reached or controlled [65]. Additionally, node jamming attacks make time-critical data unavailable [66]. This type of attack can be also performed to disrupt the communication system by decreasing the Signal-to-Interference-plus-Noise ratio (SINR), which is often greater than one in normal situations. To perform such an attack, the adversary must have knowledge about the frequency and the modulation technique used by the target device.

7) FALSE DATA INJECTION ATTACKS (FDIAs) IN PHYSICAL LAYER

Compromising the integrity of data by deliberate injection of false information is categorized as an FDIA. Generally speaking, in an FDIA, the data that is gathered by IIoT devices is manipulated to portray a fake condition in the underlying system or hide an event. In this attack, an adversary can also take advantage of the limited error rate tolerance of the system, and gradually raise the effect of false data such that the attack remains unnoticed. FDIAs in cyber-controlled networks have a significant effect on the system's performance, and can result in a system failure [67]. In FDIAs, even a small portion of false data can disrupt the entire IIoT system. Thus, adversaries can optimize their attacks to reach the intended goal with the minimum adversarial efforts, so keeping the attack stealthy [66]. In the physical layer, this type of attack can be launched by manipulating sensors physically.

8) EAVESDROPPING

In this type of attack, secret information is collected from communication nodes and devices. Corrupted devices in an IIoT system, including compromised nodes, may leak the systems' traffic and expose confidential information [68]. Additionally, network eavesdropping—which is often referred to as network snooping or sniffing—occurs when attackers exploit insecure or vulnerable networks to access the data transmitted between two devices. This attack is among the most common ones in wireless communication.

9) SIDE-CHANNEL ATTACKS

This type of attack aims to extract private information, such as encryption keys, by recording and analyzing the Side-channel activities of IIoT devices, such as timing, power consumption, and electromagnetic radiations [69]. Secret keys, for example, can be retrieved by the statistical analysis of the timing or power consumption of cryptographic algorithm executions, or the consequences of incorrect executions. The data protected in encrypted packets can be exposed by analyzing their

length and processing time. A side-channel attack is fatal when the information is extracted while a system is operating. For instance, PMU communication infrastructure is vulnerable to timing side-channel attacks, in which the Hash-based Message Authentication Code (H-MAC) algorithm can be compromised by monitoring its execution time. This attack can model some security features of the stored key, e.g., its length and processing time, to decrypt the data [70].

B. APPLICATION LAYER ATTACKS

The application layer consists of a variety of software packages without standardized privacy policies for proper access control management [58]. This motivates adversaries to target the application layer by attacks, such as code injection and FDIAs. Additionally, in an IIoT-based EPS, attackers can compromise the data—consisting of private information about users, processes, and devices—to gain information about the entire system and its control/protection strategies. The diversity of devices and their wide range of activities, on the other hand, undermine the reliability of anomaly detection mechanisms in IIoT systems, and result in high false-positive and/or false-negative alarm rates [71]. In addition, existence of a huge number of devices in the IIoT systems barricades implementation of strong audit mechanisms, thus increasing the possibility of intrusions. These vulnerabilities, among others, make the application layer an interesting target to achieve malicious goals. The following subsections elaborate on attacks that can target this layer.

1) DICTIONARY/BRUTE-FORCE ATTACKS

A dictionary attack is a brute-force technique, in which attackers bombard a device/software with a set of known credentials to guess passwords [72]. This attack is possible when authentication mechanisms are weak, and becomes easier when factory-set credentials are still in place and not updated [55]. Therefore, not updating the users' credentials [59] and utilizing weak privacy policies [58] can enable an adversary to gain high-level access to the system and control it after performing a dictionary attack. Additionally, this attack is effective when log in attempts and user credentials are not logged, or when there are devices with the same credentials.

2) SYBIL ATTACKS

Sybil nodes are edge nodes with fake identities in IIoT networks. When attackers decide to perform a sybil attack, they add and use sybil nodes in the system. As discussed before, edge nodes are easy to capture—and thus are good candidates for sybil nodes—since they often left unattended. In such a case, an attacker can simply replace the legitimate node with a sybil node. Since other legitimate nodes have often simple authentication protocols, they are unable to verify the authenticity of the node and let a malicious request from the sybil node pass, whereby corrupting the legitimate nodes. In this attack, the adversary can even gain access to many other nodes using a sybil one [73].

3) CODE INJECTION

Similar to poor/malicious updates for the perception layer, malign updates to applications and servers may trigger security problems, such as data leakage, data loss, and unwanted control. It is worth mentioning that this attack can also target the physical layer when the adversary physically inserts some malicious codes into an IIoT device. This can happen, for instance, by attaching a malicious gadget to the target node and, on occasion, rewriting the target's operating system. Structured Query Language (SQL) injection is a type of code injection attack to acquire administrator access to databases by exploiting vulnerabilities in the victim's network infrastructure.

4) ATTACKS AGAINST CLOUD SERVICES

Cloud services have inherent security problems, which are manifest in IIoT systems as well [66]. Since IIoT devices rely on service providers to keep their data safe, the most difficult task in establishing cloud-based services is to secure data. Confidentiality, integrity, authorization, data availability, and privacy are among the features that a cloud service should maintain. Data breaches, data loss, integrity violations, and unauthorized access are all possible consequences of a cloud's improper data handling. If an attack occurs while transmitting data over the cloud network, it can be considered as an attack on the network layer; however, an attack is against the application layer if this layer is compromised to target the cloud.

5) USERNAME ENUMERATION AND DISCLOSURE

To control an IIoT service, many applications use login pages that can be targeted with brute-force attacks in order to find out the user names listed on an application or a device. These attacks will lead to either username enumeration or user lockout due to failed trials [60], [74]. Username leakage can damage the privacy of users and help to initiate other attacks. The same attack can occur against cloud services as well. The authentication process and procedures used for cloud-based services are often extremely susceptible and frequently attacked. Numerous cloud services continue to rely on single-factor authentication and straightforward username and password specifications. Thus, attackers can utilize this vulnerability to their advantage while attempting to interrupt services or steal information from a company that utilizes cloud computing services.

6) ATTACKS USING VIRUSES AND MALWARE

Viruses and Worms can be injected into IIoT applications using, for instance, backdoor methods, which essentially bypass the main authorization system, embedded for developers or maintenance intentions. Primarily, default passwords and out-of-date interfaces lead to backdoor exposures [75]. In contrast to computer viruses, which need a host in order to thrive, computer worms are able to thrive on their own and propagate more quickly. A viruse can replicate itself and

spread from one IIoT device to another. It infects each system by embedding itself in a variety of applications and running the code when a user starts utilizing the infected software. With the aid of this malicious application, the adversary may steal information, create botnets, and harm the host machine. A worm, however, spreads over a network by looking for a vulnerable operating system. It operates on the system to cause damage to their host networks by, for instance, overloading web servers and occupying the bandwidth [76].

7) REVERSE ENGINEERING

Attackers can gain sensitive information about a system by reverse engineering its source codes. Using this strategy, attackers can identify sensitive information left by software programmers, such as hard-coded credentials and defects, and exploit it to launch attacks. Extracted information can be used to plan future assaults against the devices or to develop and employ malicious malware for them [77].

8) FDIAs AGAINST APPLICATION LAYER

FDIAs on the application layer differ from the same type of attack against the perception layer, which was discussed in the previous subsection. FDIAs in the previous subsection occur in the perception layer, whereas in this case false information is injected into the data or the controllers/applications that utilize the data [78]. For instance, applications such as control of renewable energy resources require a continuous authenticated flow of data in order to make accurate decisions. Therefore, an FDIA could prove fatal as it can mislead the operator into making inefficient and cost-ineffective decisions.

9) FIRMWARE MODIFICATION ATTACKS

Taking advantage of this vulnerability, an attacker can identify the weaknesses through firmware analysis and re-program an IIoT device's firmware in order to take its control [63]. The attacker can also rewrite the internal memories in the firmware [79]. By taking the control of the device successfully, an attacker can infiltrate the system and perform malicious activities. Several major factors influence the security of IIoT firmware upgrades, including (i) unauthorized access to code-signing keys or firmware signing processes, which can allow attackers to spoof trust and distribute malicious upgrades to seemingly trustworthy devices; (ii) coding weaknesses and vulnerabilities, which enable attackers to cause unpredictable program behavior or crashes, and can result in security breaches; and (iii) the lack of processes to safeguard the supply chain and prevent unsecured open-source components with embedded vulnerabilities in IIoT devices [80].

C. NETWORK LAYER ATTACKS

Attackers can also target an IIoT system from its network layer to gain important information about the system or manipulate the data. Such attacks become much easier if the data is unencrypted. Additionally, similar to application and perception layers, inadequate authentication and insufficient access control are important vulnerabilities of the network layer which can be exploited by attackers for malicious purposes. Moreover, networking protocols that perform packet routing and transmission at this layer are also breeding grounds for security problems. Therefore, these vulnerabilities attract attackers to the network layer. Major attacks against this layer are summarized as follows.

