sustainability

MDPI

Review

Smart Grid Cyber Security Enhancement: Challenges and Solutions—A Review

Turki Alsuwian [1], Aiman Shahid Butt [2] and Arslan Ahmed Amin [2,*]

[1] Department of Electrical Engineering, College of Engineering, Najran Unversity, Najran 11001, Saudi Arabia
[2] Department of Electrical Engineering, Chiniot Faisalabad Campus, FAST National University of Computer and Emerging Sciences, Chiniot 35400, Pakistan
* Correspondence: arslan.amin@nu.edu.pk

Abstract: The incorporation of communication technology with Smart Grid (SG) is proposed as an optimal solution to fulfill the requirements of the modern power system. A smart grid integrates multiple energy sources or microgrids and is supported by an extensive control and communication network using the Internet of Things (IoT) for a carbon-free, more reliable, and intelligent energy system. Along with many benefits, the system faces novel security challenges, data management, integration, and interoperability challenges. The advanced control and communication network in the smart grid is susceptible to cyber and cyber-physical threats. A lot of research has been done to improve the cyber security of the smart grid. This review aims to provide an overview of the types of cyber security threats present for smart grids with an insight into strategies to overcome the challenges. As the selection of techniques and technologies may vary according to the threats faced, therefore the adoption of researched methods is compared and discussed. As cyber-security is the greatest challenge in smart grid implementation, this review is beneficial during the planning and operation of smart grids for enhanced security.

Keywords: artificial intelligence; blockchain technology; smart grids; internet of things; power system security; machine learning; 5G technology

Citation: Alsuwian, T.; Shahid Butt, A.; Amin, A.A. Smart Grid Cyber Security Enhancement: Challenges and Solutions—A Review. *Sustainability* **2022**, *14*, 14226. https://doi.org/10.3390/su142114226

Academic Editors: Damien Guilbert, Phatiphat Thounthong and Shuhua Fang

Received: 29 August 2022
Accepted: 25 October 2022
Published: 31 October 2022

1. Introduction

The power sector of a country has become the backbone of its economy. The need to replace primitive energy systems came with advances in the field of industrialization, digitization, and electricity demand at the commercial and residential levels. Traditional power distribution systems work on phenomena of remote generation, stepping up and down voltage for transmission, distribution, and consumption based on the average demand of an area, physical protective equipment connected at various nodes, ending with metering consumer's utilization on monthly basis. On the other hand, Smart Grid (SG) is an emerging proposed technology that offers smart monitoring, inters connectivity of multiple modes of generation, two-way communication, and enhanced utilization of resources. With an increasing number of connected devices, it becomes difficult for the smart grid to access the distributed network. Therefore, to support the smart grid, the Energy Internet (EI), also known as the Internet of Things (IoT), is being utilized in the power sector for the bidirectional flow of information. It deploys sensors, actuators, Radio-frequency Identification (RFID), and microcontrollers capable of communication and computation, to achieve a two-way communication process [1]. When IoT is integrated with the SG, it forms an extensive network of a cyber-physical system capable of monitoring and controlling connected devices remotely. Many countries have already adapted to this technology; however, approaches to implementation vary according to the goals and policies of a country [2].

Transformation to the modern power sector requires a thorough analysis and planning at every level. Integration of multiple modes of power generation, securing data transferred to and fro, adopting a reliable communication protocol for big data handling, and providing

uninterrupted power supply are a few prominent factors to study before implementing this technology. Every country needs a thorough study of the process of implementation of the smart grid as it offers a huge contrast to the traditional system. Thus, a careful and in-depth study of all features is required for proper implementation.

The interconnection of numerous devices from the domestic to the commercial level forms a network of communication in SG. We may say that SG is mainly a system of communication networks and physical equipment interconnected and controlled by a central unit. The physical equipment offers more predictable, less technical, and fewer challenges due to difficult human access, and scheduled maintenance overruling the faults caused by material and equipment damage. However, the challenges encountered by the cyber network are more complex, frequent, and less predictable. Thus, cyber-security has been identified as a top power industrial security target. The researchers have been working on defining cybersecurity challenges and proposing various solutions. This paper discusses many proposed and researched strategies, such as encryption, cryptography, and device and network authentication. These strategies provide the solution to certain parts of the problem and cannot counter all the issues. Thus, a broader approach is adopted to successfully deploy the proposed system. In the last sections of the paper, we shall also discuss broader approaches to machine learning, 5G technology, blockchain, and data aggregation methods. A comparative analysis of techniques based on factors of latency, efficiency, cost, and security is also presented in this research. Thus, this paper provides a comprehensive study of various techniques and approaches adapted to over challenges faced by SGs and an analysis of their features.

This paper is organized as: in Section 2, we will have an overview of the security challenges in the IoT-supported SG technology. In Section 3, techniques and approaches are explained to counter the challenges. Section 4 discusses the latest technological developments, with discussion in Section 5. In Section 6, the study is concluded.

2. An Overview of Smart Grid Security Challenges

Although the use of IoT seems very promising, it also can lead to a disaster in the power chain if any fault occurs. Faults and challenges of the traditional network are easier to overcome as most of the faults are in either equipment or parameter variation. However, faults in SG, with IoT specifically, have mostly digital faults, such as cyber-attacks or data transfer faults. Thus, every country analyzes the communication technology and protocol standards according to the country's policies before the implementation of SG (Table 1). Refs. [3,4] explain the features of a general fault-tolerant control system. There are four steps to attack and take control over a system, which are reconnaissance, scanning, exploitation, and maintaining access, as shown in Figures 1 and 2. First, the attacker collects information about the system (reconnaissance), then looks for weak points and loopholes in the system. After scanning the system, he tries to gain full control of the system before exploiting the information by installing a stealthy program [5]. Thus, security and data protection is the biggest concern in SG. As SG utilizes a public network, according to [6,7], there is the possibility of the following:

(1) Impersonation: A hacker can act as a legitimate user in an unauthorized way, spoofing the identity of someone and making him pay for energy consumption.
(2) Data Manipulation: Data transmitted over a public network can be modified by an attacker, such as dynamic prices, and load readings.
(3) Cyber-Physical Attack: IoT-based SG is the largest cyber-physical system, with physical components of Circuit Breakers (CB), transformers, and relays along with ICT components of sensors, and microcontrollers; it is more vulnerable to DoS attacks as compared to a traditional grid system, which is generally only physical and very difficult to reach. Any attack against the availability of service is called DoS [8]. These attacks directly impact the physical layer of the system, jamming the channel and causing immense loss. Opacity is an increasing concern in a cyber-physical system. Most of

the estimation algorithms allow sharing of explicit state information with neighboring nodes, resulting in the disclosure of the state of the cyber-physical system [9,10].

(4) Privacy and Confidentiality: The security of data is an important aspect and challenge for SG. Power system monitoring can cause privacy concerns at the user end by divulging information about their routine, habits, traveling, etc. Thus, the flow of information between customers and various entities must be protected for the user to develop confidence in the power network. Eavesdropping is also an intrusion into the privacy of the network. The attacker may obtain useful information by continuously monitoring the network and eventually entering the system to obtain important information.

(5) Phishing: Phishing can be the first step in putting the customer at risk. If a customer does not discard a receipt or bill and the information is passed on to the hacker, he can manipulate the information easier to create fake messages, and emails, or obtain crucial information about the organization.

Table 1. Comparison of Smart Grid Communication Technology.

Technology	Spectrum	Data Rate	Coverage Range	Applications	Limitations
GSM	900–1800 MHz	Up to 14.4Kbps	1–10 km	AMI, Demand Response, HAN	Data rates are low
GPRS	900–1800 MHz	Up to 17 kbps	1–10 km	AMI, Demand Response, HAN	Data rates are low
3G	1.92–1.8 GHz 2.11–2.17 GHz	384 Kbps–2Mbps	1–10 km	AMI, Demand Response, WAN, NAN	High communication and computational cost
WiMAX	25 GHz, 3.5 GHz, 5.8 GHz	Up to 75 Mbps	10–50 km (LOS) 1–5 km (NLOS)	AMI, Fraud Detection, WAN	Not as widespread as other methodologies, still under research
PLC	1–30 MHz	2–3 Mbps	1–3 km	AMI, Fraud Detection	Prone to noise with power network.
ZigBee	2.4 GHz, 868–915 MHz	250 Kps	30–50 m	AMI, HAN	Very short data range, and low performance inside the building.

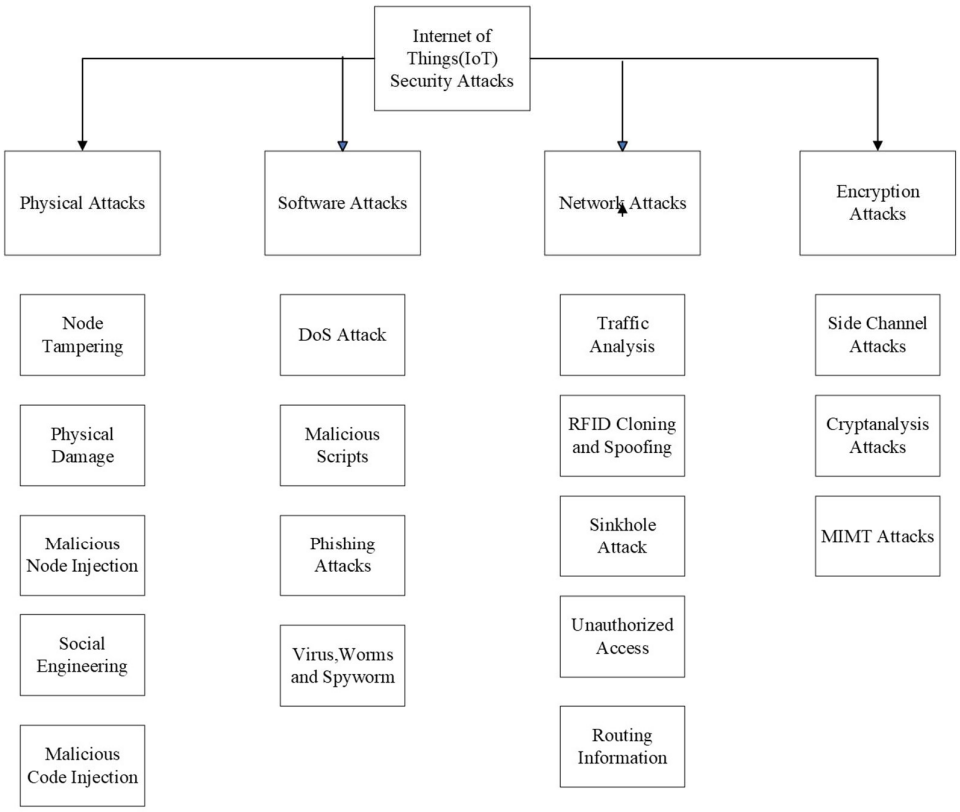

Figure 1. Types of Attacks on IoT Integrated Systems [7].

