IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received March 18, 2022, accepted April 27, 2022, date of publication May 11, 2022, date of current version May 23, 2022.

*Digital Object Identifier 10.1109/ACCESS.2022.3174259*

# Smart Grid Security and Privacy: From Conventional to Machine Learning Issues (Threats and Countermeasures)

**PARYA HAJI MIRZAEE, (Member, IEEE), MOHAMMAD SHOJAFAR, (Senior Member, IEEE), HAITHAM CRUICKSHANK, (Senior Member, IEEE), AND RAHIM TAFAZOLLI, (Senior Member, IEEE)**
5GIC and 6GIC, Institute for Communication Systems (ICS), University of Surrey, Guildford GU2 7XH, U.K.

Corresponding author: Parya Haji Mirzaee (p.hajimirzaee@surrey.ac.uk)

**ABSTRACT** Smart Grid (SG) is the revolutionised power network characterised by a bidirectional flow of energy and information between customers and suppliers. The integration of power networks with information and communication technologies enables pervasive control, automation and connectivity from the energy generation power plants to the consumption level. However, the development of wireless communications, the increased level of autonomy, and the growing sofwarisation and virtualisation trends have expanded the attack susceptibility and threat surface of SGs. Besides, with the real-time information flow, and online energy consumption controlling systems, customers' privacy and preserving their confidential data in SG is critical to be addressed. In order to prevent potential attacks and vulnerabilities in evolving power networks, the need for additional studying security and privacy mechanisms is reinforced. In addition, recently, there has been an ever-increasing use of machine intelligence and Machine Learning (ML) algorithms in different components of SG. ML models are currently the mainstream for attack detection and threat analysis. However, despite these algorithms' high accuracy and reliability, ML systems are also vulnerable to a group of malicious activities called adversarial ML (AML) attacks. Throughout this paper, we survey and discuss new findings and developments in existing security issues and privacy breaches associated with the SG and the introduction of novel threats embedded within power systems due to the development of ML-based applications. Our survey builds multiple taxonomies and tables to express the relationships of various variables in the field. Our final section identifies the implications of emerging technologies, future communication systems, and advanced industries on the security and privacy issues of SG.

**INDEX TERMS** Smart grid (SG), security, privacy, threats, machine learning (ML), adversarial machine learning (AML).

## I. INTRODUCTION

Smart Grid (SG) indicates the next generation of power grids, integrated with communication and information technologies, capable of the bidirectional flow of energy and information between suppliers and consumers [1]–[4]. The present power grid is ageing, and it cannot respond to the current ever-increasing demand for electricity anymore. It is limited in terms of utilising distributed and renewable energy resources also inefficient when facing faults and problems. Therefore, both academia and industry are motivated to move toward a power grid that reflects the modern lifestyle. [5], [6]. SG has thus been receiving significant attention in recent years.

SG is a fully automated and functional power network [7]. With the integration of renewable energy sources and information technologies, SG can optimise the future power distribution network in terms of energy consumption, cost reduction, and environmental protection [8]. One of the most sophisticated models for the SG architecture was proposed by the United States National of Standards and Technology (NIST) in [9]. The NIST's proposed architecture comprises seven domains: generation, transmission, distribution, customers, markets, operation, and customer service. The first four are responsible for generation, transmission

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

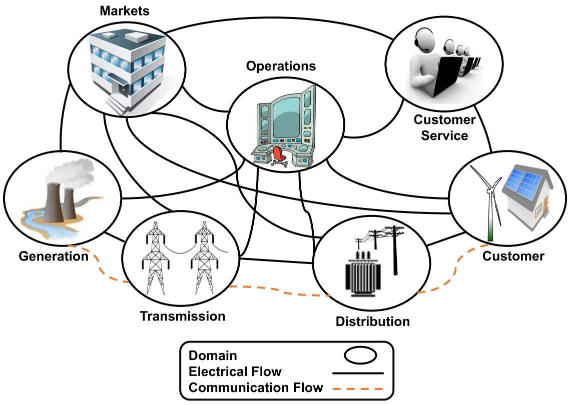

**FIGURE 1. Modified NIST smart grid architecture [9].**

distribution, and bidirectional energy flow controlled and monitored through the other three domains with the information stream. Fig. 1 illustrates the modified NIST architecture and its different domains [9].

The communication infrastructure of SG provides seamless information flow over the entire network. This online information is stored and analysed for various applications, including power generation policies, real-time energy pricing, fault detection and troubleshooting of the system. Therefore, implementing SG requires designing a communication network capable of responding to several SG applications. However, this is a challenging problem to be solved. The SG communication network is a heterogeneous network responsible for connecting multiple devices with different Quality of Service (QoS) requirements over a vast geographical area [10]. Besides, increasing wireless connectivity, autonomous systems, and more softwarisation and virtualisation functions expand future power networks' security vulnerabilities. SG can be threatened through both deliberate attacks as aggressive employees, espial agencies, hackers, or terrorist organisations, and unintentional failures such as equipment malfunctions and natural disasters [11]. Fig. 2 illustrates different SG communication links and possible vulnerabilities that adversaries may use to attack the system. This figure illustrates both inside and outside attackers who can sabotage the system on different scales and for different objectives.

SG automates and streamlines monitoring, controlling, and processing entities in real-time. SG data processing provides many potential advantages, including online reporting of users' energy consumption, dynamic billing, early detection of faults, fast detection of interruptions in energy supply, and intelligent and real-time energy planning and pricing. However, despite the advantages mentioned above, with actual energy consumption information of customers being monitored, aggregated, and analysed by suppliers, privacy exposure is another significant issue in the concept of SG to be addressed. Customers' energy consumption data contains sensitive information about their private life, daily activities, and routines. Fully deploying SGs requires maintaining the privacy of energy premises and consumers [12].

One of the critical approaches toward a reliable SG is designing a robust cyber-attack defensive system to refuge attacks threatening the network [13]. Traditionally, defensive strategies include prevention, detection and mitigation steps [14]. While prevention solutions prevent unauthorised access to the network, detection systems focus on diagnosing anomalies and suspicious traffic patterns. Additionally, mitigation schemes include developing appropriate strategies and updating policies and protocols for minimising the system's losses and costs in the post-attack state. However, existing security measures, which protect information and communication systems, do not provide adequate protection for SG. Most SG components are limited in terms of processing power and storage capacity. For this reason, they lack the ability to incorporate sophisticated security problems. Furthermore, some SG applications are latency-constrained and cannot tolerate delays resulting from security measures. Therefore, these solutions should be reconsidered according to the SG requirements [15].

Apart from conventional security solutions, recently, emerging novel data analysis methods such as Machine Learning (ML) algorithms has motivated the network developers to move toward these techniques to make a more reliable and secure power grid. High accuracy and efficiency in detecting abnormal behaviour and possible attacks make ML significantly applicable in attack detecting systems. However, there are some challenges with integrating ML technologies into SG applications. ML algorithms require high computational and storage capabilities, which are not shared by all end devices in the SG. A standard solution is to shift computations from user to edge processors and a centralised server to compensate for these limitations [16]. However, this massive amount of data sharing is inefficient regarding privacy and communication costs. Therefore, there is a trade-off between preparing data for ML algorithms for analysis and preserving the privacy of participating users. More robust research is needed to address all of these and many other challenges adequately [17]. Besides, regardless of the ML applications in defending networks against malicious activities, these systems can also be vulnerable to intrusive points. Deploying attacks against ML technologies to misguide them and falsify the decision-making system is called Adversarial Machine Learning (AML). Adversaries can interrupt these techniques in different phases, including training or testing. This can increase the risk of being disrupted by adversaries and cause irrecoverable social and financial damages to the energy system. Therefore there are still several open questions to be answered in SG's security and privacy, and the need for a comprehensive study on this field is reinforced. The driving motivation for this study is to answer the following questions:

- What is the concept of SG, its components, related technologies and requirements?
- What are the security and privacy requirements of SG, and what are the current security and privacy issues?

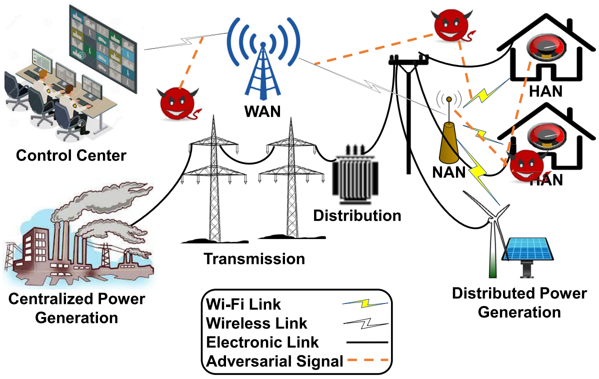

**FIGURE 2.** Possible smart grid communication attacks. HAN = home area network; NAN = neighbour area network; WAN = wide area network.

- Are attack schemes and threat categories associated with different SG services from both security and privacy perspective?
- What are SG's current security countermeasures, how does each one stack up against another, and what are their challenges and limitations?
- What role does ML play in the security of SG, and what vulnerabilities are associated with these models.
- How emerging technologies affect the security and privacy of future power networks?

To the best of our knowledge, there is a lack of a comprehensive review work that has studied and summarised all the current security and privacy attacks in SG by focusing on both conventional and novel ML-based techniques. The aforementioned questions motivate the current work to review the SG security and privacy issues, traditional solutions, and ML algorithms' contribution from both attacks and countermeasures perspectives. For ease of reading, in Table 1, we list all abbreviations used in this paper.

*Survey Organisation:* The remainder of the paper is organised as follows. In Section II, we make a comprehensive comparison between previous security and privacy-related surveys published in the literature and the scope of our work. In Section III, we present an introduction to the SG concepts, their architecture, and components, also briefly discuss SG communication infrastructure. In Section IV, we focus on the security and privacy requirements of the SG. Section V introduces various security attack scenarios and attack models threatening the SG security requirements. This section is followed by concentrating on novel attack models resulting from the integration of ML technologies and SG applications. Section VI, discusses some conventional and new countermeasures introduced to mitigate security issues in SG. In Section VII, we discuss the privacy threats in the SG system and classify attacks threatening consumers' private information. We provide the discussed solutions and countermeasures for SG customers' privacy attacks in Section VIII. Summary of observations, future research directions, and

**TABLE 1.** List of abbreviations and corresponding descriptions.

| Acronym | Description |
|---|---|
| SG | Smart Grid |
| HAN | Home Area Network |
| NAN | Neighbour Area Network |
| WAN | Wide Area Network |
| ML | Machine Learning |
| AI | Artificial Intelligence |
| DL | Deep Learning |
| AML | Adversarial Machine Learning |
| GAN | Generative Adversarial Networks |
| IDS | Intrusion Detection System |
| DSM | Demand Side Management |
| AMI | Advanced metering Infrastructure |
| SCADA | Supervisory Control and Data Acquisition |
| SM | Smart Meter |
| DER | Distributed Energy Resources |
| DA | Data Aggregator |
| RTU | Remote Terminal Unit |
| PLC | Programmable Logic Controller |
| HMI | Human Machine Interface |
| CIA | Confidentiality, Integrity, Availability |
| AAA | Authorisation, Authentication, Accountability |
| DoS | Denial of Service |
| DDoS | Distributed Denial of Service |
| FDI | False Data Injection |
| MITM | Man In The Middle |
| CDIA | Covert Data Integrity Assault |
| SVM | Support Vector Machine |
| JSMA | Jacobian-based Saliency Map Attack algorithms |
| MAC | Medium Access Control |
| PLC | Power Line Communication |
| SSE | Searchable Symmetric Encryption |
| L-BFGS | Limited-memory Broyden-Fletcher-Goldfarb-Shanno |
| MLP | Multiple Linear Regression |
| NN | Neural Network |
| FNN | Feed-forward Neural Network |
| DBN | Dynamic Bayesian Network |
| DRN | Distributed Random Forest |
| KNN | K-Nearest Neighbourhood |
| NB | Naive Bayes |
| ENN | Extended Nearest Neighbourhood |
| RF | Random Forest |
| PCA | Principal Component Analysis |
| DT | Decision Tree |
| RNN | Recurrent Neural Network |
| CNN | Convolutional Neural Network |
| GN | Generative Network |
| DN | Discriminative Network |
| TDMA | Time Division Multiple Access |
| RTT | Round Trip Time |
| RSS | Received Signal Strength |
| MTD | Moving Target Defence |
| BDD | Bad Data Detection |
| PASS | Privacy Preserving Authentication Scheme |
| HMAC | Hash-based Message Authentication Code |
| 5G | $5^{th}$ Generation of Mobile Internet |
| HetNet | Heterogeneous Network |
| D2D | Device to Device |
| MIMO | Multiple Input Multiple Output |
| SDN | Software Defined Network |
| IoT | Internet of Things |
| FL | Federated Learning |
| V2V | Vehicle to Vehicle |
| RSU | Road Side Unit |
| V2I | Vehicle to Infrastructure |
| V2G | Vehicle to Grid |
| V2N | Vehicle to Network |
| V2P | Vehicle to Pedestrian |
| V2D | Vehicle to Device |
| V2X | Vehicle to Everything |

the conclusion of survey are presented in Section IX and X respectively.

## II. REVIEWING RELATED SURVEYS AND THE SCOPE OF THIS SURVEY

We begin this section by discussing the related SG surveys addressing the security and privacy in Section II-A. Such analysis helps us to define the scope and contributions of this paper in Section II-B.

### A. STATE OF THE ART SURVEYS ON SMART GRID SECURITY AND PRIVACY

Several survey papers address the security and privacy challenges of the SG communication network. This section provides a comprehensive study and comparison between previous surveys' contribution and their methods, which can determine the motivations of this article. Our study mainly covers surveys published from 2012 to 2021, focusing on SG with a security and privacy perspective.

In 2012, Liu *et al.* [15] analysed the cybersecurity and privacy challenges of SG. They made a comparison between SG as a cyber-physical system and other information technology networks. Also, authors in [11] analysed the background and potential requirements of SG for security and privacy features, architecture design, and challenges. However, various attack definitions, comparisons, and classifications were missed in these works. Also, there has been significant developments in methodologies literature acquire to ensure that SG is a secure and reliable system since 2012.

Wang and Lu [18] presented a comprehensive overview of SG communication network architecture, its features, and protocols. They first defined generation, transmission and distribution domains in the SG and various attacks which target each domain's subsystems such as SCADA, AMI, and HAN. Then, this work is followed by security countermeasures consideration. However, this work did not consider privacy issues and SG requirements.

In [19], the authors reviewed the security issues, challenges and solutions between SG and the smart home environment. They presented different interaction scenarios for smart homes and SGs and classified the threats against these interactions as low, medium, and high based on their degree of impact. Possible security countermeasures were also considered but have not been thoroughly evaluated. Finally, they reviewed the standardisation activities related to the SG security framework.

A data-oriented survey on SG security was provided by Tan *et al.* [20]. They assessed the security and privacy needs of data packets, challenges and countermeasures throughout their lives, from data generation to acquisition, storage and processing. The paper considers the three primary data sources in SG, power generation, power transmission/distribution and load management system, including components and subsystems. In this survey, various data collection technologies, from short-range to broadband, were examined. For data processing cases, the paper studies three crucial use cases of SG in which data is processed for demand response, state estimation, and energy theft detection.

Additionally, SG security has also been studied within the cyber-physical framework in several review papers. The SG is arguably one of the most complex and robust cyber-physical systems distributed internationally [32]. Considering SG as a cyber-physical system, the authors in [21] first reviewed SG security terms from this perspective. Next, they identified attacks on the markets of generation, transmission, distribution of electricity, respectively. They also provided three basic security mechanisms: (*i*) protection, (*ii*) detection, and (*iii*) mitigation. However, the survey underestimated the importance of SG on consumers' privacy. Cao *et al.* in [30] surveyed the network attacks on cyber-physical systems such as SG. This paper proposed a different classification model for attack categories, including *i*) network attacks on the perception execution layer such as nodes, sensors and actuators. *ii*) Network attacks on the data transmission layer and *iii*) network attacks on the application layer. Defensive strategies per each attack category were also investigated. However, this paper had only a physical perspective toward the security of SG and did not study cyber-attacks comprehensively. The privacy challenges, attacks and solutions were also not considered. A recent survey on the cyber-physical security of SG has been done by [31]. This paper concentrates more on the physical layer of SG and provides a generalised state-space model for SG. Both cyber-physical threats and defensive solutions also are represented in this state-space model. This paper classifies attacks into four categories based on the cyber-physical attacks and their targets, including (*i*) data availability attacks, (*ii*) control signal attacks, (*iii*) measurement attacks, and (*iv*) control signal measurement attacks. However, the paper does not fully address privacy issues, and the ML contribution section has been investigated shortly.

Finster and Baumgart [22] discussed customer privacy-protection of the metering system of SG in detail. They first identified two main issues related to privacy in smart metering, including (*i*) metering for billing and (*ii*) metering for operations. Then specific privacy solution methods for both scenarios, including data aggregation with and without a trusted third party, anonymisation or pseudonymisation, have been studied, compared and evaluated. However, this work took into account privacy issues without security considerations.

The next paper proposed by Ferrag *et al.* [23] also focuses on the privacy preservation study of SG. They reviewed the relevant literature from 2013 to 2016. They highlighted five-class classifications for privacy-preserving schemes as (*i*) SG with the advanced metering infrastructure, (*ii*) data aggregation communications, (*iii*) SG marketing architecture, (*iv*) smart community of home gateways, and ($V$) vehicle-to-grid architecture. Besides, another classification was provided to more accurately represent privacy attacks as (*i*) key-based attacks, (*ii*) data-based attacks,

**TABLE 2.** The comparison among other surveys related to Smart Grid security and privacy issues. The symbol ✓ indicates a publication is in the scope of a domain; ✗ marks papers that do not directly cover that area.

| Survey | Comparison Criteria | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Security Issues | Privacy Issues | Security Countermeasures | Privacy Countermeasures | Attack Classification | ML Technologies | AML | GAN |
| [15] | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ |
| [11] | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ |
| [18] | ✓ | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ |
| [19] | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ |
| [20] | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ |
| [21] | ✓ | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ |
| [22] | ✗ | ✓ | ✗ | ✓ | ✓ | ✗ | ✗ | ✗ |
| [23] | ✗ | ✓ | ✗ | ✓ | ✓ | ✗ | ✗ | ✗ |
| [14] | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ |
| [24] | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ |
| [25] | ✓ | ✗ | ✓ | ✗ | ✓ | ✓ | ✗ | ✗ |
| [26] | ✓ | ✗ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ |
| [27] | ✓ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ |
| [28] | ✓ | ✗ | ✓ | ✗ | ✗ | ✓ | ✗ | ✗ |
| [29] | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ | ✗ |
| [30] | ✓ | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ |
| [31] | ✓ | ✗ | ✓ | ✗ | ✓ | ✓ | ✗ | ✗ |
| **Our work** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

(*iii*) impersonation-based attacks, and (*iv*) physical-based attacks.

In 2018, El Mrabet *et al.* [14] conducted a cybersecurity review of SG concepts after providing an overview of SG features, concept models, systems, and protocols. They studied the security attack cycle, including four steps: reconnaissance, scanning, exploitation, and maintain access. Classifications are also designed with different attacks at each point in the cycle. They presented a three-phase security strategy in terms of pre-attack, under-attack and post-attack states. An overview of each step and related interactions were also studied. Despite a comprehensive review of security concepts, little attention has been paid to privacy issues.

Recently, the authors in [24] provided a comprehensive review of security and privacy concerns of smart metering infrastructure in SG. Besides, a threat taxonomy was designed and presented. The taxonomy considered 1) system level, 2) service theft, and 3) privacy threats in SG.

The authors in [25] also studied the Internet of Things (IoT) based SG, threats, and countermeasures. They classified attacks based on targeted security criteria and network layers.

However, none of the above surveys considered ML techniques to attacks and countermeasures. There is a minimal investigation into SG security and privacy issues in the concept of ML.

Haque *et al.* [26], represent a short survey on ML algorithms' contribution in attack generation, detection and mitigation schemes for SG. This survey exclusively concentrate on ML technologies from both defensive and adversaries' points of view. Also, in [27], the general ML and Deep Learning (DL) techniques and security applications in the concept of SG were surveyed. Moreover, within [28], the authors attempt to investigate the emerging challenges of cybersecurity in the SG. The main focus of this work is on cyber-attack detection and mitigation methods, from data-driven solutions toward state estimation methods and AI-based countermeasures. Nevertheless, this paper does not investigate various attack categories threatening SG. Also, they did not address the privacy issues of these networks.

In 2021, Prasad *et al.* [29] discussed the recent approaches toward SG network communication, security and privacy challenges. This chapter comprehensively investigates different wired and wireless technologies integrated into the communication network of SG. Besides, they present a brief discussion of the security and privacy concerns of SG. From the ML point of view, this chapter only considers supervised and unsupervised algorithms and lacks in-depth investigation in this area. Finally, the hardware approach is followed, and the authors evaluate the cabling and network hardware issues in SG.

Thus, despite all the tremendous research efforts reviewed in this paper, security and privacy are still open SG challenges. Table 2 provides a comprehensive comparison among the previous survey papers in the same field, their contribution, and our work scope.

### B. THE SCOPE OF OUR SURVEY AND CONTRIBUTIONS

This paper presents a comprehensive survey on SG communication architecture, focusing on security and privacy threats and countermeasures. Inspired by the increasing use of ML algorithms in different scales of SG, our survey also conducts attention on ML-based security solutions and vulnerabilities emerging from these technologies. Although several surveys and reviewing papers on SG security and privacy issues exist, a study considering SG and ML simultaneously from a protection and attack perspective is missing. We summarise our main contributions as follows:

1) First, after presenting a thorough background for understanding SG, we provide a comprehensive picture of the SG's security and privacy requirements and the vulnerability points that threaten the SG components.
2) Second, we present a comprehensive study on the security attacks and malicious activities that sabotage the

system. This includes both traditional attacks inherited from wireless technologies and novel AML-based ones, which result from ML technologies integration into the applications of SG.

3) Third, we investigate several conventional and novel security countermeasures discussed in the literature to protect networks' components. We try to have an analytic perspective and explore the effectiveness and shortcomings of each technique.
4) We also attempted to have a more detailed investigation into the privacy challenges of the SG as well. We discussed possible privacy-violating activities which threaten the customers participating in the SG system. We then present detailed taxonomies of the discussed security and privacy attacks threatening SG, with a more detailed classification of each attack and the network requirement it sabotages.
5) Finally, we describe several open challenges and future research directions in SGs, focusing on security and privacy issues that arise with emerging industries and networking paradigms.

Comparing this survey to other reviewing papers, this is the first time that the security and privacy issues of SG are examined from both a conventional vulnerability perspective and the perspective of emerging ML-based adversarial threats. All in all, we aim to open a door toward a much more reliable network and raise the system's capability in terms of detecting and mitigating possible threats against the SG system.

## III. SMART GRID: AN OVERVIEW

The main structure of the current electricity grid was designed, implemented, and operated almost a century ago. This old power grid lacks a solid, efficient and scalable structure and is not conducive to sustaining 21st-century lifestyles and increasing energy demands [33]. Energy demand is growing exponentially, and fossil fuel resources are depleting. Climate change and greenhouse gas emissions are also becoming serious global issues. Consequently, the world is moving toward consuming more renewable energy sources. Renewable energies, however, cannot be integrated into the current network due to the unidirectional power flow in the old network and the random nature of renewables. The integration of distributed and green energies can create a reverse power flow from the consumers to the network [34], which introduces more complex power measurement problems. Additionally, consumers in the conventional grid are entirely passive, and there is no active, interactive interaction between them and the supplier. Likewise, traditional power grids cannot provide real-time information about network conditions and track users' electricity consumption [35], [36].

All of the above challenges and much more motivate governments, industry, and academia to modernise the energy supply system, i.e. SG. SG provides the possibility of smooth integration of sustainable energy sources and automated, reliable monitoring of the entire power system. Enabling a seamless flow of information can optimise energy generation, consumption, and waste [37].

An SG is a complex system with different components that work together to meet expectations, such as reliability, efficiency, and adaptability. Communication infrastructure, Advanced Metering Infrastructure (AMI), Demand Side Management (DSM), and Supervisory Control and Data Acquisition system (SCADA) are some critical components of SG [38].

### A. SMART GRID COMMUNICATION INFRASTRUCTURE

The SG's communication infrastructure should support a ubiquitous data transformation that is heterogeneous, massive in volume, and different in terms of requirements and services. This infrastructure is a hierarchical network with several subnets [39]. Communication infrastructure of SG can be divided into *three* distinct networks, Home Area Network (HAN) [40], Neighbour Area Network (NAN) [41], [42], and Wide Area Network (WAN) [43]. Each domain is made up of several components and requires exclusive technologies.

#### 1) HAN

HAN belongs to customer entities, and it is a contribution of sensors and measuring devices implemented over smart devices at consumer endpoints. Smart meters (SM) are essential components of the system. They are digital meters with microprocessors connected to communication panels and communicate as a gateway, connecting consumers and grid suppliers. The SM collects the energy consumption information of the customers. This information is utilised for real-time pricing, demand forecasting, and energy management. SM also displays control information and online energy billing to the consumers. Therefore, SMs are intermediaries that connect customers and energy providers. HANs usually cover a residential area up to 200 $m^2$ and support short-range communication technologies from 10 to 100 kb/s.

#### 2) NAN

This network aggregates SM information of neighbourhood consumers and is responsible for building up communication between network users and energy suppliers. The number of SMs interconnected to the network depends on grid topology and communication architecture. Critical data from controlling commands to real-time data inception and a probable failure message is exchanged on a NAN basis.

#### 3) WAN

WAN acts as the backbone of the SG communications. It creates a link between the concentrators, control centres, power plants and distributed energy sources. The network provides comprehensive control and monitoring of electricity generation, transmission and distribution, and covers a wide geographical area with thousands of connected devices. The WAN requires long-term technologies with a maximum data exchange capacity of 100 Mbps, as it is responsible for long-term communication of large volumes of data.

Although the integration of communication technologies can bring numerous opportunities, it can also cause various challenges. For example, vulnerability to cybersecurity attacks can be inherited from communication technologies to the grid, which can be considered a fundamental concern. Furthermore, using IP-based data wireless communication technologies within the grid means the SG can be as assailable as the Internet, which provides notable supremacy for attackers.

### B. SMART GRID ADVANCED METERING INFRASTRUCTURE

SMs are responsible for measuring power consumption in the consumer environment and act as interfaces to provide users with their consumption information and energy patterns. As SMs are distributed over a wide geographic area and are usually far from utility providers, Data Aggregators (DA) route the SMs information to the utility. The DA, also known as the data concentrator, collects multiple SMs data via NAN and sends the collected data to providers via WAN. The contribution of some of SM's neighbours, user panels, and data concentrators creates the SG metering network also known as the *AMI*. AMI, is a distributed network of measuring devices responsible for collecting, measuring and processing energy, water and gas consumption of network entities [14]. The structure of the AMI is shown in Fig. 3. AMI provides a bridge between the customer and the distribution domains and provides two-way communication between the meters and the SG distribution domain. With the help of online information flow [44], any outage or fault can be reported directly to the operators without the customer's intervention. Power quality can be controlled remotely, and large companies can offer time-based pricing policies to control peak hours. This is also considered a DSM technology [45]. AMI is also responsible for connecting small Distributed Energy Resources (DERs) to more extensive networks. The widespread integration of wireless communication technologies in AMI raises security and privacy concerns. Several attack scenarios can be performed on AMI. For instance, attackers can study consumers' power consumption patterns to extract information, plan malicious activities, send faulty commands to the system, shut down or access maliciously to SMs to change electricity prices for their benefit [46], [47].

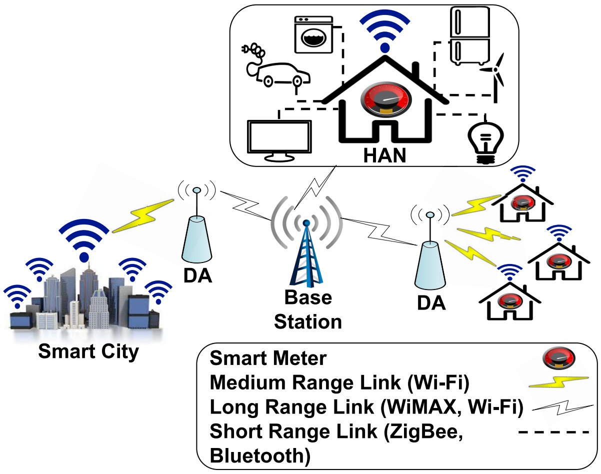
HAN
DA
Base Station
DA
Smart City
Smart Meter
Medium Range Link (Wi-Fi)
Long Range Link (WiMAX, Wi-Fi)
Short Range Link (ZigBee, Bluetooth)

**FIGURE 3. Advanced metering infrastructure. HAN = home area network; DA = data aggregator.**

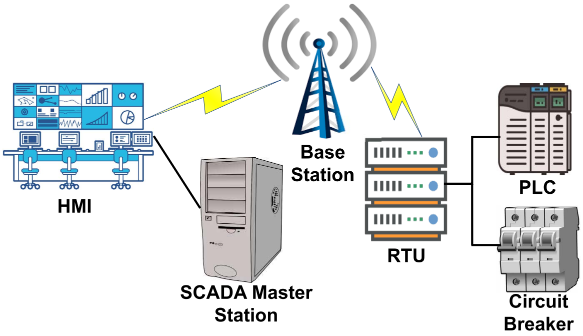

**FIGURE 4. SCADA system. HMI := human machine interface; RTU = remote terminal unit; PLC = programmable logic controller.**

### C. SMART GRID SUPERVISORY CONTROL AND DATA ACQUISITION SYSTEM

The power generation and transmission domain is controlled and supported by a pervasive system called SCADA [48]. SCADA is a centralised monitoring subsystem responsible for monitoring power generation and transmission process. It is a well-known control system in the conventional power grid and industry [37]. The SCADA system belongs to the scope of operation and includes several components such as master stations, Remote Terminal Units (RTUs), circuit breakers, Programmable Logic Controllers (PLCs), a communication network, and Human Machine Interfaces (HMIs) system [49]. Fig. 4 presents the overall architecture and essential components of SCADA. The SCADA system is one of the essential elements of the SG infrastructure because it can provide the opportunity to repair the grid itself with the remote control of the system performance. In addition, SCADA provides distance switching, circuit breaker, relay adjustment and power regulation [50]. It can also increase the system's resilience against possible attacks as it enables instant functionality for operators. SCADA decreases the operation and maintenance costs of the SG while optimises its assets [51]. By connecting communication technologies to the grid, SCADA can also connect to other subsystems via the Internet or other communication links, increasing its susceptibility to various attacks [52]. An adversary can attack SCADA in different ways. One of these attacks is to forge control and supervisory commands. It can cause circuit breakers and controllers to be incorrectly activated or deactivated or traffic to spread [53]. A well-known and devastating cyber-attack occurred in Ukraine on December 23, 2015, when hackers infiltrated Ukraine's SCADA system and remotely opened some circuit breakers in the power distribution domain. This led to a prolonged and widespread blackout that caused severe economic and social damage. This attack showed how important it is to protect the grid and its substations [54].

## IV. SECURITY AND PRIVACY: REQUIREMENTS IN SMART GRID

This section discusses SG security and privacy requirements and the required criteria for designing a secure SG system. SG security and privacy requirements must be carefully studied to design a comprehensive security architecture to protect SG from potential threats.

### A. SECURITY REQUIREMENTS OF SMART GRID

Generally, to protect the information in any system (such as SG), specific requirements must be fulfilled, including confidentiality, integrity and availability. This criterion can be described as follows:

- ***Confidentiality***: Confidentiality protects the data from unauthorised disclosure and restricts access to valid users only [55]. Confidentiality is essential both for service providers and for customers. Any unauthorised access to SG's operational data can let adversaries identify networks' vulnerability points or get privileged access to the system and perform malicious activities. The SG is responsible for protecting consumers' private information. Any disclosure of information could seriously endanger their privacy [56], [57].
- ***Integrity***: Integrity guarantees the accuracy and consistency of information and protects the data against any anonymous modification, destruction or loss [58]. Any tampered message injected into the SG can interrupt the system functionality. Critical decisions are taken based on measurements and data collection from the SG environment, such as power generation and pricing policies. Any unauthorised modification of this data can challenge the regular operation of the system.
- ***Availability***: A reliable network must be available for any permitted user [55]. In terms of the SG, high availability is one of the system's major objectives [59]; availability guarantees the reliability of the grid. SG enters various society sectors from industry to medical services, transportation education, and customers' household. Lack of services in such critical infrastructure can cause significant financial and social damage.

These are fundamental security requirements of any information related system and are abbreviated as Confidentiality, Integrity, and Availability (CIA) triad. When it comes to the SG however, the CIA triad is prioritised as AIC to emphasise the importance of the SG availability [60].

### B. PRIVACY REQUIREMENTS OF SMART GRID

Privacy in SG can be described as considering customer preference in terms of revealing their personal information or consumption diagram. Privacy is another major challenge for the SG, specifically for AMI confidentiality on the customer side [61]. Complete preservation of the life and property of consumers should be guaranteed by suppliers. Some potential privacy leakage consequences of SG systems include Identity theft, personal information leak, password exposure, determination of specific assets or appliances used by customers, etc. Mining consumers' energy consumption information can leak critical information on users' lifestyles and daily activities. For example, how many people live in a house, what they are doing, their everyday activities and plans. Several actions have been taken to guarantee the data secrecy of all energy premises. SG's basic privacy requirements can be discussed as Authentication, authorisation, Accountability, indicated as *AAA* protocol.

- ***Authentication***: Authentication models control access to the system and assure the true identity of communication parties. It is always necessary to integrate a reliable authentication scheme into the communication system to protect the transmitted data [62]. SMs as measuring devices and machines in SG are accessible by different parties and communicate regularly together. This communication can be authenticated through different secret keys exchanged between two parties. However, adversaries can masquerade themselves as legitimate users or service providers to access the network and interrupt the service [63]. Authentication techniques and security key schemes have been widely investigated in the literature. At the same time, the most prominent among these are anonymity and untraceability [64]. Fouda *et al.* [65] propose a lightweight message authentication model to gain communication trust in SG. Recently, in [66] an efficient privacy-preserving authentication scheme has been proposed for customer data in SG. This model achieves both data source and aggregation authentication.
- ***Authorisation*** : Authorisation guarantees parties' access privileges in the network to different resources based on their identity and policies. The first step in most security mechanisms is authentication, and the second step is an authorisation. Any unauthorised access to the SCADA system can cause sabotage damage to the system. The attacker can remotely control circuit breakers or RTUs and send faulty commands to disrupt the whole or a part of the network [67]. In [68], a mutual verification system for the authorisation and authentication of users was proposed. This model uses feature-based access control to verify the user's identity and role dynamically. This model can defeat multiple attacks and is an efficient model in computing and communication.
- ***Accountability***: Accountability means that every action on the network can be tracked and guarantees the responsibility and liability of the network [52]. Information about system status and activities is recorded to be available in case of demand. Accountability is required to ensure the privacy, integrity and confidentiality of the SG [60]. One of the essential characteristics of SG is the contribution of households to the electricity market. The SMs installed in each premise can provide detailed information on the consumption pattern, accurate prices, and the bill's total amount. However, this information may be inconsistent with the bills provided by small companies due to attacks. This can reduce the accountability of the SG to households [69].

## V. SECURITY: ATTACKS IN SMART GRID

In this section, we first provide details of security attacks on SG. Specifically, we explain some prominent attack technologies dealing with network vulnerabilities. Then, in Section V-B2, we outline novel attacks that threaten SG systems. These attacks are caused by ML-based technology embedded in several SG applications.

Threats targeting SG can be physical threats such as theft or tampering with equipment, environmental threats such as severe weather and natural disasters, and cyber threats. Cyber-attacks are the main contribution of this paper, and these attacks aim to manipulate, sabotage or espionage the system through interrupting the communication infrastructure of the SG [70]. Cyber attacks operate in two different modes, including passive attacks and active attacks. Here are some brief illustrations of each.

### A. PASSIVE ATTACKS

These attacks aim to gather information about the network operation and communication entities and does not destroy the connection between authorised users. These attacks are difficult to detect, so the network must come up with prevention strategies. Passive attacks can threaten network confidentiality. Two well-known passive attacks are eavesdropping and data analysis. The authors of [71] proved that the SG components are relatively weak in the fight against eavesdropping. They did this by exposing the hardware, software, and network configuration components to attacks and analysing their vulnerabilities.

### B. ACTIVE ATTACKS

Attacks categorised in this group mean to disrupt the network performance, communication between users, and data transmission over the network. Active attacks mostly violate the availability and integrity of the network. These attacks can interrupt the system functionality and cause severe economic loss and even short or long blackouts. Also, a large group of active attacks aim to modify the data (e.g., operational, controlling, monitoring and billing information) transmitted via the network. Any unauthorised access and change of this data can cause several challenges in different domains of the system.

In the following section, we present an overview of some of the most prominent attack strategies targeting various SG services. We provide a taxonomy to classify the reviewed attacks according to the security requirement they threaten.

#### 1) CONVENTIONAL SECURITY ATTACKS CLASSIFICATION IN SMART GRID

The SG is the target of a large number of attacks. Some were inherited from the integration of communication technologies, and some were explicitly designed for the SG. These attacks can endanger the grid integrity via tampering its critical data or compromise its availability by exposing latency to delay-sensitive information and affecting confidentiality by hijacking the information of both customers and electrical market [72]. Fig. 5 illustrates the proposed taxonomy which characterises each attack category to the service it violates. To facilitate comprehension of these attack scenarios, we present a comparison of their mode, primary target, and goal in Table 3.

- ***Eavesdropping & Traffic Analysis***: Eavesdropper is a passive attacker that secretly connects to the system and does not make any observable changes. Eavesdropping is a network attack and compromises the confidentiality of data traffic over the network. This can be a significant vulnerability to data disclosure on network architecture, topology, and components in AMI, SCADA and different sections of SG [73]. By listening to devices on the network and listening to SCADA components such as sensors and RTUs, an eavesdropper can access important system data [74]. If an attacker analyses the leaked information to extract data patterns, a traffic analysis attack occurs. This data can be users' personal information or network performance, and supplier policies. A traffic analysis attack can be the first step in planning other types of attacks.
- ***Denial of Service (DoS)***: One of the most devastating attacks against the SG communication network is DoS. DoS attacks mainly aim to disrupt the system functionality by exhausting network resources and violating network availability. By frequently sending meaningless requests to system components, a DoS attack prevents their normal processing behaviour. These devices cannot distinguish useless applications from normal ones; their storage and network bandwidth are occupied with many requests. As a result, the system may be unavailable for legitimate users due to a DoS attack. Distributed DoS or DDoS is when more than one adversary exists to threaten the network.

  Many devices and users are penetrating the SG system, which increases the risk for DoS and DDoS threats dramatically. The severe impact of the DoS attack on the load frequency control system of SG was studied by [75]. They modelled the power system state space under the DoS attack as a switched system. In this model, the DoS attack is formulated as a switch operation (on/off) in communication channels. This is due to the unavailability of sensing channels in the event of a DoS attack. In this case, they proved the devastating effect of DoS on the dynamic performance of the power system. Later, in [76], a new DoS attack against AMI was proposed in SG called puppet. The puppet attack scenario is as follows, one of the normal nodes selected as the intruder's puppet. When the puppet receives attack packets from the attacker, it is under his control and is flooded by several packets unless the network is occupied and out of service. Simulations show how puppet attacks can reduce AMI performance. A DoS attack scheme is presented in [77] to disrupt the SG state estimation. In this model, the attacker tries to prevent the system from receiving or transmitting important information. This can be done by jamming the signal or a blackhole strategy, in which the attacker drops or encapsulates messages sent or received from a node.

- ***Jamming***: The jamming attack scenario attempts to reduce the available spectrum for legal users of the network. Jamming attack reduces the signal-to-noise ratio significantly through radiation of malicious electromagnetic signals to occupy the system bandwidth. The jamming attack can be considered one of the DoS attack samples, as it can disrupt the system for providing service [78]. Data collected from all sensors, SMs and AMI devices under analysis are reported to service providers for state estimation and power pricing. If this reporting follows a static and scheduled pattern, an attacker can access the pattern and jam the communication interface [79]. A jamming attack against a state estimator can cause incorrect power pricing and decrease the reliability of utilities. Ma *et al.* [80] described an attack scenario in which the attacker jams a limited number of signal channels carrying measurement data. I this work, the attackers aim to change the locational marginal energy price and obtain profit.
- ***False Data Injection (FDI)***: The state estimator is a critical part of the SG energy control system and is responsible for evaluating the grid's state variables, voltage magnitude, angles, and load. It is about minimising error estimation and working with the Bad Data Detection (BDD) system to detect any abnormal data measurement trends [81]. FDI is a destructive cybercrime that mainly threatens these fundamental state estimation operating modules. The primary purpose of this attack is to change the original data to mislead the system [82]. Modified data is injected into the SG for various purposes such as power theft, load reduction, delay, or data blocking [83]. Information manipulation in energy consumption is one of the most common attacks on the energy measurement system. The adversary's goal is to report fake data to pay less for their electricity consumption or force others to pay more [84]. Liu *et al.* [85] are one of the pioneers in addressing this topic. They presented FDI attacks from the attackers' point of view. The attacker injects manipulated measurements to mislead state estimations and bypass existing BDD systems. They also examine two realistic attack models. Later, in [86], Lo *et al.* defined a new type of FDI attack, the Combination Sum of Energy Profiles (CONSUMER). In this scenario, a malicious user breaches his neighbours' SMs and intends to reduce his consumption bill by increasing the neighbouring SMs readings. They proved that this attack is not detectable with BDD. FDI attack model with the aim of price manipulation is presented in [77]. In this attack model, the attacker aims to change the electricity price in two critical time slots. First, the attacker has the power to raise the price when the price is low; this will, in turn, cause consumers to reduce usage and cause an over-generation of electricity to be wasted. Second, an attacker might also display a price that is lower than what the market costs. Due to low prices, the energy demand increases; this model can cause even more losses, leading to generators' exhaustion and line failure.
- ***Man In The Middle (MITM)***: The next most common type of attack involves a MITM attack. A cyber-attacker puts himself in a conversation between two legitimate hosts and prevents the parties' normal interaction. The MITM attacker can eavesdrop on the communication and access to information or impersonate both entities and alter the data transferred in the conversation. Therefore as a MITM perpetrator intrudes on the network, he can also inject false data into the system. MITM can compromise security criteria such as confidentiality through eavesdropping, integrity through modification or loss of packet, and availability by disrupting the overall connection [87]. The MITM attack is also one of the most devastating attacks, mainly threatening industrial remote control components under SG surveillance systems [88], [89]. It should be noted that a MITM attacker needs high computing capabilities to launch an attack [90]. In order to conduct a MITM attack, the attacker must first gain access to the supervisory network by compromising an internal server. The next step will be to implement traffic diversion so packets can be accessed in both directions [91]. In [92], the authors launch a MITM attack after simulating the SG on a real testbed. The MITM attacker in this work discontinues the connection between the metering unit and the electronic devices. Placing as the intermediate, the attacker can modify the information flow by delaying or manipulating the data packets between metering and consuming devices. The simulation results revealed that the attacker could hide the voltage fluctuations and faults from the controllers by replaying recorded data. Wlazlo *et al.* in [93] performed four multi-step MITM attacks that hijacked SCADA communication protocols such as DNS3 in SG. These attack frameworks are designed to inject false data and false commands into an emulated synthetic power grid.
- ***Message Replay***: Replay attacks are similar to MITM attacks in their procedure and requirements [91]. After being well placed between two communication parties, the attacker captures an authorised recently transmitted message and resends it in different time slots [94]. Because the fake data is close to benign, the state estimation and detectors cannot detect the intrusion. Message replay occurs when an attacker accesses the SM's processor and can send commands to the system. An adversary needs to extract information from consumer appliances and SMs by analysing the data transmitted between them. In this regard, forging an electric bill to reduce its reported consumption can benefit a household at the expense of the utility provider [95]. Zhao *et al.* [96] defined the replay attack scheme in which the attacker secretly penetrates the network with the aim of message replay attack and records system measurements for a while. Then the attacker starts

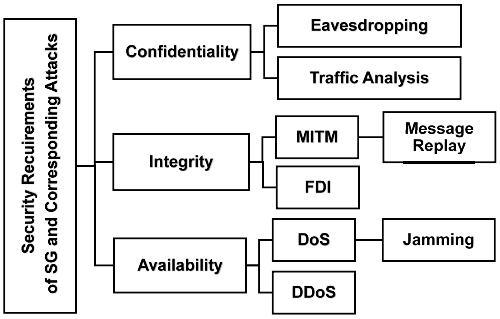

**FIGURE 5.** Security requirements and attacks targeting smart grid.

changing current measurements with previous measurements and injecting them into the network over and over again [96]. This can lead to incorrect energy pricing or incorrect forecasts for power generation actions. Because the modified data follows the same network strategy, traditional BDDs cannot detect the attack well.

### 2) MACHINE LEARNING-BASED ATTACKS IN SMART GRID

ML algorithms use statistical schemes to create semi-intelligence and prediction capabilities for systems without human interactions [99]. ML techniques work by feeding data into a computer algorithm and training it to extract patterns from data, predict or classify them through confidential information in training data [100]. Some available ML algorithms include: supervised (predictive), unsupervised (pattern discovery), semi-supervised, and reinforcement ML algorithms [101]. ML techniques have been widely used in different applications of SGs, from controlling and monitoring power systems to abnormally diagnosis and attack detection due to their high effectiveness, precision, and accuracy [102]. Resource management [103], usage pattern prediction [104] and attack detection, spam filters and malware activities [102] are among ML applications. The main contribution of ML-based techniques for cybersecurity objectives was in attack and anomalous behaviour detection and classification, network risk scoring and optimisation of security analysis [100], [105].

Although ML algorithms are widely used in SG security, adversaries can use these methods to threaten the network also [100]. Unauthorised access to the system through password detection [106], malware production [107], and phishing, in which victims' personal information is disclosed through the collection of real data from their accounts or emails, are some ML-based attacks against cyber systems. Recently, Nawaz *et al.* in [98] proposed an ML-based FDI attack against the SG measurement matrix. This study tried to model the dependency variables, such as network voltage, current, real power, and reactive power, and construct attack vectors. Three methods have been considered for applying erroneous data to the measurement system, including linear regression, time-stamped linear regression, and delta threshold. These faulty samples were designed based on linearity between sensor measurements, partial linearity, and nonlinear considerations. Additionally, these attack models were tested against defence techniques such as BDD, AC state estimation, and Support Vector Machine (SVM). It has been shown that as the attack vectors increase in nonlinearity, defenders fail to detect these samples.

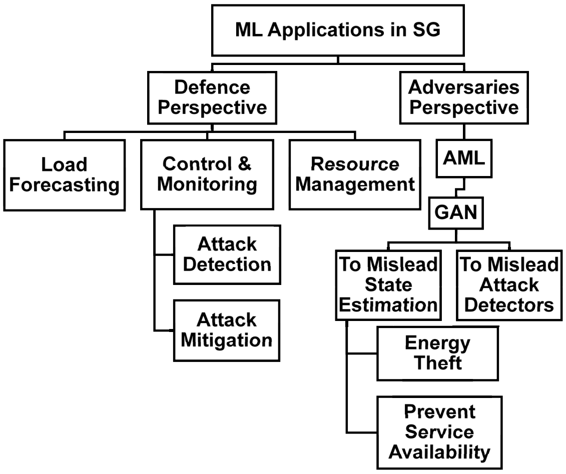

**FIGURE 6.** Machine learning applications in smart grid.

The ML techniques used in SG are also susceptible to a group of attacks called AML [108]. In AML, adversaries are also armed by ML systems and try to mislead the SG ML algorithms through injecting wrong inputs or alter the training samples to fool the learning system or deceive it to make wrong decisions [109]. ML-based applications of SG such as, load forecasting, energy pricing, attack detecting, and etc. are susceptible to AML attacks.

#### a: ADVERSARIAL MACHINE LEARNING

In particular, adversarial attack strategies can be classified into two basic classes: poisoning [110] and evasion attacks [111].

- ***Poisoning attack***: A poisoning strategy, also known as causative attack [112], attempts to falsify the ML algorithm during the training step by injecting wrong inputs [113] or model parameters [114].
- **Evasion attack**: In the evasion attack, attackers try to mislead the ML algorithm in the testing phase to make a wrong decision [115]. Fig 7 illustrates a schematic of the poisoning and evasion attack on a SCADA system.

There is also another classification method based on adversaries' knowledge. In this method, attackers are categorised based on their knowledge of the training dataset, learning algorithm, and samples [115]. The adversaries are classified as *white-box*, *black-box* and *grey-box* [116].

- **White-box:** In a white-box attack, the attacker has deep knowledge of the detection algorithm, classification technique, and system model. They know exactly the features, thresholds, and training parameters.
- **Black-box:** In contrast, a black-box attacker only knows the general terms of the detection model but does not know the exact parameters.

**TABLE 3. Smart grid adversarial security attacks.**

| Attack | Classification | Primary Component Targets | Attack Goal | Compromised Services | | |
|---|---|---|---|---|---|---|
| | | | | Availability | Confidentiality | Integrity |
| DoS/DDoS | Active | Load frequency control of SG [75], AMI [76], The state estimation disruption [77] | Disrupt the system functionality | ✓ | ✗ | ✗ |
| Jamming | Active | AMI and measuring data system [80] | Disrupt the services | ✓ | ✗ | ✗ |
| Eavesdropping & Traffic Analysis | Passive | AMI [97], RTUs and sensors in SCADA [74] | Gain information | ✗ | ✓ | ✗ |
| FDI | Active | State estimation [82], BDD [85], compromising neighbourhood SMs [86], Measurement system [98] | Manipulate data, Energy theft | ✓ | ✗ | ✓ |
| MITM | Active | SCADA system [89], SCADA communication protocols [93] | Unauthorised access, FDI | ✗ | ✓ | ✓ |
| Message Replay | Active | State estimation [94] | Unauthorised access to system | ✗ | ✗ | ✓ |

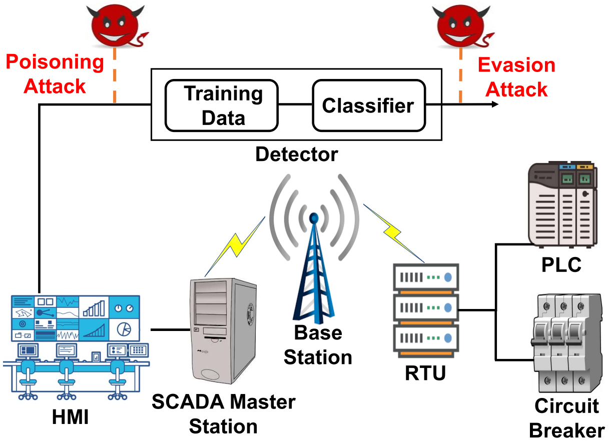

**FIGURE 7. Poisoning and evasion attack models in smart grid SCADA system.**

- **Grey-box:** Finally, in a grey-box attack, the attackers have limited information about the state of the system. Attackers are assumed to be aware of features and learning algorithms but not of training dataset and classification parameters [116].

Although AML models are new, these technologies have received considerable attention, and there are different literature investigating AML, its capabilities, and case studies in communication networks and the SG concept. However, this is an entirely new concept, especially in power grid applications. Therefore, we try to provide a holistic study on literature considering AML applications in SG from an adversaries perspective in the following. This includes attack scenarios designed to sabotage different SG services or sidestep decision making systems in SG.

In [115], the authors focus on the impact of poisoning and evasion attacks on the FDI detectors in the power state estimation system. They first considered an adversarial label flipping poisoning attack in which the attacker attempts to flip training labels to contaminate the learning process. Secondly, they studied an evasion attack model, the targeted fast gradient sign method, in which the adversary tries to make noise in the classification gradient direction of the model. Finally, the impact of adversarial samples on two supervised training algorithms, including SVM and Multilayer Perceptrons (MLP), was investigated. The results confirm how destructive these attacks are and how they could reduce the accuracy of detection systems. Sayghe *et al.* in [117] have made a further effort and tried to analyse the impact of adversarial attacks on DL-based algorithms, which are used to detect FDI attacks on power system state estimation. The impact of two kinds of adversarial attacks against the MLP has been examined: the Limited-memory Broyden-Fletcher-Goldfarb-Shanno (L-BFGS) and the Jacobian-based Saliency Map Attack algorithms (JSMA) [117]. Because adversarial samples are very similar to their actual samples, L-BFGS is an optimisation algorithm that generates values very close to specific input samples. In comparison, the JSMA attack attempts to create saliency maps. This visualisation map can identify which features must be effectively disturbed to achieve an adversarial target. The results demonstrate how these attacks can dramatically decline the accuracy of the FDI detection system.

Load prediction is essential for power suppliers. Utility companies rely on load forecasting data to adjust generation, increase efficiency and decrease energy waste. Liang *et al.* in [118] have considered an attack scenario in which the adversary tries to damage the accuracy of the load prediction while the poisoning attack has not been detected by surveillance systems using the attack strategy. Multiple Linear Regression (MLR) and Neural Network (NN) training systems were used as the detection models in this work. Then, the error rate was checked to evaluate the impact of the designed poisoning attack. The results showed that a poisoning attack could dramatically increase the absolute error rate. Besides [119], demonstrated the effect of JSMA on classification operation of supervised learning. To do this, they investigated the supervised models' performance in defending against AML for intrusion detection objectives in industrial control systems.

Similar work was done by Erba *et al.* in [120], they considered DL anomaly detection systems in industrial control systems. They considered two attack schemes, attacks against the integrity and ones against the availability of the systems. They attempted to trigger the detection schemes. In [121], an investigation is conducted on an event-cause analysis framework based on NNs for the power grid. These systems have also been studied in terms of their vulnerability to malicious data tampering attacks. This malicious data is aimed to cause limited disturbance on voltage or current data in the network. However, the results show that this minor disruption disables the network defence mechanisms to detect the mismatch. To obtain this misleading data, they used a fast gradient sign method proposed in [123]. Also, a defence

**TABLE 4.** Smart grid adversarial machine learning attacks. Ref. = reference.

| Attack Technique | Attack Class | Compromised Service | Attack Target | Attacker's Knowledge | Ref. |
|---|---|---|---|---|---|
| Adversarial Label Flipped Attack | Poisoning | State estimation | To decrease the FDI detection accuracy of SVM classifier | White-box | [115] |
| Targeted Fast Gradient Sign Method | Evasion | State estimation | To decrease the FDI detection accuracy of MLP classifier | White-box | [115] |
| L-BFGS & JSMA | Evasion | State estimation | To decrease the FDI detection accuracy of MLP classifier | White-box | [117] |
| Modifying temperature and load data | Poisoning | Load forecasting system | To reduce the accuracy of MLR based load forecasting system | Black-box | [118] |
| Jacobian–based Saliency Map Attack and Fast Gradient Sign Method | Evasion | Industrial control system | To defeat the MLP based IDS | White/Grey-box | [119] |
| Integrity and Availability | Evasion | Industrial control system | To reduce the accuracy of Deep-learning based anomaly detection | White/Black-box | [120] |
| Fast gradient sign method | Poisoning | Event caused analysis system | Misclassify the events | Black-box | [121] |
| Modify the meter's measurement | Evasion | Energy theft detection systems | To defeat three NNs based energy theft detectors (FNN, RNN, CNN) | Black-box | [122] |

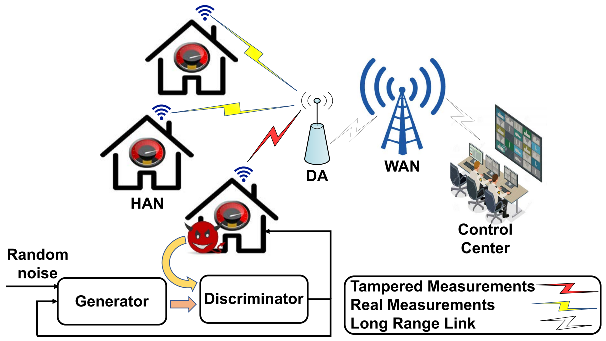

**FIGURE 8.** Energy theft attack based on GAN.

mechanism has been proposed to counteract the injection of manipulated data.

Energy theft is one major problem utility companies encounter around the world. It can cause considerable financial losses for energy suppliers. ML techniques are widely used to detect energy theft [124], [125]. Li *et al.* in [122] considered the accuracy of ML energy theft detection algorithms under well-constructed perturbations to verify inputs. To evaluate their work, they applied small fake measurements to three NN training algorithms, Feed-Forward NN (FNN), Recurrent NN (RNN), and Convolutional NN (CNN). The results demonstrate how energy thieves can bypass the ML-based detection systems. Table 4 shows the different AML attacks, their techniques and targets.

### b: GENERATIVE ADVERSARIAL NETWORKS

GAN [126] is an advanced ML technique that can extract a completely unknown probability from row data. GANs were initially thought of as unsupervised Deep NNs (DNNs) [126]. GAN generally consists of two major rival networks, Generative Network (GN) and Discriminative Network (DN). While the first one is fed through Gaussian noise and tries to generate fake data near the real version to deceive its rival, the second one tries to distinct the original data from the crafted one and minimise its detection error. This is very similar to the system scenario, GN acts as a malware attacker, and its purpose is to sabotage the network, and DN plays the role of the security system.

GAN methods have been widely used to generate synthetic data for various purposes. Public data security and privacy do not allow providers to access their information quickly. This is one of the significant problems with advanced learning techniques. ML algorithms are highly dependent on the volume of data they are trained with, so it is impossible to use these methods in a limited distribution system data set and analyse, predict or estimate possible outcomes. To overcome this problem, authors in [127] propose synthetic data generation with GAN. Maximum mean discrepancy analysis revealed that the probability distribution of the synthetic and real data are similar. It means the manipulated data are very similar to the actual samples.

In [128], a new technique for generating building electrical load information is proposed. The building's electrical charge profile has various applications in different areas, especially for the utilities to build grid interactions, load forecasting, and waste control. This approach follows three stages; firstly, they normalise customers' load profiles to 95% of the peak load annually to ensure the similarity of magnitude for different buildings. Then, the cluster load profiles into 19 groups using the k-means clustering algorithm. Finally, GAN generates the load profiles of each cluster [128]. Comparing the crafted data and the open-source Building Data Genome Project database in key features like mean, standard deviation, and distribution of critical parameters (baseload, peak load, peak load duration, rise time, and fall time) reveal the validation of the method. To generate large adversarial samples, Ying *et al.* in [129] recruited GAN to build adequate negative samples, built with predefined attacks to improve the training approach and the detection system performance. According to the results, this technique improved the efficiency and accuracy of the detection system nearly by 4%.

However, none of those mentioned above works investigated GAN-based attacks targeting the SG. This technology can be used widely by adversaries to sabotage the system. One of the pioneers in these terms were Ahmadian *et al.* [130]. The authors investigate injecting false data by the GAN into the RTUs, defeating the SCADA system, and obtaining profit from controlling the demand message. Also, the attackers try to be undetected by system detectors. On the other hand, the energy system operator aims to detect the FDI. In [131], a GAN-based poisoning attack is designed for energy theft purposes. They proved how easily ML algorithms could break through adversarial examples. To fool the detectors, a DNN-based GAN system was used to inject false data into the ML detectors to perform incorrect classification. The generator tries to build crafted data near the original one, and the discriminator tries to detect the tampered data from the real one. Fig. 8 illustrates an attack scenario in which a dishonest customer can manipulate his real information to reduce the amount of energy consumption measurements. The detectors on the control side can hardly detect this tampered data. We provide a taxonomy in Fig. 6 which shows different ML, AML and GAN applications in SG from both the defence and attack perspectives.

## VI. SECURITY: COUNTERMEASURES FOR SMART GRID

There is a three-phase security mechanism in communication and information systems, including prevention, detection, and mitigation. Prevention mechanisms use security models to prevent unauthorised access to critical systems. However, an attacker can still find a way to attack the system, and detection methods are used to ensure fast and reliable attack diagnosis. Finally, suppliers must consider the best ways to mitigate the damage in the event of a network attack.

This section tries to provide security countermeasures related to prevention and detection strategies for the attacks discussed in Section V. First, we study conventional and common techniques in cyber systems' security. Next, we try to investigate ML algorithm applications in securing SG. Finally, we individually review different attacks and various security techniques confronting them in SG, both for conventional methods and ML-based models. It is worth noting that this paper focuses mainly on detection strategies after a brief discussion of prevention solutions. Therefore, the study of mitigation schemes is beyond the scope of this article.

### *A. CONVENTIONAL SECURITY COUNTERMEASURES*

1) ***Cryptography***: Cryptography is one of the most applicable prevention systems in security-critical systems. In cryptography, the message is encrypted, so it is only recognisable to authorised communication parties with the keys for decryption. There is two primary cryptography encoding. First is the symmetric, where the encryption and decryption keys are the same. Second is the asymmetric algorithm that has different keys for encryption and decryption [132]. Cryptography can be a promising solution against eavesdropping and espionage based attacks. The information must be encrypted to enhance reliability and observe or prevent any illegal access to the SG. Encryption techniques alter the dataset into cyphered and unrecordable text [133]. However, there are some limitations to the widespread use of cryptography in the SG. The first is the computational constraint due to the limitation of residential meters' computational capabilities and storage capacity. Second, the limitations of channel bandwidth. There are different communication platforms in which the transmission of SG information occurs, and each requires a different bandwidth. Finally, connectivity constraints take a longer time for SG connections than for Internet connections [52]. Many papers are still exploring different methods of encryption on the SG.
In [134], an encrypted data trading model for an intelligent network is presented. This model is based on homogeneous encryption, and public (symmetric) key cryptography is used as the primary security method. In 2017, a slight authentication and key exchange model was proposed by [135] for the SG. This algorithm has proposed mutual authentication, key agreement, key refreshment, and multicast mechanism to ensure SG's confidentiality. However, Shariat *et al.* [136] proved that this scheme fails to detect replay attacks. Li *et al.* in [137] designed a comparatively applicable and straightforward Searchable Symmetric Encryption (SSE) model. SSE is a technology that allows customers to record data and documents in cyphertext format and search keywords in their documents. This paper presents a practical and straightforward SSE model with limited data leakage. A lightweight cryptography technique was used to encrypt the susceptible data in [138]. The proposed algorithm called PICO consumes relatively fewer sources than other cryptography algorithms. Then, a reversible histogram data conceal technique is used to wrap the key. The key management issue is a challenging problem of cryptography-based security mechanisms. If the key is not well protected, it may be revealed to the attacker. The key exposure to adversaries can threaten the security and privacy of customers. The authors in [46] examined the main issues related to AMI in SG management following presenting a comprehensive study over AMI. The system features security challenges and the role of key management systems in AMI. This paper examines key management in various modes of transmission, such as unicast, broadcast and multicast communication modes. Finally, it provides a detailed classification of key management approaches, followed by potential challenges to guide future studies.
2) ***Intrusion Detection Systems***: An intruder refers to any unauthorised user who intends to break or misuse the

**TABLE 5.** Summary of attack detection models, and pros & cons of each. Ref. = reference.

| Attack | Countermeasure | Pros | Cons | Ref. |
|---|---|---|---|---|
| FDI | Residual based model | Computationally efficient and high accuracy for direct attack detection | Fails to detect stealth attacks | [139]–[141] |
| | Hybrid IDS | High efficiency | Lack of details about detection rate & Mechanism for CONSUMER attack | [86] |
| | Supervised detection | High accuracy & High efficiency | Lack of robustness & Fails to detect or classify zero day attacks & Not applicable in real world | [142], [143] |
| | Supervised/Semi-supervised detection | Holistic comparison among different ML algorithms | The stealth FDI attack model was not considered | [102] |
| | Neuro-fuzzy controller | High accuracy to detect FDI attack | Fail to detect attack if the attacker does not change the voltage | [144] |
| | Deep-learning | Good performance | Not using realistic data | [145] |
| | Supervised and DL | Holistic comparison among different ML algorithms | Not providing classification between different attack scenarios | [146] |
| DoS/DDoS | Path identifier (Pi) | Lightweight scheme & Good performance in large scale DDoS attack | Lack of scalability | [147] |
| | Specification-based IDS | Low fault negative rate | Unable to detect unknown attacks | [148] |
| | Anomaly-based IDS | Bandwidth efficiency | Lack of a unique mechanism for different attack scenarios | [149] |
| | Supervised classification (SVM) | High classification accuracy & High efficiency | Not applicable in real time system | [150] |
| MITM | Device authentication | High security & robustness | Lack of efficiency & High computation & High energy consumption | [151] |
| | Mutual authentication | High efficiency | Vulnerable to password hash models | [152] |
| | Supervised detection (SVM, KNN, NB) | High accuracy specially for KNN and NB | Not realistic dataset | [153] |
| Eavesdropping and Traffic Analysis | SDN-based topology | Simple management model | Vulnerable to DoS and MITM attacks | [74] |
| | Authentication encryption | Data confidentiality & Data integrity | Lack of accuracy | [154] |
| | Random data sparsity | Using renewable batteries to conceal the consumption information of users | High computational complexity | [155] |
| Jamming | MTD | Good performance to detect jamming attack | High computational performance and cause uncertainty to state estimation | [79] |
| Message Replay | Additive signal noise | Good detection rate | Decreases control performance | [156] |
| | Periodic additive signal noise | High efficiency | Tradeoff between the control management loss and attack detection | [157] |

system. An IDS is a detection system to detect any intrusion and illegal entry into the network. *Anomaly-based*, *signature-based*, and *specification-based* detection are some detecting methodologies introduced in the literature. In anomaly-based detection techniques, a set of expected behaviour (whitelist) is defined for the system, and deviations from these typical patterns are considered an attack. There is a high probability of fault in this method. Signature-based detection, however, provides a predefined dataset of attack manners (blacklist); this method is unable to detect new and zero-day attacks. Finally, specification detection uses logical specifications to identify any escape from common behavioural boundaries [158].

IDS systems have been extensively studied in SG. An anomaly detector was designed by Ten *et al.* in [159]. This substation intrusion detector can also be used to extract traces of intruders. This helps to identify the attackers better and can create a blacklist of attacker features for signature-based detection. Abnormal behaviour detection was proposed based on three algorithms: transaction-based model, hidden Markov model and feature-assisted tracking. This model is a local substation-based detector that can be extended to large-scale use cases. A distributed architecture for implementing IDS over the SG network is also presented in [160]. It is a three-tier IDS network that implements IDS modules through the HAN, NAN, and WAN networks and tracks communications to determine possible anomalies. IDSs are installed on SMs, gateways, and control centres to provide visibility at the system level in this hierarchical structure. The authors in [161] introduced a detection and prevention algorithm to detect an attack within substations. They focused mainly on the units of measurement phasors as sensor nodes and the centraliser of the phasor data as the central node. The proposed IDS manages the data exchanged between the two entities. Also, the Time Division Multiple Access (TDMA) algorithm is used to prevent packet loss and leads to efficient use of the channel and reduction of queue latency. Moreover [162], provided an intrusion detection framework for SGs where each HAN and NAN are equipped with IDS sensors, while several sensors are implemented over WAN. Also, a central management unit monitors distributed IDSs. Distributed sensors send malicious activity to the centralised IDS unit, which monitors these alerts using anomaly-based detection methods.

Also, the main contribution of papers [163]–[165] has been in anomaly detection. In [163], three different anomalies, energy theft through bypassing meters, electromagnetic distortion due to radio frequency interference (RFI) and communication interference due to attacks, have been tested. This article examines time series analysis to identify anomalies in SMs' data. Rossi *et al.* in [164] presented a realistic report on the study of collective and contextual anomaly behaviour in the data of electricity distribution companies in the Czech Republic. They proposed a related new approach to the diagnosis of anomalies. Instead of investigating only single events to detect an anomaly, they proposed a collective anomaly detection approach. In this model, a set of events is evaluated based on their appearance patterns to detect abnormal behaviour. Finally, in [165], the authors addressed the issue of imbalanced data in the SG. The total volume of normal data is much larger than the attack samples. This can lead to misunderstandings about the data recognition and classification system. They proposed a resampling method to generate a data set for training anomaly-based IDS to overcome this issue. The evaluation results demonstrate how this method can improve the detection of minority samples in an unbalanced data set.

Apart from anomaly-based detectors, in [166], the authors have designed a specification-based intrusion detection sensor to detect any intruder penetration to AMI. This sensor monitors the traffic flow between meters, access points, and concentrators on different layers, networks, transmissions, and applications to track the system's normal behaviour. However, this is an expensive method because it requires a separate sensor network to detect any violations within the network. Whereas, in [167], the authors introduced IDS for the NAN system of AMI. This model is cheaper than [166] because it is based on NAN features and does not require separate execution to monitor nodes. Also, in [168], specification-based detection is implemented on HAN. The layered IDS was proposed for ZigBee technology protection to implement HAN. However, the proposed method was tested only on known attacks, and unknown attacks were not considered.

### B. ML-BASED SECURITY COUNTERMEASURES

The best way to ensure cybersecurity is to model the attackers' behaviour, goals, and resources. After that, possible defensive strategies can be well established based on each attack exclusively. This is how ML-based detectors work. A wide range of papers has been investigating ML techniques for SG security. However, ML is considerably used to act as a discriminator of any abnormality or attack in detection systems [169]. ML-based detectors rely heavily on the system data; in other words, they depend on the system's historical data for training the algorithm. ML-based security schemes can perform supervised, unsupervised or reinforcement learning. The detection of attacks is based on the learning procedure of each model. In supervised learning schemes, every training data is presented with its correspondence output. Every data sample is associated with an output which indicates the label of the sample and reveals if it is a normal input or attacked one [170]. Supervised learning algorithms are used widely for attack detection in various sectors. While the unsupervised learning mode is based on unlabelled data and is basically for clustering row data into clusters. Unsupervised learning are popular for anomaly detection problems and compensate the need for labelling training data. Finally, the reinforcement learning scheme is based on interaction of the ML processor and the environment. Decisions in this scheme are taken online based on the feedbacks received.

The most important security countermeasures and attack identification are discussed individually for each attack from now on. Because detection strategies play an increasing role and ML techniques are widely used in this field, this section discusses detection solutions for different attack types in more details.

### C. A DISCUSSION OF SECURITY SOLUTIONS BASED ON ATTACKS CLASSIFICATION

To better understand existing solutions, we discuss the countermeasures proposed in the literature for different attack categories separately in this section.

- ***Eavesdropping & Traffic Analysis***: Eavesdropping attacks are not easily detected due to their passive nature. Prevention mechanisms are far superior to detection countermeasures. Eavesdropping can be a threat to various systems' components. Listening to NAN traffic and reading SMs traffic can seriously threaten the system confidential data. The Software Defined Network (SDN)-based SCADA architecture is proposed by [74] to prevent eavesdropping. SDN-based SCADA traffic is distributed in several directions. Therefore, even if one of the paths is listened to by an intruder, the whole message transmitted between SCADA components is protected from being captured by adversaries. This model is based on SDN characteristics in which communication routing paths connecting the SCADA devices are modified frequently. This dynamicity limits eavesdroppers to get more knowledge and inherit information from the network. Also, they proved that faster change in routing could make eavesdropping even much more difficult. However, very short lifetime routing can cause overhead and management complexity in the SCADA system, and there must be a clear trade-off between these two.

  An authenticated encryption model is recommended by [154] to reduce critical data interception, such that the model can protect the confidentiality and integrity of the data generated in SG. This article presents three authentication methods, including message signing with a private key, using encryption and message authentication code, and finally, authenticated encryption. However, the paper does not provide any simulation results to confirm the performance of protection methods. Recently, Ergen *et al.* in [155] proposed a wholly

**TABLE 6.** ML-based algorithms for attack detection in SG. Ref. = reference; NM = Not mentioned.

| Machine Learning Category | Algorithm | The Investigated Dataset and Testbed | Performance Evaluation | The Targeted Attack | | | | | Ref. |
|---|---|---|---|---|---|---|---|---|---|
| | | | | FDI | DoS/ DDoS | Jamming | MITM | Message Replay | |
| Supervised Learning | SVM | Simulation/ IEEE-9, 30, 57, 118 bus | 0.86 | ✓ | ✗ | ✗ | ✗ | ✗ | [142] |
| | | Simulation/ IEEE-30 bus | 1.00 | ✓ | ✗ | ✗ | ✗ | ✗ | [143] |
| | | Simulation/ IEEE-14 bus | 0.979 | ✓ | ✗ | ✗ | ✗ | ✗ | [171] |
| | | NSL-KDD dataset | 0.67 | ✗ | ✓ | ✗ | ✗ | ✗ | [160] |
| | | RSS dataset | 0.8 | ✗ | ✗ | ✗ | ✓ | ✗ | [153] |
| | | KDD99 | 0.98 | ✗ | ✓ | ✗ | ✗ | ✗ | [150] |
| | KNN | Simulation/ IEEE-9, 30,57, 118 bus | 0.9 | ✓ | ✗ | ✗ | ✗ | ✗ | [142] |
| | | Simulation/ IEEE-30 bus | 0.95 | ✓ | ✗ | ✗ | ✗ | ✗ | [143] |
| | | RSS dataset | 0.99 | ✗ | ✗ | ✗ | ✓ | ✗ | [153] |
| | ENN | Simulation/ IEEE-30 bus | 0.98 | ✓ | ✗ | ✗ | ✗ | ✗ | [143] |
| | DT | KDD99 | 0.96 | ✗ | ✓ | ✗ | ✗ | ✗ | [150] |
| | NB | KDD99 | 0.70 | ✗ | ✓ | ✗ | ✗ | ✗ | [150] |
| | | RSS dataset | 0.97 | ✗ | ✗ | ✗ | ✓ | ✗ | [153] |
| Unsupervised Learning | iforest | SE-MF dataset | 0.90 | ✓ | ✗ | ✗ | ✗ | ✗ | [172] |
| | DBN | NM | 0.99 | ✓ | ✗ | ✗ | ✗ | ✗ | [173] |
| Reinforcement Learning | SARSA | Simulation/ IEEE-14 bus | 0.99 | ✓ | ✓ | ✓ | ✗ | ✗ | [174] |
| | Deep Q-learning | Simulation/ IEEE-9 14,30 bus | 1.00 | ✓ | ✗ | ✗ | ✗ | ✗ | [175] |
| Deep Learning | DRF | Simulation/ IEEE-14 bus | 0.95 | ✓ | ✗ | ✗ | ✗ | ✗ | [145] |

new and computationally efficient scheme for data protection. In the multi-meter energy routing model, the data sparsity is taken randomly from several meters. Besides, renewable batteries are used to hide households energy consumption information. This method can prevent eavesdropping on approximately 75% of the data.

- ***DoS/DDoS***: DoS and DDoS cannot be hidden because they are active attacks that make the services unavailable to users. Anomaly detection methods are the main countermeasures against DoS and DDoS attacks. IDS can be a promising solution for this category of attack detection, especially anomaly-based detection. A detection method for detecting DoS attack was studied in [148]. The authors in [147] introduced Path identifier (Pi), a new technique to defend against DDoS attack. In this approach, the victim can limit any possible attacks that match previous attack signatures using the complete binary tree model. However, in the binary tree model, a router is assumed to have only two interfaces. While routers usually have more than two interfaces in reality, hence this model is not scalable for real systems. To protect the SCADA system against DDoS attacks, an IDS is suggested in [149]. It uses Time-to-Live (TTL) metrics to identify normal and abnormal packets. Because DoS and DDoS attacks usually occur outside the network, expecting more TTL for malicious packets is acceptable. Also, ML-based detectors have been considered widely to compensate for DoS attacks. In 2011, [160] proposed an SVM classifier and studied the NSL-KDD dataset to detect anomalies in the dataset. However, the accuracy of this model was not high enough. Recently, this problem has been further studied, and some literature has reviewed various ML algorithms to detect DoS attacks in the SG system. In [150], the authors used an SVM classifier to detect a DoS attack and examined their model on the KDD99 dataset. When data is collected from the network, the Principal Multiplier Analysis (PCA) method reduces the feature dimensions. Next, the SVM classifier is used to distinguish incorrect measurements from correct ones. The SVM classification capability is compared to the decision tree (DT) and the NB network regarding the accuracy, precision, recall and F1 score indicators. Based on the results, the SVM classifier performs better than other classifiers. Kurt *et al.* [174] utilised an online detection algorithm, which is based on reinforcement learning to detect DoS and some other attacks. The training process of this detector is based on a model-free reinforcement learning algorithm called SARSA. The attacker learns a Q-table after each training episode based on the cost it receives from interacting with the environment. This approach performed well compared with the Euclidean and the cosine-similarity-based detectors.
- ***Jamming***: Algin *et al.* [79] proposed a dynamic data transaction to report AMI data. This model relies on the Moving Target Defence (MTD) mechanism. MTD uses random reporting time instead of static time and changes the time slots assigned to each meter unpredictable to the jammers. The unexpected change of time plan for transmitting the information declines the jamming attack

effect of SMs on a large scale. This model also reduces packet transmission time along with network collisions. The jamming attack scenario was investigated on the issue of SG status estimation in [174]. The authors also propose an online reinforcement learning detection instead of conventional strategies based on supervised and offline learning. The evaluation results show the effectiveness of this model in detecting jamming attacks.

- ***FDI***: FDI is one of the most common attacks against SG components. The state estimation depends largely on measurements collected from the environment, and an attacker can carry out devastating attacks by injecting false information into the system. The BDD system is responsible for detecting FDI attacks. However, older BDD systems cannot detect complex data injections attacks based on residual measurements [139]. An attacker who knows the system topology can design his incorrect data to bypass the BDD [140] and cause incorrect state estimation. Numerous solutions to this problem have been explored in the literature. Lo and Ansari in [86] suggested that more limited energy consumption restrictions be introduced within the grid, also proposed to install sensors distributed in the network topology to increase grid visibility and the detection rate of a specific FDI attack, i.e. CONSUMER attack. They proved that as the number of grid sensors increases, the CONSUMER attack's detection rate also improves. However, in terms of the status assessment process, a new equivalent measurement change is proposed in [141] instead of the common residual state estimation weighted least squares. This work detects false data via the residual searching scheme, and they test the FDI attack with IEEE 14 bus system.

  The study in [142] was one of the first works to develop the idea of using supervised and semi-supervised classifiers to identify FDI. The work formulated FDI detection as a feature classification problem and solved the problem using three categories of supervised classification algorithms over a centralised architecture, K-Nearest Neighbourhood (KNN), SVM and sparse logistic regression. To complete this work, the authors in [102] proposed semi-supervised and online learning techniques in addition to supervised algorithms for different attack scenarios and provided a comparative method to reveal the advantages and disadvantages of each method. However, attack strength parameters such as magnitude, number of attacker nodes and attack scale are not considered in [142] and [102]. Also, the importance of the stealth attack scenario, in which the attackers are aware of the network structure, was not considered. Later, in [143], two parameters were considered to describe the attack strength including, the attacks' nodes number and magnitude of attacks. Yan *et al.* [143] also considered the impact of stealth FDI attack and compared the performance of three supervised learning algorithms, SVM, KNN and Extended KNN (ENN). This paper also tried to solve the binary classification problem of detecting false data. They first examined the limitations of traditional residual-based detection and then proposed supervised techniques as secondary detectors of residual-based BDDs. They considered balanced (the number of attacked measurements and safe measurements are equal) and imbalanced (the number of attacked measurements is significantly more or less than safe measurements) datasets to investigate detectors' accuracy. Based on their results, all three classifiers performed well to identify direct attacks on balanced and unbalanced datasets. While for stealthy attacks, KNN and ENN failed to win 100%. The SVM detector performed best to detect the stealth attack model and detected almost all inaccurate measurements.

  In [144], a Neuro-fuzzy controller is used to estimate the voltage and detect false data incidents. They compared traditional false data detector and their semi-intelligent method. Archived information is used for training purposes in their design, and the detector can detect normal and abnormal behaviours well. The results showed that the proposed model is very accurate in identifying false injected data. A similar study was done in [145] by Ashrafuzzaman *et al.* They considered DL-based stealthy FDI attack against state estimator in SG and compared the results with the other three ML algorithms in terms of accuracy and precision. The DL approach performed best among all the techniques.

  In [146], they conducted a comprehensive study and examined twelve different ML algorithms to detect abnormal behaviours. Six supervised and six DL algorithms were examined in this work. These methods were used to detect an anomalous pattern to identify attacks such as DoS, data injection, worms, and other attacks. The results showed that the *random forest* algorithm performed the best in accuracy, while the Naive Bayes (NB) classification had the worst results. The authors of [172] considered Covert Data Integrity Assault (CDIA) and FDI attack against the integrity of the system and to sidestep the BDD of SG. To identify the CDIA, they also proposed an unsupervised algorithm called isolation forest on unlabelled data. The detection hypothesis in this scheme is based on the assumption that the attack has the shortest path length in a random forest construction. The evaluation results show better performance of this algorithm compared to the supervised schemes. Unsupervised ML-based detection was the approach used by Karimipour *et al.* [173] based on a statistical correlation between measurements. This model uses Dynamic Bayesian Networks (DBN) to extract features and build the model. This helps detecting not observable attacks in large scale SG. The DL model also uses a restricted Boltzmann machine to verify the performance of its proposed scheme. The model was evaluated on IEEE 39, 118 and 2848 bus systems, which showed 99% accuracy against a negligible error rate. In addition, the results show that increasing the scatter of the attack leads to a more accurate detection. A reinforcement learning detection model is presented in [174]. This paper first formalised the FDI attack impact on state estimation, then established a state machine for the SG scenario and two pre-attack and post-attack states. Then, this work proposed a model-free reinforcement algorithm called SARSA to collect measurements and costs from the system to build the model. However, to reduce computational complexity, papers typically consider a DC power system model. The state estimation corresponding to this DC assumption is linear, while An *et al.* in [175] examines the AC model and considers the non-linear problem of state estimation. They proposed a deep Q-learning algorithm to study the data integrity attack. A comparison of the results shows that this model performs better than previous algorithms.

- ***MITM***: When a MITM attacker invades the network, the attacker places himself between the access point and one of the clients and controls the connection. Encryption and authentication methods are the best solutions discussed in the literature to tackle MITM attacks. A novel authentication method is proposed for entities in HAN by [151]. The authors in [152] designed an efficient authentication algorithm to defend against internal MITM attackers. The authentication mechanism between SM and the server is done through a password. This mechanism can reduce the number of steps and packets exchanged and effectively defended against a potential MITM attacker. In addition, a public key encryption method was introduced for efficient key management. However, as the number of stealth and more sophisticated attackers increases, we need more robust defence mechanisms. Apart from the step-by-step attacks designed by [93], the authors also propose the configuration of snort IDS to detect MITM attacks better. Various network metrics were monitored, including retransmission rate and average Return Time (RTT). The extracted features can help better train IDS and identify attack traces.

  Anomaly detection with advanced classification tools can be a promising way to detect MITM attacks also. The packet size, number, and delay can be parameters that are studied to detect MITM. Dong *et al.* in [153] have proposed a new algorithm for detecting MITM in a fixed wireless network that can be very similar to HAN, NAN, and WAN. They studied the RTT measurement and Received Signal Strength (RSS) measurement to detect anomalies. Because spoofed packets traverse additional links between the attacker's machine and the victim's location, there is additive delay to the communication process. The increase in RTT and RSS fluctuations was compared with normal fluctuations and was eventually identified as an attack footprint. This study included SVM, KNN, and NB classifiers. The results showed that SVM has less accuracy and complexity than the other two algorithms. However, since RTT can be increased due to network congestion, this feature is not enough to detect abnormal data.
- ***Message Replay***: The idea of adding a random noise signal to protect the control system against a replay attack was first proposed in [156]. This additional signal works as an authenticator signal. Suppose the system does not respond to the additional noise, the probability of the attack increases. This scheme, however, increases the detection performance at the expense of system control degradation. Later, Tran *et al.* [157] improved this design to make it more efficient in terms of system management. In this model, the random signal is added periodically only for a short time slot. Because network devices follow normal conditions without artificial noise, the control system's performance is not significantly affected. A similar approach was also proposed in [96], which adds a random increment to the control measurements and make the BDD more sensitive to fluctuations. In this case, if, in response to a replay attack, the estate estimation deviates even on a small scale, the detectors can identify anomalous measurements.

A summary of detection schemes for various attack models in the SG system proposed in the literature is illustrated in Table 5. Besides, Due to the wide use of ML algorithms in attack detection, Table 6 provides more details on ML-based detection schemes proposed in the literature, including the corresponding algorithm and performance evaluation of each.

## VII. PRIVACY: ATTACKS IN SMART GRID

Privacy and protecting the personal information of customers are essential requirements of SG. Information leakage is a significant threat against SG users. An attacker can first passively attack the network, eavesdrop on data flow, and obtain information from the customers consumption data. Later this information can be used for threatening victims. Generally, there are five categories of privacy introduced in [176] including the privacy of location, privacy of state of body & mind, privacy of social life, the privacy of behaviour and activities, and media privacy. In SG, we mainly face the privacy of the location and privacy of customers' behaviour and activities. Here, for more details, threats to customers privacy are classified into three main classes: Personal Information Leak, Identity Theft, and Social Engineering attacks.

Table 7 depicts an overview of possible threats breaching the privacy of the customers, the target of each attack and the compromised service.

### A. PERSONAL INFORMATION LEAK ATTACK

Users' personal information must be protected against unauthorised access, disclosure and use. As discussed, adversaries can use advanced analytical tools to extract important information from SG traffic. This information leak can be used to abuse financially or even threaten their lives. Mainly, information disclosure attacks target the authentication criteria of

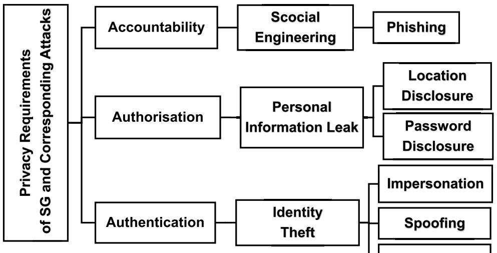

**FIGURE 9.** Privacy requirements of smart grid, and attacks corresponding to each.

the system's privacy. Following are some critical information leak attacks in SG:

- ***Location Disclosure***: There are several ways to estimate the user's location. The latency attack, in which the attacker computes various routes' delay in the network and then, by analysing this data, can estimate the approximate location of each user [177]. The measurement packets of premises are periodically transmitted over AMI infrastructure. The latency attack can compromise network-connected SMs. Another attack that can show the user's location to adversaries is Brute force Attacks. In this attack, the attacker tracks the packet message hop by hop until it reaches the destination [178].
- ***Password Disclosure***: One of the most common ways to authenticate and protect the security and privacy of users is to obtain a password to restrict access to any system. Passwords are easily enforceable, and users can use them without any participation. Also, passwords are vulnerable to different password guessing tools such as HashCat [179], password sniffing, and dictionary attacks. Besides, the investigations over many password datasets proved that users usually tend to use passwords that can be guessed with expected patterns, numbers, and strings [179]. An autonomous GAN-based password guessing scheme is proposed in [179]. Evaluations showed how this model could generate large volumes of matching passwords.
- ***Eavesdropping***: Eavesdropping is not only a security attack but also a threat to SG customer privacy. The eavesdropper can take advantage of network vulnerabilities and access customer information by listening to AMI traffic flow and channels between users and control centres [180]. This traffic contains detailed information about customers' daily routines, which can be a considerable concern for their privacy.
- ***Sniffing***: Packet sniffing monitors and records data packets in a network. If the packets are not encrypted properly, the sniffer can detect users' passwords and identities. SMs are the main target for sniffing. TCP/IP packets of SMs sent over the network can be sniffed and analysed by tools such as Wireshark [25].

### B. IDENTITY THEFT

When an adversary attempts to hide his identity under a legitimate identity system, he faces an identity theft attack. Identity theft can occur at various SG scales, from stealing IP meters to impersonating network suppliers and creating fraud against users. Identity theft is a threat to the authorisation of the network.

- ***Impersonation***: A network intruder can impersonate as legal forwarding nodes by exploiting the MAC frame field. Also, during authentication between SMs and gateways, an adversary can initiate an impersonation attack when he can fake one of the identities of the SG legitimate parties [181]. Considering the aforementioned threats, impersonation is a significant threat to SG components and entities. In particular, privacy is seriously threatened if an attacker, as a legal partner of the system, accesses users' private information, obtains information about neighbouring meters, and learns about their lifestyle and activities. Leea *et al.* [182] demonstrated how the previous authentication mechanism proposed by Yeh, Shen and Hwang [183] in 2002 was vulnerable to server impersonation attacks. The model proposed in [183] which is abbreviated as YSH scheme, utilises a smart card for the login process with only using a hash function to keep the model efficient. While this problem was solved by [182], through a S/Key based mutual authentication between meters and the servers of SG.
- ***Masquerading***: Another major attack targeting SG systems is masquerading. Masquerading is when an attacker tries to masquerade and replace someone's identity for another person. This class of attack can cause relatively more dangerous effects than other intrusive attacks, as the adversary can obtain super privilege through mimicking a legitimate user [184]. Masquerading breaches privacy first by obtaining the access information of users and stealing their identity and later can make multiple security attacks after gaining access to the system. Most conventional IDSs fail to detect this attack, and administrative security centres of the SG need to take more intelligent approaches.
- ***Spoofing***: While masquerading attacker uses a 'mask' to be concealed under, spoofing attackers pretend to be legitimate network users, communicating from a fake trusted source. Spoofing can be a threat to security or privacy based on the intent of the attacker. Attackers can use their fake identities to control the network to obtain the identity and password of actual users in the system. There are three main types of packet spoofing, including MAC spoofing, ARP spoofing and IP spoofing. All of them are illegal modification schemes for spoofing. Nodes and sensors equipped with GPS transceivers are essential parts of the control system of SG, specifically the SCADA network. GPSs are vulnerable to attacks such as FDI and spoofing. GPS spoofing is due to transmitters mimicking the GPS signal to change the GPS time estimated by the GPS receiver. SG vulnerability to GPS sensor spoofing has been analysed in [185]. Specifically, this work proved the vulnerability of power

**TABLE 7.** Smart grid privacy attacks.

| Attack | Classification | Attack Target | Compromised Services | | |
|---|---|---|---|---|---|
| | | | Authentication | authorisation | Accountability |
| Location Disclosure | Personal Information Leak | To get access to smart meter location via latency attack [177] & Brute force attack [178] | ✓ | ✓ | ✗ |
| Password Disclosure | Personal Information Leak | To decrypt the users password and get access to their private information [179] | ✓ | ✓ | ✗ |
| Eavesdropping | Personal Information Leak | Eavesdropping for information disclosure [180] | ✗ | ✓ | ✗ |
| Sniffing | Personal Information Leak | TCP/IP packets sniffing [25] | ✓ | ✓ | ✗ |
| Phishing | Social Engineering | interrupt the Ukraine power network service [189] | ✗ | ✓ | ✗ |
| Impersonation | Identity Theft | Impersonate legal forwarding nodes to collect information of SMs [182] | ✗ | ✗ | ✓ |
| Masquerading | Identity Theft | Privilege access and information theft [184] | ✗ | ✗ | ✓ |
| Spoofing | Identity Theft | GPS data manipulation [185] | ✗ | ✗ | ✓ |

measurement units as primary measuring components utilised for state estimation in case of a GPS spoofing attack. If the measurements of an area are revealed to adversaries through GPS spoofing, the privacy of the residents' information and location of that region can also be triggered.

### C. SOCIAL ENGINEERING ATTACKS

Social engineering is a tactic to fraud users into using social techniques to access private data [186] and their credentials. Social engineering attacks are non-technical attacks using human psychology tricks to deceive victims. Different cyber social engineering attacks threatening users' information confidentiality. However, we are mainly discussing a group of social engineering attacks integrated into SG. Social engineering attacks are threats toward the accountability of SG.

- ***Phishing***: Phishing is a social engineering attack to gain access to victims' personal information by sending fraudulent emails or messages [187]. Holm *et al.* [188] conducted two real phishing experiments on a Swedish electrical power company and reported how power utility companies could also become phishing victims. The famous cyber-attacks against Ukraine's power distribution system were launched in 2015 [189] by a phishing email. The email contained a malware-rigged attachment in Word or Excel documents. When users in companies opened infected documents, malware penetrated their systems and could steal important information as the VPN secret keys and control the system remotely [190].
  Fig. 9 illustrates a taxonomy of the context discussed in this section, including privacy attacks and the corresponding requirements in the SG area.

## VIII. PRIVACY: COUNTERMEASURES FOR SMART GRID

In this section, we discuss several approaches presented in the literature to counter attacks on the privacy of the SG system.

Providing privacy means aggregating the customer's consumption information without disclosing their information. There are several privacy preservation techniques based on cryptography and authentication. However, conventional solutions cannot be directly implemented through SG due to these schemes' computational costs. Therefore, new techniques are recommended considering the characteristics of SG [191].

- ***Identity Encryption***: Encrypting the identity of individuals is a key step in keeping information confidential [206], [207]. It is one type of public key encryption designed for SMs to protect family identities from information disclosure [192]. Although this scheme is computationally efficient, it increases the volume of data and can cause unwanted delays [208]. Wang in [191] proposed a combination of an identity-based encryption scheme with an identity-based signature scheme to protect customers' privacy in SG. Both encryption and signature schemes in this model have the same private and public parameters for efficiency. It is a five-phase protocol that includes initialisation, registration, collection, aggregation, and decoding. The model has been validated by a comprehensive study of various attack scenarios in SG. Finally, the implementation results on the Edison platform proves the performance efficiency of this protocol on limited devices such as SMs.
- ***ID Anonymisation***: Anonymity means that the user's identity in the system should never be revealed from his data or activities. Anonymity refers to protocols that separate the message from its original identity to be secure. The study in [193] provides Elderberry, a peer-to-peer intelligent measurement model. The meters information is anonymised within peer to peer categories of randomly organised meters. Random selection of group meters makes the location of meters untraceable. This can preserve the location disclosure threat of SMs in SG. ID anonymisation can protect against various information disclosure attacks. However, the Elderberry method is not robust enough for some attacks. For example, consider a case that an attacker can use publicly accessible information as auxiliary data to access sensitive information. Thus, this attacker aims to intercept the energy consumption of particular users or a particular group of residents in an area and violate the privacy of those users [209]. Elderberry method as an ID anonymisation method is unable to conceive the sensitive information from the normal ones, and such activity leads to detouring the control policy to protect data.

**TABLE 8.** Summary of privacy countermeasures. Ref. = reference.

| Preservation Scheme | Description | Pros | Cons | Ref. |
|---|---|---|---|---|
| Identity Encryption | Using encryption system to conceal customers' identity | Computationally efficient and reliable in some scale | Increased data size and latency | [191], [192] |
| ID Anonymisation | Separates the user's information from his ID | Preserve customers privacy | Limits utilities to gain enough information from data analysing activities | [193] |
| Pseudonymity | Protecting users' identity through pseudonymous IDs | Being able to re-identified and re-generated the real ID of users if required | Cause unwanted computation load on SMs | [194] |
| Blind Signature | Blinding the content of data packets before it is signed to be untraceable to unauthorised access | As the identity of the customer is blinded, even the disclosure of information does not threaten the users | Changing and signing the request may cause unwanted latency | [195]–[197] |
| BLH | Hides real customers consumption pattern under battery charge and discharge | Prevent SMs data leakage | High cost and limited capacity and maximum battery charge/discharge | [198], [199] |
| Differential Privacy | Obfuscate the original data | Achieving privacy protection of users on a large scale | Reduces the accuracy of the measuring information | [200], [201]<br>[202] |
| Federated ML | Decentralises learning process and keeps the row data by the customers side | Create large scale data sharing and prevent information leakage | SMs computation limitations in the training phase | [203]–[205] |

- ***Pseudonymity***: Pseudonymity techniques involve using unreal names to display messages. Pseudonymous smart metering provides legitimate customers pseudonyms without their identity disclosure [210]. In [194], a privacy-preserving authentication scheme for SG (PASS) is proposed. The hash-based message authentication code (HMAC) is used for the authentication procedure within substations. In this model, the SMs data is authenticated before reaching the control centre. Pseudonymised data is restorable to its original state as well. This helps to re-identify the information.
- ***Blind Signature***: An alternative way to protect untraceable data transmissions is blind signature [211]. In this method, the customer's genuine content (party 2) message is disguised and blinded before it is signed by the control centre (party 3), and then the third party can verify that the packet has been signed by party 1, without knowing the requester identity and the date of signature [212]. When a customer submits a credential anonymously to a metering system, the control centre cannot identify which customer is requesting, yet it can verify the signature to confirm that it is from a valid customer [195]. The model is generated based on the assumption that SMs can communicate with the control centre via a secured communication link, and third parties cannot read the contents without the key concerned. While in previous work, the integration of electrical information has not been considered, Kong *et al.* [196] ensured data integrity through homomorphic encryption and offered group-based blind signature anonymous authentication to protect the privacy of SG customers. Finally, in [197], a private power request scheme based on blind signature has been proposed. This is a credential-based model with unforgeability, untraceability, and verifiability capabilities proved by authors.
- ***Battery-based Load Hiding (BLH)***: BLH is one of the most effective ways to deal with SMs data leakage [198]. In this way, the batteries are installed in the house and the actual pattern of energy consumption of the users while charging and discharging the batteries is hidden. The main limitations of BLH are its high cost and limitations in capacity and maximum battery charge/discharge. The measurement of privacy criteria, data storage specifications, technologies and BLH algorithms have been examined in a recent study by [199]. The authors argue that constructing the original unprotected consumer load profile would offer the best privacy measure. Nevertheless, assessing the constructability of the consumer load profile under a privacy protection scheme has not been achieved yet.
- ***Differential Privacy***: Recently, differential privacy has also been widely used to obfuscate the original data [201]. This model was first proposed by [213] and is based on the distribution of additive random noises among SM readings so that demand collectors cannot identify individual customer data. Bao and Lu [202] in 2015 introduced a novel differential private data aggregation with fault tolerance capability for collecting residual energy measurements. The proposed model is based on the improvement of the Boneh–Goh–Nissim cryptosystem [214]. This design is efficient in terms of storage capacity and computing. However, the result of this model in the accuracy and integrity of measurement data has not been evaluated. A deferentially private metering scheme was proposed in [200]. In this model, utilities periodically collect data from SMs and derive aggregated statistics such that the detailed information on the user's consumption is not deduced. SMs in large clusters periodically send measurements to suppliers. These measurements are sufficiently noisy and encrypted so that the power suppliers cannot extract individual nodes information. Even if differential privacy can protect customers' privacy, there is a tradeoff between users' privacy and the accuracy of the data aggregated by providers. Therefore, differential privacy cannot be widely used in the SG metering system. Since very accurate and spotless information is required for energy consumption, billing and demand forecasting missions [215].

- ***Federated Learning***: As mentioned in Section V, ML technologies are executed widely for demand anticipation, fault forecasting, fault detection and, in particular, for attack detection. However, this requires high access to detailed information on SM measurements which can cause the system particularly prone to privacy attacks. It is also impossible to move all these computations to user sides due to the limited computational space and storage of these nodes. To address this problem, the term Federated Learning (FL) has recently been proposed by the literature to preserve customers' privacy using ML technologies [216]. FL is a distributed decentralised learning approach proposed mainly to reduce the privacy risk for users. This model keeps the training data on the premises sides, and the first training stage takes place privately by SM nodes [217]. Then, to build a generative scheme and collaborate with the network, each user shares their training parameters with a server located in the data aggregator. Finally, the average of all models is calculated to produce a global model, and this model will be broadcasted again to users so that they can update their local training model. Cao *et al.* [203] developed a FL system for the IoT and SG data-sharing approach called IFed. Using FL enables power grid users to transmit training models instead of real sensitive data. This can help the tradeoff between user privacy and access to data. Providers on the Ifed model do not provide users with privacy as a trusted third party while assisting users in training their model with an update received from the global server, i.e. power provider. They also categorised users based on different privacy requirements and provided stronger privacy guarantees for sensitive users.
  Recently, the authors in [204] proposed an FL-based power consumption forecasting model without sharing individual power tracking. This collaborative based power consumption pattern learning could benefit both clients and society through preserving their factual information. This study considers two federated models for two different scattered data types, horizontally where the data are scattered in the sample space. Also, a vertical federated learning scheme is provided for data samples scattered in the feature space. In the horizontal model, the training is done locally on each side, and the parameters are encrypted when sharing with the same central server. However, in the vertical framework, customers are not even willing to share training parameters. In this case, no real data or parameters are shared, and only essential results are shared in the encrypted model. In [205], a federated-based intrusion detection was proposed. In this scheme, decentralised DL-based IDSs perform under a federated architecture to promote customers' privacy as well as security protection. FL is a robust model that can be applied in different SG use cases requiring customers to collaborate with privacy concerns. This area is still fresh and can have several research directions for the future. A summary of countermeasures discussed in this section to preserve users' privacy in the SG technology is provided in Table 8.

## IX. SUMMARY OF SURVEY FINDINGS AND SMART GRID SECURITY AND PRIVACY FUTURE RESEARCH AREAS

The comprehensive overview of the security and privacy aspects of SG and the survey findings is now summarised in this section. Additionally, this section discusses potential future challenges and directions for future security and privacy research with emerging technologies in SG. Although several of them have already been discussed in previous sections, we address a few additional challenges and open research topics.

### *A. SURVEY FINDINGS*

The purpose of the survey was to examine the security and privacy aspects of SG, make a literature review of previous adversarial threats, and study new AML techniques targeting SG security and privacy requirements. Furthermore, we examined the measurement attempts made by researchers to address such vulnerabilities.

Considering the importance of the SG, its security is a challenging issue. While there is no robust security framework for the various layers and components of the SG against current attack methods, new attack scenarios are constantly being generated by adversaries. In addition, customers' privacy concerns are an obstacle to vast data flow and analysis to discover attacks from the clients' side.

Fundamental differences in the goals of SG and other information systems differentiate the security strategies of the two systems. Therefore, all previous cryptography, encryption, and authentication techniques are not compatible with SG applications. Hence, exclusive protocols standardisation for SG should be established. New AI methodologies and techniques can make SG secure and more reliable. On the other hand, the terms AML contribution in SG still requires further research from the literature.

### *B. POTENTIAL FUTURE RESEARCH AREAS*

This section outlines future security and privacy opportunities and challenges raised with integrating SG into advanced communication technologies, such as 5G, beyond 5G and 6G. Also, various peripheral technologies that facilitate the implementation of SG have been addressed shortly from both a security and privacy perspective.

#### 1) 5G TECHNOLOGIES

Large-scale 5G implementation activities have begun around the world. 5G technology, compared to the older generation of communication technologies, offers a wide range of services and technologies, including ubiquitous connectivity and coverage, relatively low latency, high reliability and scalability that can serve SG. Fig 10 shows that SG is implemented through the 5G network architecture and its various components. As shown, different services in different domains work

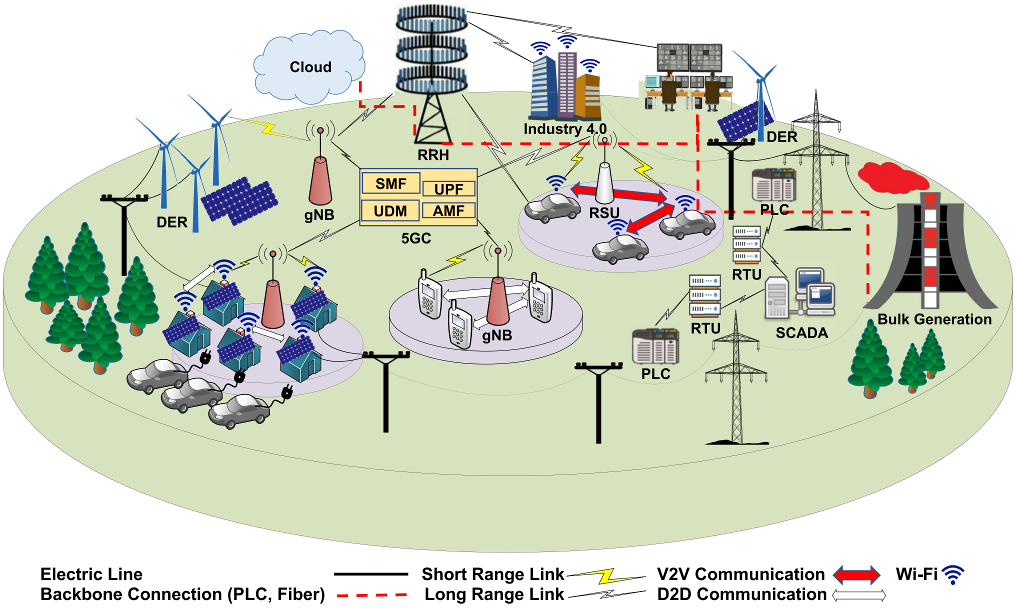

**FIGURE 10. Smart grid system over 5G network providing the infrastructure for future smart city. DER := distributer energy resources; RRH := remote radio head; 5GC := 5G core; RSU := road side unit; AMF := access and mobility management function; SMF := session management function; UPF := user plane function; UDM := unified data management.**

in parallel on 5G. The important thing is that the functionality of these services must not disrupt other sections. While 5G provides the communication infrastructure for this vast connection, SG provides the energy needed for this huge human, vehicles, machinery and devices network. Below is a brief overview of the technologies used in 5G, their contribution to SG and the security and privacy concerns associated to each.

- ***HetNet***: Heterogeneous networks (HetNet) are multi-tier networks that can increase efficiency, flexibility, and wireless coverage. Devices in each layer of HetNets have different communication parameters, such as power transmission, coverage and operating frequencies. The SG communication network is inherently heterogeneous and consists of three layers, as discussed in Section III, HAN, NAN, and WAN [218], with several different devices. See Fig. 10, gNBs act as gateways, connecting HANs to the NAN and NAN toward WAN. The 5G core with different functionalities is logically distributed over various gNBs to cover a wide geographical area. However, the HetNet architecture is more vulnerable to eavesdropping than single-layer networks. In addition, the high density of devices in small cells can also increase concerns regarding SG users' privacy in terms such as location disclosure [219].
- ***D2D***: In Device to Device (D2D) communication, nodes can communicate autonomously without a base station interval. D2D communication increases spectrum efficiency through exploiting spatial reuse and offload traffic from the network infrastructure. This communication model has several use cases in different sections of future communication society (see vehicular communications and SG in Fig 10). For example, in the AMI system of SG, SMs can operate in a mesh architecture network. Each group of SMs has a cluster head such that the communication between SMs and this cluster head is based on D2D communication mode [220]. However, this infrastructure-less communication is less secure than the device to stations communication, specifically for attacks as jamming [221].
- ***Massive MIMO***: Massive Multiple Input Multiple Output (MIMO) technology places a massive volume of low-power antennas in a base station. This is significantly more than the number of users whom are being served [222]. Massive MIMO provides high energy and spectrum efficiency. Massive MIMO can be widely used in NAN and WAN networks [223]. Deng *et* . [224] demonstrated the improvement of secrecy performance in a two-tier HetNet using massive MIMO. Besides, in [225], a rather robustness of massive MIMO against passive eavesdropping is proved. However, attackers can come up with strategies to overcome this obstacle, such as having the device equipped with an extensive antenna array for eavesdropping.
- ***Massive SDN***: Software-Defined Networks (SDN) separates the control plane from the data plane and provides centralised control, elasticity, and programmability for the SG communication network. SDN integration in SG makes the communication flexible, self-configurable, programmable and scalable. A novel SDN-enabled multi-attribute-based secure communication protocol is proposed by [226] for the SG devices. Multiple SDN controller frameworks are proposed for designing an IDS implemented over SCADA system in SG environment [227]. However,

centralisation, limited forwarding table storage capacity, lack of authentication, and time stamping makes SDN susceptible to DoS, DDoS, MITM, and message replay attacks.

- ***Massive IoT***: Massive Internet of Things (IoT) refers to the world in which every object is equipped with a communication and computing device and can operate as a part of a widespread network [228]. The growing number of devices connected to this system is beyond imagination [229]. It brings large-scale connectivity to all aspects of our daily lives. SG can be considered one of the most extensive IoT networks connecting several devices consuming energy, monitoring, control, and processing. A 5G-based IoT network for demand response applications is examined in the SG model by [230]. However, mainly these connected devices have limited computation power and storage capacity. This makes researchers design security algorithms efficient and lightweight enough for the devices to be capable of using them effectively.
- ***Cloud Computing***: As a new computing model, cloud computing provides on-demand computing facilities and shared resources via the Internet. With cloud computing, computing, storage, and network management are centralised in the clouds, referring to data centres, backbone IP networks, and cellular core networks. Cloud computing serves as a utility provider based on extended storage and computational devices. Cloud computing sustains elastic storage and memory devices. This is very useful for SG systems that integrate multiple heterogeneous devices, such as home appliances, SMs, substations, sensors, and communication networks [231]. With providing powerful computation resources, cloud computing can serve various SG applications including, demand management [232], dynamic energy pricing [233], security analysis [234], real-time control and monitoring [235]. Numerous computation-intensive problems of SG can benefit from cloud computing, such as state estimation, load forecasting, fault detection, and self-healing. This is also beneficial for ML-based security analysis and attack detection applications requiring large amounts of data analysis and complicated problems. Cloud computing is not a new concept, but there is still room for research to integrate its application into critical infrastructures such as SG. Cloud computing compensates for the computation and storage deficiency at the cost of increased communication overhead and prolonged latency. There is a consensus that is only relying on cloud computing is insufficient for real-time applications of power networking to be realised. Therefore, the cloud computing subject still requires improvement to be effectively incorporated into the future power infrastructure. Another major limitation toward deploying cloud computing infrastructure to the power networks is information disclosure and privacy threats. The energy consumption of customers is aggregated on remote public large data centres for computation objectives, which could invade privacy policies [236]. Accordingly, promoting customer privacy is a crucial future research direction in remote computing technologies. It would be possible to integrate privacy-preserving schemes like differential privacy and FL into cloud computing applications of SG in the future.
- ***Edge Computing***: While the communication overhead and propagation delays of cloud computing remain one of its critical disadvantages, a new platform in computing is taking place as processing nodes begin to shift closer to the network edges, i.e. edge computing. The concept of edge computing refers to the provision of IT and cloud computing capabilities in the radio access network within the proximity of customers [237]. With edge computing, propagation delays could be reduced compared to cloud computing. Data propagation delay over the edge can be limited, especially in dense small cells such as NANs and across the D2D communication range for the metering network of SG. Low information concentration, distributed deployment, and small-scale edge servers make them less susceptible to security attacks than fully centralised cloud servers. In addition, with more private ownership of edge servers, the privacy issue of some customers can be addressed at some scale. However, privacy vulnerabilities in edge-based energy management have not been fully addressed [238]. In some cases, the term edge is interchangeable with the term fog [239]. However, the term fog has a much broader definition than the typical notion of edge. Fog expands the definition of edge devices, including smartphones and set-top boxes. Indeed, fog and edge are relevant because of the traditional cloud's shortcomings and the advent of new computing opportunities.

### 2) BEYOND 5G/6G

While 5G is not yet fully implemented and fully delivered, the next generation of communications, 6G, is gaining attraction. Higher rates, spectrum efficiency, ubiquitous coverage and even shorter delays are the motivations for this move. 6G is intelligent and independent and has extensive services equipped with AI. 6G envisages an integrated network in space, air, land and sea. These heterogeneous environments are compatible with 6G technology. However, SG intends to monitor the entire process of online electricity distribution and ensure the reliability and security of services. 6G, with ultra-reliability and minimal latency, can meet SG communication needs precisely.

### 3) EMERGING TECHNOLOGIES

Communication technologies have penetrated almost every aspect of the community. Now, expectations go beyond mobile connectivity for cellphone devices and human interactions. Industry, health care, transportation, education, and almost all social services can benefit from massive connectivity. Since each part requires energy preparation and energy source, the SG concept is also an integral part of this model. The following is a brief description of some of these areas.

- ***Big Data***: As SGs are implemented, there is a substantial increase in the amount of data to be processed. Numerous sensors, SMs, and monitoring devices will be installed on different levels of the network to generate real-time data describing the state of the network [240]. The unprecedented volume of data, its instant frequency generation, and the heterogeneity of the data generated by the SG components bring the term energy big data into the SG industry. Similar security and privacy challenges are associated with the SG energy big data analysis. Adversaries can use the data to make decisions affecting the safe operation of the SG infrastructure. Customers' consumption information contains privacy-sensitive information that is required to be protected [103]. However, SG energy big data presents challenges to conventional data transferring, storing, and processing methods. Energy big data analytics requires new ML theories and technologies. Also, multiple big data solutions are based on cloud computing to provide the required computation and processing resources. Therefore, existing energy big data calculations inherit cloud computing security and privacy challenges as well [241].
- ***Industry 4.0***: The digitisation, automation, and widespread integration of the Internet into industrial and factory environments have created the fourth industrial revolution called Industry 4.0 [242]. The main goal of Industry 4.0 is to move from traditional factories to a networked and integrated network of machines that operate even independently and without any human resource interference. This can provide faster, more flexible and efficient facilities for producing higher quality goods at a lower cost [243]. Industry 4.0 of controlling, developing and maintaining the product line remotely. It even involves changing policies and production characteristics automatically. In addition, Industry 4.0 has paved the way for an intelligent power grid and the SG concept. Fahim *et al.* in [244] proposed the concept of SG Industry 4.0 (SGI 4.0) and studied the different wired and wireless communication technologies used in SG with their advantages and features in the concept of SGI 4.0. SGI 4.0 scalability makes power management more flexible on all domains from generation to the user because it provides remote power plants and distribution lines. In [245], the SG paradigm is investigated as a case study in the intelligent manufacturing area. This paper presents a comprehensive review of ML and DL algorithms from a communication perspective. Each algorithm has been evaluated in terms of its features, applications, and efficiency. The paper analysed ML and DL use cases in SG enabled smart manufacturing in case of efficiency and effectiveness.
Online maintenance, custom production for each person, and even simultaneous customer feedback can be implemented in Industry 4.0, also called *smart factory*. The technology also enables manufacturers to monitor the entire factory remotely and even virtually extend or build new production lines [246]. Furthermore, intelligent robots connected to ubiquitous communication networks enable production systems to perform complex and dangerous tasks without endangering workers' lives. In this case, a very safe and secure energy network is one of the basic requirements [246]. Small fluctuations or disruptions of the power supply system can cause devastating losses. In this regard, security challenges still need to be studied extensively, and several research areas can be done on this concept. In addition, there is another view of security, because industrial complexes typically consume too much energy, a malicious customer may intend to mislead his consumption pattern and steal energy from the grid, which in the long run term can cause extensive damage to providers or even cause prolonged and widespread power outages.
- ***Distributed Electrical Vehicle***: The distribution of electric vehicles is the next big step in reducing greenhouse gas emissions and creating a green and sustainable environment. The concept of intelligent transpiration is enabled by the communication capabilities of electric vehicles. However, the concept of vehicular communication is much more than just Vehicle to Vehicle (V2V) communications. New emerging communication schemes such as Vehicle to Infrastructure (V2I) such as Road Side Units (RSUs), see Fig. 10, Vehicle to Grid (V2G), Vehicle to Network (V2N), Vehicle to Pedestrian (V2P), and Vehicle to Device (V2D) make this area and its standardisation more controversial [247]. In this case, the term Vehicle to Everything (V2X) communication is proposed to gather all possible interaction scenarios between vehicles and their surroundings [248].
However, electric vehicular' dynamic systems and their unpredictable demand make the load forecasting and demand anticipation challenging for SG suppliers. This scheme is more challenging during peak hours when the system fails to provide the required power by all car owners, and this may cause passengers to wait for charging before landing at their destination. In addition, the electric vehicles' batteries typically take a while to be recharged fully. Simultaneously, the smart vehicular system can also boost the SG by injecting stored power into the network in demand. This paradigm is a part of the V2G model, using the vehicles' chargeable batteries as distributed energy storage capacities [249]. However, security and reliability are also a concern in this platform. In [250], the impact of FDI on the charging programme of electric vehicles was considered a major problem. Power suppliers plan to charge electric vehicles at regular intervals when consumption is limited, such as late at night. On the other hand, discharge stored

electricity from vehicles' batteries can ease SG rush hours demand during peak hours. This process is called valley filling and peak shaving. Piperigkos *et al.* [250] considered the attack scenario in which the adversary tries to forge the plan and send a charge request during peak hours or a discharge request to the providers during valley hours. They proved how the attacks could degrade the charging profile of the grid. Despite these investigations, considerable security challenges need to be investigated in different scenarios in life-critical vehicular communication schemes.

- ***Blockchain***: It is a decentralised consensus-based system, performing as a distributed ledger for sharing, synchronising and storing blocks of digital data. The integrity, consistency and credibility of data are ensured among users without a trusted third party authorisation [251]. They guarantee through saving and publishing all changes that any participant makes on the data to all other entities. Blockchain ensures accountability and transparency of the system by tracking participants' activities and open-source data-sharing platforms. SG requires a distributed computation and storage system with a decentralised architecture and a massive number of components. Blockchain involves all nodes in the verification process of data, and this can dispose of the computation load of central centres. It also preserves the system from various data tampering attacks [252].
  As discussed in section III, the AMI network provides an interactive platform through which utilities, energy producers, controlling entities, and consumers can exchange information. In [253], blockchain is used for demand response programmes of providers. Using blockchain technology, this work creates a decentralised, secure, and automated energy network, allowing participants to operate independently without being supervised centrally. Energy consumption information of customers is stored in blocks that are resilient to any manipulations. Authors in [254] focused on industrial control systems and their security and reliability issues. Their proposed architecture is based on blockchain and was introduced to preserve the plant operational data records. The integrity of data is ensured using an integrity checker along with a blockchain mechanism. In addition, data redundancy is achieved by implementing an efficient replication mechanism and is capable of being recovered after attacks. Despite all the opportunities blockchain systems add to SG services, multiple privacy and security issues remain unaddressed. Though users in blockchain are associated with pseudonyms to hide their identities, public access to real information about transactions can cause critical privacy concerns. As the SG blockchain network expands to cover large areas, this creates multiple and long chains, complicating maintaining security problems.
- ***Smart City***: The concept of a smart city relates to the living standards of residents and the comprehensive services they receive from energy to transportation, education, health care and entertainment [246]. The definition of a smart city may vary from community to community, and its development and expectations may not be fully defined. However, all definitions agree on the fact that a smart city must be smart and sustainable. The term smart refers to the online connection of the entire system, quick decision-making and the ability to manage remotely. This requires all IoT, D2D and other machine types and machine to human communication infrastructure to perform in harmony together. Sustainability also includes clean energy production, consumption and waste management. This can be achieved through a well-established SG, which provides clean, reliable and adequate energy for the smart society. However, concerns about citizens' privacy and residents in smart cities are still acute, and this challenge needs to be addressed in depth [255]. Fig. 10 represents a general picture of the future smart city environment, technologies and services provided by 5G communication networks as key enabler systems and the SG infrastructure. As illustrated in this figure, distributed renewable energy generation systems operate along with massive power plants to meet society's energy demand efficiently. Further, the embedded communication system allows information to flow from the utility controlling centre to customers, industries, and vehicular networks within the transportation system.

## X. CONCLUSION

Smart Grids foster quality improvements in the distribution of energy compared with legacy power networks. SGs include heterogeneous networks and rely heavily on communication networks, machine-type services, and automated remote control units. Such complex systems are vulnerable to several threats. The purpose of this survey was to provide a comprehensive overview of cyber-security and privacy issues in the SG and examine the most probable cyber-attacks that threaten power systems' infrastructure, network protocols, and applications. Overall, this survey was an attempt to cover the following context:

- We first provided an overview of the basic concepts of SG, its different services, subsystems, and components.
- The SG security requirements were then fully discussed. This was followed by various definitions and classifications of security attacks. ML-based threats against SG security requirements were also defined and reviewed in this section.
- Existing countermeasures, including prevention and detection strategies, were comprehensively explored. This survey also includes a comprehensive study on the contribution of new ML defence solutions.
- SG privacy was approached in the same way. First, the basic requirements and concepts related to privacy were studied. Potential privacy threats were examined, explained and classified in the next step, then

the existing countermeasures with their advantages and disadvantages were discussed.

- By reviewing the general guidelines and future challenges, we attempted to summarise possible research guidelines and open-ended challenges in SG.

It is important to note that a completely secure system never exists, and security concerns are never entirely eliminated in an information system. Therefore, even after full implementation, these strategies must be periodically updated and upgraded. This paper can motivate the research community to investigate the available shortcomings of the SG system.

## REFERENCES

[1] Z. Fan, P. Kulkarni, S. Gormus, C. Efthymiou, G. Kalogridis, M. Sooriyabandara, Z. Zhu, S. Lambotharan, and W. H. Chin, "Smart grid communications: Overview of research challenges, solutions, and standardization activities," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 21–38, Feb. 2013.

[2] M. Ghorbanian, S. H. Dolatabadi, M. Masjedi, and P. Siano, "Communication in smart grids: A comprehensive review on the existing and future communication and information infrastructures," *IEEE Syst. J.*, vol. 13, no. 4, pp. 4001–4014, Dec. 2019.

[3] M. Fathi and H. Bevrani, "Statistical cooperative power dispatching in interconnected microgrids," *IEEE Trans. Sustain. Energy*, vol. 4, no. 3, pp. 586–593, Jul. 2013.

[4] L. M. Camarinha-Matos, "Collaborative smart grids—A survey on trends," *Renew. Sustain. Energy Rev.*, vol. 65, pp. 283–294, Nov. 2016.

[5] B. A. Akyol, H. Kirkham, S. L. Clements, and M. D. Hadley, "A survey of wireless communications for the electric power system," Pacific Northwest Nat. Lab., Richland, WA, USA, Tech. Rep. PNNL-19084, 2010.

[6] P. P. Parikh, M. G. Kanabar, and T. S. Sidhu, "Opportunities and challenges of wireless communication technologies for smart grid applications," in *Proc. IEEE PES Gen. Meeting*, Jul. 2010, pp. 1–7.

[7] S. Grid, "2030: A national vision for electricity's second 100 years," United States America Dept. Energy, Washington, DC, USA, Tech. Rep., 2003.

[8] C. W. Gellings, *The Smart Grid: Enabling Energy Efficiency and Demand Response*. Lilburn, GA, USA: The Fairmont Press, 2009.

[9] C. Greer, D. A. Wollman, D. E. Prochaska, P. A. Boynton, J. A. Mazer, C. T. Nguyen, G. J. FitzPatrick, T. L. Nelson, G. H. Koepke, and A. R. Hefner, Jr., "NIST framework and roadmap for smart grid interoperability standards, release 3.0," Nat. Inst. Standards Technol. Eng. Lab., Gaithersburg, MD, USA, Tech. Rep., Oct. 2014.

[10] R. Ma, H.-H. Chen, Y.-R. Huang, and W. Meng, "Smart grid communication: Its challenges and opportunities," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 36–46, Mar. 2013.

[11] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 998–1010, Oct. 2012.

[12] A. A. Khan, V. Kumar, M. Ahmad, and S. Rana, "LAKAF: Lightweight authentication and key agreement framework for smart grid network," *J. Syst. Archit.*, vol. 116, Jun. 2021, Art. no. 102053.

[13] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber–physical security of a smart grid infrastructure," *Proc. IEEE*, vol. 100, no. 1, pp. 195–209, Jan. 2012.

[14] Z. E. Mrabet, N. Kaabouch, H. E. Ghazi, and H. E. Ghazi, "Cyber-security in smart grid: Survey and challenges," *Comput. Elect. Eng.*, vol. 67, pp. 469–482, Apr. 2018.

[15] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen, "Cyber security and privacy issues in smart grids," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 981–997, Oct. 2012.

[16] D. Puthal, S. P. Mohanty, S. Wilson, and U. Choppali, "Collaborative edge computing for smart villages," *IEEE Consum. Electron. Mag.*, vol. 10, no. 3, pp. 68–71, Jan. 2021.

[17] H. M. Khan, A. Khan, F. Jabeen, and A. U. Rahman, "Privacy preserving data aggregation with fault tolerance in fog-enabled smart grids," *Sustain. Cities Soc.*, vol. 64, Jan. 2021, Art. no. 102522.

[18] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Comput. Netw.*, vol. 57, no. 5, pp. 1344–1371, Apr. 2013.

[19] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1933–1954, 4th Quart., 2014.

[20] S. Tan, D. De, W.-Z. Song, J. Yang, and S. K. Das, "Survey of security advances in smart grid: A data driven approach," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 397–422, 1st Quart., 2017.

[21] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: A survey," *IET Cyber-Phys. Syst., Appl.*, vol. 1, no. 1, pp. 13–27, 2016.

[22] S. Finster and I. Baumgart, "Privacy-aware smart metering: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1732–1745, May 2014.

[23] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, "A systematic review of data protection and privacy preservation schemes for smart grid communications," *Sustain. Cities Soc.*, vol. 38, pp. 806–835, Aug. 2018.

[24] P. Kumar, Y. Lin, G. Bai, A. Paverd, J. S. Dong, and A. Martin, "Smart grid metering networks: A survey on security, privacy and open research issues," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2886–2927, Feb. 2019.

[25] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Comput. Netw.*, vol. 169, Mar. 2020, Art. no. 107094.

[26] N. I. Haque, M. H. Shahriar, M. G. Dastgir, A. Debnath, I. Parvez, A. Sarwat, and M. A. Rahman, "Machine learning in generation, detection, and mitigation of cyberattacks in smart grid: A survey," 2020, *arXiv:2010.00661*.

[27] N. N. Thilakarathne, M. K. Kagita, D. S. Lanka, and H. Ahmad, "Smart grid: A survey of architectural elements, machine learning and deep learning applications and future directions," 2020, *arXiv:2010.08094*.

[28] F. Mohammadi, "Emerging challenges in smart grid cybersecurity enhancement: A review," *Energies*, vol. 14, no. 5, p. 1380, Mar. 2021.

[29] D. Prasad, R. P. Singh, S. Mukherjee, S. Chattaraj, K. Sarkar, and M. I. Khan, "Approaches to smart grid network communication and security," in *Advances in Smart Grid Power System*. Amsterdam, The Netherlands: Elsevier, 2021, pp. 103–158.

[30] L. Cao, X. Jiang, Y. Zhao, S. Wang, D. You, and X. Xu, "A survey of network attacks on cyber-physical systems," *IEEE Access*, vol. 8, pp. 44219–44227, 2020.

[31] H. Zhang, B. Liu, and H. Wu, "Smart grid cyber-physical attack and defense: A review," *IEEE Access*, vol. 9, pp. 29641–29659, 2021.

[32] D. Zhang, Q.-G. Wang, G. Feng, Y. Shi, and A. V. Vasilakos, "A survey on attack detection, estimation and control of industrial cyber–physical systems," *ISA Trans.*, vol. 116, pp. 1–16, Oct. 2021.

[33] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, "Smart grid technologies: Communication technologies and standards," *IEEE Trans. Ind. Informat.*, vol. 7, no. 4, pp. 529–539, Nov. 2011.

[34] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid—The new and improved power grid: A survey," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 944–980, 4th Quart., 2012.

[35] C.-H. Lo and N. Ansari, "The progressive smart grid system from both power and communications aspects," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 3, pp. 799–821, Jul. 2012.

[36] A. Abdrabou, "A wireless communication architecture for smart grid distribution networks," *IEEE Syst. J.*, vol. 10, no. 1, pp. 251–261, Mar. 2016.

[37] M. Erol-Kantarci and H. T. Mouftah, "Smart grid forensic science: Applications, challenges, and open issues," *IEEE Commun. Mag.*, vol. 51, no. 1, pp. 68–74, Jan. 2013.

[38] A. Zaballos, A. Vallejo, and J. M. Selga, "Heterogeneous communication architecture for the smart grid," *IEEE Netw.*, vol. 25, no. 5, pp. 30–37, Sep./Oct. 2011.

[39] W. Wang, Y. Xu, and M. Khanna, "A survey on the communication architectures in smart grid," *Comput. Netw.*, vol. 55, no. 15, pp. 3604–3629, 2011.

[40] M. Kuzlu, M. Pipattanasomporn, and M. Rahman, "Communication network requirements for major smart grid applications in HAN, NAN and WAN," *Comput. Netw.*, vol. 67, pp. 74–88, Jul. 2014.

[41] M. Erol-Kantarci and H. T. Mouftah, "Energy-efficient information and communication infrastructures in the smart grid: A survey on interactions and open issues," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 179–197, Mar. 2015.

[42] W. Meng, R. Ma, and H.-H. Chen, "Smart grid neighborhood area networks: A survey," *IEEE Netw.*, vol. 28, no. 1, pp. 24–32, Jan. 2014.

[43] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, "A survey on smart grid potential applications and communication requirements," *IEEE Trans. Ind. Informat.*, vol. 9, no. 1, pp. 28–42, Feb. 2012.

[44] R. R. Mohassel, A. Fung, F. Mohammadi, and K. Raahemifar, "A survey on advanced metering infrastructure," *Int. J. Elect. Power Energy Syst.*, vol. 63, pp. 473–484, Dec. 2014.

[45] Y. Kabalci, "A survey on smart metering and smart grid communication," *Renew. Sustain. Energy Rev.*, vol. 57, pp. 302–318, May 2016.

[46] A. Ghosal and M. Conti, "Key management systems for smart grid advanced metering infrastructure: A survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2831–2848, Mar. 2019.

[47] N. K. Singh and V. Mahajan, "End-user privacy protection scheme from cyber intrusion in smart grid advanced metering infrastructure," *Int. J. Crit. Infrastructure Protection*, vol. 34, Sep. 2021, Art. no. 100410.

[48] J. Gao, J. Liu, B. Rajan, R. Nori, B. Fu, Y. Xiao, W. Liang, and C. L. P. Chen, "SCADA communication and security issues," *Secur. Commun. Netw.*, vol. 7, no. 1, pp. 175–194, Jan. 2014.

[49] M. S. Thomas, P. Kumar, and V. K. Chandna, "Design, development, and commissioning of a supervisory control and data acquisition (SCADA) laboratory for research and training," *IEEE Trans. Power Syst.*, vol. 19, no. 3, pp. 1582–1588, Aug. 2004.

[50] K. Sayed and H. A. Gabbar, "Scada and smart energy grid control automation," in *Smart Energy Grid Engineering*. Amsterdam, The Netherlands: Elsevier, 2017, pp. 481–514.

[51] T.-H. Kim, "Securing communication of SCADA components in smart grid environment," *Int. J. Syst. Appl., Eng. Develop.*, vol. 5, no. 2, pp. 135–142, 2011.

[52] S. Iyer, "Cyber security for smart grid, cryptography, and privacy," *Int. J. Digit. Multimedia Broadcast.*, vol. 2011, pp. 1–8, Oct. 2011.

[53] H. H. Safa, D. M. Souran, M. Ghasempour, and A. Khazaee, *Cyber Security of Smart Grid and SCADA Systems, Threats and Risks*. Edison, NJ, USA: IET, 2016.

[54] G. Yadav and K. Paul, "Architecture and security of SCADA systems: A review," *Int. J. Crit. Infrastruct. Protection*, vol. 34, Sep. 2021, Art. no. 100433.

[55] F. M. Cleveland, "Cyber security issues for advanced metering infrasttructure (AMI)," in *Proc. 21st IEEE Power Energy Soc. Gen. Meeting-Convers. Del. Electr. Energy*, Jul. 2008, pp. 1–5.

[56] M. Kim, "A survey on guaranteeing availability in smart grid communications," in *Proc. 14th Int. Conf. Adv. Commun. Technol. (ICACT)*, 2012, pp. 314–317.

[57] A. Farao, E. Veroni, C. Ntantogian, and C. Xenakis, "P4G2Go: A privacy-preserving scheme for roaming energy consumers of the smart grid-to-go," *Sensors*, vol. 21, no. 8, p. 2686, Apr. 2021.

[58] W. Stallings, *Cryptography and Network Security, 4/E*. London, U.K.: Pearson, 2006.

[59] M. Scholl and R. Jain, "Availability and sensitivity analysis of smart grid components," Tech. Rep., 2011. [Online]. Available: http://www1.cse.wustl.edu/~jain/cse567-11/index.html

[60] J. Liu, Y. Xiao, and J. Gao, "Achieving accountability in smart grid," *IEEE Syst. J.*, vol. 8, no. 2, pp. 493–508, Jun. 2014.

[61] S. Uludag, S. Zeadally, and M. Badra, "Techniques, taxonomy, and challenges of privacy protection in the smart grid," in *Privacy in a Digital, Networked World*. Cham, Switzerland: Springer, 2015, pp. 343–390.

[62] N. Chowdhury, "A survey of cryptography-based authentication for smart grid communication," in *Computer Security*. Cham, Switzerland: Springer, 2020, pp. 52–66.

[63] D.-E. Cho, S.-S. Yeo, and S.-J. Kim, "Authentication method for privacy protection in smart grid environment," *J. Appl. Math.*, vol. 2014, pp. 1–10, Jan. 2014.

[64] L. Zhang, L. Zhao, S. Yin, C.-H. Chi, R. Liu, and Y. Zhang, "A lightweight authentication scheme with privacy protection for smart grid communications," *Future Gener. Comput. Syst.*, vol. 100, pp. 770–778, Nov. 2019.

[65] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. Shen, "A lightweight message authentication scheme for smart grid communications," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 675–685, Dec. 2011.

[66] Z. Guan, Y. Zhang, L. Zhu, L. Wu, and S. Yu, "EFFECT: An efficient flexible privacy-preserving data aggregation scheme with authentication in smart grid," *Sci. China-Inf. Sci.*, vol. 62, no. 3, p. 32103, Mar. 2019.

[67] C. R. Taylor, C. A. Shue, and N. R. Paul, "A deployable SCADA authentication technique for modern power grids," in *Proc. IEEE Int. Energy Conf. (ENERGYCON)*, May 2014, pp. 696–702.

[68] N. Saxena, B. J. Choi, and R. Lu, "Authentication and authorization scheme for various user roles and devices in smart grid," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 5, pp. 907–921, May 2016.

[69] J. Liu, Y. Xiao, and J. Gao, "Accountability in smart grids," in *Proc. IEEE Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2011, pp. 1166–1170.

[70] M. Z. Gunduz and R. Das, "Analysis of cyber-attacks on smart grid applications," in *Proc. Int. Conf. Artif. Intell. Data Process. (IDAP)*, Sep. 2018, pp. 1–5.

[71] C. Valli, A. Woodward, C. Carpene, P. Hannay, M. Brand, R. Karvinen, and C. Holme, "Eavesdropping on the smart grid," in *Proc. Austral. Digit. Forensics Conf.*, pp. 54–60.

[72] N. M. Pindoriya, D. Dasgupta, D. Srinivasan, and M. Carvalho, "Infrastructure security for smart electric grids: A survey," in *Optimization and Security Challenges in Smart Power Grids*. Cham, Switzerland: Springer, 2013, pp. 161–180.

[73] J. Chaudhry, U. Qidwai, and M. H. Miraz, "Securing big data from eavesdropping attacks in SCADA/ICS network data streams through impulsive statistical fingerprinting," in *Proc. Int. Conf. Emerg. Technol. Comput.* Cham, Switzerland: Springer, 2019, pp. 77–89.

[74] E. Germano da Silva, L. A. Dias Knob, J. A. Wickboldt, L. P. Gaspary, L. Z. Granville, and A. Schaeffer-Filho, "Capitalizing on SDN-based SCADA systems: An anti-eavesdropping case-study," in *Proc. IFIP/IEEE Int. Symp. Integr. Netw. Manage. (IM)*, May 2015, pp. 165–173.

[75] S. Liu, X. P. Liu, and A. El Saddik, "Denial-of-service (DoS) attacks on load frequency control in smart grids," in *Proc. IEEE PES Innov. Smart Grid Technol. Conf. (ISGT)*, Feb. 2013, pp. 1–6.

[76] P. Yi, T. Zhu, Q. Zhang, Y. Wu, and L. Pan, "Puppet attack: A denial of service attack in advanced metering infrastructure network," *J. Netw. Comput. Appl.*, vol. 59, pp. 325–332, Jan. 2016.

[77] M. Attia, S. M. Senouci, H. Sedjelmaci, E.-H. Aglzim, and D. Chrenko, "An efficient intrusion detection system against cyber-physical attacks in the smart grid," *Comput. Electr. Eng.*, vol. 68, pp. 499–512, May 2018.

[78] M. M. Pour, A. Anzalchi, and A. Sarwat, "A review on cyber security issues and mitigation methods in smart grid systems," in *Proc. SoutheastCon*, Mar. 2017, pp. 1–4.

[79] R. Algin, H. O. Tan, and K. Akkaya, "Mitigating selective jamming attacks in smart meter data collection using moving target defense," in *Proc. 13th ACM Symp. QoS Secur. Wireless Mobile Netw. (Q SWinet)*, 2017, pp. 1–8.

[80] J. Ma, Y. Liu, L. Song, and Z. Han, "Multiact dynamic game strategy for jamming attack in electricity market," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2273–2282, Sep. 2015.

[81] A. Anwar, A. N. Mahmood, and M. Pickering, "Modeling and performance evaluation of stealthy false data injection attacks on smart grid in the presence of corrupted measurements," *J. Comput. Syst. Sci.*, vol. 83, no. 1, pp. 58–72, Feb. 2017.

[82] E. Hossain, I. Khan, F. Un-Noor, S. S. Sikander, and M. S. H. Sunny, "Application of big data and machine learning in smart grid, and associated security concerns: A review," *IEEE Access*, vol. 7, pp. 13960–13988, 2019.

[83] R. Nawaz, M. A. Shahid, I. M. Qureshi, and M. H. Mehmood, "Machine learning based false data injection in smart grid," in *Proc. 1st Int. Conf. Power, Energy Smart Grid (ICPESG)*, Apr. 2018, pp. 1–6.

[84] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011.

[85] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 13, pp. 1–33, May 2011.

[86] C.-H. Lo and N. Ansari, "CONSUMER: A novel hybrid intrusion detection system for distribution networks in smart grid," *IEEE Trans. Emerg. Topics Comput.*, vol. 1, no. 1, pp. 33–44, Jun. 2013.

[87] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 2027–2051, 3rd Quart., 2016.

[88] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, E. G. Im, Z. Yao, B. Pranggono, and H. F. Wang, "Man-in-the-middle attack test-bed investigating cyber-security vulnerabilities in smart grid SCADA systems," 2012, p. 138.

[89] E. N. Yrlmaz, H. H. Sayan, F. Üstünsoy, S. Gönen, and G. Karacayilmaz, "Cyber security analysis of DoS and MitM attacks against PLCs used in smart grids," in *Proc. 7th Int. Istanbul Smart Grids Cities Congr. Fair (ICSG)*, Apr. 2019, pp. 36–40.

[90] S. Adepu, N. K. Kandasamy, J. Zhou, and A. Mathur, "Attacks on smart grid: Power supply interruption and malicious power generation," *Int. J. Inf. Secur.*, vol. 19, pp. 1–23, Apr. 2019.

[91] R. Khan, P. Maynard, K. McLaughlin, D. M. Laverty, and S. Sezer, "Threat analysis of BlackEnergy malware for synchrophasor based real-time control and monitoring in smart grid," in *Proc. Electron. Workshops Comput.*, Oct. 2016, pp. 53–63.

[92] B. Chen, K. L. Butler-Purry, A. Goulart, and D. Kundur, "Implementing a real-time cyber-physical system test bed in RTDS and OPNET," in *Proc. North Amer. Power Symp. (NAPS)*, Sep. 2014, pp. 1–6.

[93] P. Wlazlo, A. Sahu, Z. Mao, H. Huang, A. Goulart, K. Davis, and S. Zonouz, "Man-in-the-middle attacks and defense in a power system cyber-physical testbed," 2021, *arXiv:2102.11455*.

[94] T. S. Ustun, S. M. Farooq, and S. M. S. Hussain, "A novel approach for mitigation of replay and masquerade attacks in smartgrids using IEC 61850 standard," *IEEE Access*, vol. 7, pp. 156044–156053, 2019.

[95] Z. A. Baig and A.-R. Amoudi, "An analysis of smart grid attacks and countermeasures," *J. Commun.*, vol. 8, no. 8, pp. 473–479, 2013.

[96] J. Zhao, J. Wang, and L. Yin, "Detection and control against replay attacks in smart grid," in *Proc. 12th Int. Conf. Comput. Intell. Secur. (CIS)*, Dec. 2016, pp. 624–627.

[97] D. Grochocki, J. H. Huh, R. Berthier, R. Bobba, W. H. Sanders, A. A. Cárdenas, and J. G. Jetcheva, "AMI threats, intrusion detection requirements and deployment recommendations," in *Proc. IEEE 3rd Int. Conf. Smart Grid Commun. (SmartGridComm)*, Nov. 2012, pp. 395–400.

[98] R. Nawaz, R. Akhtar, M. A. Shahid, I. M. Qureshi, and M. H. Mahmood, "Machine learning based false data injection in smart grid," *Int. J. Electr. Power Energy Syst.*, vol. 130, Sep. 2021, Art. no. 106819.

[99] D. G. Victor, *How Artificial Intelligence Will Affect the Future of Energy and Climate* (A BluePrint for the Future of AI). Brookings Institute, Jan. 2019.

[100] M. Rege and R. B. K. Mbah, "Machine learning for cyber defense and attack," *Data Anal.*, p. 83, Nov. 2018.

[101] A. Dey, "Machine learning algorithms: A review," *Int. J. Comput. Sci. Inf. Technol.*, vol. 7, no. 3, pp. 1174–1179, 2016.

[102] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor, "Machine learning methods for attack detection in the smart grid," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 27, no. 8, pp. 1773–1786, Mar. 2015.

[103] Y. Sun, M. Peng, Y. Zhou, Y. Huang, and S. Mao, "Application of machine learning in wireless networks: Key techniques and open issues," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3072–3108, 4th Quart., 2019.

[104] B. Li, S. Gangadhar, S. Cheng, and P. K. Verma, "Predicting user comfort level using machine learning for smart grid environments," in *Proc. ISGT*, Jan. 2011, pp. 1–6.

[105] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1153–1176, Oct. 2016.

[106] K. Trieu and Y. Yang, "Artificial intelligence-based password brute force attacks," in *Proc. MWAIS*, vol. 39, 2018.

[107] W. Hu and Y. Tan, "Generating adversarial malware examples for black-box attacks based on GAN," 2017, *arXiv:1702.05983*.

[108] L. Huang, A. D. Joseph, B. Nelson, B. I. Rubinstein, and J. D. Tygar, "Adversarial machine learning," in *Proc. 4th ACM Workshop Secur. Artif. Intell.*, 2011, pp. 43–58.

[109] B. Biggio, G. Fumera, and F. Roli, "Security evaluation of pattern classifiers under attack," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 4, pp. 984–996, Apr. 2013.

[110] B. Biggio, B. Nelson, and P. Laskov, "Poisoning attacks against support vector machines," 2012, *arXiv:1206.6389*.

[111] B. Biggio, I. Corona, D. Maiorca, B. Nelson, N. Šrndić, P. Laskov, G. Giacinto, and F. Roli, "Evasion attacks against machine learning at test time," in *Proc. Eur. Conf. Mach. Learn. Knowl. Discovery Databases*. Cham, Switzerland: Springer, 2013, pp. 387–402.

[112] E. Tabassi, K. J. Burns, M. Hadjimichael, A. D. Molina-Markham, and J. T. Sexton, "A taxonomy and terminology of adversarial machine learning," NIST IR, Tech. Rep., Oct. 2019, pp. 1–29.

[113] I. Moisejevs, "Poisoning attacks on machine learning," Tech. Rep., vol. 29, Jan. 2019, p. 2020. [Online]. Available: https://towardsdatascience.com/poisoning-attacks-on-machine-learning-1ff247c254db

[114] G. Costa, F. Pinelli, S. Soderi, and G. Tolomei, "Covert channel attack to federated learning systems," 2021, *arXiv:2104.10561*.

[115] A. Sayghe, O. M. Anubi, and C. Konstantinou, "Adversarial examples on power systems state estimation," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Feb. 2020, pp. 1–5.

[116] B. Biggio and F. Roli, "Wild patterns: Ten years after the rise of adversarial machine learning," *Pattern Recognit.*, vol. 84, pp. 317–331, Dec. 2018.

[117] A. Sayghe, J. Zhao, and C. Konstantinou, "Evasion attacks with adversarial deep learning against power system state estimation," in *Proc. IEEE Power Energy Society General Meeting*, Aug. 2020, pp. 1–5.

[118] Y. Liang, D. He, and D. Chen, "Poisoning attack on load forecasting," in *Proc. IEEE Innov. Smart Grid Technol. Asia (ISGT Asia)*, May 2019, pp. 1230–1235.

[119] E. Anthi, L. Williams, M. Rhode, P. Burnap, and A. Wedgbury, "Adversarial attacks on machine learning cybersecurity defences in industrial control systems," 2020, *arXiv:2004.05005*.

[120] A. Erba, R. Taormina, S. Galelli, M. Pogliani, M. Carminati, S. Zanero, and N. O. Tippenhauer, "Constrained concealment attacks against reconstruction-based anomaly detectors in industrial control systems," 2019, *arXiv:1907.07487*.

[121] I. Niazazari and H. Livani, "Attack on grid event cause analysis: An adversarial machine learning approach," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Feb. 2020, pp. 1–5.

[122] J. Li, Y. Yang, and J. S. Sun, "SearchFromFree: Adversarial measurements for machine learning-based energy theft detection," 2020, *arXiv:2006.03504*.

[123] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and harnessing adversarial examples," 2014, *arXiv:1412.6572*.

[124] M. Zanetti, E. Jamhour, M. Pellenz, M. Penna, V. Zambenedetti, and I. Chueiri, "A tunable fraud detection system for advanced metering infrastructure using short-lived patterns," *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 830–840, Jan. 2017.

[125] P. Jokar, N. Arianpoo, and V. C. M. Leung, "Electricity theft detection in AMI using customers' consumption patterns," *IEEE Trans. Smart Grid*, vol. 7, no. 1, pp. 216–226, Jan. 2016.

[126] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, "Generative adversarial nets," in *Proc. Adv. Neural Inf. Process. Syst.*, 2014, pp. 2672–2680.

[127] C. Zhang, S. R. Kuppannagari, R. Kannan, and V. K. Prasanna, "Generative adversarial network for synthetic time series data generation in smart grids," in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids (SmartGridComm)*, Oct. 2018, pp. 1–6.

[128] Z. Wang and T. Hong, "Generating realistic building electrical load profiles through the generative adversarial network (GAN)," *Energy Buildings*, vol. 224, Oct. 2020, Art. no. 110299.

[129] H. Ying, X. Ouyang, S. Miao, and Y. Cheng, "Power message generation in smart grid via generative adversarial network," in *Proc. IEEE 3rd Inf. Technol., Netw., Electron. Autom. Control Conf. (ITNEC)*, Mar. 2019, pp. 790–793.

[130] S. Ahmadian, H. Malki, and Z. Han, "Cyber attacks on smart energy grids using generative adverserial networks," in *Proc. Global Conf. Signal Inf. Process. (Globalsip)*, Nov. 2018, pp. 942–946.

[131] F. Marulli and C. A. Visaggio, "Adversarial deep learning for energy management in buildings," in *Proc. SummerSim*, 2019, pp. 1–50.

[132] A. Kumar and A. Agarwal, "Research issues related to cryptography algorithms and key generation for smart grid: A survey," in *Proc. 7th India Int. Conf. Power Electron. (IICPE)*, Nov. 2016, pp. 1–5.

[133] O. G. Abood, M. A. Elsadd, and S. K. Guirguis, "Investigation of cryptography algorithms used for security and privacy protection in smart grid," in *Proc. 19th Int. Middle East Power Syst. Conf. (MEPCON)*, Dec. 2017, pp. 644–649.

[134] X. He, M.-O. Pun, and C.-C.-J. Kuo, "Secure and efficient cryptosystem for smart grid using homomorphic encryption," in *Proc. IEEE PES Innov. Smart Grid Technol. (ISGT)*, Jan. 2012, pp. 1–8.

[135] L. Yan, Y. Chang, and S. Zhang, "A lightweight authentication and key agreement scheme for smart grid," *Int. J. Distrib. Sensor Netw.*, vol. 13, no. 2, 2017, Art. no. 1550147717694173.

[136] M. Shariat and M. Safkhani, "How the control over smart meters is lost in the Yan et al. Lightweight AKA scheme for smart grids," in *Proc. 9th Int. Conf. Inf. Knowl. Technol. (IKT)*, Oct. 2017, pp. 82–84.

[137] J. Li, X. Niu, and J. S. Sun, "A practical searchable symmetric encryption scheme for smart grid data," 2018, *arXiv:1808.00645*.

[138] M. Kaur, P. Jain, and R. Kumar, "Data encryption and key wrapping for the smart grid security," *Int. J. Eng. Tech. Res.*, vol. 9, no. 8, Aug. 2019.

[139] S. Ahmed, Y. Lee, S.-H. Hyun, and I. Koo, "Covert cyber assault detection in smart grid networks utilizing feature selection and Euclidean distance-based machine learning," *Appl. Sci.*, vol. 8, no. 5, p. 772, 2018.

[140] A. Monticelli, "Electric power system state estimation," *Proc. IEEE*, vol. 88, no. 2, pp. 262–282, Feb. 2000.

[141] Z. Hu, Y. Wang, X. Tian, X. Yang, D. Meng, and R. Fan, "False data injection attacks identification for smart grids," in *Proc. 3rd Int. Conf. Technol. Adv. Electr., Electron. Comput. Eng. (TAEECE)*, Apr. 2015, pp. 139–143.

[142] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor, "Smarter security in the smart grid," in *Proc. IEEE 3rd Int. Conf. Smart Grid Commun. (SmartGridComm)*, Nov. 2012, pp. 312–317.

[143] J. Yan, B. Tang, and H. He, "Detection of false data attacks in smart grid with supervised learning," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, Jul. 2016, pp. 1395–1402.

[144] H. Hosseini, S. M. T. Bathaee, A. Abedini, M. Hosseina, and A. Fereidunain, "Defending false data injection attack on smart grid network using neuro-fuzzy controller," *J. Intell. Fuzzy Syst.*, vol. 27, no. 3, pp. 1457–1467, 2014.

[145] M. Ashrafuzzaman, Y. Chakhchoukh, A. A. Jillepalli, P. T. Tosic, D. C. de Leon, F. T. Sheldon, and B. K. Johnson, "Detecting stealthy false data injection attacks in power grids using deep learning," in *Proc. 14th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2018, pp. 219–225.

[146] N. Elmrabit, F. Zhou, F. Li, and H. Zhou, "Evaluation of machine learning algorithms for anomaly detection," in *Proc. Int. Conf. Cyber Secur. Protection Digit. Services (Cyber Secur.)*, Jun. 2020, pp. 1–8.

[147] A. Yaar, A. Perrig, and D. Song, "Pi: A path identification mechanism to defend against DDoS attacks," in *Proc. 19th Int. Conf. Data Eng.*, 2003, pp. 93–107.

[148] J. Hong, C.-C. Liu, and M. Govindarasu, "Detection of cyber intrusions using network-based multicast messages for substation automation," in *Proc. ISGT*, Feb. 2014, pp. 1–5.

[149] S. Shitharth and D. P. Winston, "A novel IDS technique to detect DDoS and sniffers in smart grid," in *Proc. World Conf. Futuristic Trends Res. Innov. Social Welfare (Startup Conclave)*, Feb. 2016, pp. 1–6.

[150] W. Zhe, C. Wei, and L. Chunlin, "DoS attack detection model of smart grid based on machine learning method," in *Proc. IEEE Int. Conf. Power, Intell. Comput. Syst. (ICPICS)*, Jul. 2020, pp. 735–738.

[151] B. Vaidya, D. Makrakis, and H. T. Mouftah, "Device authentication mechanism for smart energy home area networks," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2011, pp. 787–788.

[152] H. Nicanfar, P. Jokar, K. Beznosov, and V. C. M. Leung, "Efficient authentication and key management mechanisms for smart grid communications," *IEEE Syst. J.*, vol. 8, no. 2, pp. 629–640, Jun. 2014.

[153] Z. C. Dong, R. Espejo, Y. Wan, and W. Zhuang, "Detecting and locating man-in-the-middle attacks in fixed wireless networks," *J. Comput. Inf. Technol.*, vol. 23, no. 4, pp. 283–293, 2015.

[154] M. Salpekar, "Protecting smart grid and advanced metering infrastructure," in *Proc. 2nd Int. Conf. I-SMAC (IoT Social, Mobile, Analytics Cloud) (I-SMAC)I-SMAC (IoT Social, Mobile, Analytics Cloud) (I-SMAC), 2nd Int. Conf.*, Aug. 2018, pp. 22–26.

[155] C. Ergen and B. Gulbahar, "Theoretical modelling of smart meter privacy protection with multi-meter energy routing," in *Proc. IEEE Int. Conf. Smart Internet Things (SmartIoT)*, Aug. 2020, pp. 140–146.

[156] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Proc. 47th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Sep. 2009, pp. 911–918.

[157] T.-T. Tran, O.-S. Shin, and J.-H. Lee, "Detection of replay attacks in smart grid systems," in *Proc. Int. Conf. Comput., Manage. Telecommun. (ComManTel)*, Jan. 2013, pp. 298–302.

[158] R. Berthier, W. H. Sanders, and H. Khurana, "Intrusion detection for advanced metering infrastructures: Requirements and architectural directions," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, Oct. 2010, pp. 350–355.

[159] C.-W. Ten, J. Hong, and C.-C. Liu, "Anomaly detection for cybersecurity of the substations," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 865–873, Dec. 2011.

[160] Y. Zhang, L. Wang, W. Sun, R. C. Green, and M. Alam, "Distributed intrusion detection system in a multi-layer network architecture of smart grids," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 796–808, Dec. 2011.

[161] V. V. V., N. Radhika, and V. Vanitha, "Intruder detection and prevention in a smart grid communication system," *Proc. Technol.*, vol. 21, pp. 393–399, Jan. 2015.

[162] I. Ullah and Q. H. Mahmoud, "An intrusion detection framework for the smart grid," in *Proc. IEEE 30th Can. Conf. Electr. Comput. Eng. (CCECE)*, Apr. 2017, pp. 1–5.

[163] T. Andrysiak, Ł. Saganowski, and P. Kiedrowski, "Anomaly detection in smart metering infrastructure with the use of time series analysis," *J. Sensors*, vol. 2017, pp. 1–15, Jul. 2017.

[164] B. Rossi, S. Chren, B. Buhnova, and T. Pitner, "Anomaly detection in smart grid data: An experience report," in *Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC)*, Oct. 2016, pp. 002313–002318.

[165] C. Promper, D. Engel, and R. C. Green, "Anomaly detection in smart grids with imbalanced data methods," in *Proc. IEEE Symp. Ser. Comput. Intell. (SSCI)*, Nov. 2017, pp. 1–8.

[166] R. Berthier and W. H. Sanders, "Specification-based intrusion detection for advanced metering infrastructures," in *Proc. IEEE 17th Pacific Rim Int. Symp. Dependable Comput.*, Dec. 2011, pp. 184–193.

[167] N. Beigi-Mohammadi, J. Mišić, H. Khazaei, and V. B. Mišić, "An intrusion detection system for smart grid neighborhood area network," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2014, pp. 4125–4130.

[168] P. Jokar, H. Nicanfar, and V. C. M. Leung, "Specification-based intrusion detection for home area networks in smart grids," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Oct. 2011, pp. 208–213.

[169] R. C. Borges Hink, J. M. Beaver, M. A. Buckner, T. Morris, U. Adhikari, and S. Pan, "Machine learning for power system disturbance and cyber-attack discrimination," in *Proc. 7th Int. Symp. Resilient Control Syst. (ISRCS)*, Aug. 2014, pp. 1–8.

[170] A. S. Musleh, G. Chen, and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2218–2234, May 2020.

[171] J. Sakhnini, H. Karimipour, and A. Dehghantanha, "Smart grid cyber attacks detection using supervised learning and heuristic feature selection," in *Proc. IEEE 7th Int. Conf. Smart Energy Grid Eng. (SEGE)*, Aug. 2019, pp. 108–112.

[172] S. Ahmed, Y. Lee, H. Seung-Ho, and I. Koo, "Unsupervised machine learning-based detection of covert data integrity assault in smart grid networks utilizing isolation forest," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 10, pp. 2765–2777, Mar. 2019.

[173] H. Karimipour, A. Dehghantanha, R. M. Parizi, K.-K. R. Choo, and H. Leung, "A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids," *IEEE Access*, vol. 7, pp. 80778–80788, 2019.

[174] M. N. Kurt, O. Ogundijo, C. Li, and X. Wang, "Online cyber-attack detection in smart grid: A reinforcement learning approach," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5174–5185, Sep. 2018.

[175] D. An, Q. Yang, W. Liu, and Y. Zhang, "Defending against data integrity attacks in smart grid: A deep reinforcement learning-based approach," *IEEE Access*, vol. 7, pp. 110835–110845, 2019.

[176] D. Eckhoff and I. Wagner, "Privacy in the smart city—Applications, technologies, challenges, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 489–516, Sep. 2018.

[177] R. Boussada, M. E. Elhdhili, and L. A. Saidane, "A survey on privacy: Terminology, mechanisms and attacks," in *Proc. IEEE/ACS 13th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Nov. 2016, pp. 1–7.

[178] J.-F. Raymond, "Traffic analysis: Protocols, attacks, design issues, and open problems," in *Designing Privacy Enhancing Technologies*. Cham, Switzerland: Springer, 2001, pp. 10–29.

[179] B. Hitaj, P. Gasti, G. Ateniese, and F. Perez-Cruz, "PassGAN: A deep learning approach for password guessing," in *Proc. Int. Conf. Appl. Cryptogr. Netw. Secur.* Cham, Switzerland: Springer, 2019, pp. 217–237.

[180] H. Shen, M. Zhang, and J. Shen, "Efficient privacy-preserving cube-data aggregation scheme for smart grids," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 6, pp. 1369–1381, Jun. 2017.

[181] J. Xia and Y. Wang, "Secure key distribution for the smart grid," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1437–1443, Sep. 2012.

[182] W.-B. Leea, T.-H. Chen, W.-R. Sun, and K. I.-J. Ho, "An S/Key-like one-time password authentication scheme using smart cards for smart meter," in *Proc. 28th Int. Conf. Adv. Inf. Netw. Appl. Workshops*, May 2014, pp. 281–286.

[183] T.-C. Yeh, H.-Y. