Vulnerabilities and Challenges in IoT-Enabled Smart Grids

Subjects: Engineering, Electrical & Electronic | Telecommunications | Energy & Fuels

Contributor: Arman Goudarzi , Farzad Ghayoor , Muhammad Waseem , Shah Fahad , Issa Traore

Internet of Things (IoT) has appeared as one of the enabling technologies for smart energy grids by delivering abundant cutting-edge solutions in various domains, including critical infrastructures. As IoT-enabled devices continue to flourish, one of the major challenges is security issues, since IoT devices are connected through the Internet, thus making the smart grids vulnerable to a diverse range of cyberattacks.

smart grid | Internet of Things (IoT) | cybersecurity strategies | 5G networks | cyber-physical adversaries | cybersecurity | internet of energy (IoE)

1. Introduction

1.1. Emerging Smart Grids

With the expansion of cities and the proliferation of the population, the need for a flexible and intelligent type of electrical grid that could accommodate the diverse demand of different customers has increased. In 2007, the National Institute of Standards and Technology (NIST) proposed a framework for the future electrical grid to guarantee the reliable, scalable, secure, interoperable, and manageable operation of electrical grids while being cost-effective [1]. **Figure 1** shows the evolution of electrical grids toward the future grid, known as the smart grid system.

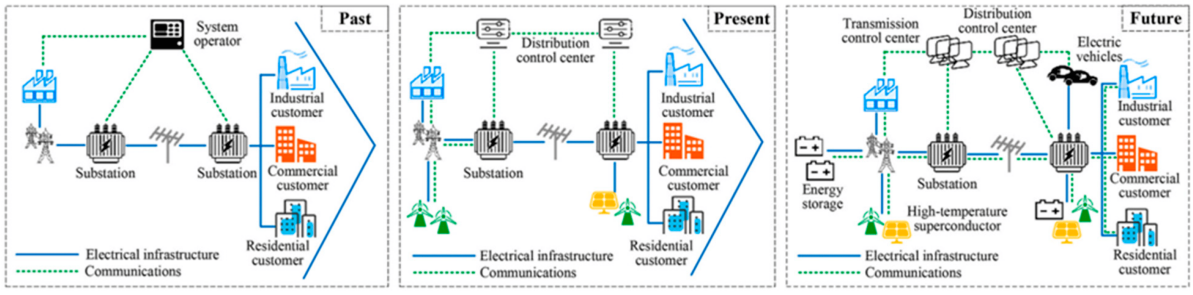

Figure 1. Evolution of electrical grids—from traditional grids to smart grids [2].

In a smart grid system, renewable energy resources such as wind, solar, and power storage units are integrated into the grid system. These new power generation technologies, which may be smaller, more widely distributed, and more ecologically friendly, could preserve grid resilience and disperse overload centers [3]. The smart grid

employs a widespread sensor network supported by a two-way communication system for constant monitoring of the grid status. The bidirectional communication network allows the exchange of measurement data and control signals between grid entities, improving the grid and user asset monitoring and management. Moreover, to process the collected data within the required time frames, the smart grid should be supported by sufficient computational resources. The control and monitoring are conducted in a more distributed way, as the volume of the collected data is enormous, and the sensors are dispersed across the entire grid.

As a result of such capabilities, the smart grid can manage the supply-demand balance of energy more effectively, securely, and reliably. Moreover, the smart grid can be considered an enabler for the realization of smart homes and electric transportation, providing a platform for customers' participation with utility companies and helping reduce carbon emissions. The merits of smart grids in comparison to traditional electrical grids are presented in **Table 1** [2][4]. However, these advantages would be obtained at the cost of increasing the grid's complexity and infrastructure, which demands an ongoing effort to overcome challenges using emerging technologies and solutions [5][6].

Table 1. Advantages of smart grids over traditional grids.

Features	Traditional Grid	Smart Grid
Communication	One-way communication	Two-way communication with interaction
Power generation	Centralized	Distributed generation, provides support during peak hours when load demand increases
Topology	Radial	Different network topology
Operation and maintenance	Manual monitoring, periodic equipment maintenance	Real-time monitoring, prognostic, and event-driven maintenance
Power restoration	Manual equipment checks and time-based maintenance	Self-healing; smart grid can anticipate, identify, and respond to faults and outages
Reliability	Prone to failure and cascading outages	Pro-active, real-time, and islanding
Metering	Electro-mechanical	Advanced metering arrangement that drives the facility to track and regulate energy consumption
Customer participation	Limited interaction or none	Extensive interaction
Power quality control	Less use of sensors and less power quality	Contains numerous modules, for example, sensors, smart meters, and technologies on the distribution grid that aid in

Features	Traditional Grid	Smart Grid
		managing the parameters, such as voltage and power factor, to improve the power quality
Renewable power source integration	Optimized for non-renewable resources	Offers essential insights and enables automation for renewable power resources to supply electricity to grids while their management is being optimized
Operational cost and wastage at peak hour	High at peak hours	Low at peak hour due to distributed generation and control over the power consumption

One of the cutting-edge solutions in the field of telecommunication is the Internet-of-Things (IoT) concept. The IoT is generally considered a network of devices embedded with electronics, software, sensors, and actuators capable of exchanging information through communication networks, such as the Internet. The IoT supports bidirectional communications and distributed computational capabilities, so it can be considered a potential solution to address inescapable difficulties in transitioning traditional energy networks into updated smart grid systems [7][8].

In a smart grid environment, services such as large-scale integration of distributed renewable energy resources, the establishment of live, real-time data communication between consumers and service providers regarding tariff information and energy consumption, and infrastructure to collect and transfer statistics of the grid's parameters for analysis, and mechanisms to implement necessary actions based on such analyses are required [9]. For intelligent decision-making, the smart energy grid creates a large amount of data and information that have to be transported, processed, and stored [10]. In this regard, the IoT, considering its multifaceted benefits in numerous industries, appears to be a suitable solution with significant potential to be used in the smart energy grid system. In addition to the increased accuracy and competency that can be added to the system through the IoT's intelligent and proactive features, the IoT can assist in a smooth transformation of the legacy power grid into a smart energy system that would be more efficient [11][12].

The main concerns in a traditional power grid system are power quality and dependability, both of which may be addressed with the help of the IoT as it offers better control of these issues. By introducing intelligent information-processing features during the electricity flow between the service provider and consumers, advanced metering infrastructure (AMI) assisted by smart metering (SM) technologies can facilitate the transformation of a conventional power grid system into a smart grid system [12]. Through the combination of sensing and actuation systems in the AMI, the IoT offers significant potential for optimizing and regulating energy use. This integrated system collects a massive quantity of data and information from many parts of the grid system, including energy usage, voltage readings, current readings, and phase measurements. Cutting-edge IoT technology can collect large amounts of data and transmit and analyze them intelligently, allowing for better energy grid management [13]. Power generation infrastructure management, supervisory control, and data acquisition (SCADA) connected systems for managing transmission and distribution operations, advanced metering infrastructure, and carbon footprint and environmental monitoring are all examples of areas where IoT technologies can have a significant impact on smart energy grid systems. Advanced cloud and edge computing technologies can enable distributed monitoring and management of dispersed energy resources, and provide answers to the old centralized SCADA system's cyber vulnerabilities [14].

Moreover, the IoT-enabled smart grid can operate and manage the electrical grid more efficiently as it can seamlessly be integrated with other smart entities, such as smart appliances, smart homes, smart buildings, and smart cities, to access and control more devices over the Internet. However, this requires using more advanced computational capabilities and resource-allocation mechanisms. Despite gaining more efficiency in monitoring and operation of the energy system, the IoT-enabled smart grid implementation comes with a set of obstacles. For instance, IoT cyber adversaries can impose smart grids onto several attacks that can be classified into three main categories: operational, economic, and system security. Several examples of these damages are listed as follows [15][16]:

- Localized and large-scale power outages.
- Significant business loss to the utilities and electricity markets.
- Social security threats to customers by publicizing their information.
- Manipulation of energy consumption records.
- Interrupting the process of transactive energy systems.