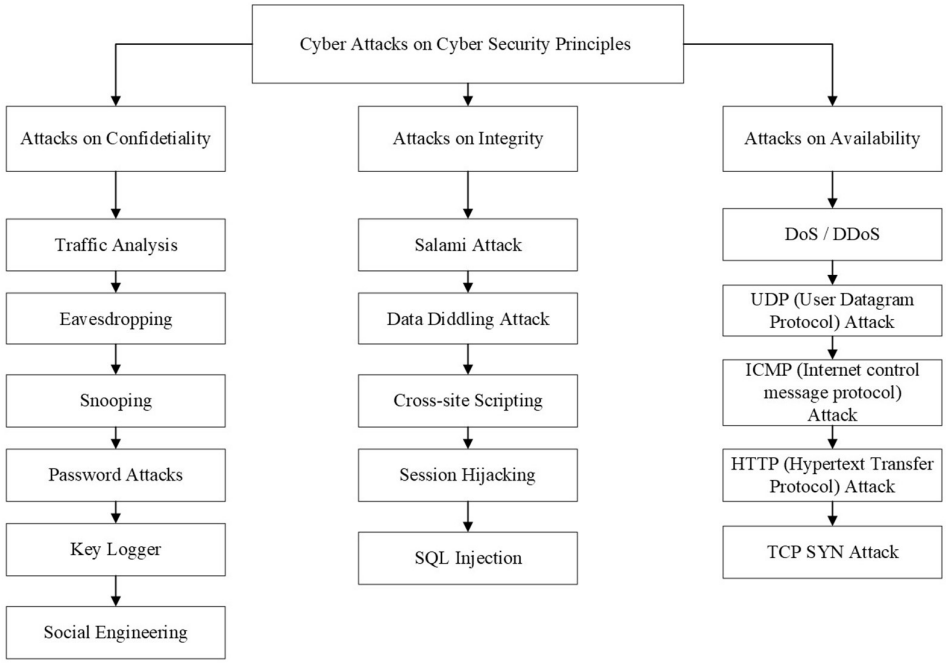

Figure 2. Classification of Cyber-attack [11,12].

3. Techniques to Overcome Security Challenges

Several techniques and countermeasures are used and proposed to provide the smart grid with the required security. Usually, we classify solutions to security and big data problems which are discussed in detail below. However, the solution to the above-mentioned problem cannot be achieved using one specific solution. There should be multiple techniques deployed to form a global, unified strategy. Security of smart grid is a major area

of research usually divided into detection, countering, and securing. The following figure shows three main points of security. The following strategies are proposed to overcome this problem. The first step is to improve protection against any malicious attacks. The system should be prepared for any potential attack. With help of the following, we can achieve the purpose:

3.1. Pre Attack

The first step is to improve protection against any malicious attacks. The system should be prepared for any potential attack. With help of the following, we can achieve the purpose.

Cryptography: Cryptography is an important technique to provide security to the SG End-to-end encryption is a common cryptography technique for secure communication. Encryption can either be symmetric or unsymmetrical. In symmetric cryptography, messages are encrypted and decrypted using the same key [13]. This technique often suffers from exhaustion issues; however, it is faster compared to unsymmetrical cryptography. The other type of encryption asymmetric encryption uses public and private key pairs to encrypt and decrypt data. RSA (Rivest, Shamir, and Adleman) is a commonly used asymmetric algorithm for communication data security. Since the smart grid is an extensive network with many subsystems, it has various components with different working algorithms co-existing. Therefore, a combination of both techniques is also common, however the preference for one key depends on factors of data size, level of security required, and speed of execution [14,15]. For a multi-agent system, there is always the risk of eavesdropping and differentially private distributed convex unconstrained optimization. Here every agent tries to minimize the aggregate sum of their individual objective functions [16]. The objective is to maintain the requirements of smoothness and convexity while keeping the attributes differentially private.

Authentication and Key Management: Authentication means verifying an object before it enters the system. Authentication can be of a network, a device, or a code. For multicasting purposes, secret info asymmetry, time asymmetry, and hybrid asymmetry are used. Key management is an important aspect of authentication. Key management is categorized as Public Key management (PKI) or Shared key management. In public key management, security between two parties is verified by an external third party called a certificate authority. In shared key management, four steps are followed. Key Generation, Key Distribution, Key Storing, and Key Update. Based on the extensive distribution network of SG, there should be consideration of specific key requirements as discussed in [17]. The selection of framework relies on various factors, including scalability, evolution ability, and security; however, after thorough comparison, Advanced Key Management Architecture (ASKMA) and Scalable Method of Cryptographic Key (SMOCK) management showed promising results for smart grid. A certificate-based encryption method is the latest tool presented in [18], which gives certificates of operation and safety to controllers and data users. The computation and communication results show a tremendous reduction in cost at a much higher safety rate. Most authentication methods have high computational and communication costs, a lightweight authentication protocol is recommended in [19]. The author analyzes the security and cost efficiency of the researched method through comparison with other technologies.

Code Attestation: There is recent research on code attestation both through software and hardware. It provides feedback to stakeholders about the quality of the software, product, or service under test. It thus prevents malware to hide. Even in some cases, malware can change signature execution code, and hardware-based code attestation can be utilized. More techniques of attestation are provided in [20].

Device Security: IoT-based smart grid is loaded with communication components. Any weak point offered in any device can lead to the risk of collapse of the whole system, thus a need to regularly configure all devices becomes necessary for the integrity of the

supply chain in SG. Recommended technologies are Host IDS, host data loss prevention (DLP), and automated security compliance checks [21].

3.2. Under Attack

Once the system or a part of the system is under attack, there are two steps to counter it. One is to detect the attack, to know where the attack occurred, the parts of the system affected by the attack, and the type of attack. The other task is to counter the attack. During attack detection techniques, Data Loss Prevention (DLP) & Intrusion Detection Systems (IDS) are recommended.

- Intrusion Detection System (IDS): An intrusion detection technique scans the system continuously for any malicious activity and reports any anomaly detected. This way, once a malicious device or network is detected, it is isolated from the system and reported either to a centralized security system or to an administrator. The intrusion detection techniques are classified into the following five types also described in [22,23].
- Network Intrusion Detection System is employed at certain planned points in the system from where most of the data passes to monitor the flowing traffic in all directions. It hits the alarm to the administrator once an anomaly matches the behavior or certain virus
- Host Intrusion Detection System only monitors incoming and outgoing data packets and checks for any suspicious activity. It takes snapshots of data and keeps on comparing them to previous data packets to check for abnormalities.
- The other techniques include protocol-based, application-based, and hybrid intrusion detection techniques. Authors in [24] proposed cyber security solutions for the fog-based smart grid SCADA system. It proposed a multilayer approach and categorizes the solution into four categories of intrusion detection, authentication, key management, and privacy-preserving approaches. However, IDS has several limitations, such as a high rate of false positives. In [25], IDS based on data mining algorithms is suggested, which can overcome this problem. For the SCADA system, security is enhanced through recent machine learning models based on preprocessing, clustering, feature selection, and classification. A recent study in [26], used by Markov, a Chain Clustering model is used, followed by Rapid Probabilistic Correlated Optimization for feature selection, ending with the Block Correlated Neural Network technique for classification. Similarly, the authors of [27,28], have recommended clustering and fused optimization-based classification methodologies for SCADA security.
- Data Loss Prevention (DLP): DLP techniques are used and designed to prevent the unauthorized use and transmission of confidential information without the loss of important data or obtaining data affected by the virus. This means this technique fights malicious activity to cause any harm to data and any prevention technique to act on data. DLPs generally perform periodic audits to verify the security criterion is being met. Network DLP and Host-based DLP are common strategies used, as discussed in detail in [29]. After the detection of an attack, it is countered with pushback and configuration methods. In this technique, the router is configured to push back all unauthorized IPs. In configuration techniques, the network topology is changed. This results in isolating the attacker from the system and stops the attack at an early stage as discussed in detail in [30,31].

3.3. Post Attack

Post attack techniques are used to identify the entity involved once the attack is detected at a later stage. Forensic is a key strategy used. Forensic studies analyze and intercept digital attacks and investigate hacking protocols, cyber terrorism, and digital espionage.

4. Recent Development in Technology

4.1. Blockchain Technology

Blockchain technology is an underlying technology that works on the principle of Bitcoin where transactions (of data) are performed by encrypting data into packets and transferring them to the desired location without the need for a third party. However, it does involve a computing power provider called miners, which secures transactions [32]. This approach suggests, as explained in [33,34], that following a centralized approach makes the system more vulnerable and requires more cost for communication infrastructure. Thus, decentralization is the requirement of EI. The decentralized units work independently and do not require a central trusted authority. Thus, adopting decentralization solves many problems that a centralized network has, such as total network collapse, modifications or alterations in data packets, privacy leakages, and single point of failure. In light of the proposed idea, blockchain and edge computing provide promising opportunities.