1) MAN IN THE MIDDLE (MITM) ATTACK

The communication between two victim IIoT devices may be intercepted by a third agent or device that privately hands over messages between the victims without letting them know they are actually conversing with the agent. This way the agent can either eavesdrop on the conversation or inject malicious information [81]. This type of intrusion may occur mostly when there is no or a poor encryption mechanism in place [60].

2) DoS AND DDoS ON NETWORK LAYER

As described in previous sections, the compromised nodes or devices can send large unwanted data traffic, so that the gateways or routers become unreachable and critical services become disabled [82]. Due to the wide deployment of networking protocols, DoS and DDoS attacks are very common on the IIoT network layer. Another reason for abundance of DoS and DDoS attacks against this layer is that IIoT systems may use the networking protocols and media—for communication and data sharing—that are already used in other networks, so the same vulnerabilities threaten IIoT ecosystems as well.

3) SPOOFING

Spoofing occurs when an attacker succeeds to pretend itself as a legitimate source and gains control over a data stream, such as GPS and network time protocol (NTP) [64]. This attack is carried out by disguising the attacker's identity and pretending as a trusted source instead. This type of attack often leads to data leakage, and can be leveraged to design more sophisticated attacks.

4) FDIA THROUGH THE NETWORK LAYER

Insertion, manipulation, and replay are different types of FDIA in the network layer [58]. An attacker can insert malicious packets into the network such that they appear authentic and be hard to detect. Additionally, using an FDIA in the network layer, an attacker can manipulate existing packets by changing their header and data. In more sophisticated FDIAs, an attacker can replace the packets previously recorded during an event with the actual ones, so faking the event when it is not actually happening [57], [58]. It should be mentioned that since IIoT networks do not often enjoy sophisticated authentication protocols, FDIAs in these networks are easier to perform.

5) SINKHOLE ATTACKS

This type of threat is the most destructive routing attack in an IIoT paradigm, in which messages/communications in a

system are routed to anywhere the attacker pleases [83]. In a sinkhole attack, false information is sent to surrounding nodes by a malicious node. This malicious node can successfully connect and blend into the network, due to poor authentication, and announces that it is the shortest path for messages to reach the destination. Thus, the attacker can gain the full control of communications [84].

VI. SECURITY ENHANCEMENT OF IIoT SYSTEMS IN EPSs

A. PREVENTING CYBER-ATTACKS IN IIoT SYSTEMS

This subsection elaborates on the techniques that can prevent cyber-attacks in IoT systems in general, and in IIoT networks in particular.

1) EDGE PROTECTION

As seen in the vulnerabilities section earlier, there are various weaknesses that can be potentially exploited when it comes to edge nodes/devices that are responsible for interacting with the physical environment and the system [57], [85]. The first step to prevent cyber-attacks in the perception layer is to design the IIoT systems physically secure. For instance, IIoT devices need to have secure chips, chip connections, radio-frequency circuits, data acquisition, and antennas [86]. Additionally, IIoT devices can be further protected in various ways, such as by trojan activation, circuit modification, and securing their firmware.

- *Trojan activation:* Trojans are malware that disguise themselves as legitimate. They are known to change the heat distribution of a system. Hence, a trojan activation is an approach that continuously compares the heat distribution in the current system with the recorded heat distribution of a trojan-/malware-free system [87]. Similarly, when an edge node is under brute force/DoS attack, it would be utilizing a lot more power, which can be detected when the system is regularly monitored and its power consumption is compared with normal operation [88].
- *Circuit modification:* Modifying the circuit of edge devices, e.g., installing sleep/kill or self-destruction mechanisms, can protect edge devices against cyber-attacks. When there is unauthorized access to or tampering with a device, the sleep/kill or self-destruction mechanism would automatically kill or destroy the device, so it cannot work anymore and be controlled by an attacker. Additionally, it could put the node to turn inactive for a duration of time or until a security team looks into it. Circuit modification could also include adding randomized delay [69] or intentionally generated noise [89] during normal operation of a device so an attacker cannot find out what the process or device is, so preventing side-channel attacks.
- *Secure firmware update:* Securely updating firmware is a way to avoid malicious firmware modification to IIoT devices. To securely update a firmware, the server can issue a command to broadcast that there is a new version of firmware available. A node with the new firmware already installed would announce an advertisement which would alert its neighboring nodes that an update is available. The nodes that received the advertisement would then proceed to check whether they have the new version or not; if not, they would broadcast a request to receive the updates from the server. The nodes need to authenticate that the received update packets are from a legitimate source [57].

2) PATCH MANAGEMENT TECHNIQUES

Manufacturers of the majority of IIoT devices do not often supply security fixes for customers, or even the customers do not put in enough efforts to install the security updates. As a result, a huge number of IIoT devices have been deployed with known vulnerabilities [90]. Patching all devices in a timely manner is essential for securing the IIoT system, since it removes vulnerabilities and therefore reduces the risk of attacks against industrial processes [91]. Thus, internal mechanisms for patching vulnerabilities, without waiting for the next scheduled maintenance time, must be reinforced in many firms [92]. Manufacturers must also provide security fixes for all their devices on a regular basis throughout the prolonged lifespan of such devices. Automated patch installation may make this procedure easier for a large number of IIoT devices. Patching industrial systems, on the other hand, usually involves a thorough testing step prior to installation to ensure that the patch is compatible with the present configuration. To enhance safety and limit the possibility of process downtime, the National Institute of Standards and Technology (NIST) advises regression testing as a part of a systematic patch management approach [93]. Additionally, the Internet Engineering Task Force (IETF) on software updates for IoT offers an automatic firmware upgrade method for resource-constrained devices in the context of the IoT and IIoT [94], [95]. This approach ensures a consistent description of the relevant entities, security threats, and assumptions for each update, as well as secure end-to-end transfer of new firmware to devices.

There are also methods for actively detecting security problems and vulnerabilities in IIoT installations, such as evaluating IIoT devices during their idle moments or assessing vulnerabilities using an IIoT network graph [96], [97]. Idle intervals have little effect on industrial operations, making them especially helpful for safety- and mission-critical activities [96]. These methods form the first step in identifying existing security defects and their consequences for the systems, as well as taking appropriate actions, such as isolating susceptible devices.

3) ACCESS CONTROL AND PROVISION OF TRUSTED EXECUTION ENVIRONMENTS

Even if IIoT devices are patched regularly, the existence of vulnerabilities cannot be totally ruled out, since manufacturers may not be aware of some security defects in their products, known as zero-day vulnerabilities. Furthermore, manufacturers may terminate support for outdated equipment. Thus, additional protection techniques are required to avoid attacks on IIoT devices and subsequent assaults

on other linked devices. To this aim, NIST recommends a defense-in-depth design, which uses internal firewalls and demilitarized zones to reduce the effects of assaults. Furthermore, fine-grained security policies that restrict access to computing and networking resources for each device, and even inside a device for particular applications and tasks, can minimize the risk of attacks.

Various techniques have recently been developed to particularly address the implementation of hardware-security technologies, such as trusted execution environments, in industrial cases [98], [99]. The ability to serve time-critical applications is a key barrier when considering such technologies in the context of IIoT. First prototype assessments indicate that with the support of trusted execution environments, even resource-constrained devices may safely conduct safety- and mission-critical activities. However, such methods are only relevant to future device generations if the necessary hardware is available. Enforcing security policies within the network is a possible approach for outdated and non-patchable systems. This is an appropriate approach to prevent follow-up attacks from infected devices to other portions of the network, in addition to providing extra security against unauthorized access to such devices.

The IETF has also suggested Manufacturer Usage Description (MUD) [100], in which the manufacturers of IIoT devices establish networking rules based on device functionalities, i.e., most IIoT devices have a very defined purpose and hence do not require full network access to complete their functions. All connections that do not conform with the set of MUD rules are subsequently blocked by a central enforcer within the local network, limiting the potential for assaults. It is also demonstrated that automated techniques may be used to construct MUD rules, and thus this approach supports previously deployed devices, even when manufacturers do not offer the necessary rules [101]. Software Defined Networking (SDN) approach can be also used to implement regulations in industrial networks [102], [103].