To counterattack the aforementioned challenges, several technologies, such as machine learning methods, artificial intelligence (AI), blockchain, and multifactor authentication systems, have been developed [17].

2. Cyber-Physical Security Vulnerabilities and Challenges in IoT-Enabled Smart Grids

2.1. General Definitions, Framework, and Guidelines

The energy grid systems have become more intelligent and interactive with the widespread use of IoT-based technologies, which improves the system's consistency, efficiency, and adaptability. Cybersecurity vulnerabilities, on the other hand, are becoming increasingly common. Thus, this section will discuss the security issues in IoT-connected smart energy systems and their corresponding mitigation strategies. **Figure 2** portrays the general paradigm of cyber-physical security in smart energy grids [18]. Five significant causes make smart grids vulnerable to cyberattacks [19]:

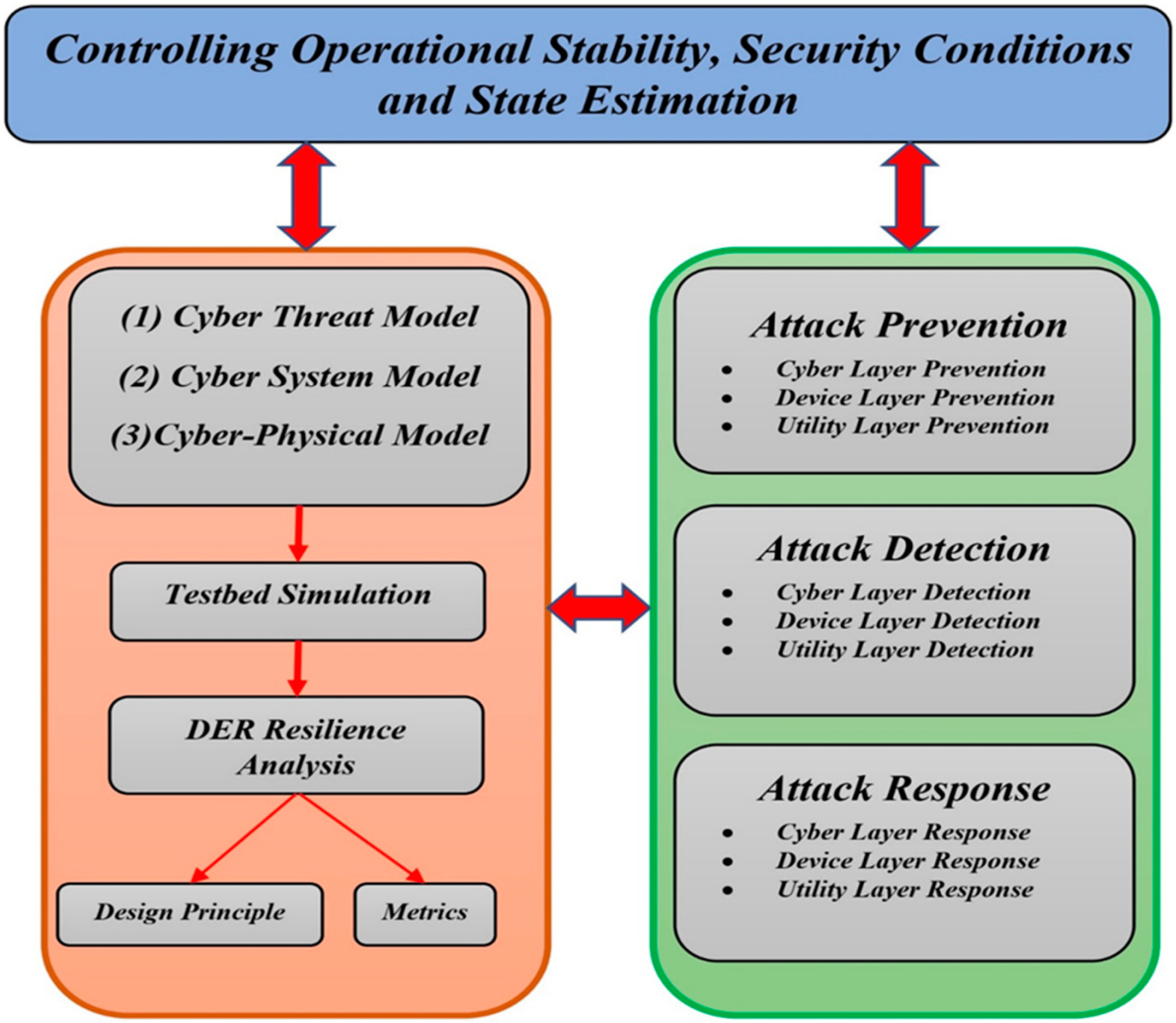

Figure 2. General paradigm of cybersecurity in smart grids.

(1) Ever-increasing development of intelligent electronic devices (IEDs): The number of attack sites grows in lockstep with the number of devices in the network. Even if a single point's security is breached, the entire network system is affected.

(2) Unregulated installation of third-party components: Experts advise against using third-party components because they make the network more vulnerable to hacking. These devices might be infected with Trojans, which could then spread to other network devices.

(3) Insufficient personal training: To use any technology, appropriate training is required. When employees are not properly trained, they are more likely to fall prey to phishing scams.

(4) Insecure Internet protocols: In terms of data transfer, not all protocols are secure. Unencrypted data transport is used by several protocols. As a result, they are easy targets for man-in-the-middle attacks that extract data.

(5)

Maintenance: The primary objective of maintenance is to keep things running smoothly. It can also be used as a vector for cyberattacks. Operators frequently deactivate a security system during maintenance to undertake tests.

The abovementioned five causes may compromise one of the five main goals of the cybersecurity framework in smart grids [20][21][22]:

(1) Authentication: The ability to verify the identity of any smart grid communication device. For example, to bill the relevant user, the energy provider must validate each smart meter.

(2) Authorization: Ensures that an authenticated person or an object is authorized to accomplish certain tasks or has been granted the necessary privileges to access a certain category of resources. For example, an agent requires authorization to access and conduct manual configuration on a smart meter.

(3) Availability: Ensures that when a user needs some resources and/or data, they are always available for usage.

(4) Confidentiality: Guarantees that only the intended recipients have access to data that has been stored or transmitted. For example, only smart grid operators and energy providers should be aware of the end users' consumption patterns and data.

(5) Integrity: Certifies that received data have not been tampered with in any manner. For example, smart meters must ensure the integrity of software updates as well as the source origin.

2.2. Main Cyberattack Strategies in IoT-Enabled Smart Grids

Cyber adversaries utilize four key access and control methods to target devices: scanning, surveillance, maintenance, and manipulation. During the first step, reconnaissance, the attacker collects and acquires information about their target. They seek to discover the system's weaknesses in the second step. These moves are intended to help understand and recognize the services available and running on the open ports and the hosting device characteristics (e.g., operating system, manufacturer). During the target exploitation time, they aim to gain concession control over the entire system. After gaining target administrator access, the final step must be completed so that access may be maintained indefinitely. This is accomplished by installing a covert and undetectable application that allows them to quickly return to the target system. Security requirements are a concession in the smart grid, as attackers take the same procedures. At each stage, they use a variety of tactics to breach a specific system [23]. **Figure 3** demonstrates a stepwise procedure of cyberattacks during the exploitation of cyber adversaries [24], where **Table 2** presents how each type of attack can compromise system security [25]. **Figure 4** vividly shows how cyber attackers can breach systems' security.