Blockchain technology [35] is a collection of blocks. These blocks record different blocks of data, information, and transaction history. They link together to form a chain to address the cryptographic hash of the data stored in the last block. Hence, new blocks are generated which keep on adding to the chain at regular intervals. The replication of the chain occurs across the network. The data in chains are locked and verified through various techniques against any modification. In SG, blockchain contributes in the following ways.

4.1.1. Advanced Metering Infrastructure:

A lot of information is generated about billing, payment records, and energy consumption by AMI devices (Figure 3). This information is communicated to a central unit, which not only gets exposed to attacks but also becomes difficult to transmit this big data over miles. Thus in [36], a model is proposed with smart contracts that add a block whenever a transaction is made. Contract technology is an automatic execution of certain conditions once predecided requirements are met. In [37], a model for smart energy grids is proposed which is based on the energy generation at the distributed end and remote monitoring to avoid one-point failure [37,38].

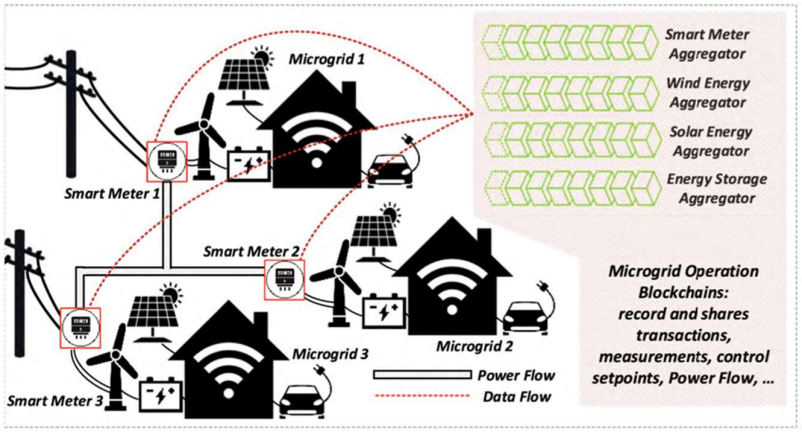

Figure 3. Blockchain for Advanced Metering Infrastructure.

The author in [39] proposes a united blockchain and edge computing technology, emphasizing energy security. As opposed to central data centers, here blockchain mainly ensures the privacy of all participants in a decentralized data storage to protect against malicious activities within the communication channels. The research work in [40] introduces a reliable energy scheduling model through the blockchain and smart contract. This addresses the growing privacy concerns of a centralized system for financial and behavioral information [41].

4.1.2. Monitor, Measure, Control, and Protect

Blockchain technology is used to monitor various parameters of power devices through sensors and the Power Management Units (PMUs) [42] and share this information with MTUs, which are considered control centers (Figure 4). This status information is then shared among grid operators, suppliers, and consumers for intelligent governance to enhance the grid's stability and monitor power theft and loss. A discussion on general blockchain protection mechanisms is discussed in [43]. In [44], the authors present a blockchain and smart contract-based monitoring system. It ensures the security of every transaction occurring between parties after they meet the terms predefined.

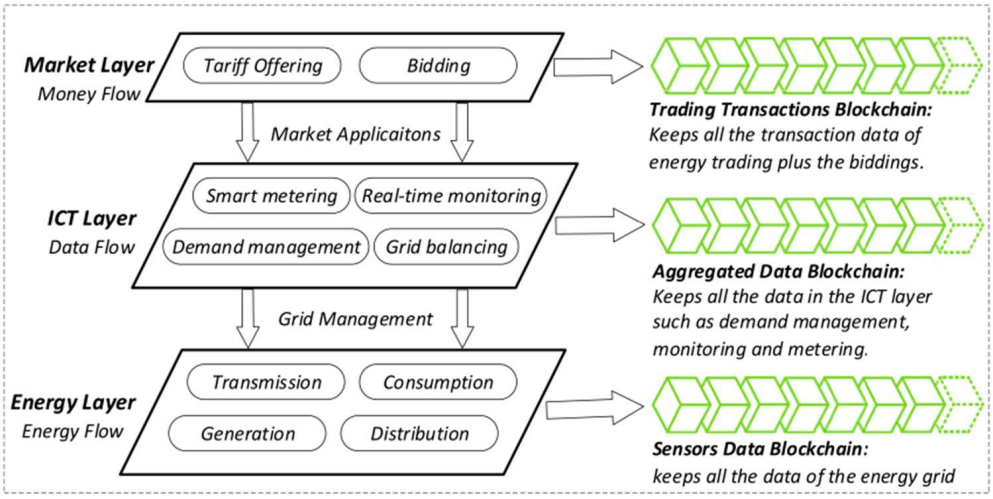

Figure 4. Blockchain to monitor, measure, control, and protect [35].

4.1.3. Use of Blockchain in Microgrid

With the penetration of DERs, MG is becoming an integral part of SG. Microgrids work on geographically available renewable resources to meet the energy demand of a certain area. Surplus energy is then shared with other microgrids through a central unit. However, MG can face the problem of variations in available resources, such as solar or wind. For this purpose, the DERs scheduling technique based on blockchain is used. It helps to provide a trustworthy platform so DERs can be trusted. [45] presents a smart contract-assisted architecture to facilitate decentralized optimization. It distributes the operator's role across various entities of microgrids.

The authors in [46] focus on the problem of voltage regulations in microgrid networks that result from power penetration. The voltage is regulated through active output power using the droop loop control law [47]:

$$v_u = v_{ref} - \gamma(g_u - p_u) \tag{1}$$

v_u and v_{ref} are the output voltage of DER and the reference value for MG.
The output reactive power can be determined by active output power (q_u) as:

$$q_u = \sqrt{s_{max}^2 - p_u^2} \tag{2}$$

s_{max}^2 is the maximum tolerable apparent power, p_u^2 is the maximum tolerable active power. DER should equally participate in voltage control over time:

$$M\,1_k = \frac{k}{U_f} 1\,U_f \tag{3}$$

where $1\,U_f$ is all one vector of length U_f, k is constant.

It is important to consider this parameter, as both under-voltage and overvoltage cause damage to the system. Overheating is caused by overvoltage which can damage power system infrastructure. On the other hand, under-voltage can cause the system to collapse. The authors introduce a proportional-fairness control scheme to control voltage violations. The work in [48] addresses the voltage regulation problem where they introduce a transactive energy system (TES) which also follows principles of blockchain technology.

4.1.4. Blockchain in Decentralized Energy Trading

With a growing number of consumers and producers, energy trading becomes a rising need. A smart grid with help of DERs should be able to reduce peak load, operating on islanded and with grid mode using the bidirectional flow of energy. The Peer-to-peer (P2P) energy trading method seems a promising future technology. In this method, trading is performed between two parties, and data is stored in a chain of blocks. In [49], the authors introduce an energy coin and peer-to-peer (P2P) energy trading system for energy harvesting and a credit-based payment scheme. Authors in [50] introduce a token-based decentralized system named PriWatt which is based on the principles of Bitcoin. This system consists of blockchain-assisted smart contracts, multi-signatures, and anonymous encrypted messaging streams. In [51], the authors present a technique to facilitate P2P energy trading using a blockchain-based crowdsourced energy system (CES) at the distribution level.

A comparison of reviewed publications on blockchain features is given in Table 2.

Table 2. Literature Review on the Use of Blockchain in Smart Grid.

Application of Blockchain	Reference
Power flow	[52,53]
Demand Response	[46,54,55]
Security and Privacy	[56–59]

4.1.5. Challenges of Blockchain Technology

Blockchain technology has recently gained popularity for its applications in smart grid, however, it has many technical limitations [33,60].

1. One of the main challenges faced by smart grid is theoretical throughput, which means the number of transactions per minute. According to [61], the number of transactions performed by blockchain is five per second. The small number will limit blockchain applications in e-commerce as it requires quicker and large transactions every second. This will increase the cost of the communication network.
2. Another important issue of blockchain technology is high latency, which is time to process the transaction and more time to provide security for the double transaction. To overcome the issue, the authors of [62] propose a bitcoin protocol that reduces latency greatly by increasing the number of nodes and decoupling the bitcoin network by two planes.
3. As the application of blockchain continues to grow, the size and bandwidth have been a rising concern. As new data is added, new blocks keep on accumulating, and broadcasting all the dates will keep increasing the cost. A probable solution is to keep on deleting old data blocks as proposed by the authors in [63].
4. Identity threat is a main risk of blockchain. Identity in the blockchain is the combination of public and private keys. The overall security of blockchain lies behind the private keys. In [64], the authors provide a solution for password-protecting the private key. In this way even if the key is stolen, the funds will remain protected

4.2. 5G Technology

The fifth generation of mobile network5Gbenefits the SG through its ultra-reliable and low latency rate in contrast to previous generations. In comparison to previous generations, 5G offers two main features, which are machine-type communication (MTC) and ultra-reliable and low latency communication (uRLLC). The 5G network can support SG with its machine-type communication (MTC) feature in many ways: smart metering, handling a huge volume of data, low latency, fault localization, vehicle-to-grid (V2G), and integration of DERs [65] (Table 3). Another distinguishing feature of 5G technology is the millimeter wave (mmWave). As the relationship between wavelength and frequency is given by [66]:

$$\lambda = \frac{v}{f} = \frac{c}{f} \tag{4}$$

where v is regarded as the same as c, which is the speed of light, f is the frequency, and λ is the wavelength. The speed of light is constant, and 5G has a frequency that may increase up to 100 GHz, therefore 5G can offer a high band spectrum called millimeter wave (mmWave) [67]. In [7,68], the authors explain using 5G cellular technology for distributed monitoring and control. The approach is based on considering two network systems, i.e., centralized network management (CNM) and distributed network management (DNM) [69], as shown in Figure 5. It compares the performance of 5G with 4G-LTE technology and results based on simulations show a significant reduction in latency and system response in case of faults.

Refs. [13,70] compare different communication technologies, such as power line communication (PLC), Fiber Optics, and 5G wireless communication technology on parameters of cost, the distance of coverage, noise effect, and security. Much research has been made to implement this technology for SG, such as in [71], where 5G-based fog and cloud computing is suggested to implement extensive connectivity and faster communication among electrical vehicles. In [72,73], the authors explain extended mobile edge computing based on 5G to increase overall network capacity for the transmission of big data packets. Moreover, in [74] electric vehicles (EVs) are programmed to participate in DR by transferring power consumption data to the DR calculator. To summarize, 5G technology can support the smart grid in the following ways [75].

(1) Massive links of flexible loads: A prominent feature of 5G technology is its ability to simultaneously connect with several communication devices through controllers that can be built-in or present at the terminal end of any device using its massive machine-type communication (mMTC) feature.
(2) Fast transfer speed and low communication latency for remote control: The communication method based on 5G has reliable and low latency communication (uRLLC) features. Faster communication and low latency time are key parameters for communication and in 5G technology, the response time can be as low as 1 ms, which is negligible for frequency regulation services [69]. Therefore, the 5G network helps to reduce instability in the communication network and better performance in frequency regulation parameters for countering oscillations.
(3) Rigorous Security and Improved User Privacy: Network based on 5G architecture can enhance privacy, provide a secure data transfer, and support diversified services via the end-to-end service level agreement (SLA) assurance [76]. Network function virtualization (NFV) and software-defined networking (SDN) methods lay the foundation of physical 5G for customized need-based services of network topologies, referred to as network slices. SDN works on the principle of separating the control plane which decides where data needs to be trafficked from the data plane, which pushes the packets of data toward the destination. NFV works on accelerating service by allowing network operators to route traffic through various functions.
(4) High reliability and low power consumption: Demand response is an important feature to calculate system efficiency and reliability. For SM, a system may have to

face sudden failures, causing delayed smart responses, reducing the effectiveness of the system, and inefficiency of the system to fulfill the requirements [77]. Based on the test of factory automation in [78], the uRLLC feature of 5G networks can guarantee as low as a few sub-milliseconds radio transmissions, which is reliable enough to support DR in power systems. Then, 5G can transfer data at a much higher speed, estimated to be 100 times greater than that of 4G.

Table 3. Characteristics of 5G Technology.

Grid Characteristics	5G Technology							
	Availability	**Coverage**	**Energy Usage Reduction**	**Battery Life Devices**	**Increased Connectivity**	**Bandwidth Per Unit Area**	**Latency**	**Data Rate Improvement**
Accommodation in all generation, storage Options [80]	Yes	No	No	No	Yes	No	Yes	Yes
Enable New Product Service and Market [81]	Yes	No	Yes	Yes	Yes	Yes	Yes	No
Provide the power quality for the range of needs [82]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Optimization of utilization and operating efficiency [83]	Yes	Yes	Yes	No	Yes	No	Yes	Yes
Provides resiliency to disturbances [84]	Yes	Yes	Yes	No	No	Yes	No	Yes
Attacks and Natural Disasters	Yes	Yes	Yes	No	No	No	Yes	Yes
Enable User's Participation [85]	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes

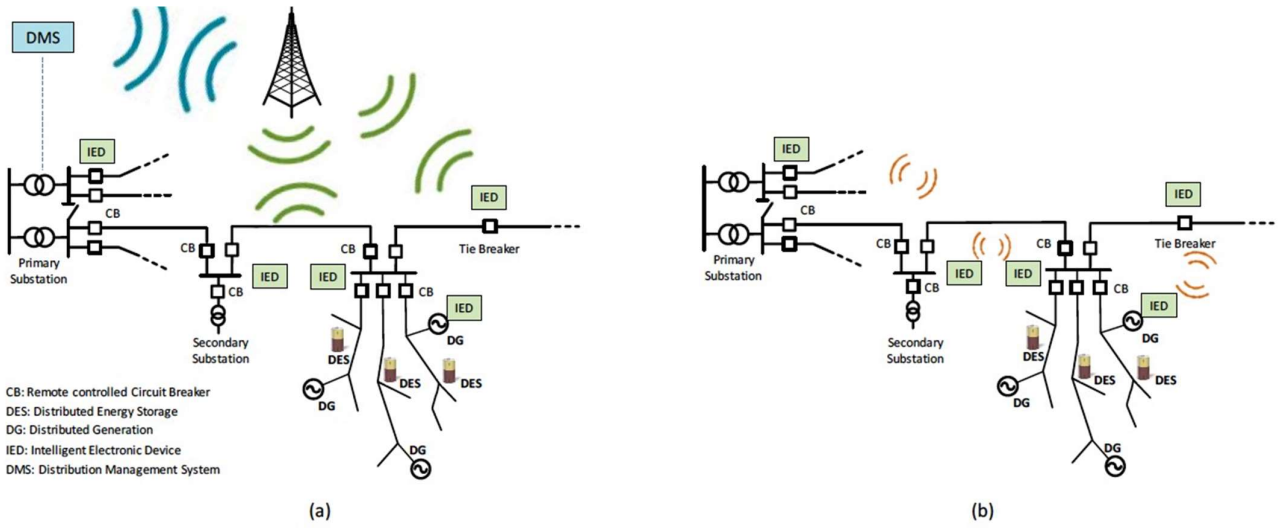

Figure 5. Distributed Monitoring (**a**) 4G LTE, (**b**) 5G Technology [75,79].

4.3. Artificial Intelligence and Machine Learning

4.3.1. Artificial Intelligence

Artificial Intelligence (AI) is rapidly changing our daily life activities. AI is rapidly revolutionizing power systems with its advanced techniques. With new components and features of the smart grid, AI can be the optimal solution to growing and evolving power systems. State-of-the-art artificial intelligence techniques can support various applications in a distributed SG, such as transmission line security, fastest communication between stakeholders, large data management, priority setting, and detection of malicious attacks, along with many others. In particular, artificial techniques are applied in various applications for smart grids. These techniques can be used to forecast the power generation of renewable energy which is essentially helpful for the smart grid to calculate available resources and avoid unpredicted circumstances. Similarly, AI can also help diagnose faults in the system and protect equipment in the power system. Artificial intelligence is also used to observe consumer consumption behavior, load forecasting, and calculate network security. As the SG involves various stakeholders, such as energy producers, markets, and consumers, artificial intelligence can potentially help to increase the reliability of the smart grid. AI techniques can be classified into four categories based on area, i.e., Expert System (ES), Fuzzy Logic (FL) [86], Artificial Neural Network (ANN), and Evolutionary Computation (EC).

(a) Expert System: It is a program based on Boolean logic that tries to apply human expertise in a certain domain. The knowledge base is organized in the form of IF-THEN rules. The statement is connected by a logical operator (AND, OR, NOT) [87].

$$\text{IF X = A AND Y = B THEN Z = C}$$

(b) Fuzzy Logic: Fuzzy Logic in a multivalued system in which variables are represented as fuzzy sets.

(c) Artificial Neural Network (ANN): It is the most complex and generic form of AI in which the program tries to emulate the human biological nervous system and formulates behavioral responses based on the non-linear inputoutput behavior of the nature of the brain.

In [88], the authors propose an unsupervised scheme for the detection of CDIAs in SG communications networks. The proposed scheme is based on a state-of-the-art algorithm called iForest. The iForest, or isolation forest plots, are the points based on interpolation to isolate the data point which shows distinct characteristics as compared to the rest of the data interpolation and trend. The performance of the technique has been tested by comparing it to IEEE standards, which show that the proposed scheme reasonably improves detection accuracy in the operational environment. Therefore, these make AI techniques popular and suitable. Similarly, the decision tree is another tool used for classification and prediction. The author in [89] uses a CART algorithm-based decision tree that evaluates an anomaly based on an intrusion detection database. In the paper [90], the fundamentals of three AI techniques for STLF, which are Artificial Neural Network ANN, Support Vector Machine SVM, and Adaptive Neuro-Fuzzy Inference System ANFIS, are described in detail. These techniques are able to deal with complex systems with high reliability and accuracy of results, wide area applications, and much less computational cost (Table 4). The comparison with other AI techniques is not added as their application will be very limited with reduced model accuracy.

Table 4. Comparison of Artificial Intelligence Techniques for SG [85].

AI Technique	Advantages	Disadvantages
ANN	• Artificial Neural Network (ANN) is less complex than other AI methods. • Multi-layered mechanism to understand and detect relationships between variables. • Can work with many training algorithms.	• More computational cost. • Tends to overfit. • The empirical nature of model development.
SVM	• With the help of regulation parameters, the overfitting problem can be avoided, as observed in ANN. • Has higher efficiency when the data set has a clear margin between classes. • Expert knowledge about the problem can be built by kernel trick.	• It is not suitable for the large data set. • With overlapping classes, this technique does not work well. • The testing phase is relatively slow.
ANFIS	• A combination of ANN and fuzzy systems is a so-called neuro-fuzzy system that is capable of eliminating the basic problems in fuzzy system design and using the learning ability of an ANN of automatic fuzzy if-then rule generation and parameter optimization.	• Sensitive to initial number of fuzzy rules (number of choices). • Computational complexity increases as the number of fuzzy rules increases.

4.3.2. Machine Learning

Machine Learning (ML) and Data learning (DL) are becoming increasingly popular in the field of data exploration. Most machine learning techniques are characterized as supervised, unsupervised, and reinforcement learning patterns [91,92] The first one works by providing labels to data for algorithms to work. These labels work as a set of predefined instructions for the data. The second technique, on the contrary, works by segregating data into groups based on their similarity. Finally, the reinforcement technique, in which the operator works by interacting with the environment and using human-level integration to reinforce input to predict the output. These technologies work on the principle of differentiating 'normal' data from 'abnormal' data by studying the algorithm and patterns of interaction. [93] presents the thematic taxonomy of ML and DT used for IoT-integrated devices, as shown in Figure 6 The supervised learning method is a widely used machine learning method. It collects the data in the form of (x, y) and corresponding expected (x*, y*) [94]. It works on the prediction of y* in response to a query x*. A novel human-level control through a reinforcement technique called a Qnetwork agent uses reinforcement learning [95]. Q-learning learning can be defined by the equation:

$$Q^{new}(s_t, a_t) = Q(s_t, a_t) + \alpha \times (r_t + \gamma \times maxQ(\, s_{t+1}, a) - Q(s_t, a_t)) \quad (5)$$

when $Q(s_t, a_t)$ is the current value, α is the learning rate, r_t is the reward, γ is the discount factor, max $Q(s_{t+1}, a)$ is the estimate of optimal future value and lastly, $Q(s_t, a_t)$ is the current value.