4) CRYPTOGRAPHY AND AUTHENTICATION MECHANISMS

Encryption is a critical tool for ensuring data secrecy and may also be used to provide authentication. However, a large number of IIoT devices are resource-constrained, necessitating the usage of lightweight symmetric-key encryption techniques rather than computationally more-costly public-key cryptographic methods. However, symmetric-key cryptography often lacks a secure and scalable management infrastructure, making the secrecy of participants difficult [104]. Furthermore, both public-key and symmetric-key cryptographic approaches often produce unacceptable delays for safety- and mission-critical procedures, preventing factory operators from using encryption and authentication at all. Additionally, the increasing data transmission between devices in IIoT systems, as well as the rising reliance of such systems on cloud services, necessitate robust data security against unwanted access. As a result, new encryption and authentication technologies that are specially adapted to the IIoT paradigm are necessary.

The first group of studies concentrates on resource-constrained devices and suggests techniques to minimize latency and hence allow lightweight authentication and encryption in industrial communication settings. For instance, to allow authentication of resource-constrained devices, the authors of [105] use a lightweight authentication technique based on only hash and XOR operations. In this method, smart sensors with secure elements and routers with trusted platform module are taken into account. The proposed authentication mechanism is performed in two steps: (a) the registration phase, in which each smart sensor registers with an authentication server and the routers are given secure pre-shared keys issued by the server; and (b) the mutual authentication phase, in which the sensor and the router establish mutual authentication. The second group of studies concentrates on protecting IIoT communications with other entities, such as cloud services [106], [107], [108], [109]. These methods use certificateless searchable public-key encryption, which allows for easy key management across a wide number of IIoT devices. The core concept is that data is encrypted before being sent to a cloud service, and the encrypted data is searchable, such that data is only decrypted after being retrieved from the cloud. Such techniques, however, might endanger the confidentiality and integrity of the information, since secrecy and authenticity of outsourced data cannot be guaranteed when dealing with an expanding number of devices and connections [110]. Finally, the last group of studies focuses on user authentication, and develops techniques for authorizing users to access IIoT devices. For instance, researchers have proposed an anonymous lightweight user authentication approach for IIoT paradigms [111]. This approach performs authentication using personal biometrics, passwords, and smart cards with the fuzzy extractor to confirm the user's biometrics. It also includes phases for smart card revocation, password/biometric update, and IIoT device addition. Additionally, the authors of [112] have developed a privacy-preserving biometric-based authentication protocol using elliptic curve cryptography. In this method, when a user desires to access a node's sensory data, their authentication should be approved by a gateway and agree on a session key that will encrypt future interactions. Similarly, a Context Sensitive seamless Identity Provisioning (CSIP) architecture is developed in [113] for IIoT devices to validate users. The CSIP presents a two-part mutual authentication technique based on hashes and mutual authentication values.

5) SECURING COMMUNICATION

Secure and reliable communication is necessary for transmitting vital information across all the layers of an IIoT system, and also for operating it safely and smoothly [57]. In addition to cryptographic strategies and IDSs, there are several other techniques to secure the communication of information in IIoT-based systems, which include • *Role-based*

authorization: A role-based authorization mechanism needs to be implemented in order to verify requests and messages being sent from various sources. Only legitimate sources, such as those devices that are part of the system, must be allowed to interact with each other, and other outside sources should be prohibited. This barricades attackers, since no message/packet will be passed without authorization [114].

• *Security routing protocol* Routing is a process in which the best path between a data source and its destination is determined. The routing information, however, is often accessible to attackers, since it is not encrypted. This problem can be addressed by implementing an authentication process based on lightweight cryptographic algorithms to secure routing protocols [115].

6) TRAINING AND ASSESSING OF EMPLOYEES

Successful attack protection does not rely solely on technology; it also relies heavily on people, such as workers and managers, as well as implementing security policies and procedures within corporations. Enhancing the awareness of employees, as well as training and assessing them are more difficult in IIoT paradigms than in consumer IoT contexts, since a higher number of employees are involved. Thus, improving employees' cyber situational awareness—i.e., making them aware of possible security threats and hazards, and the need for security measures—is a necessary step toward securing corporations against cyber-attacks [116]. For instance, Open Web Application Security Project (OWASP) foundation presents generic security principles to improve the awareness of manufacturers, developers, and users in the context of IIoT [117]. Additionally, as demonstrated in [118], merely transferring information is insufficient to enhance users' behaviors. Yet, practical awareness via direct contact and hands-on experience through security testbeds can make the employees aware of security challenges and countermeasures in IIoT systems, and can change their long-term behaviors more effectively [119], [120]. Finally, a periodical security review of the current system is required to determine whether the security measures are appropriate. There are a number of tools, such as the cyber-security evaluation tool [94] and the IIoT analysis framework [121] to make it easier to examine the security of bigger installations, and are therefore particularly useful for strengthening and evaluating the security of IIoT systems.

B. INTRUSION DETECTION IN IIoT NETWORKS

Detecting attacks against IIoT systems requires broad network, data, and equipment inspections for identifying the signs of abnormal behaviors or malfunctions based on the network behavior. IDSs are critical for identifying malicious activities in a timely manner, and for preventing their subsequent damage to IIoT systems. They are especially important when preventative security measures are not properly deployed. In most cases, existing IDSs for traditional IT networks cannot be used in IIoT paradigms, due to reasons such as lack of interoperability [122]. For instance, ICSs are dominated by real-time processes and resource-constrained devices, which are less frequent in traditional IT networks. Additionally, since not all the data traffic flows via a single central point, IIoT networks generally require numerous vantage points for IDSs. Apart from these complications, there are some privileges for deploying IDSs in IIoT systems. For example, in contrast to random communication in IT networks, predictable industrial operations enjoy more regular network traffic patterns, making identification of anomalies easier [123]. The following subsections elaborate on available IDSs for IIoT-based applications in EPSs.

1) TRADITIONAL IDSs

Traditionally, IDSs observe and analyze the network for attacks mainly by looking for attack signatures and traffic, anomalous activities, or system specifications. Signatures are patterns that under-attack networks display, and specifications are the rules for valid and correct operation of the system [124], [125]. Traditional IDSs can be signature-based, anomaly-based, or specification-based.

Signature-based IDSs attempt to model the malicious behavior of an attack, i.e., its signature, for detecting them. Therefore, signature-based IDSs can only detect attacks whose signatures are known, since they lack the ability of generalization. Additionally, modeling the signature of attacks might be challenging in some cases. Anomaly-based IDSs, on the other hand, detect attacks by probing the behaviors of nodes, such as their usual message emanations, and comparing them with previously known valid behaviors. In fact, an anomaly-based IDS learns the natural behavior of a system, and detects attacks when the system behavior deviates from natural. An anomaly-based IDS can be either model-based—if the attack-free operation can be accurately modeled by physical equations—or learning-based, if the natural behavior is modeled by using Artificial Intelligence (AI). It should be noted that only the former type is categorized as traditional anomaly-based IDS [126]. The system model used for traditional model-based methods can be (i) differential, algebraic, or a combination of both, (ii) linear or nonlinear, and (iii) parameter-varying or -invariant. A model-based anomaly detection method can be used in conjunction with the traffic information anomaly detection techniques to improve the attack detection accuracy [127]. Even though anomaly-based IDSs are able to identify previously unknown attacks, they have relatively high false alarm rates, since previously unseen behaviors might be confused with attacks.

A specification-based method is a type of traditional IDS, which reduces the false alarm rates of anomaly-based detection techniques by distinguishing natural unknown behaviors of the system from attacks. System specifications, which signify the system's expected behaviors, are key components of specifications-based IDSs. In this type of methods, abnormal behaviors of a system are detected as a breach of security. When sufficient information about a system's behaviors is not available, a specification source is developed by simulation. This source is then used to identify intrusions by monitoring

the deviation of system behaviors from simulated attack-free specifications [128].

2) MACHINE-LEARNING-BASED IDSs

Attack detection has experienced a great evolution with recent advancements in Machine Learning (ML) and AI. ML-based techniques can address the shortcomings of anomaly- and signature-based IDSs by exploiting an intelligent model trained based on the data collected from IIoT systems in attack-free conditions and during attacks. Thus, ML IDSs are able to detect both previously seen and unseen cyber-attacks [129], [130]. In general, ML-based IDSs for IIoT systems can be categorized into supervised, unsupervised, semi-supervised, and Reinforcement Learning (RL) methods [131], [132].

a: SUPERVISED ML METHODS

Supervised learning happens when a large amount of labeled data is used to train a model for either classification or regression. Classification can determine whether or not an attack has occurred, whereas regression gives the probability of attacks. Classification models include, but are not limited to, Neural Network (NN), Support Vector Machine (SVM), and K-Nearest Neighbor (KNN) methods. These algorithms can be employed to analyze IIoT network data or nodes, and find out malign ones using a model that is trained based on the previously seen instances of attack and attack-free operation [133]. More information about supervised ML methods can be found in [134].