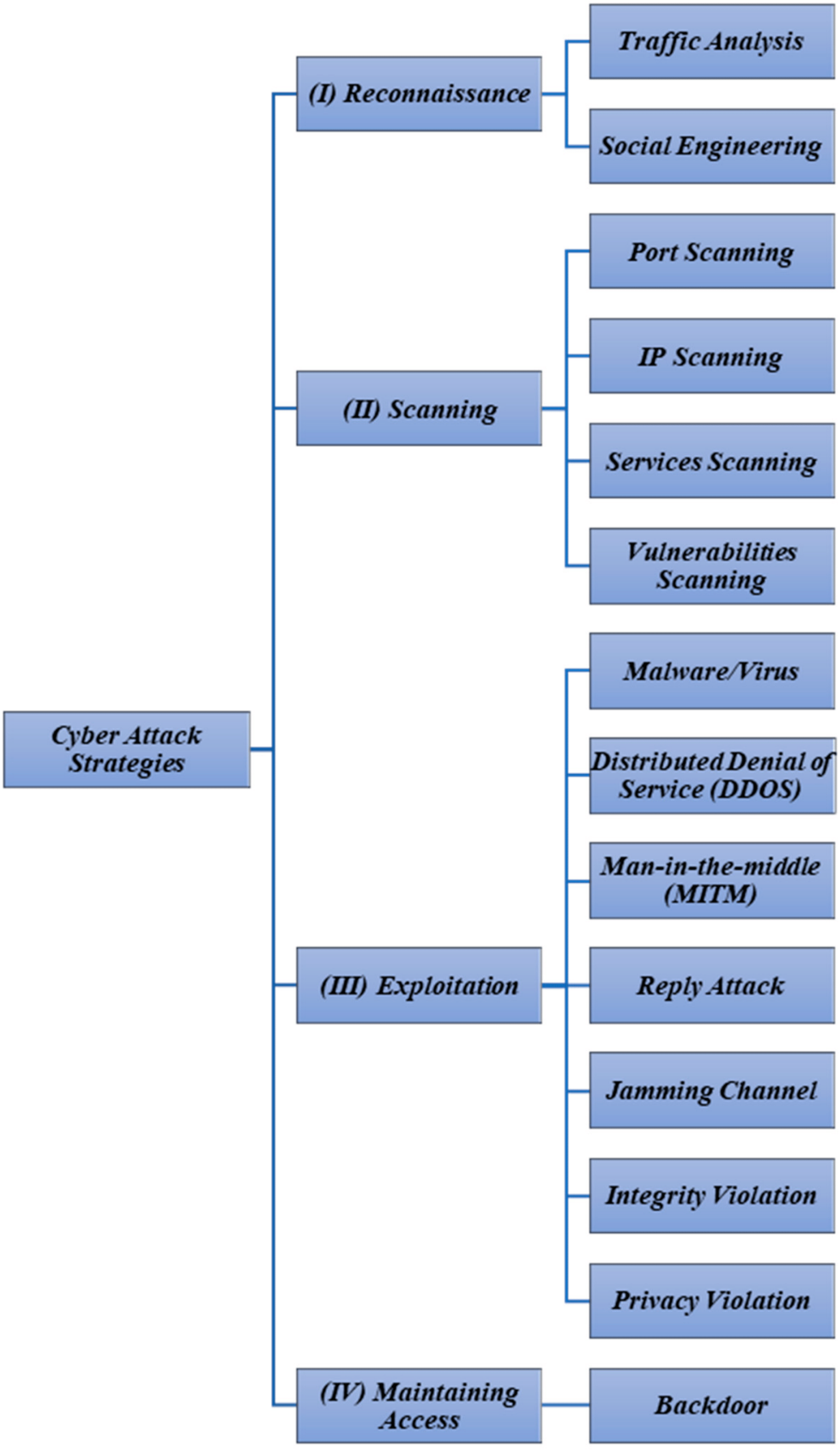

Figure 3. Stepwise cyberattack strategies in IoT-enabled smart grids.

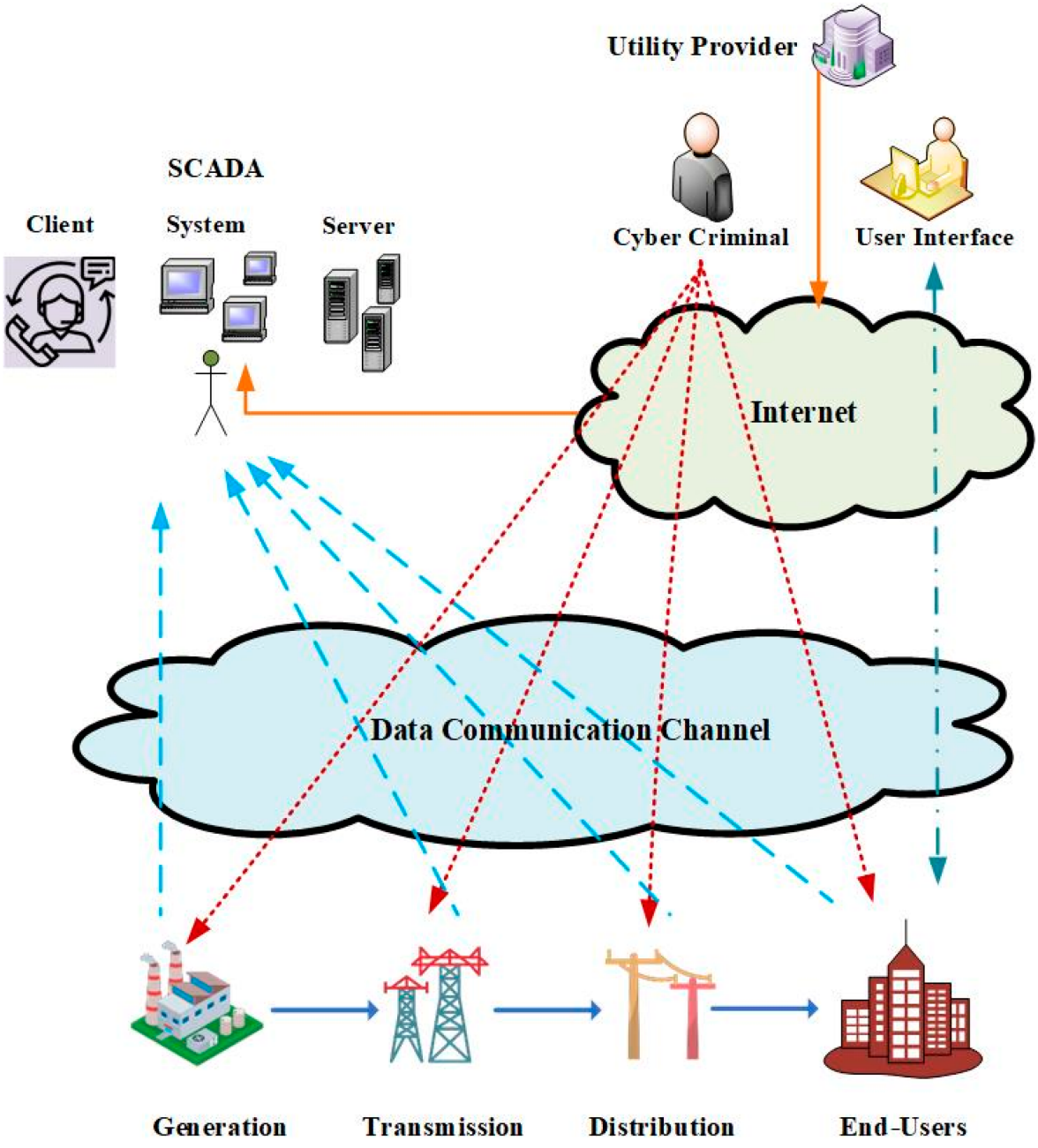

Figure 4. Different cyberattack approaches in IoT-enabled smart grids.

Table 2. Goals of security that have been jeopardized because of an attack.

Attack Category	Security Goals	Description	References
Flooding attack	Availability	Deterring users from utilizing resources	[26]
Denial of service	Availability	Stop serving of user's request	[27]
Jamming channel	Availability	Jamming the network	[28]
Buffer overflow	Availability and confidentiality	Overwriting the memory of the buffer	[29]

Attack Category	Security Goals	Description	References
False data injection (FDI)	Integrity	Tampering the real data	[30]
Social engineering	Integrity and confidentiality	Attacking humans instead of machines or networks	[31]
MITM	Confidentiality	Extracting packet information between sender and receiver	[19]
Packet sniffing	Confidentiality	Analyzing the packet	[32]
Session hijacking	Integrity and confidentiality	Obstructing the user from resources for a particular amount of time	[33]
Data manipulation	Integrity	Data tampering	[34]
Replay attack	Integrity	Send data continuously	[35]

2.2.1. Reconnaissance Definition and Strategies

The reconnaissance procedure includes attacks such as traffic analysis and social engineering. In social engineering, instead of focusing on technology abilities, the focus is on the human connection and social engineering that revolves around it. Persuasion and communication gain are used by an attacker to earn the user's trust in order to access private and credential information, such as PINs or passwords, to log in to the server. Password and phishing attempts, for example, have become commonplace in social engineering. The traffic analysis monitors and analyzes network traffic to determine which machines and hosts connect to the network, obtaining their IP addresses. Social engineering and traffic analysis are the main threats to information security [36].

2.2.2. Scanning Strategies

Scanning is the next step in detecting all the available network machines and hosts. IP addresses, ports, utilities, and security issues are all factors to consider while scanning. An intruder would normally start identifying the network by scanning the hosts connected to their newly acquired IP addresses. Then, they examine each port to establish which ones are available. This scan is performed on any found host network. The attacker then runs a service scan to see what service or device is running behind each open port. Vulnerability scanning is the final stage, which identifies defects, goals, and vulnerabilities associated with each service system on the target devices to be attacked at a later stage. Modbus and DNP3 are two industrial protocols that are vulnerable to scan attacks. Instead of utilizing the scanning Modbus network approach, TCP/Modbus was created to safeguard it. The attack involves delivering an innocuous message to all networked computers to capture their data. On the SCADA Modbus network, Mods scan is a well-known scanner that can discover and open TCP/Modbus connections, and identify system IP addresses and slave IDs [37].

2.2.3. Exploitation Strategies

The third step, exploitation, involves hostile operations attempting to acquire control of the IoT-enabled smart energy system components and exploiting vulnerabilities. Viruses, worms, and Trojan horses infect the human–machine interface (HMI). Privacy violations, channel jamming, integrity breaches, and other assaults, such as denial of service (DOS), man-in-the-middle (MITM), and replay attacks, are all instances of these activities. Viruses are programs that infect computers, devices, and/or machines in smart energy systems. A worm is a self-replicating program. It infects the system and other devices by spreading across the network, copying itself, and infecting them. A Trojan horse is computer software that impersonates a beneficial function on the target computer [38].

2.2.4. Maintaining Access

In the final step, the attacker utilizes a specific attack to gain permanent access to the target, such as backdoors, infections, and Trojan horses. Undetectable software, such as a backdoor, is installed on the target surreptitiously so that it may be accessed fast and simply. Assume that the attacker has successfully created a backdoor into the SCADA server control: in such a situation, they will be able to launch a series of attacks against the system, having a severe impact on the entire power system. On the IT network, the security requirements are established in order of importance: (1) confidentiality, (2) integrity, and (3) availability [39].

2.3. Adverse Impacts of Cyberattacks on Smart Grids

In the following, several examples related to the negative impacts of cyberattacks on the safe operation (from economic and stability points of view) of IoT-enabled smart grids will be discussed.

2.3.1. Electricity Market Losses

Cyberattacks on smart energy systems have significant potential economic and physical consequences. Even though the current study has focused on cyber technical/physical attacks on smart grids, it is also critical to pay greater attention to cyberattacks in terms of associated economic risks. Smart grids have had severe economic difficulty with cyberattacks, particularly renewable energy resources with a high penetration level. Electricity markets are a mix of real-time and day-ahead trading [40]. The day-ahead market is primarily concerned with finding the most cost-effective solution to optimization and load forecasting problems. Since load forecasting is impacted by fake data injection (FDI) cyberattacks in the day-ahead market, the optimization algorithms would be unable to accurately determine the location marginal prices (LMPs) of the grid [41]. On the other hand, the real-time market assesses the dispatched power from each generating unit to meet the required load demand of each bus [42]. It is also necessary to calculate the power that flows through transmission lines to achieve the congestion pattern and consequently evaluate real-time LMPs. Thus, FDI attacks can impact precise state estimation of the power grids in the real-time electricity markets [43][44].

2.3.2. Power System Stability

The FDI attacks have had major technological and physical consequences for IoT-enabled smart grids. In the case of FDI attacks, smart grids must usually deal with steady-state stability and transient effects. The impact of FDI

attacks on steady-state stability on voltage control demands current/voltage/power management and energy management of smart grids is very significant. Furthermore, cyberattacks have a negative influence on electrical grid steady-state functioning, whereas the FDI attacks have harmed the dynamic and transient stability of smart grids. FDI can also impact the smart grid frequency control system. However, the goal will be to maintain rotor angle stability [45].

2.3.3. Energy Theft

The widespread use of IoT-aided AMI in the smart energy grid allows for the transmission of massive energy data and information in a more reliable, efficient, and effective manner for smart grid system management. It replaced the existing analog meter reading and data gathering system with a digital system. Those massive volumes of acquired data and information are wirelessly transferred for further processing with the help of IoT technology, which significantly reduces labor-intensive operations. In the energy sector, energy theft has become a major cause of concern. Both energy service providers and consumers have suffered significant financial losses because of energy theft. The most basic kind of energy theft is tampering with an energy meter so that it can no longer record real energy use and thereby alter the energy bill. Energy theft usually entails circumventing the energy meter so that energy may be consumed without being recorded for billing purposes [46][47][48].

2.3.4. Disruption of Service in Critical and Non-Critical Facilities

Cyberattacks against automation equipment in critical and non-critical facilities can be conducted to achieve the goals listed below [49]:

(1) To gain initial access, for example, via hacking smart lights, to gain Wi-Fi authentication and eventually control of Wi-Fi network devices.

(2) To cause an indirect service disruption, for example, by using a thermostat to manage the building's air conditioning system from afar.

(3) To obtain and disseminate information. Use an application that hacks smart gadgets, such as smart televisions, to make them act as though they are turned off and then use the microphone to record and leak conversations surrounding them.

(4) System abuse, such as producing light flashing at a certain frequency, might trigger epileptic seizures in individuals.

(5) To initiate an intensified attack against critical facilities such as hospitals through a number of targeted smart devices. To deactivate smart home automation systems by targeting a large number of IoT-enabled smart home automation devices in a short amount of time.

2.3.5. Disruption of Transactive Energy Systems

The transactive energy system employs this integrated notion of economic and operational mechanisms to dynamically maintain demand and supply balance across the grid system, hence improving the energy grid's efficiency and reliability. For decision-making and demand response programs, the transactive energy control mechanism is heavily reliant on the cyber system of distributed edge computing and IoT-enabled technologies. This system necessitates a large amount of data to be transmitted across various market processes. Cyberattacks can be performed through the following procedure in order to disrupt the safe operation of transactive energy systems [50]:

(1) Malware injection in the system can result in a large-scale power outage or data theft.

(2) Cybercriminals can tamper with or damage smart meters for several purposes.

(3) To interrupt the transactive system by manipulating the control signals of the relay and circuit breaker.

2.3.6. Environmental Security

Environmental security is critical in the implementation of smart energy grids because it aids in the control and avoidance of potentially catastrophic effects on infrastructures caused by natural or artificially induced environmental hazards such as floods, tremors, earthquakes, landslides, falling trees, and bushfires. In such circumstances, smart action based on environmental concerns is performed primarily by delivering appropriate threat alerts based on collected data and providing alternate feeders for vital infrastructure. Although this feature of smart grids' security is classified as non-technical in this study, it has both technical and non-technical ramifications in some areas.

The capacity of a system's response to failure, in terms of its ability to restore service (by utilizing an improvised alternate feeder if appropriate) or provide adequate data to enable system operators to restore service, is of the highest importance in smart grids. This is accomplished mostly by automatic switching in the event of outages or failures. Natural catastrophes, harsh temperatures, peak, and fossil oil depletion, global energy market instability, terrorism, sabotage, vandalism, and other similar variables all have adverse impacts on the system's resiliency [51]. A geographic information system (GIS) is based on the real-time data that are captured by deployed IoT devices such as smart meters to aid data analytics methods that predict natural disasters and thus have a crucial role in providing timely and accurate environmental threat alerts.

2.4. Detection and Mitigation of IoT-Enabled Cyberattacks

Customers (consumers and prosumers), electric utilities, power system operators, and third-party service providers can be assumed to be stakeholders of smart grids. The data administration of smart grids, particularly in terms of smart meters, becomes a demanding task due to the participation of various stakeholders. There are several frameworks that provide guidelines for integrating security and privacy across several domains to enhance the security and privacy protection of all involved entities. Security is divided into three categories by the framework:

communication security, secure computing, and system control security. Cryptography, route security, and network privacy are all aspects of communication security.

A key goal in the management of communication security is to successfully achieve end-to-end encryption and multiple hop routing that can assure the security of transferred data. In [52], the authors described the major functionalities of smart meters, which includes tracking the quantity of utilized energy as well as voltage and frequency. The implemented smart meters are also in charge of providing data to the grid via a secure communication channel, as well as managing load switches by operators to prevent blackouts in emergency situations. Additionally, this research showed that high-assurance smart meters could be implemented (HASM).

Various techniques have been proposed in the literature to address cybersecurity backgrounds, elements, challenges, and potential solutions for smart energy grids. However, as the complexity of the grid increases with the significant deployment of smart IoT devices, most recent studies have found that the integration of AI techniques is one of the most effective solutions. According to several research findings, the smart grid is similarly vulnerable to human errors, which can be caused by social engineering attacks. Therefore, to investigate the most promising recent methods for safeguarding IoT-enabled smart grids, these methods are divided into two main categories: non-human-centric and human-centric methods.

2.4.1. Non-Human-Centric Methods

The non-human-centric methods can be categorized into three classes: (1) machine-learning-based methods, (2) cloud-computing-based methods, and (3) blockchain-based methods.

Machine-Learning-Based Methods

In the smart grid infrastructure, thousands of sensors are deployed. These sensors continually monitor the states of the devices to which they are connected, generating a massive quantity of data in the form of log files or time-series data. The data that are produced by sensors are saved on a cloud server, which must be preprocessed before being sent. Local servers are another option for servers. However, the maximum level of data security is achieved by storing data on a local server. Nevertheless, they constrain the ability of pattern recognition features or forecasts by advanced optimization algorithms.

In the past few years, machine-learning methods have proved to be effective in detecting cyberattacks. Machine learning identifies intrusions based on past data, as opposed to rule-based techniques. To anticipate power system disruptions, a combination of JRipper and Adaboost was formulated in [53]. The model generated three groups based on the attack data, natural disturbances, and the state of no event. False data injection attack (FDIA) is another popular type of attack that can seriously damage smart energy systems. By tampering with data that are collected from smart meters, FDIA can financially impact utilities and consumers. In [54], a model was analyzed on an IEEE 14-bus test system. The efficiency and performance of the ensemble-based learning (EBL) model were compared with several algorithms such as linear regression (LR), naïve-Bayes (NB), decision tree (DT), and support vector machine (SVM), where the obtained results demonstrated that the unsupervised EBL model

outperformed all the other algorithms with an accuracy of 73%. In [55], the authors proposed a robust deviation-based detection method to efficiently defend the system against an FDIA. Additionally, an exponential weighting function in combination with a Kalman filter was implemented to retain the original weighted least squares estimator. The experimental results confirmed the efficacy of the proposed detection method against FDIA attacks. In this study, the influence of various attack strengths and noise on detection performance was also investigated. In [56], a deep learning technique based on a conditional deep belief network model was proposed to identify the behavioral characteristics of FDI attacks on a real-time basis. In the presented method, the detection mechanism relaxes the beliefs for the potential attack scenarios and attains high accuracy. Moreover, the formulated optimization model was able to distinguish similar behavior that takes place in the process of energy theft. The performance of the presented method was illustrated through two simulation cases on IEEE 118-bus and IEEE 300-bus test systems, where the scalability of the proposed model was also examined.

Occasionally, a smart grid may be subjected to distributed denial-of-service (DDoS) attacks. DDoS attacks jeopardize the availability of communication servers. The fundamental goal of a DDoS attack is to flood the communication server with false requests, causing it to become unusable for communication. In [57], the authors proposed a DDoS attack detection method based on a multilevel auto-encoder formulation. Multiple levels of shallow and deep auto-encoders were trained in an unsupervised approach which was employed to encode training and test data for feature extraction and generation purposes. In the final stage of the algorithm, a unified detection model was constructed by combining the multilevel features using a kernel learning algorithm. The obtained results of their algorithm showed its functionality by achieving high prediction accuracy where it outperforms all the other compared methods.

Cloud-Computing-Based Methods

In [58], to ease the inconvenience of working on encrypted data, an attribute-based online/offline searchable encryption scheme was proposed. In the first step, encryption and trapdoor algorithms were divided into two phases. In the second step, both the encryption and attribute control policy were performed in the offline mode. In the next step, the proposed scheme was secured against two attacks: (1) chosen plaintext and (2) chosen keyword attacks. Ultimately, the applicability of the presented method in a cloud-based smart grid was tested. In [59], the authors analyzed a fundamental security problem in the scalable architecture of smart grid cloud services. They evaluated risks involved in IoT-enabled smart grid security in terms of five distinctive features: (1) policy and organizational risks, (2) general technical risks, (3) SaaS risks, (4) PaaS risks, and (5) IaaS risks. The presented evaluation model was based on deep belief networks, which comprised multiple RBMs and a BP neural network (BPNN). The RBMs were trained by means of a greedy training algorithm, and then BPNN was employed for fine-tuning purposes. Their obtained results found that the mean absolute error (MAE), mean relative error (MRE), and mean square error (MSE) of the proposed model are the lowest in comparison to all the other methods [60].

Blockchain-Based Methods

The integration of blockchain with IoT-enabled smart grids is becoming a complicated key solution for accelerating a broad range of security functionalities in smart energy systems [61]. The current centralized ledger system can be

transferred by blockchain-based techniques into a distributed ledger thanks to the existence of public key algorithms. Blockchain methods offer end-to-end encryption technology based on their distributed processing structure that guarantees the safety and reliability of communication [62]. In [63], a blockchain-based security method that facilitates secure and authorized access to smart city resources was presented. The proposed method comprised an authentication and authorization process for constrained environments based on two models: (1) a blockchain model and (2) object security architecture (OSCAR) for the IoT. The blockchain-based method laid out an adaptable and untrustworthy authorization system, while OSCAR used a public ledger to construct multicast classes for authorized customers. Furthermore, a meteor-based application was created to provide a user-friendly interface for heterogeneous smart city technology. Through this application, users were able to interact and operate with smart city resources such as traffic lights, smart energy meters, and security cameras. In [64], a new distributed authentication and authorization protocol for IoT-enabled smart grids based on blockchain-based methods was proposed to address information leaks, illegal access, and identity theft issues. The protocol introduced combined the decentralized authentication and immutable ledger properties of blockchain architectures that are applicable for power systems to achieve both identity authentication and resource authorization for smart energy systems. In [65], a model-based architecture was proposed that considered an interoperable blockchain-based local energy market for consumers and prosumers in a residential microgrid (MG) framework. The research identified 21 organizational, informational, technological, and blockchain needs for a local energy market and its underlying information system using the IoT-enabled smart grid architecture. According to the Landau Microgrid case study, the biggest hurdle was a clear value proposition for key stakeholders, standardization of data exchange, and appropriate physical implementation [66].

2.4.2. Human-Centric Methods

- *Multifactor Authentication*

When two successive authentication procedures are combined, the password-breaking algorithm becomes exponentially more complicated. Unauthorized users will have less access to the data because of the multifactor authentication process. Multifactor authentication approaches include SMS token authentication, email token authentication, hardware token authentication, software token authentication, and phone authentication.

- *Employee Training*

Hackers are increasingly targeting humans because of technological advancements that have made attacks on smart equipment more complicated. Attackers are using machine-learning technologies to recognize human behaviors and create a variety of scenarios. Thus, employee training plays a critical role in limiting the hackers' success in their malicious intent.

- *Password Strength*

The use of strong passwords minimizes the likelihood of an attack on the integrity or confidentiality of data. Password-guessing attacks are more likely with weak passwords. Password guessing is a method of gaining

access to a system by guessing passwords and gaining access to a targeted device. In addition, the attacker consumes network resources and bandwidth to carry out several attacks that consequently limit the access of legitimate users to the resources.

- *Operating System (OS) Protection*

Users are one of the weakest links in the context of cybersecurity, and one of the biggest challenges with users is that they cannot be taught in the same way as staff. Thus, smart devices such as smart meters and smart inverters must be protected against cyberattacks. Tamper-proofing the devices' internal operating systems is one of the most effective approaches for protecting devices against cybercriminals.

- *Customers' Protection against Third-Party Applications*

Customers should always be wary of applications that request authorization. Customers keep sensitive data on their devices, and some third-party apps request more information than they require. Around 98.5 percent of consumers ignore or just sometimes accept the permissions requested by applications without thinking twice. It has been reported that 93.6 percent of users accept the applications' terms and conditions instantaneously or within one minute.

- *Reporting of Malicious Behavior*

Customers should be able to readily report any suspected attack on a platform created by utilities. The destruction would grow exponentially as the time gap between the attack and the time of the report increases. A delay in reporting an attack jeopardizes not only the privacy of one client but also the privacy of other connected customers in the grid.

References

1. Massoud Amin; A Smart Self-Healing Grid: In Pursuit of a More Reliable and Resilient System [In My View]. *IEEE Power and Energy Magazine* **2013**, *12*, 112-110, 10.1109/mpe.2013.2284646.
2. Dongming Fan; Yi Ren; Qiang Feng; Yiliu Liu; Zili Wang; Jing Lin; Restoration of smart grids: Current status, challenges, and opportunities. *Renewable and Sustainable Energy Reviews* **2021**, *143*, 110909, 10.1016/j.rser.2021.110909.
3. Arman Goudarzi; Yanjun Li; Ji Xiang; Efficient energy management of renewable resources in microgrids. *null* **2020**, *1*, 285-321, 10.1016/b978-0-12-821726-9.00013-8.
4. S. M. Abu Adnan Abir; Adnan Anwar; Jinho Choi; A. S. M. Kayes; IoT-Enabled Smart Energy Grid: Applications and Challenges. *IEEE Access* **2021**, *9*, 50961-50981, 10.1109/access.2021.3067331.

5. Eunice Espe; Vidyasagar Potdar; Elizabeth Chang; Prosumer Communities and Relationships in Smart Grids: A Literature Review, Evolution and Future Directions. *Energies* **2018**, *11*, 2528, 10.3390/en11102528.
6. Maria Lorena Tuballa; Michael Lochinvar Abundo; A review of the development of Smart Grid technologies. *Renewable and Sustainable Energy Reviews* **2016**, *59*, 710-725, 10.1016/j.rser.2016.01.011.
7. Ata Ullah; Muhammad Azeem; Humaira Ashraf; Abdulellah A. Alaboudi; Mamoona Humayun; Nz Jhanjhi; Secure Healthcare Data Aggregation and Transmission in IoT—A Survey. *IEEE Access* **2021**, *9*, 16849-16865, 10.1109/access.2021.3052850.
8. Marco Pau; Edoardo Patti; Luca Barbierato; Abouzar Estebsari; Enrico Pons; Ferdinanda Ponci; Antonello Monti; A cloud-based smart metering infrastructure for distribution grid services and automation. *Sustainable Energy, Grids and Networks* **2018**, *15*, 14-25, 10.1016/j.segan.2017.08.001.
9. G. Sekhar Reddy; N. Rakesh Naik; A. Prashanth; B. Pranay Kumar; An Efficient Spam Detection Technique for IoT Devices Using Machine Learning. *International Journal for Research in Applied Science and Engineering Technology* **2022**, *10*, 1001-1005, 10.22214/ijraset.2022.42311.
10. Quang-Tu Doan; A. S. M. Kayes; Wenny Rahayu; Kinh Nguyen; Integration of IoT Streaming Data With Efficient Indexing and Storage Optimization. *IEEE Access* **2020**, *8*, 47456-47467, 10.1109/access.2020.2980006.
11. Liang Xiao; Xiaoyue Wan; Xiaozhen Lu; Yanyong Zhang; Di Wu; IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security?. *IEEE Signal Processing Magazine* **2018**, *35*, 41-49, 10.1109/msp.2018.2825478.
12. Dimitris Geneiatakis; Ioannis Kounelis; Ricardo Neisse; Igor Nai-Fovino; Gary Steri; Gianmarco Baldini; Security and privacy issues for an IoT based smart home. *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* **2017**, *1*, 1, 10.23919/mipro.2017.7973622.
13. Jinping Chang; Seifedine Nimer Kadry; Sujatha Krishnamoorthy; Review and synthesis of Big Data analytics and computing for smart sustainable cities. *IET Intelligent Transport Systems* **2020**, *14*, 1363-1370, 10.1049/iet-its.2020.0006.
14. Wenjuan Li; Man Ho Au; Yu Wang; A fog-based collaborative intrusion detection framework for smart grid. *International Journal of Network Management* **2020**, *31*, 1, 10.1002/nem.2107.
15. Eman Hammad; Abhijit Kumar Nag; Anitha Chennamaneni; Mohsen Aghashahi; Erdogan Dogdu; A Deep-Defense Approach for Next -Gen Cyber - Resilient Inter-Dependent Critical Infrastructure Systems. *2021 Resilience Week (RWS)* **2021**, *1*, 1-7, 10.1109/rws52686.2021.9611790.

16. Jesús Lázaro; Armando Astarloa; Mikel Rodríguez; Unai Bidarte; Jaime Jiménez; A Survey on Vulnerabilities and Countermeasures in the Communications of the Smart Grid. *Electronics* **2021**, *10*, 1881, 10.3390/electronics10161881.
17. Mohammad Kamrul Hasan; Ali Alkhalifah; Shayla Islam; Nissrein B. M. Babiker; A. K. M. Ahasan Habib; Azana Hafizah Mohd Aman; Arif Hossain; Blockchain Technology on Smart Grid, Energy Trading, and Big Data: Security Issues, Challenges, and Recommendations. *Wireless Communications and Mobile Computing* **2022**, *2022*, 1-26, 10.1155/2022/9065768.
18. Dennis Agnew; Nader Aljohani; Reynold Mathieu; Sharon Boamah; Keerthiraj Nagaraj; Janise McNair; Arturo Bretas; Implementation Aspects of Smart Grids Cyber-Security Cross-Layered Framework for Critical Infrastructure Operation. *Applied Sciences* **2022**, *12*, 6868, 10.3390/app12146868.
19. Shahid Tufail; Imtiaz Parvez; Shanzeh Batool; Arif Sarwat; A Survey on Cybersecurity Challenges, Detection, and Mitigation Techniques for the Smart Grid. *Energies* **2021**, *14*, 5894, 10.3390/en14185894.
20. The Smart Grid Interoperability Panel–Smart Grid Cybersecurity Committee; Guidelines for smart grid cybersecurity. *Guidelines for smart grid cybersecurity* **2014**, *1*, 1, 10.6028/nist.ir.7628r1.
21. Aarti Agarkar; Himanshu Agrawal; A review and vision on authentication and privacy preservation schemes in smart grid network. *Security and Privacy* **2019**, *2*, e62, 10.1002/spy2.62.
22. Khaled Shuaib; Zouheir Trabelsi; Mohammad Abed-Hafez; Ahmed Gaouda; Mahmoud Alahmad; Resiliency of Smart Power Meters to Common Security Attacks. *Procedia Computer Science* **2014**, *52*, 145-152, 10.1016/j.procs.2015.05.049.
23. Juhar Ahmed Abdella; Khaled Shuaib; An Architecture for Blockchain based Peer to Peer Energy Trading. *2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)* **2019**, *1*, 412-419, 10.1109/iotsms48152.2019.8939195.
24. G. Dileep; A survey on smart grid technologies and applications. *Renewable Energy* **2019**, *146*, 2589-2625, 10.1016/j.renene.2019.08.092.
25. Arman Goudarzi; Farzad Ghayoor; Muhammad Waseem; Shah Fahad; Issa Traore; A Survey on IoT-Enabled Smart Grids: Emerging, Applications, Challenges, and Outlook. *Energies* **2022**, *15*, 6984, 10.3390/en15196984.
26. Fengli Zhang; Michael Mahler; Qinghua Li; Flooding attacks against secure time-critical communications in the power grid. *2017 IEEE International Conference on Smart Grid Communications (SmartGridComm)* **2017**, *1*, 449-454, 10.1109/smartgridcomm.2017.8340726.
27. Alvin Huseinovic; Sasa Mrdovic; Kemal Bicakci; Suleyman Uludag; A Taxonomy of the Emerging Denial-of-Service Attacks in the Smart Grid and Countermeasures. *2018 26th Telecommunications Forum (TELFOR)* **2018**, *1*, 1-4, 10.1109/telfor.2018.8611847.

28. Mehmet Necip Kurt; Yasin Yilmaz; Xiaodong Wang; Real-Time Detection of Hybrid and Stealthy Cyber-Attacks in Smart Grid. *null* **2018**, *null*, null.
29. Jacob Sakhnini; Hadis Karimipour; Ali Dehghantanha; Reza M. Parizi; Gautam Srivastava; Security Aspects of Internet of Things aided Smart Grids: a Bibliometric Survey. *null* **2020**, *null*, null.
30. Lei Cui; Youyang Qu; Longxiang Gao; Gang Xie; Shui Yu; Detecting false data attacks using machine learning techniques in smart grid: A survey. *Journal of Network and Computer Applications* **2020**, *170*, 102808, 10.1016/j.jnca.2020.102808.
31. Zakaria El Mrabet; Naima Kaabouch; Hassan El Ghazi; Hamid El Ghazi; Cyber-security in smart grid: Survey and challenges. *Computers & Electrical Engineering* **2018**, *67*, 469-482, 10.1016/j.compeleceng.2018.01.015.
32. Chen Peng; Hongtao Sun; Mingjin Yang; Yu-Long Wang; A Survey on Security Communication and Control for Smart Grids Under Malicious Cyber Attacks. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* **2018**, *49*, 1554-1569, 10.1109/tsmc.2018.2884952.
33. Xiaoge Huang; Zhijun Qin; Hui Liu; A Survey on Power Grid Cyber Security: From Component-Wise Vulnerability Assessment to System-Wide Impact Analysis. *IEEE Access* **2018**, *6*, 69023-69035, 10.1109/access.2018.2879996.
34. Xinan Wang; Di Shi; Jianhui Wang; Zhe Yu; Zhiwei Wang; Online Identification and Data Recovery for PMU Data Manipulation Attack. *IEEE Transactions on Smart Grid* **2019**, *10*, 5889-5898, 10.1109/tsg.2019.2892423.
35. Bashar Alohali; Kashif Kifayat; Qi Shi; William Hurst; Replay Attack Impact on Advanced Metering Infrastructure (AMI). *null* **2016**, *null*, 52-59, 10.1007/978-3-319-47729-9_6.
36. Muhammad Baqer Mollah; Jun Zhao; Dusit Niyato; Kwok-Yan Lam; Xin Zhang; Amer M. Y. M. Ghias; Leong Hai Koh; Lei Yang; Blockchain for Future Smart Grid: A Comprehensive Survey. *IEEE Internet of Things Journal* **2020**, *8*, 18-43, 10.1109/jiot.2020.2993601.
37. Andreas Burg; Anupam Chattopadhyay; Kwok-Yan Lam; Wireless Communication and Security Issues for Cyber–Physical Systems and the Internet-of-Things. *Proceedings of the IEEE* **2017**, *106*, 38-60, 10.1109/jproc.2017.2780172.
38. Tonghe Wang; Haochen Hua; Zhiqian Wei; Junwei Cao; Challenges of blockchain in new generation energy systems and future outlooks. *International Journal of Electrical Power & Energy Systems* **2021**, *135*, 107499, 10.1016/j.ijepes.2021.107499.
39. Zoaya Mohammadi; Smitha Joyce Pinto; Gayadhar Panda; Surmila Thokchom; A Survey of Cyber Security in Smart Microgrid. *null* **2022**, *null*, 687-698, 10.1007/978-981-16-9033-4_51.

40. Arman Goudarzi; Z.N.C. Viray; Pierluigi Siano; Andrew G. Swanson; John V. Coller; Mehdi Kazemi; A probabilistic determination of required reserve levels in an energy and reserve co-optimized electricity market with variable generation. *Energy* **2017**, *130*, 258-275, 10.1016/j.energy.2017.04.145.
41. Marilyn A. Brown; Shan Zhou; Majid Ahmadi; Smart grid governance: An international review of evolving policy issues and innovations. *WIREs Energy and Environment* **2018**, *7*, 1, 10.1002/wene.290.
42. Arman Goudarzi; Shah Fahad; Jiahua Ni; Farzad Ghayoor; Pierluigi Siano; Hassan Haes Alhelou; A sequential hybridization of ETLBO and IPSO for solving reserve-constrained combined heat, power and economic dispatch problem. *IET Generation, Transmission & Distribution* **2022**, *16*, 1930-1949, 10.1049/gtd2.12404.
43. Arman Goudarzi; Chunwei Zhang; Shah Fahad; Ali Jafer Mahdi; A hybrid sequential approach for solving environmentally constrained optimal scheduling in co-generation systems. *Energy Reports* **2021**, *7*, 3460-3479, 10.1016/j.egyr.2021.05.078.
44. Shah Fahad; Arman Goudarzi; Ji Xiang; Demand Management of Active Distribution Network Using Coordination of Virtual Synchronous Generators. *IEEE Transactions on Sustainable Energy* **2020**, *12*, 250-261, 10.1109/tste.2020.2990917.
45. Abdallah Farraj; Eman Hammad; Deepa Kundur; On the Impact of Cyber Attacks on Data Integrity in Storage-Based Transient Stability Control. *IEEE Transactions on Industrial Informatics* **2017**, *13*, 3322-3333, 10.1109/tii.2017.2720679.
46. Muhammad Waseem; Zhenzhi Lin; Shengyuan Liu; Zhang Jinai; Mian Rizwan; Intisar Ali Sajjad; Optimal BRA based electric demand prediction strategy considering instance-based learning of the forecast factors. *International Transactions on Electrical Energy Systems* **2021**, *31*, e12967, 10.1002/2050-7038.12967.
47. Muhammad Waseem; Zhenzhi Lin; Shengyuan Liu; Intisar Ali Sajjad; Tarique Aziz; Optimal GWCSO-based home appliances scheduling for demand response considering end-users comfort. *Electric Power Systems Research* **2020**, *187*, 106477, 10.1016/j.epsr.2020.106477.
48. Muhammad Waseem; Zhenzhi Lin; Shengyuan Liu; Zhi Zhang; Tarique Aziz; Danish Khan; Fuzzy compromised solution-based novel home appliances scheduling and demand response with optimal dispatch of distributed energy resources. *Applied Energy* **2021**, *290*, 116761, 10.1016/j.apenergy.2021.116761.
49. Tahir Khan; Miao Yu; Muhammad Waseem; Review on recent optimization strategies for hybrid renewable energy system with hydrogen technologies: State of the art, trends and future directions. *International Journal of Hydrogen Energy* **2022**, *47*, 25155-25201, 10.1016/j.ijhydene.2022.05.263.

50. Reza Zamani; Mohsen Parsa-Moghaddam; Mahmoud-Reza Haghifam; Dynamic Characteristics Preserving Data Compressing Algorithm for Transactive Energy Management Frameworks. *IEEE Transactions on Industrial Informatics* **2022**, *18*, 7587-7596, 10.1109/tii.2022.3144463.
51. Ayyoob Sharifi; Yoshiki Yamagata; Principles and criteria for assessing urban energy resilience: A literature review. *Renewable and Sustainable Energy Reviews* **2016**, *60*, 1654-1677, 10.1016/j.rser.2016.03.028.
52. Jan Tobias Mühlberg; Sara Cleemput; Mustafa A. Mustafa; Jo Van Bulck; Bart Preneel; Frank Piessens; An Implementation of a High Assurance Smart Meter Using Protected Module Architectures. *null* **2016**, *null*, 53-69, 10.1007/978-3-319-45931-8_4.
53. Raymond C. Borges Hink; Justin M. Beaver; Mark A. Buckner; Tommy Morris; Uttam Adhikari; Shengyi Pan; Machine learning for power system disturbance and cyber-attack discrimination. *2014 7th International Symposium on Resilient Control Systems (ISRCS)* **2014**, *1*, 1-8, 10.1109/isrcs.2014.6900095.
54. Mohammad Ashrafuzzaman; Saikat Das; Yacine Chakhchoukh; Sajjan Shiva; Frederick T. Sheldon; Detecting stealthy false data injection attacks in the smart grid using ensemble-based machine learning. *Computers & Security* **2020**, *97*, 101994, 10.1016/j.cose.2020.101994.
55. Chao Pei; Yang Xiao; Wei Liang; Xiaojia Han; A Deviation-Based Detection Method Against False Data Injection Attacks in Smart Grid. *IEEE Access* **2021**, *9*, 15499-15509, 10.1109/access.2021.3051155.
56. Youbiao He; Gihan J. Mendis; Jin Wei; Real-Time Detection of False Data Injection Attacks in Smart Grid: A Deep Learning-Based Intelligent Mechanism. *IEEE Transactions on Smart Grid* **2017**, *8*, 2505-2516, 10.1109/tsg.2017.2703842.
57. Shan Ali; Yuancheng Li; Learning Multilevel Auto-Encoders for DDoS Attack Detection in Smart Grid Network. *IEEE Access* **2019**, *7*, 108647-108659, 10.1109/access.2019.2933304.
58. Nabeil Eltayieb; Rashad Elhabob; Alzubair Hassan; Fagen Li; An efficient attribute-based online/offline searchable encryption and its application in cloud-based reliable smart grid. *Journal of Systems Architecture* **2019**, *98*, 165-172, 10.1016/j.sysarc.2019.07.005.
59. Weitao Ha; Liping Chen; Jun Liu; Cloud service security evaluation of smart grid using deep belief network. *International Journal of Sensor Networks* **2019**, *33*, 109, 10.1504/ijsnet.2020.10030098.
60. Leila Bagherzadeh; Hossein Shahinzadeh; Hossein Shayeghi; Abdolmajid Dejamkhooy; Ramazan Bayindir; Mohammadreza Iranpour; Integration of Cloud Computing and IoT (CloudIoT) in Smart Grids: Benefits, Challenges, and Solutions. *2020 International Conference on Computational Intelligence for Smart Power System and Sustainable Energy (CISPSSE)* **2020**, *1*, 1-8, 10.1109/cispsse49931.2020.9212195.

61. Vasudev Dehalwar; Mohan Lal Kolhe; Shreya Deoli; Mahendra Kumar Jhariya; Blockchain-based trust management and authentication of devices in smart grid. *Cleaner Engineering and Technology* **2022**, *8*, 1, 10.1016/j.clet.2022.100481.
62. Samreen Mahmood; Mehmood Chadhar; Selena Firmin; Cybersecurity Challenges in Blockchain Technology: A Scoping Review. *Human Behavior and Emerging Technologies* **2022**, *2022*, 1-11, 10.1155/2022/7384000.
63. Muhammad Asif; Zeeshan Aziz; Maaz Bin Ahmad; Adnan Khalid; Hammad Abdul Waris; Asfandyar Gilani; Blockchain-Based Authentication and Trust Management Mechanism for Smart Cities. *Sensors* **2022**, *22*, 2604, 10.3390/s22072604.
64. Yuxin Zhong; Mi Zhou; Jiangnan Li; Jiahui Chen; Yan Liu; Yun Zhao; Muchuang Hu; Distributed Blockchain-Based Authentication and Authorization Protocol for Smart Grid. *Wireless Communications and Mobile Computing* **2021**, *2021*, 1-15, 10.1155/2021/5560621.
65. Benedikt Kirpes; Esther Mengelkamp; Georg Schaal; Christof Weinhardt; Design of a microgrid local energy market on a blockchain-based information system. *it - Information Technology* **2019**, *61*, 87-99, 10.1515/itit-2019-0012.
66. Simone Fischer-Hübner; Cristina Alcaraz; Afonso Ferreira; Carmen Fernandez-Gago; Javier Lopez; Evangelos Markatos; Lejla Islami; Mahdi Akil; Stakeholder perspectives and requirements on cybersecurity in Europe. *Journal of Information Security and Applications* **2021**, *61*, 102916, 10.1016/j.jisa.2021.102916.