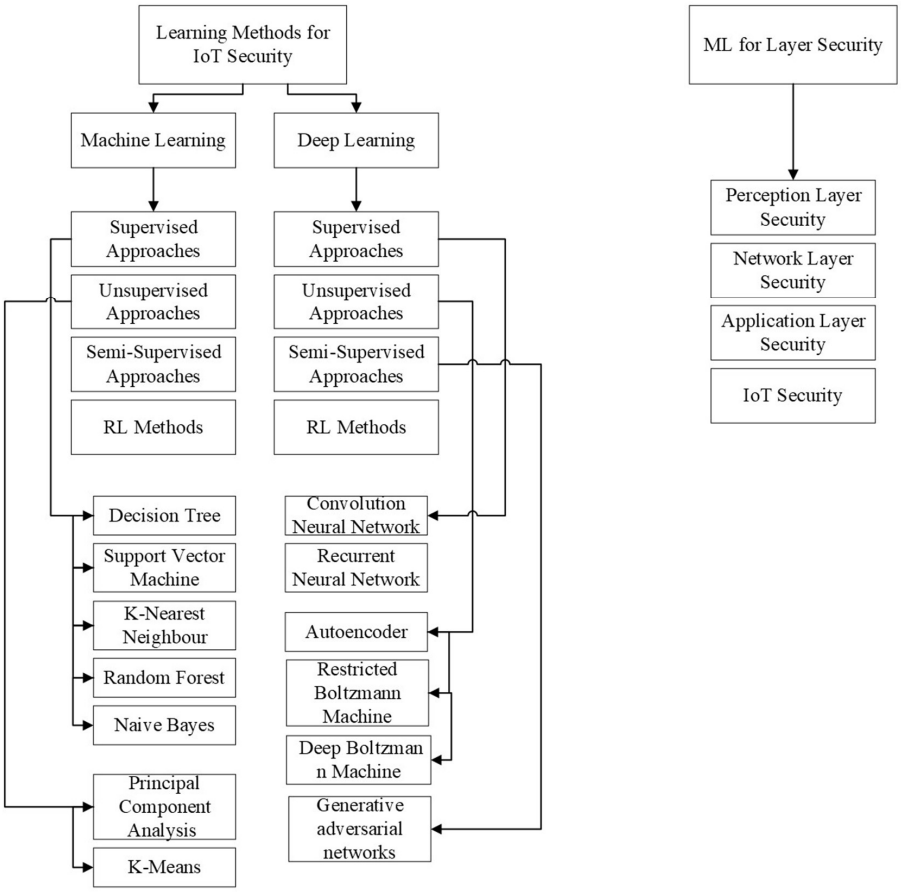

Figure 6. Taxonomy of Machine Learning for IoT Security [83].

Since wireless communication is widely operational worldwide, to deploy machine learning, compatibility route for a Wireless System Network (WSN), challenges of data limitation, and fault tolerance scalability need to be considered.

The author in [96,97] discusses the symbolic dynamic filtering (SDF) technique to monitor regular interactions between subsystems while improving computational efficiency. Proposed techniques utilize machine learning (MI) and Dynamic Bayesian Network (DBN) techniques to detect unobservable false data injection (FDI) attacks and patterns of changes in the attack [98]. The scalability of the technique is tested on IEEE systems and the results show the percentage of false alarms to be less than 2%. Similarly, the paper [99] presents a smart machine learning-based algorithm to reduce electricity expenditure and optimize generation cost along with carbon emission reduction. It calculates a reduction of 41% in end-use cost, 18% in generation cost, and approx. 20% in carbon emissions. Authors in [100] provide ML solutions in integration with Gaussian Process Regression (GPR) to cope with the problem of parameter variations that arise in mutual energy trade between Energy Districts (ED) and SG. The model is compared with the optimization energy management model (EMM) on parameters of prosumer energy cost (PEC), prosumer energy surplus (PEC), and grid revenue (GR). The Gaussian neighboring function is given as:

$$h\,(t) = \frac{1}{\sigma\sqrt{2\pi}} \mathrm{e}^{-\frac{(x-\mu)^2}{2\sigma^2}} \tag{6}$$

where μ stands for mean, σ is the standard deviation.

The article [101] proposes real-time monitoring of grid information as a high-frequency measurement in contrast to current standards of information transmission over 15 min (Figure 6). It also provides a solution to cope with traffic due to high-frequency measurement by compressing with the reconstruction method ensuring minimum error at the receiving end. Other machine learning techniques, such as supervised learning: K-nearest neighbor (k-NN) can be used for query processing [102,103], but this strategy can be inaccurate for high dimensional data [104]; Decision Tree (DT) which is a classification method to categorize data before making a decision working with only linear data [93,105]; *Neural Networks [NN]* which are used in chains of decision algorithms to segregate complex and linear functions for solving network challenges [106]; Support vector machines (SVM) can be used to investigate malicious behavior in data by comparing temporal and spatial correlations [107]; Bayesian Statistics is based on statistical data analysis methods, such as probability distribution to detect uncertainty [108]. Similarly for unsupervised learning, K-means clustering [109], and Principle Component Analysis (PCA) [110], a comparison table is given in Table 5.

Table 5. Comparison of Machine Learning Approaches.

Approaches	Machine Learning Algorithm	Complexity	Characteristics
System Dependability	NNs	High	Estimate the dependability metric
Fault Detection		Moderate	Dynamic fault detection model
Metric Map	DT	Low	Link Quality Estimation
Assessing accuracy and reliability metrics	GP	Moderate	Information Processing Tasks
A QoS schedular	RL	Low	QoS task scheduler for adaptive multimedia sensor networks
Uncertainty and coverage factors		Moderate	Investigate coverage problems
QoS-aware power management		Low	QoS-aware power management in energy harvesting sensor nodes
QoS provisioning		Low	A structure modeling toll for QoS provisioning

Machine learning approaches have a greater advantage over other technologies in terms of detection methodologies and advanced monitoring and detection algorithms. Malware is a rising issue and counter approaches of machine learning show advances in design and systems that can automatically detect malicious activity and malware detection. However, a major drawback of these approaches is the accuracy, especially for Deep Learning (DL) approaches. DL approaches are novel, less understood, and lack a general understanding of the public, which causes errors. Thus, human supervision should be there when applying machine-learning approaches [111].

5. Discussion

Based on the above-mentioned properties and features of various approaches to provide security to the SG, in addition, to counter communication problems, we can analyze them on basis of latency, cost, security, complexity, interoperability, and carbon emission. Blockchain is the most known and implemented of these technologies. It offers low-cost, less complex solutions for SGs; however, it lacks the diversity of services and requires additional security measures. Moreover, 5G is the newest of all and has been

emerging since then. It offers a high-speed and secure network for smart grids along with data handling features. The high cost and carbon emission rate are factors that restrict this technology. AI certainly offers promising solutions; however, it also comes with a high cost and extensive training for stakeholders due to its complex connectivity. The summary of the analysis is shown in Table 6.

Table 6. A Comparison between Features of Advanced Technologies for Smart Grid Cyber Security.

Approach	Latency	Interoperability	Cost	Complexity	Carbon Emission	Security	Data Handling
Blockchain and Edge Computing	Medium	High	Low	Low	Low	Medium	Medium
5G technology	Low	Medium	High	Medium	High	High	High
Artificial Intelligenece	Low	Medium	High	High	Medium	High	High
Machine Learning	Low	Medium	High	High	Low	Hugh	High

Limitation of research: The research presents a comprehensive overview of security enhancement methodologies for smart grids. However, a smart grid comes with many other challenges and threats which are not the focus of this research.

Future Research Direction: In terms of the future direction of research on smart grids, the following areas can be explored:

- Utilization of a dedicated domestic communication network for power IoT to send and receive energy-related data on a dedicated network to provide more privacy to consumers
- Effect of environmental factors on a smart grid's performance and robustness. Due to climate change, and other environmental factors, if any link in the chain of smart grid technology is affected, the smart grid will have loose ends. In this regard, it is researched how this technology can be entirely shifted to wireless technology.
- Integrating smart grid technology with traditional power systems. This can enroute revolutionize the power system gradually but effectively and through the gradual economic burden. The research will be useful for developing and underdeveloped countries.

6. Conclusions

In this paper, solutions to various security and communication challenges for SG were presented The research was based on the motivation to revolutionize the energy sector with an SG supported by IoT. This paper explains the capacities and capabilities of researched approaches and techniques to overcome these challenges. We comprehensively discussed the types and subtypes of these technologies along with features and researched and surveyed proposals. Through this study, we analyzed the utilization of these techniques and approaches for the efficient application of IoT-based smart grids. We also compared them on multiple factors to find out the more efficient of these. This opens opportunities for future research as many approaches proposed in this paper are still under research and the final judgment call of efficiency can only be after a full understanding of them. However, many countries have and are already investing in SG technology based on their energy goals.

Author Contributions: Conceptualization, A.A.A.; Formal analysis, A.S.B.; Funding acquisition, T.A.; Investigation, A.S.B.; Methodology, A.A.A.; Project administration, A.A.A. and T.A.; Resources, A.A.A. and T.A.; Software, A.A.A. and T.A.; Supervision, A.A.A. and T.A.; Validation, A.A.A.; Visualization, A.A.A.; Writing—Original draft, A.S.B.; Writing—Review & Editing, A.A.A. and T.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not Required.

Informed Consent Statement: Not Required.

Data Availability Statement: Not Required.

Acknowledgments: The authors would like to thank their colleagues for their suggestions on how to improve the paper's quality.

Conflicts of Interest: The authors declare no conflict of interest in preparing this paper.

Abbreviations

Abbreviation	Description
MG	Microgrid
SG	Smart Grid
IoT	Internet of Things
DER	Distribution Energy Resource
DR	Demand Response
EV	Electrical Vehicle
AMI	Advanced Metering Infrastructure
RFID	Radio Frequency Infrastructure
PV	Photo Voltaic
RES	Renewable Energy Resources
FAN	Field Area Network
FDI	False Data Injection
PMU	Power Management Units
DDoS	Distributed Denial of Service
ICS	Wireless Sensor Network
PKI	Public Key Infrastructure
EI	Energy Internet
CB	Circuit Breaker
DoS	Denial of Service
DLP	Data Loss Prevention
IDS	Intrusion Detection System
TES	Transactive Energy System
DL	Deep Learning
ML	Machine Learning
AI	Artificial Intelligence

References

1. Babar, M.; Tariq, M.U.; Jan, M.A. Secure and resilient demand side management engine using machine learning for IoT-enabled smart grid. *Sustain. Cities Soc.* **2020**, *62*, 102370. [CrossRef]
2. Khatua, P.K.; Ramachandaramurthy, V.K.; Kasinathan, P.; Yong, J.Y.; Pasupuleti, J.; Rajagopalan, A. Application and assessment of internet of things toward the sustainability of energy systems: Challenges and issues. *Sustain. Cities Soc.* **2020**, *53*, 101957. [CrossRef]
3. Amin, A.A.; Mahmood-ul-Hasan, K. Unified Fault-Tolerant Control for Air-Fuel Ratio Control of Internal Combustion Engines with Advanced Analytical and Hardware Redundancies. *J. Electr. Eng. Technol.* **2021**, *17*, 1947–1959. [CrossRef]
4. Amin, A.A.; Hasan, K.M. A review of Fault Tolerant Control Systems: Advancements and applications. *Measurement* **2019**, *143*, 58–68. [CrossRef]
5. Wilamowski, B.M.; Irwin, J.D. Power Electronics and Motor Drives. Available online: https://www.routledge.com/Power-Electronics-and-Motor-Drives/Wilamowski-Irwin/p/book/9781138077478 (accessed on 19 September 2022).
6. A 5G Cellular Technology for Distributed Monitoring and Control in Smart Grid. Available online: https://www.researchgate.net/publication/318019902_A_5G_Cellular_Technology_for_Distributed_Monitoring_and_Control_in_Smart_Grid (accessed on 10 September 2022).
7. Almasarani, A.; Majid, M.A. 5G-Wireless sensor networks for smart grid-accelerating technology's progress and innovation in the kingdom of Saudi arabia. *Procedia Comput. Sci.* **2021**, *182*, 46–55.
8. Rajendran, G.; Sathyabalu, H.V.; Sachi, M.; Devarajan, V. Cyber Security in Smart Grid: Challenges and Solutions. In Proceedings of the 2019 2nd International Conference on Power and Embedded Drive Control (ICPEDC), Chennai, India, 21–23 August 2019; pp. 546–551. [CrossRef]
9. Yin, X.; Zamani, M.; Liu, S. On Approximate Opacity of Cyber-Physical Systems. *IEEE Trans. Autom. Control* **2021**, *66*, 1630–1645. [CrossRef]

10. Zeng, W.; Koutny, M. Quantitative Analysis of Opacity in Cloud Computing Systems. *IEEE Trans. Cloud Comput.* **2021**, *9*, 1210–1219. [CrossRef]
11. Moongilan, D. 5G wireless communications (60 GHz band) for smart grid? An EMC perspective. In Proceedings of the IEEE International Symposium on Electromagnetic Compatibility (EMC), Ottawa, ON, Canada, 25–29 July 2016; pp. 689–694. [CrossRef]
12. Brar, H.; Kumar, G. Cybercrimes: A Proposed Taxonomy and Challenges. *J. Comput. Netw. Commun.* **2018**, *2018*, 1798659. [CrossRef]
13. Bose, B.K. Artificial Intelligence Techniques in Smart Grid and Renewable Energy Systems—Some Example Applications. *Proc. IEEE* **2017**, *105*, 2262–2273. [CrossRef]
14. Khodayar, M.; Wu, H. Demand Forecasting in the Smart Grid Paradigm: Features and Challenges. *Electr. J.* **2015**, *28*, 51–62. [CrossRef]
15. Gunduz, M.Z.; Das, R. Cyber-security on smart grid: Threats and potential solutions. *Comput. Netw.* **2020**, *169*, 107094. [CrossRef]
16. Nozari, E.; Tallapragada, P.; Cortés, J. Differentially private distributed convex optimization via objective perturbation. In Proceedings of the 2016 American Control Conference (ACC), Boston, MA, USA, 6–8 July 2016; pp. 2061–2066. [CrossRef]
17. Lai, C.S.; Lai, L.L. Application of Big Data in Smart Grid. In Proceedings of the 2015 IEEE International Conference on Systems, Man, and Cybernetics, Hong Kong, China, 9–12 October 2015; pp. 665–670. [CrossRef]
18. Mohammadpourfard, M.; Weng, Y.; Pechenizkiy, M.; Tajdinian, M.; Mohammadi-Ivatloo, B. Ensuring cybersecurity of smart grid against data integrity attacks under concept drift. *Int. J. Electr. Power Energy Syst.* **2020**, *119*, 105947. [CrossRef]
19. LAKAF: Lightweight Authentication and Key Agreement Framework for Smart Grid Network—ScienceDirect. Available online: https://www.sciencedirect.com/science/article/abs/pii/S1383762121000461 (accessed on 10 September 2022).
20. Mo, Y.; Kim, T.H.-J.; Brancik, K.; Dickinson, D.; Lee, H.; Perrig, A.; Sinopoli, B. Cyber–Physical Security of a Smart Grid Infrastructure. *Proc. IEEE* **2012**, *100*, 195–209. [CrossRef]
21. Hussain, S.; Ullah, I.; Khattak, H.; Adnan, M.; Kumari, S.; Ullah, S.S.; Khan, M.; Khattak, S. A Lightweight and Formally Secure Certificate Based Signcryption With Proxy Re-Encryption (CBSRE) for Internet of Things Enabled Smart Grid. *IEEE Access* **2020**, *8*, 93230–93248. [CrossRef]
22. LeMay, M.; Gross, G.; Gunter, C.; Garg, S. Unified Architecture for Large-Scale Attested Metering. In Proceedings of the IEEE Hawaii International Conference on System Sciences, Waikoloa, HI, USA, 3–6 January 2007; p. 115. [CrossRef]
23. Goyal, V.; Pandey, O.; Sahai, A.; Waters, B. Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the ACM Conference on Computer and Communications Security, Alexandria, VA, USA, 30 October 2006; pp. 89–98. [CrossRef]
24. Ferrag, M.A.; Babaghayou, M.; Yazıcı, M.A. Cyber security for fog-based smart grid SCADA systems: Solutions and challenges. *J. Inf. Secur. Appl.* **2020**, *52*, 102500. [CrossRef]
25. Waters, B. Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization. Available online: https://eprint.iacr.org/undefined/undefined (accessed on 19 September 2022).
26. Shitharth; Kantipudi, M.P.; Sangeetha, K.; Kshirsagar, P.; Thanikanti, S.B.; Haes Alhelou, H. An Enriched RPCO-BCNN Mechanisms for Attack Detection and Classification in SCADA Systems. *IEEE Access* **2021**, *9*, 156297–156312. [CrossRef]
27. Khadidos, A.O.; Manoharan, H.; Selvarajan, S.; Khadidos, A.O.; Alyoubi, K.H.; Yafoz, A. A Classy Multifacet Clustering and Fused Optimization Based Classification Methodologies for SCADA Security. *Energies* **2022**, *15*, 3624. [CrossRef]
28. Shitharth, S.; Satheesh, N.; Kumar, B.P.; Sangeetha, K. IDS Detection Based on Optimization Based on WI-CS and GNN Algorithm in SCADA Network. In *Architectural Wireless Networks Solutions and Security Issues*; Springer: Singapore, 2021; pp. 247–265. [CrossRef]
29. Li, Q.; Xiong, H.; Zhang, F.; Zeng, S. An Expressive Decentralizing KP-ABE Scheme with Constant-Size Ciphertext. *Int. J. Netw. Secur.* **2013**, *15*, 161–170.
30. Lai, J.; Deng, R.H.; Li, Y.; Weng, J. Fully secure key-policy attribute-based encryption with constant-size ciphertexts and fast decryption. In Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security, Kyoto, Japan, 6 June 2014; pp. 239–248. [CrossRef]
31. Tajer, A. False Data Injection Attacks in Electricity Markets by Limited Adversaries: Stochastic Robustness. *IEEE Trans. Smart Grid* **2019**, *10*, 128–138. [CrossRef]
32. Chauhan, S.; Agarwal, N.; Kar, A. Addressing Big Data Challenges in Smart Cities: A Systematic Literature Review. *Info* **2016**, *18*, 73–90. [CrossRef]
33. Khan, F.; Asif, M.; Ahmad, A.; Alharbi, M.; Aljuaid, H. Blockchain Technology, Improvement Suggestions, Security Challenges on Smart Grid and Its Application in Healthcare for Sustainable Development. *Sustain. Cities Soc.* **2020**, *55*, 102018. [CrossRef]
34. Saha, M.S.; Li, R.; Sun, X. High loading and monodispersed Pt nanoparticles on multiwalled carbon nanotubes for high performance proton exchange membrane fuel cells. *J. Power Sources* **2008**, *177*, 314–322. [CrossRef]
35. Musleh, A.S.; Yao, G.; Muyeen, S.M. Blockchain Applications in Smart Grid–Review and Frameworks. *IEEE Access* **2019**, *7*, 86746–86757. [CrossRef]
36. Mollah, M.B.; Zhao, J.; Niyato, D.; Lam, K.-Y.; Zhang, X.; Ghias, A.M.Y.M.; Koh, L.H.; Yang, L. Blockchain for Future Smart Grid: A Comprehensive Survey. *IEEE Internet Things J.* **2021**, *8*, 18–43. [CrossRef]
37. Mylrea, M.; Gourisetti, S.N.G. Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security. In Proceedings of the 2017 Resilience Week (RWS), Wilmington, DE, USA, 18–22 September 2017; pp. 18–23. [CrossRef]

38. Campagna, N.; Caruso, M.; Castiglia, V.; Miceli, R.; Viola, F. Energy management concepts for the evolution of smart grids. In Proceedings of the 2020 8th International Conference on Smart Grid (icSmartGrid), Paris, France, 17–19 June 2020.
39. Gai, K.; Wu, Y.; Zhu, L.; Xu, L.; Zhang, Y. Permissioned Blockchain and Edge Computing Empowered Privacy-Preserving Smart Grid Networks. *IEEE Internet Things J.* **2019**, *6*, 7992–8004. [CrossRef]
40. Antal, C.; Cioara, T.; Antal, M.; Anghel, I.; Salomie, I.; Bertoncini, M. Blockchain Based Decentralized Management of Demand Response Programs in Smart Energy Grids. *Sensors* **2018**, *18*, 162. [CrossRef]
41. Joseph, A.; Balachandra, P. Smart grid to energy internet: A systematic review of transitioning electricity systems. *IEEE Access* **2020**, *8*, 215787–215805. [CrossRef]
42. Butt, A.; Huda, N.; Amin, A.A. Design of fault-tolerant contr ol system for distributed energy resources based power network using Phasor Measurement Units. *Meas. Control* **2022**. [CrossRef]
43. Tan, S.; Wang, X.; Jiang, C. Privacy-Preserving Energy Scheduling for ESCOs Based on Energy Blockchain Network. *Energies* **2019**, *12*, 1530. [CrossRef]
44. Maw, A.; Adepu, S.; Mathur, A. ICS-BlockOpS: Blockchain for operational data security in industrial control system. *Pervasive Mob. Comput.* **2019**, *59*, 101048. [CrossRef]
45. Guerrero, J.; Vasquez, J.C.; Alcala, J.; Vicuna, L.; Castilla, M. Hierarchical Control of Droop-Controlled AC and DC Microgrids—A General Approach Toward Standardization. *Ind. Electron. IEEE Trans.* **2011**, *58*, 158–172. [CrossRef]
46. Gao, J.; Asamoah, K.; Sifah, E.; Smahi, A.; Xia, Q. GridMonitoring: Secured Sovereign Blockchain Based Monitoring on Smart Grid. *IEEE Access* **2018**, *6*, 9917–9925. [CrossRef]
47. Munsing, E.; Mather, J.; Moura, S. Blockchains for decentralized optimization of energy resources in microgrid networks. In Proceedings of the 2017 IEEE Conference on Control Technology and Applications (CCTA), Maui, HI, USA, 27–30 August 2017; pp. 2164–2171. [CrossRef]
48. Danzi, P.; Angjelichinoski, M.; Stefanović, Č.; Popovski, P. Distributed proportional-fairness control in microgrids via blockchain smart contracts. In Proceedings of the 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm), Dresden, Germany, 23–27 October 2017; pp. 45–51. [CrossRef]
49. Dang, C.; Zhang, J.; Kwong, C.P.; Li, L. Demand Side Load Management for Big Industrial Energy Users Under Blockchain-Based Peer-to-Peer Electricity Market. *IEEE Trans. Smart Grid* **2019**, *10*, 6426–6435. [CrossRef]
50. Li, Y.; Yang, W.; He, P.; Chen, C.; Wang, X. Design and management of a distributed hybrid energy system through smart contract and blockchain. *Appl. Energy* **2019**, *248*, 390–405. [CrossRef]
51. Noor, S.; Yang, W.; Guo, M.; Dam, K.; Wang, X. Energy Demand Side Management within micro-grid networks enhanced by blockchain. *Appl. Energy* **2018**, *228*, 1385–1398. [CrossRef]
52. Bergquist, J.; Laszka, A.; Sturm, M.; Dubey, A. On the design of communication and transaction anonymity in blockchain-based transactive microgrids. In Proceedings of the 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers, Las Vegas, NV, USA, 11–15 December 2017; pp. 1–6. [CrossRef]
53. Casado-Vara, R.; Prieto, J.; Corchado, J.M. How Blockchain Could Improve Fraud Detection in Power Distribution Grid. In Proceedings of the International Joint Conference SOCO'18-CISIS'18-ICEUTE'18, Cham, Switzerland, 6–8 June 2019; pp. 67–76. [CrossRef]
54. DeCusatis, C.; Lotay, K. Secure, Decentralized Energy Resource Management Using the Ethereum Blockchain. In Proceedings of the 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications, New York, NY, USA, 1–3 August 2018; pp. 1907–1913. [CrossRef]
55. Sestrem Ochôa, I.; Augusto Silva, L.; de Mello, G.; Garcia, N.M.; de Paz Santana, J.F.; Quietinho Leithardt, V.R. A cost analysis of implementing a blockchain architecture in a smart grid scenario using sidechains. *Sensors* **2020**, *20*, 843. [CrossRef]
56. Wang, S.; Taha, A.; Wang, J.; Kvaternik, K.; Hahn, A. Energy Crowdsourcing and Peer-to-Peer Energy Trading in Blockchain-Enabled Smart Grids. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *49*, 1612–1623. [CrossRef]
57. Aitzhan, N.; Svetinovic, D. Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams. *IEEE Trans. Dependable Secure Comput.* **2016**, *15*, 840–852. [CrossRef]
58. Kounelis, I.; Steri, G.; Giuliani, R.; Geneiatakis, D.; Neisse, R.; Nai Fovino, I. Fostering consumers' energy market through smart contracts. In Proceedings of the 2017 International Conference in Energy and Sustainability in Small Developing Economies (ES2DE), Funchal, Portugal, 10–12 July 2017. [CrossRef]
59. (PDF) Blockchain Based Transactive Energy Systems for Voltage Regulation in Active Distribution Networks. Available online: https://www.researchgate.net/publication/340916228_Blockchain_Based_Transactive_Energy_Systems_for_Voltage_Regulation_in_Active_Distribution_Networks (accessed on 19 September 2022).
60. Hassan, M.U.; Rehmani, M.H.; Chen, J. Optimizing blockchain based smart grid auctions: A green revolution. *IEEE Trans. Green Commun. Netw.* **2021**, *6*, 462–471. [CrossRef]
61. Xu, X.; Pautasso, C.; Zhu, L.; Gramoli, V.; Ponomarev, A.; Tran, A.B.; Chen, S. The Blockchain as a Software Connector. In Proceedings of the 2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA), Venice, Italy, 5–8 April 2016; pp. 182–191. [CrossRef]
62. Eyal, I.; Gencer, A.E.; Sirer, E.; Van Renesse, R. Bitcoin-NG: A Scalable Blockchain Protocol. In Proceedings of the 13th USENIX Symposium on Networked Systems Design and Implementation, Santa Clara, CA, USA, 16–18 March 2015.

63. Kim, N.; Kang, S.M.; Hong, C.S. Mobile charger billing system using lightweight Blockchain. In Proceedings of the 2017 19th Asia-Pacific Network Operations and Management Symposium (APNOMS), Seoul, Korea, 27–29 September 2017; pp. 374–377. [CrossRef]
64. Sohaib, O.; Naderpour, M.; Hussain, W.; Martinez, L. Cloud Computing Model Selection for E-commerce Enterprises Using a New 2-tuple Fuzzy Linguistic Decision-Making Method. *Comput. Ind. Eng.* **2019**, *132*, 47–58. [CrossRef]
65. Agiwal, M.; Roy, A.; Saxena, N. Next Generation 5G Wireless Networks: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 1617–1655. [CrossRef]
66. Elkashlan, M.; Duong, T.; Chen, H.-H. Millimeter-wave communications for 5G: Fundamentals: Part I (Guest Editorial). *Commun. Mag. IEEE* **2014**, *52*, 52–54. [CrossRef]
67. Garau, M.; Anedda, M.; Desogus, C.; Ghiani, E.; Murroni, M.; Celli, G. A 5G Cellular Technology for Distributed Monitoring and Control in Smart Grid. In Proceedings of the 2017 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), Cagliari, Italy, 7–9 June 2017. [CrossRef]
68. Wei, M.; Wang, W. Toward distributed intelligent: A case study of peer to peer communication in smart grid. In Proceedings of the 2013 IEEE Global Communications Conference (GLOBECOM), Atlanta, GA, USA, 9–13 December 2013; pp. 2210–2216. [CrossRef]
69. Hui, H.; Ding, Y.; Shi, Q.; Li, F.; Song, Y.; Yan, J. 5G network-based Internet of Things for demand response in smart grid: A survey on application potential. *Appl. Energy* **2020**, *257*, 113972. [CrossRef]
70. Shahinzadeh, H.; Mirhedayati, A.-S.; Shaneh, M.; Nafisi, H.; Gharehpetian, G.B.; Moradi, J. Role of joint 5G-IoT framework for smart grid interoperability enhancement. In Proceedings of the 2020 15th International Conference on Protection and Automation of Power Systems (IPAPS), Shiraz, Iran, 30–31 December 2020.
71. Tao, M.; Ota, K.; Dong, M. Foud: Integrating Fog and Cloud for 5G-Enabled V2G Networks. *IEEE Netw.* **2017**, *31*, 8–13. [CrossRef]
72. De Dutta, S.; Prasad, R. Security for Smart Grid in 5G and Beyond Networks. *Wirel. Pers. Commun.* **2019**, *106*, 261–273. [CrossRef]
73. Borgaonkar, R.; Anne Tøndel, I.; Zenebe Degefa, M.; Gilje Jaatun, M. Improving smart grid security through 5G enabled IoT and edge computing. *Concurr. Comput. Pract. Exp.* **2021**, *33*, e6466. [CrossRef]
74. Zhang, Y.; Li, J.; Zheng, D.; Li, P.; Tian, Y. Privacy-preserving communication and power injection over vehicle networks and 5G smart grid slice. *J. Netw. Comput. Appl.* **2018**, *122*, 50–60. [CrossRef]
75. Zhang, Y.; Zhao, J.; Zheng, D. Efficient and Privacy-Aware Power Injection over AMI and Smart Grid Slice in Future 5G Networks. *Mob. Inf. Syst.* **2017**, *2017*, 3680671. [CrossRef]
76. Huawei Joins Forces with China Telecom and China's State Grid to Develop 5G Slicing Solution for Power Industry—Huawei Press Center. Available online: https://www.huawei.com/en/news/2017/9/ChinaTelecom-StateGrid-Joint-Innovation-Project (accessed on 19 September 2022).
77. IET Digital Library: Challenges and opportunities of 5G in power grids. Available online: https://digital-library.theiet.org/content/journals/10.1049/oap-cired.2017.0374 (accessed on 10 September 2022).
78. Helen, L.; Zahariadis, T.; Sarakis, L.; Tsampasis, E.; Voulkidis, A.; Velivasaki, T. Smart Grid: A demanding use case for 5G technologies. In Proceedings of the 2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Athens, Greece, 19–23 March 2018; pp. 215–220. [CrossRef]
79. 5g_nework_architecture_whitepaper_en.pdf. Available online: https://carrier.huawei.com/~{}/media/CNBG/Downloads/Program/5g_nework_architecture_whitepaper_en.pdf (accessed on 10 September 2022).
80. Zhou, Z.; Tan, L.; Gu, B.; Zhang, Y.; Wu, J. Bandwidth Slicing in Software-Defined 5G: A Stackelberg Game Approach. *IEEE Veh. Technol. Mag.* **2018**, *13*, 102–109. [CrossRef]
81. Shahzad, K.; Amin, A.A. Optimal Planning of Distributed Energy Storage Systems in Active Distribution Networks using Advanced Heuristic Optimization Techniques. *J. Electr. Eng. Technol.* **2021**, *16*, 2447–2462. [CrossRef]
82. Ahmadzadeh, S.; Parr, G.; Zhao, W. A Review on Communication Aspects of Demand Response Management for Future 5G IoT-Based Smart Grids. *IEEE Access* **2021**, *9*, 77555–77571. [CrossRef]
83. Jia, H.; Ding, Y.; Song, Y.; Singh, C.; Li, M. Operating Reliability Evaluation of Power Systems Considering Flexible Reserve Provider in Demand Side. *IEEE Trans. Smart Grid* **2018**, *10*, 3452–3464. [CrossRef]
84. Yilmaz, O.; Wang, Y.-P.; Johansson, N.; Nadia, B.; Ashraf, S.; Sachs, J. Analysis of ultra-reliable and low-latency 5G communication for a factory automation use case. In Proceedings of the 2015 IEEE International Conference on Communication Workshop (ICCW), London, UK, 8–12 June 2015; pp. 1190–1195. [CrossRef]
85. Shafik, W.; Matinkhah, M. Smart Grid Empowered By 5G Technology. In Proceedings of the 2019 Smart Grid Conference (SGC), Tehran, Iran, 18–19 December 2019. [CrossRef]
86. Riaz, U.; Amin, A.A.; Tayyeb, M. Design of active fault-tolerant control system for Air-fuel ratio control of internal combustion engines using fuzzy logic controller. *Sci. Prog.* **2022**, *105*, 368504221094723. [CrossRef] [PubMed]
87. Shahbaz, M.H.; Amin, A.A. Design of Active Fault Tolerant Control System for Air Fuel Ratio Control of Internal Combustion Engines Using Artificial Neural Networks. *IEEE Access* **2021**, *9*, 46022–46032. [CrossRef]
88. Ullah, Z.; Al-Turjman, F.; Mostarda, L.; Gagliardi, R. Applications of Artificial Intelligence and Machine learning in smart cities. *Comput. Commun.* **2020**, *154*, 313–323. [CrossRef]

89. Taghavinejad, S.; Taghavinejad, M.; Shahmiri, L.; Zavvar, M.; Zavvar, M. Intrusion Detection in IoT-Based Smart Grid Using Hybrid Decision Tree. In Proceedings of the 2020 6th International Conference on Web Research (ICWR), Tehran, Iran, 22–23 April 2020; pp. 152–156. [CrossRef]
90. Zor, K.; Timur, O.; Teke, A. A state-of-the-art review of artificial intelligence techniques for short-term electric load forecasting. In Proceedings of the 2017 6th International Youth Conference on Energy (IYCE), Budapest, Hungary, 21–24 June 2017; pp. 1–7. [CrossRef]
91. Unsupervised Machine Learning-Based Detection of Covert Data Integrity Assault in Smart Grid Networks Utilizing Isolation Forest. Available online: https://www.researchgate.net/publication/331543051_Unsupervised_Machine_Learning-Based_Detection_of_Covert_Data_Integrity_Assault_in_Smart_Grid_Networks_Utilizing_Isolation_Forest (accessed on 19 September 2022).
92. Abu-Mostafa, Y.S.; Magdon-Ismail, M.; Lin, H.-T. *Learning from Data*; AMLBook: New York, NY, USA, 2012.
93. Safavian, S.R.; Landgrebe, D. A survey of decision tree classifier methodology. *IEEE Trans. Syst. Man Cybern.* **1991**, *21*, 660–674. [CrossRef]
94. Jordan, M.I.; Mitchell, T.M. Machine learning: Trends, perspectives, and prospects. *Science* **2015**, *349*, 255–260. [CrossRef] [PubMed]
95. Saranya, S.; Princy, M. Routing Techniques in Sensor Network–A Survey. *Procedia Eng.* **2012**, *38*, 2739–2747. [CrossRef]
96. Routing Techniques in Wireless Sensor Networks: A Survey. Available online: https://ieeexplore.ieee.org/document/1368893 (accessed on 10 September 2022).
97. Abu Alsheikh, M.; Lin, S.; Niyato, D.; Tan, H.P. Machine Learning in Wireless Sensor Networks: Algorithms, Strategies, and Applications. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1996–2018. [CrossRef]
98. Karimipour, H.; Dehghantanha, A.; Parizi, R.; Choo, K.-K.R.; Leung, H. A Deep and Scalable Unsupervised Machine Learning System for Cyber-Attack Detection in Large-Scale Smart Grids. *IEEE Access* **2019**, *7*, 80778. [CrossRef]
99. Shahbaz, M.H.; Arslan, A.A. A Review of Classical and Modern Control Techniques Utilized in Modern Microgrids. *Recent Adv. Electr. Electron. Eng.* **2021**, *14*, 459–472. [CrossRef]
100. Ahmed, W.; Ansari, H.; Khan, B.; Ullah, Z.; Ali, S.M.; Mehmood, C.A.A.; Qureshi, M.B.; Hussain, I.; Jawad, M.; Khan, M.U.S.; et al. Machine Learning Based Energy Management Model for Smart Grid and Renewable Energy Districts. *IEEE Access* **2020**, *8*, 185059–185078. [CrossRef]
101. Das, L.; Garg, D.; Srinivasan, B. NeuralCompression: A machine learning approach to compress high frequency measurements in smart grid. *Appl. Energy* **2020**, *257*, 113966. [CrossRef]
102. Winter, J.; Xu, Y.; Lee, W.C. Energy Efficient Processing of K Nearest Neighbor Queries in Location-aware Sensor Networks. In Proceedings of the Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, San Diego, CA, USA, 17–21 July 2005; pp. 281–292. [CrossRef]
103. Jayaraman, P.P.; Zaslavsky, A.; Delsing, J. Intelligent Processing of K-Nearest Neighbors Queries Using Mobile Data Collectors in a Location Aware 3D Wireless Sensor Network. In *International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems*; Springer: Berlin/Heidelberg, Germany, 2010; Volume 6098, pp. 260–270. [CrossRef]
104. Beyer, K.; Goldstein, J.; Ramakrishnan, R.; Shaft, U. When Is "Nearest Neighbor" Meaningful? In *Database Theory—ICDT'99*; Springer: Berlin/Heidelberg, Germany, 1999; pp. 217–235. [CrossRef]
105. A Survey of Decision Tree Classifier Methodology. Available online: https://ieeexplore.ieee.org/document/97458 (accessed on 10 September 2022).
106. Lippmann, R. An introduction to computing with neural nets. *IEEE ASSP Mag.* **1987**, *4*, 4–22. [CrossRef]
107. Steinwart, I.; Christmann, A. Support Vector Machines for Classification. In *Support Vector Machines*; Springer: New York, NY, USA, 2008; pp. 285–329. [CrossRef]
108. Box, G.E.P.; Tiao, G.C. Bayesian Assessment of Assumptions 2 Comparison of Variances. In *Bayesian Inference in Statistical Analysis*; John Wiley & Sons, Ltd.: Hoboken, NJ, USA, 1992; pp. 203–243. [CrossRef]
109. Kanungo, T.; Mount, D.M.; Netanyahu, N.S.; Piatko, C.D.; Silverman, R.; Wu, A.Y. An efficient k-means clustering algorithm: Analysis and implementation. *IEEE Trans. Pattern Anal. Mach. Intell.* **2002**, *24*, 881–892. [CrossRef]
110. Jolliffe, I.T. (Ed.) Principal Component Analysis and Factor Analysis. In *Principal Component Analysis*; Springer: New York, NY, USA, 2002; pp. 150–166. [CrossRef]
111. Handbook of Big Data Privacy. Available online: https://link.springer.com/book/10.1007/978-3-030-38557-6 (accessed on 10 September 2022).