- *NNs:* This ML-based technique comprises several layers of neurons, and can be trained to estimate a function that maps the set of input features (or data) to attack/normal classifications [135]. Multi-Layer Perceptron (MLP) networks are a category of NNs that can be augmented with some layers, such as convolutional layers to form the Convolutional NN (CNN) [136]. Recurrent NN (RNN) [137], Long Short Term Memory (LSTM) [138], and gated recurrent units [139] are other types of NNs that can be used for detecting attacks in IIoT systems. Additionally, thanks to technological advancements in parallel processing, deep learning—which is a term used for both CNNs and MLPs with a relatively large number of layers—has received great attention for detecting cyber-attacks against IoT and IIoT systems [136].
- *SVM:* This supervised ML technique detects intrusions against IIoT networks by classifying data into two categories, i.e., attack and attack-free. SVM-based IDSs are efficient, since they are (i) suitable for low-power devices, such as those used in the IIoT systems, and (ii) extremely scalable, due to their simplicity and the ability of intrusion detection in real-time. The challenge of using SVM is in finding support vectors, which are used to classify unknown traffics as either attack-free or malicious [140].
- *KNN:* This supervised ML algorithm can be used for both classification and regression. In this method, new data points are assigned a value and classified depending on how closely they resemble the data of the training set. One criterion for measuring resemblance between a new data point and the ones in the training set is the Euclidean distance between them. This method can identify suspicious activities in IIoT systems in EPSs [141].

b: UNSUPERVISED ML METHODS

These ML models extract information and hidden patterns from the raw data without requiring the label of data. Unsupervised models that are able to cluster the input data include, but are not limited to, Principal Component Analysis (PCA) and K-means Clustering [133]. More information about semi-supervised ML methods can be found in [134].

- *PCA:* This unsupervised ML method computes the principal components of a dataset and usees them to reduce the dimension of the data. In fact, PCA generates uncorrelated features from the initial correlated ones to lower the feature space. Thus, due to its dimension reduction capability, PCA is appropriate for IIoT systems with massive data. Integrating PCA with other ML techniques can result in stronger IDSs [142].
- *K-means clustering:* This approach divides the data into k clusters and assigns each observation to a cluster whose mean is nearest to the observation. Hyper-parameter K is usually selected manually to control the learning process, and the centroids are found iteratively using some initial random points. The fact that K-means clustering method does not require data labels makes it suitable for IIoT dataset, which is often unlabeled [143].

c: SEMI-SUPERVISED ML METHODS

This family of ML techniques trains the model using a small amount of labeled data and a large quantity of unlabeled data. In fact, semi-supervised ML is a special instance of weak supervision. Semi-supervised techniques are useful when the costs of labeling are relatively high, and a good learning accuracy is required. One example of semi-supervised learning is to combine clustering and classification algorithms. The former method categorizes the most relevant samples of the and into several clusters, and the latter approach labels the unlabeled data based on the clusters and uses it to train the model. Self-training, co-training, multi-view learning, and generative adversarial network, are other examples of semi-supervised ML techniques that can be used for developing IDSs [144]. More information about semi-supervised ML methods can be found in [145].

d: RL TECHNIQUES

RL is a mixture of both supervised and unsupervised learning methods, where the output is improved in every iteration based on trial and error [146]. An RL model learns the optimal actions in an environment, e.g., in an IIoT system, which is usually modeled by a Markov Decision Process (MDP) [147]. In this process, the environment is described with a number of states and a set of actions for each state. Therefore, in each state, the RL model has a number of actions to take, and is rewarded or penalized based on its state and chosen

action. States also change according to actions, usually probabilistically and according to a transition matrix that shows the probability of going from one state to another under each of actions. RL is useful when the classification boundary between attack-free and malicious traffic may change depending on attack parameters and strategies. In such situations, RL continuously updates the classification boundaries, allowing the model to adapt to new intrusions [148].

C. INTEGRATION OF BLOCKCHAIN FOR SECURING IIoT SYSTEMS IN EPSs

Blockchain is an emerging technology that can benefit IIoT systems in EPSs by enhancing their security requirements for interconnection, permission control, and data exchange [12]. In Blockchain systems, data is protected by cryptographic encryption, and devices in the network are protected by their unique identifiers [149]. The architecture, challenges, and applications of Blockchain in the energy industry are reviewed in [150]. Additionally, implementation of Blockchain in smart grids has been investigated in [151], [152], and [153]. The authors of [151] discuss the need for security in smart grids, and use Rainbowchain, which employs seven authentication methods, to provide enhanced performance and security than the conventional Blockchain architectures. This approach, however, can reveal the personal information of consumers. To address this problem, a privacy-preserving and efficient data aggregation technique that splits users into groups is developed in [152]. In this method, each group has its own private Blockchain to record the data of its members.

Blockchain is also proposed for IIoT-based peer-to-peer energy trading in smart grids and microgrids, since the lack of trust and transparency in the energy market raises concerns regarding the safety and privacy of users. The authors of [153] have developed a safe and secure energy trading system, known as the energy Blockchain, using the Consortium Blockchain technology. They have also devised a credit-based payment system to eliminate transaction delays and facilitate fast payment and frequent energy trading. In this technique, energy transactions are signed and audited by other parties, making them verifiable and secure. In another study, researchers have developed an efficient and secure decentralized keyless signing technique based on the Consortium Blockchain [154].In this technique service providers are able to monitor each other on a Blockchain without the need for a Trusted Third Party (TTP). Similarly, a peer-to-peer electricity trading system with Consortium Blockchain has been developed in [155] to strengthen the transactions' security without relying on a TTP. In this method, local aggregators use the Blockchain to publicly audit and share transaction records without relying on a TTP. Additionally, electricity pricing and the amount of traded electricity are solved via an iterative double auction process that iterates over time. In another study, a new Blockchain-based algorithm, known as Hyper Delegation Proof of Randomness (HDPoR), has been proposed in [156]. This study also develops an efficient and secure peer-to-peer transaction service model for renewable energy sources.

VII. CONCLUSION

IIoT deployment has brought about various opportunities for EPSs, such as enhancing asset visibility, energy management, and control of distributed generation, as well as reducing energy losses. However, the security challenges of IIoT systems have barricaded large-scale deployment of IIoT-based applications in EPSs. This paper, first elaborated on IIoT-based applications in EPSs, and discussed the most common IIoT architectures for implementing these applications. It also highlighted the major security requirements of IIoT-based systems. Afterwards, the vulnerabilities of IIoT systems were explained, and the attacks that can take advantage of such vulnerabilities were classified based on their entry layer. Additionally, the paper examined various prevention and detection strategies for addressing the vulnerabilities of IIoT systems in EPSs and mitigating intrusions before they damage the system. Finally, to improve the security of IIoT-based applications in EPSs, possibilities for implementing technologies such as Blockchain, ML, and AI were discussed.

The presented work in this paper can be extended in several directions. Developing cyber-security solutions for each IIoT-based application in EPSs requires an in-depth analysis of that application and identifying its cyber-security specifications. Therefor, it is more effective if security enhancement measures are designed for each IIoT application based on the features and specifications of that application, rather than developing generic solutions. Additionally, a suitable solution for securing large scale systems, such as EPSs, is employing the Blockchain. Thus, another potential direction for future research includes tailoring the Blockchain technology for IIoT-based applications in EPSs.

REFERENCES

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generat. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.
[2] L. Da Xu, W. He, and S. Li, "Internet of Things in industries: A survey," *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2233–2243, Nov. 2014.
[3] *IoT Connections Outlook*. Accessed: Jul. 20, 2022. [Online]. Available: https://www.ericsson.com/en/mobilityreport/dataforecasts/iot-connections-outlook
[4] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: Perspectives and challenges," *Wireless Netw.*, vol. 20, no. 8, pp. 2481–2501, Nov. 2014.
[5] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, "Anatomy of threats to the Internet of Things," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1636–1675, 2nd Quart., 2018.
[6] T. Yu, V. Sekar, S. Seshan, Y. Agarwal, and C. Xu, "Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the Internet-of-Things," in *Proc. 14th ACM Workshop Hot Topics Netw.*, Nov. 2015, pp. 1–7.
[7] K. Henning, "Recommendations for implementing the strategic initiative industrie 4.0," Industrie 4.0 Work. Group, Munich, Germany, Final Rep., 2013.
[8] Q. Zhang, C. Zhu, L. T. Yang, Z. Chen, L. Zhao, and P. Li, "An incremental CFS algorithm for clustering large data in industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 13, no. 3, pp. 1193–1201, Jun. 2017.

[9] H. Jaidka, N. Sharma, and R. Singh, "Evolution of IoT to IIOT: Applications & challenges," in *Proc. Int. Conf. Innov. Comput. Commun. (ICICC)*, 2020, pp. 1–6.

[10] A. Sajid, H. Abbas, and K. Saleem, "Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges," *IEEE Access*, vol. 4, pp. 1375–1384, 2016.

[11] P. Mathur, "Overview of IoT and IIoT," in *IoT Machine Learning Applications in Telecom, Energy, and Agriculture*. Berkeley, CA, USA: Apress, 2020, pp. 19–43.

[12] J. Sengupta, S. Ruj, and S. D. Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *J. Netw. Comput. Appl.*, vol. 149, Jan. 2020, Art. no. 102481.

[13] B. Cao, X. Wang, W. Zhang, H. Song, and Z. Lv, "A many-objective optimization model of industrial Internet of Things based on private blockchain," *IEEE Network*, vol. 34, no. 5, pp. 78–83, Sep./Oct. 2020.

[14] S. Mumtaz, A. Alsohaily, Z. Pang, A. Rayes, K. F. Tsang, and J. Rodriguez, "Massive Internet of Things for industrial applications: Addressing wireless IIoT connectivity challenges and ecosystem fragmentation," *IEEE Ind. Electron. Mag.*, vol. 11, no. 1, pp. 28–33, Mar. 2017.

[15] M. Yonezawa, "Application of the IIOT to equipment maintenance," Yokogawa Tech. Rep. English Ed., Musashino, Japan, Tech. Rep., 2018, vol. 61, no. 1.

[16] P. Zhang, Y. Y. Wu, and H. Zhu, "Open ecosystem for future industrial Internet of Things (IIoT): Architecture and application," *CSEE J. Power Energy*, vol. 6, no. 1, pp. 1–11, Mar. 2020.

[17] V. Domova and A. Dagnino, "Towards intelligent alarm management in the age of IIOT," in *Proc. Global Internet Things Summit (GIoTS)*, 2017, pp. 1–5.

[18] G. Bedi, G. K. Venayagamoorthy, R. Singh, R. R. Brooks, and K.-C. Wang, "Review of Internet of Things (IoT) in electric power and energy systems," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 847–870, Apr. 2018.

[19] E. Kabalci, A. Gorgun, and Y. Kabalci, "Design and implementation of a renewable energy monitoring system," in *Proc. 4th Int. Conf. Power Eng., Energy Electr. Drives*, May 2013, pp. 1071–1075.

[20] T. Bayar, "Cybersecurity in the power sector," *Power Eng. Int.*, vol. 22, pp. 12–16, Oct. 2014.

[21] M. Mwanza and K. Ulgen, "Sustainable electricity generation fuel mix analysis using an integration of multicriteria decision-making and system dynamic approach," *Int. J. Energy Res.*, vol. 44, no. 12, pp. 9560–9585, Oct. 2020.

[22] M. Annunziata, G. Bell, R. Buch, S. Patel, and N. Sanyal, "Powering the future: Leading the digital transformation of the power industry," General Electric Company, Boston, MA, USA, Tech. Rep. 1, 2016.

[23] A. Samreen, P. Sathish, and N. A. Manga, "Low cost IoT based emission monitoring system for thermal power plants," in *Proc. Innov. Power Adv. Comput. Technol. (I-PACT)*, vol. 1, 2019, pp. 1–5.

[24] N. P. G. Bhavani, K. Sujatha, R. S. Ponmagal, and T. K. Reddy, "Monitoring of SO_2 emissions in power plants using Internet of Things," in *Proc. Int. Conf. Energy, Commun., Data Analytics Soft Comput. (ICECDS)*, Aug. 2017, pp. 1064–1067.

[25] E. S. Rubin, C. Chen, and A. B. Rao, "Cost and performance of fossil fuel power plants with CO_2 capture and storage," *Energy Policy*, vol. 35, no. 9, pp. 4444–4454, Sep. 2007.

[26] U. Cali, M. Kuzlu, M. Pipattanasomporn, J. Kempf, and L. Bai, *Digitalization of Power Markets and Systems Using Energy Informatics*. Cham, Switzerland: Springer, 2021.

[27] S. Bahrami and M. Hadi Amini, "A decentralized framework for real-time energy trading in distribution networks with load and generation uncertainty," 2017, *arXiv:1705.02575*.

[28] J. An, Z. Zou, G. Chen, Y. Sun, R. Liu, and L. Zheng, "An IoT-based life cycle assessment platform of wind turbines," *Sensors*, vol. 21, no. 4, p. 1233, Feb. 2021.

[29] S. Karad and R. Thakur, "Efficient monitoring and control of wind energy conversion systems using Internet of Things (IoT): A comprehensive review," *Environ., Develop. Sustainability*, vol. 23, no. 10, pp. 14197–14214, Oct. 2021.

[30] F. F. Ahmad, C. Ghenai, and M. Bettayeb, "Maximum power point tracking and photovoltaic energy harvesting for Internet of Things: A comprehensive review," *Sustain. Energy Technol. Assessments*, vol. 47, Oct. 2021, Art. no. 101430.

[31] R. Gore and S. P. Valsan, "Big data challenges in smart grid IoT (WAMS) deployment," in *Proc. 8th Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2016, pp. 1–6.

[32] X. Chen, J. Liu, X. Li, L. Sun, and Y. Zhen, "Integration of IoT with smart grid," in *Proc. IET Int. Conf. Commun. Technol. Appl. (ICCTA)*, 2011, pp. 723–726.

[33] L. Zhao, I. B. M. Matsuo, Y. Zhou, and W.-J. Lee, "Design of an industrial IoT-based monitoring system for power substations," *IEEE Trans. Ind. Appl.*, vol. 55, no. 6, pp. 5666–5674, Nov. 2019.

[34] Y. Zhen, X. Li, Y. Zhang, L. Zeng, Q. Ou, and X. Yin, "Transmission tower protection system based on Internet of Things in smart grid," in *Proc. 7th Int. Conf. Comput. Sci. Educ. (ICCSE)*, Jul. 2012, pp. 863–867.

[35] M. S. Hossain, N. A. Madlool, N. A. Rahim, J. Selvara, A. K. Pandey, and A. F. Khan, "Role of smart grid in renewable energy: An overview," *Renew. Sustain. Energy Rev.*, vol. 60, pp. 1168–1184, Jul. 2016.

[36] N. H. Motlagh, M. Mohammadrezaei, J. Hunt, and B. Zakeri, "Internet of Things (IoT) and the energy sector," *Energies*, vol. 13, no. 2, p. 494, 2020.

[37] M. Avci, M. Erkoc, and S. S. Asfour, "Residential HVAC load control strategy in real-time electricity pricing environment," in *Proc. IEEE Energytech*, May 2012, pp. 1–6.

[38] C. K. M. Lee, S. Z. Zhang, and K. K. H. Ng, "Development of an industrial Internet of Things suite for smart factory towards re-industrialization," *Adv. Manuf.*, vol. 5, no. 4, pp. 335–343, Dec. 2017.

[39] X. Chen, L. Sun, H. Zhu, Y. Zhen, and H. Chen, "Application of Internet of Things in power-line monitoring," in *Proc. Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discovery*, Oct. 2012, pp. 423–426.

[40] J. Liu, X. Li, X. Chen, Y. Zhen, and L. Zeng, "Applications of Internet of Things on smart grid in China," in *Proc. 13th Int. Conf. Adv. Commun. Technol. (ICACT)*, 2011, pp. 13–17.

[41] Q. Ou, Y. Zhen, X. Li, Y. Zhang, and L. Zeng, "Application of Internet of Things in smart grid power transmission," in *Proc. 3rd FTRA Int. Conf. Mobile, Ubiquitous, Intell. Comput.*, Jun. 2012, pp. 96–100.

[42] Y. Wang, W. Lin, T. Zhang, and Y. Ma, "Research on application and security protection of Internet of Things in smart grid," ICISCE, Shenzhen, China, Tech. Rep. 1, 2012.

[43] M. F. Zia, M. Benbouzid, E. Elbouchikhi, S. M. Muyeen, K. Techato, and J. M. Guerrero, "Microgrid transactive energy: Review, architectures, distributed ledger technologies, and market analysis," *IEEE Access*, vol. 8, pp. 19410–19432, 2020.

[44] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015.

[45] Y. Harbi, Z. Aliouat, S. Harous, A. Bentaleb, and A. Refoufi, "A review of security in Internet of Things," *Wirel. Pers. Commun.*, vol. 108, no. 1, pp. 325–344, Sep. 2019.

[46] A. R. Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in the Internet of Things," *Digit. Commun. Netw.*, vol. 4, no. 2, pp. 118–137, 2018.

[47] S. Alam, M. M. R. Chowdhury, and J. Noll, "Interoperability of security-enabled Internet of Things," *Wireless Pers. Commun.*, vol. 61, no. 3, pp. 567–586, 2011.

[48] R. Rivest and S. Dusse, *The MD5 Message-Digest Algorithm*, document RFC 1321, 1992.

[49] A. R. Chowdhury, T. Chatterjee, and S. DasBit, "LOCHA: A light-weight one-way cryptographic hash algorithm for wireless sensor network," *Proc. Comput. Sci.*, vol. 32, pp. 497–504, 2014.

[50] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[51] H. Aksu, L. Babun, M. Conti, G. Tolomei, and A. S. Uluagac, "Advertising in the IoT era: Vision and challenges," *IEEE Commun. Mag.*, vol. 56, no. 11, pp. 138–144, 2018.

[52] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of Things: A survey of existing protocols and open research issues," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1294–1312, 3rd Quart., 2015.

[53] S. Gusmeroli, S. Piccione, and D. Rotondi, "A capability-based security approach to manage access control in the Internet of Things," *Math. Comput. Model.*, vol. 58, no. 5, pp. 1189–1205, Sep. 2013.

[54] S. Misra, M. Maheswaran, and S. Hashmi, *Security Challenges and Approaches in Internet of Things*. Cham, Switzerland: Springer, 2017.

[55] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2702–2733, 3rd Quart., 2019.

[56] C. Xenofontos, I. Zografopoulos, C. Konstantinou, A. Jolfaei, M. K. Khan, and K.-K.-R. Choo, "Consumer, commercial, and industrial IoT (In)security: Attack taxonomy and case studies," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 199–221, Jan. 2022.

[57] A. Mosenia and N. K. Jha, "A comprehensive study of security of Internet-of-Things," *IEEE Trans. Emerg. Topics Comput.*, vol. 5, no. 4, pp. 586–602, Oct. 2017.

[58] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless sensor network security: A survey," in *Security in Distributed, Grid, Mobile, and Pervasive Computing*. Boca Raton, FL, USA: Auerbach Publications, Jan. 2006.

[59] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, and Y. A. Bangash, "An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10250–10276, May 2020.

[60] X. Liu, C. Qian, W. G. Hatcher, H. Xu, W. Liao, and W. Yu, "Secure Internet of Things (IoT)-based smart-world critical infrastructures: Survey, case study and research opportunities," *IEEE Access*, vol. 7, pp. 79523–79544, 2019.

[61] M. Abomhara and G. M. Køien, "Cyber security and the Internet of Things: Vulnerabilities, threats, intruders and attacks," *J. Cyber Secur.*, vol. 4, no. 1, pp. 65–88, 2015.

[62] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2005, pp. 49–63.

[63] E. Bertino and N. Islam, "Botnets and Internet of Things security," *Computer*, vol. 50, no. 2, pp. 76–79, Feb. 2017.

[64] A. Hamza, H. Habibi Gharakheili, and V. Sivaraman, "IoT network security: Requirements, threats, and countermeasures," 2020, *arXiv:2008.09339*.

[65] M. U. Farooq, M. Waseem, S. Mazhar, A. Khairi, and T. Kamal, "A review on Internet of Things (IoT)," *Int. J. Comput. Appl.*, vol. 113, no. 1, pp. 1–7, 2015.

[66] X. Yang, X. Zhang, J. Lin, W. Yu, X. Fu, and W. Zhao, "Data integrity attacks against the distributed real-time pricing in the smart grid," in *Proc. IEEE 35th Int. Perform. Comput. Commun. Conf. (IPCCC)*, Dec. 2016, pp. 1–8.

[67] L. Schenato, B. Sinopoli, M. Franceschetti, K. Poolla, and S. S. Sastry, "Foundations of control and estimation over lossy networks," *Proc. IEEE*, vol. 95, no. 1, pp. 163–187, Jan. 2007.

[68] K. Hamlen, M. Kantarcioglu, L. Khan, and B. Thuraisingham, "Security issues for cloud computing," *Int. J. Inf. Secur. Privacy (IJISP)*, vol. 4, no. 2, pp. 36–48, 2010.

[69] Y. Zhou and D. Feng, "Side-channel attacks: Ten years after its publication and the impacts on cryptographic module security testing," *IACR Cryptol. ePrint Arch.*, vol. 2005, p. 388, Sep. 2005.

[70] M. S. Esfahani, "Security analysis of phasor measurement units in smart grid communication infrastructures," Ph.D. dissertation, Dept. Comput. Electron. Eng., Univ. Nebraska-Lincoln, Lincoln, NE, USA, 2014.

[71] Z. B. Celik, P. McDaniel, G. Tan, L. Babun, and A. S. Uluagac, "Verifying Internet of Things safety and security in physical spaces," *IEEE Secur. Privacy*, vol. 17, no. 5, pp. 30–37, Sep. 2019.

[72] M. Alsaleh, M. Mannan, and P. C. van Oorschot, "Revisiting defenses against large-scale online password guessing attacks," *IEEE Trans. Depend. Sec. Comput.*, vol. 9, no. 1, pp. 128–141, Jan./Feb. 2012.

[73] J. R. Douceur, *The Sybil Attack*, P. Druschel, F. Kaashoek, and A. Rowstron, Eds. Berlin, Germany: Springer, 2002.

[74] P. Cisar and S. M. Cisar, "General vulnerability aspects of Internet of Things," in *Proc. 16th IEEE Int. Symp. Comput. Intell. Informat. (CINTI)*, Nov. 2015, pp. 117–121.

[75] M. Stanislav and T. Beardsley, "Hacking IoT: A case study on baby monitor exposures and vulnerabilities," Rapid7, Boston, MA, USA, Tech. Rep. 1, 2015.

[76] P. Podder, M. R. H. Mondal, S. Bharati, and P. K. Paul, "Review on the security threats of Internet of Things," 2021, *arXiv:2101.05614*.

[77] S. Berger, O. Bürger, and M. Röglinger, "Attacks on the industrial Internet of Things—Development of a multi-layer taxonomy," *Comput. Secur.*, vol. 93, Jun. 2020, Art. no. 101790.

[78] P. Anand, Y. Singh, A. Selwal, M. Alazab, S. Tanwar, and N. Kumar, "IoT vulnerability assessment for sustainable computing: Threats, current solutions, and open challenges," *IEEE Access*, vol. 8, pp. 168825–168853, 2020.

[79] H. Elmiligi, F. Gebali, and M. W. El-Kharashi, "Multi-dimensional analysis of embedded systems security," *Microprocessors Microsyst.*, vol. 41, pp. 29–36, Mar. 2016.

[80] M. Bettayeb, Q. Nasir, and M. A. Talib, "Firmware update attacks and security for IoT devices: Survey," in *Proc. ArabWIC 6th Annu. Int. Conf. Res. Track (ArabWIC)*, 2019, pp. 1–6.

[81] F. Aliyu, T. Sheltami, and E. M. Shakshuki, "A detection and prevention technique for man in the middle attack in fog computing," *Proc. Comput. Sci.*, vol. 141, pp. 24–31, Jan. 2018.

[82] R. E. Navas, H. Le Bouder, N. Cuppens, F. Cuppens, and G. Z. Papadopoulos, "Demo: Do not trust your neighbors! A small IoT platform illustrating a man-in-the-middle attack," in *Proc. Int. Conf. Ad-Hoc Netw. Wireless*. Cham, Switzerland: Springer, 2018, pp. 120–125.

[83] R. K. Stephen and L. Arockiam, "An enhanced technique to detect sinkhole attack in Internet of Things," *Int. J. Eng. Res. Technol.*, vol. 5, no. 13, pp. 1–4, 2018.

[84] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: Internet of Threats? A survey of practical security vulnerabilities in real IoT devices," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8182–8201, Oct. 2019.

[85] X. Yang, L. Shu, Y. Liu, G. P. Hancke, M. A. Ferrag, and K. Huang, "Physical security and safety of IoT equipment: A survey of recent advances and opportunities," *IEEE Trans. Ind. Informat.*, vol. 18, no. 7, pp. 4319–4330, Jul. 2022.

[86] Y. Lu and L. D. Xu, "Internet of Things (IoT) cybersecurity research: A review of current research topics," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2103–2115, Apr. 2019.

[87] M. Tehranipoor and F. Koushanfar, "A survey of hardware Trojan taxonomy and detection," *IEEE Design Test Comput.*, vol. 27, no. 1, pp. 10–25, Feb. 2010.

[88] A. N. Nowroz, K. Hu, F. Koushanfar, and S. Reda, "Novel techniques for high-sensitivity hardware trojan detection using thermal and power maps," *IEEE Trans. Comput.-Aided Design Integr.*, vol. 33, no. 12, pp. 1792–1805, Dec. 2014.

[89] M. Zhang and N. K. Jha, "FinFET-based power management for improved DPA resistance with low overhead," *ACM J. Emerg. Technol. Comput. Syst.*, vol. 7, no. 3, pp. 1–16, Aug. 2011.

[90] M. Patton, E. Gross, R. Chinn, S. Forbis, L. Walker, and H. Chen, "Uninvited connections: A study of vulnerable devices on the Internet of Things (IoT)," in *Proc. IEEE Joint Intell. Secur. Informat. Conf.*, Sep. 2014, pp. 232–235.

[91] E. Bertino, K.-K.-R. Choo, D. Georgakopolous, and S. Nepal, "Internet of Things (IoT): Smart and secure service delivery," *ACM Trans. Internet Technol.*, vol. 16, no. 4, pp. 1–7, Dec. 2016.

[92] M. Höst, J. Sönnerup, M. Hell, and T. Olsson, "Industrial practices in security vulnerability management for IoT systems—An interview study," in *Proc. Int. Conf. Softw. Eng. Res. Pract. (SERP)*, in The Steering Committee of The World Congress in Computer Science, Computer · · ·. Athens, Greece: CSREA Press, 2018, pp. 61–67.

[93] K. Stouffer, J. Falco, and K. Scarfone, "Guide to industrial control systems (ICS) security, NIST spec," *Publ*, vol. 800, p. 82, May 2011.

[94] M. Serror, S. Hack, M. Henze, M. Schuba, and K. Wehrle, "Challenges and opportunities in securing the industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 17, no. 5, pp. 2985–2996, May 2021.

[95] S. He, W. Ren, T. Zhu, and K.-K.-R. Choo, "BoSMoS: A blockchain-based status monitoring system for defending against unauthorized software updating in industrial Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 2, pp. 948–959, Feb. 2019.

[96] J. L. Flores and I. Mugarza, "Runtime vulnerability discovery as a service on industrial Internet of Things (IIoT) systems," in *Proc. IEEE 23rd Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, Sep. 2018, pp. 948–955.

[97] G. George and S. M. Thampi, "A graph-based security framework for securing industrial IoT networks from vulnerability exploitations," *IEEE Access*, vol. 6, pp. 43586–43601, 2018.

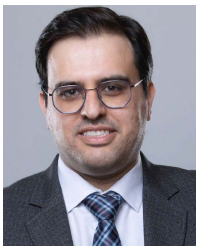
[98] C. Lesjak, D. Hein, and J. Winter, "Hardware-security technologies for industrial IoT: TrustZone and security controller," in *Proc. IECON 41st Annu. Conf. IEEE Ind. Electron. Soc.*, Nov. 2015, pp. 002589–002595.

[99] S. Pinto, T. Gomes, J. Pereira, J. Cabral, and A. Tavares, "IIoTEED: An enhanced, trusted execution environment for industrial IoT edge devices," *IEEE Internet Comput.*, vol. 21, no. 1, pp. 40–47, Jan./Feb. 2017.

[100] E. Lear and B. Weis, "Slinging MUD: Manufacturer usage descriptions: How the network can protect things," in *Proc. Int. Conf. Sel. Topics Mobile Wireless Netw. (MoWNeT)*, Apr. 2016, pp. 1–6.
[101] A. Hamza, D. Ranathunga, H. H. Gharakheili, M. Roughan, and V. Sivaraman, "Clear as MUD: Generating, validating and applying IoT behavioral profiles," in *Proc. Workshop IoT Secur. Privacy*, Aug. 2018, pp. 8–14.
[102] D. Henneke, L. Wisniewski, and J. Jasperneite, "Analysis of realizing a future industrial network by means of software-defined networking (SDN)," in *Proc. IEEE World Conf. Factory Commun. Syst. (WFCS)*, May 2016, pp. 1–4.
[103] M. Ranganathan, D. Montgomery, and O. I. El Mimouni, "Soft MUD: Implementing manufacturer usage descriptions on OpenFlow SDN switches," ThinkMind, Valencia, Spain, Tech. Rep. 1, 2019.
[104] D. Chen, M. Nixon, T. Lin, S. Han, X. Zhu, A. Mok, R. Xu, J. Deng, and A. Liu, "Over the air provisioning of industrial wireless devices using elliptic curve cryptography," in *Proc. IEEE Int. Conf. Comput. Sci. Autom. Eng.*, vol. 2, Jun. 2011, pp. 594–600.
[105] A. Esfahani, G. Mantas, R. Matischek, F. B. Saghezchi, J. Rodriguez, A. Bicaku, S. Maksuti, M. G. Tauber, C. Schmittner, and J. Bastos, "A lightweight authentication mechanism for M2M communications in industrial IoT environment," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 288–296, Feb. 2019.
[106] A. Karati, S. K. H. Islam, and M. Karuppiah, "Provably secure and lightweight certificateless signature scheme for IIoT environments," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3701–3711, Aug. 2018.
[107] Y. Zhang, R. Deng, D. Zheng, J. Li, P. Wu, and J. Cao, "Efficient and robust certificateless signature for data crowdsensing in cloud-assisted industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 15, no. 9, pp. 5099–5108, Sep. 2019.
[108] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1495–1505, Apr. 2019.
[109] S. Shamshad, K. Mahmood, S. Hussain, S. Garg, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, "An efficient privacy-preserving authenticated key establishment protocol for health monitoring in industrial cyber–physical systems," *IEEE Internet Things J.*, vol. 9, no. 7, pp. 5142–5149, Apr. 2022.
[110] M. Ma, D, He, D. Kumar, K.-K. R. Choo, and J. Chen, "Certificateless searchable public key encryption scheme for industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 2, pp. 759–767, May 2017.
[111] J. Srinivas, A. K. Das, M. Wazid, and N. Kumar, "Anonymous lightweight chaotic map-based authenticated key agreement protocol for industrial Internet of Things," *IEEE Trans. Dependable Secure Comput.*, vol. 17, no. 6, pp. 1133–1146, Nov. 2018.
[112] C. Li and B. Palanisamy, "Privacy in Internet of Things: From principles to technologies," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 488–505, Aug. 2019.
[113] D. Airehrour, J. A. Gutierrez, and S. K. Ray, "Sectrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things," *Future Gener. Comput. Syst.*, vol. 93, pp. 860–876, Apr. 2019.
[114] S. Misra and A. Vaish, "Reputation-based role assignment for role-based access control in wireless sensor networks," *Comput. Commun.*, vol. 34, no. 3, pp. 281–294, 2011.
[115] A. Chehri and G. Jeon, "Routing protocol in the industrial Internet of Things for smart factory monitoring," in *Innovation in Medicine and Healthcare Systems, and Multimedia*. Singapore: Springer, 2019, pp. 505–515.
[116] U. Franke and J. Brynielsson, "Cyber situational awareness—A systematic review of the literature," *Comput. Secur.*, vol. 46, pp. 18–31, Oct. 2014.
[117] S. Forsstrom, I. Butun, M. Eldefrawy, U. Jennehag, and M. Gidlund, "Challenges of securing the industrial Internet of Things value chain," in *Proc. Workshop Metrology Ind. 4.0 IoT*, Apr. 2018, pp. 218–223.
[118] M. Bada, A. M. Sasse, and J. R. C. Nurse, "Cyber security awareness campaigns: Why do they fail to change behaviour?" 2019, *arXiv:1901.02672*.
[119] A. P. Mathur and N. O. Tippenhauer, "SWaT: A water treatment testbed for research and training on ICS security," in *Proc. Int. Workshop Cyber-Phys. Syst. Smart Water Netw. (CySWater)*, Apr. 2016, pp. 31–36.
[120] D. Antonioli, H. R. Ghaeini, S. Adepu, M. Ochoa, and N. O. Tippenhauer, "Gamifying ICS security training and research: Design, implementation, and results of S3," in *Proc. Workshop Cyber-Phys. Syst. Secur. PrivaCy*, Nov. 2017, pp. 93–102.
[121] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The industrial Internet of Things (IIoT): An analysis framework," *Comput. Ind.*, vol. 101, pp. 1–12, Oct. 2018.
[122] C. J. Zhou, S. Huang, N. Xiong, S.-H. Yang, H. Li, Y. Qin, and X. Li, "Design and analysis of multimodel-based anomaly intrusion detection systems in industrial process automation," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 45, no. 10, pp. 1345–1360, Oct. 2015.
[123] J. Hiller, M. Henze, M. Serror, E. Wagner, J. N. Richter, and K. Wehrle, "Secure low latency communication for constrained industrial IoT scenarios," in *Proc. IEEE 43rd Conf. Local Comput. Netw. (LCN)*, Oct. 2018, pp. 614–622.
[124] R. G. Bace and P. Mell, "Intrusion detection systems," NIST Special Publication Intrusion Detection Syst., Gaithersburg, MD, USA, Tech. Rep. 1, 2001.
[125] S. Kalyani and D. Vydeki, "Survey of rank attack detection algorithms in Internet of Things," in *Proc. Int. Conf. Adv. Comput., Commun. Informat. (ICACCI)*, Sep. 2018, pp. 2136–2141.
[126] P. Kaur, M. Kumar, and A. Bhandari, "A review of detection approaches for distributed denial of service attacks," *Syst. Sci. Control Eng.*, vol. 5, no. 1, pp. 301–320, Jan. 2017.
[127] L. Zhou and H. Guo, "Anomaly detection methods for IIoT networks," in *Proc. IEEE Int. Conf. Service Oper. Logistics, Informat. (SOLI)*, Jul. 2018, pp. 214–219.
[128] L. O. Nweke, "A survey of specification-based intrusion detection techniques for cyber-physical systems," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 5, pp. 1–9, 2021.
[129] A. N. Jahromi, H. Karimipour, A. Dehghantanha, and K.-K.-R. Choo, "Toward detection and attribution of cyber-attacks in IoT-enabled cyber–physical systems," *IEEE Internet Things J.*, vol. 8, no. 17, pp. 13712–13722, Sep. 2021.
[130] Z. Ma, J. Ma, Y. Miao, X. Liu, K.-K.-R. Choo, Y. Gao, and R. H. Deng, "Verifiable data mining against malicious adversaries in industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 18, no. 2, pp. 953–964, Feb. 2022.
[131] Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, and K. Sakurai, "Machine learning-based IoT-botnet attack detection with sequential architecture," *Sensors*, vol. 20, no. 16, p. 4372, Aug. 2020.
[132] M. A. Ferrag, O. Friha, L. Maglaras, H. Janicke, and L. Shu, "Federated deep learning for cyber security in the Internet of Things: Concepts, applications, and experimental analysis," *IEEE Access*, vol. 9, pp. 138509–138542, 2021.
[133] S. H. Haji and S. Y. Ameen, "Attack and anomaly detection in IoT networks using machine learning techniques: A review," *Asian J. Res. Comput. Sci.*, vol. 9, pp. 30–46, Jun. 2021.
[134] J. Asharf, N. Moustafa, H. Khurshid, E. Debie, W. Haider, and A. Wahab, "A review of intrusion detection systems using machine and deep learning in Internet of Things: Challenges, solutions and future directions," *Electronics*, vol. 9, no. 7, p. 1177, Jul. 2020.
[135] K. Hornik, "Approximation capabilities of multilayer feedforward networks," *Neural Netw.*, vol. 4, no. 2, pp. 251–257, 1991. [Online]. Available: https://www.sciencedirect.com/science/article/pii/089360809190009T
[136] S. Lawrence, C. L. Giles, A. C. Tsoi, and A. D. Back, "Face recognition: A convolutional neural-network approach," *IEEE Trans. Neural Netw.*, vol. 8, no. 1, pp. 98–113, Jan. 1997.
[137] T. Mikolov, M. Karafiát, L. Burget, J. Černocký, and S. Khudanpur, "Recurrent neural network based language model," in *Proc. 11th Annu. Conf. Int. Speech Commun. Assoc.*, vol. 2, 2010, pp. 1045–1048.
[138] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Comput.*, vol. 9, no. 8, pp. 1735–1780, 1997.
[139] C. Xu, J. Shen, X. Du, and F. Zhang, "An intrusion detection system using a deep neural network with gated recurrent units," *IEEE Access*, vol. 6, pp. 48697–48707, 2018.
[140] C. Ioannou and V. Vassiliou, "Network attack classification in IoT using support vector machines," *J. Sensor Actuator Netw.*, vol. 10, no. 3, p. 58, Aug. 2021.
[141] H. H. Pajouh, R. Javidan, R. Khayami, A. Dehghantanha, and K.-K. R. Choo, "A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in IoT backbone networks," *IEEE Trans. Emerg. Topics Comput.*, vol. 7, no. 2, pp. 314–323, Apr./Jun. 2019.
[142] J. Zhang, "Machine learning with feature selection using principal component analysis for malware detection: A case study," 2019, *arXiv:1902.03639*.

[143] S. M. Tahsien, H. Karimipour, and P. Spachos, "Machine learning based solutions for security of Internet of Things (IoT): A survey," *J. Netw. Comput. Appl.*, vol. 161, Jul. 2020, Art. no. 102630. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804520301041
[144] O. Y. Al-Jarrah, Y. Al-Hammdi, P. D. Yoo, S. Muhaidat, and M. Al-Qutayri, "Semi-supervised multi-layered clustering model for intrusion detection," *Digit. Commun. Netw.*, vol. 4, no. 4, pp. 277–286, Nov. 2017.
[145] M. A. Alsoufi, S. Razak, M. M. Siraj, I. Nafea, F. A. Ghaleb, F. Saeed, and M. Nasser, "Anomaly-based intrusion detection systems in IoT using deep learning: A systematic literature review," *Appl. Sci.*, vol. 11, no. 18, p. 8383, Sep. 2021.
[146] C. Wu, J. Shi, Y. Yang, and W. Li, "Enhancing machine learning based malware detection model by reinforcement learning," in *Proc. 8th Int. Conf. Commun. Netw. Secur.*, 2018, pp. 74–78.
[147] G. Kalnoor and S. Gowrishankar, "Markov decision process based model for performance analysis an intrusion detection system in IoT networks," *J. Telecommunictions Inf. Technol.*, no. 3, pp. 42–49, Sep. 2021.
[148] W. Liang, W. Huang, J. Long, K. Zhang, K.-C. Li, and D. Zhang, "Deep reinforcement learning for resource protection and real-time detection in IoT environment," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6392–6401, Jul. 2020.
[149] L. W. S. Raza and T. Voigt, "IoT-enabled smart energy grid: Applications and challenges," *Ad-Hoc Netw.*, vol. 11, no. 8, pp. 2661–2674, 2013.
[150] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. McCallum, and A. Peacock, "Blockchain technology in the energy sector: A systematic review of challenges and opportunities," *Renew. Sustain Energy Rev.*, vol. 100, pp. 143–174, Feb. 2019.
[151] S.-K. Kim and J.-H. Huh, "A study on the improvement of smart grid security performance and blockchain smart grid perspective," *Energies*, vol. 11, no. 8, p. 1973, Jul. 2018.
[152] Z. Guan, Z. Guan, G. Si, X. Zhang, L.Wu, N. Guizani, X. Du, and Y. Ma, "Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities," *IEEE Commun. Mag.*, vol. 56, no. 7, pp. 82–88, Jul. 2018.
[153] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3690–3700, Aug. 2017.
[154] H. Zhang, J. Wang, and Y. Ding, "Blockchain-based decentralized and secure keyless signature scheme for smart grid," *Energy*, vol. 180, pp. 955–967, Aug. 2019.
[155] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3154–3164, Dec. 2017.
[156] J.-H. Huh and K. Seo, "Blockchain-based mobile fingerprint verification and automatic log-in platform for future computing," *J. Supercomputing*, vol. 75, no. 6, pp. 3123–3139, Jun. 2019.

HAMED SARJAN received the B.Sc. degree in electrical engineering from the Department of Electrical and Computer Engineering, University of Semnan, Iran, in 2013, and the M.Sc. degree in electrical engineering from the Ferdowsi University of Mashhad, Iran, in 2017. He is currently pursuing the M.Sc. degree with the Department of Electrical Engineering, Lakehead University, Thunder Bay, ON, Canada. His current research interest includes cyber-security of power systems.



AMIR AMELI (Member, IEEE) received the B.Sc. degree in electrical engineering from the Iran University of Science and Technology, Tehran, Iran, in 2011, the M.Sc. degree in electrical engineering from the Sharif University of Technology, Tehran, in 2013, and the Ph.D. degree in electrical engineering from the University of Waterloo, Waterloo, ON, Canada, in 2019. He was a Postdoctoral Fellow at the Department of Electrical and Computer Engineering, University of Waterloo, from August 2019 to July 2020. He is currently an Assistant Professor with the Department of Electrical Engineering, Lakehead University, Thunder Bay, ON, Canada. His current research interests include power systems cyber-security and protection.

MOHSEN GHAFOURI (Member, IEEE) received the B.Sc. and master's degrees in electrical engineering from the Sharif University of Technology, Tehran, Iran, in 2009 and 2011, respectively, and the Ph.D. degree in electrical engineering from Polytechnique Montreal, Montreal, QC, Canada, in 2018. He was a Researcher at the Iranian Power System Research Institute, Sharif University of Technology, from 2011 to 2014. In 2018, he was a Researcher with CYME International, Eaton Power System Solutions, Montreal. In August 2018, he joined as a Horizon Postdoctoral Fellow at the Security Research Group, Concordia University, Montreal, where he is currently an Assistant Professor. His research interests include cyber-security of smart grids, power system modeling, microgrid, wind energy, and control of industrial processes.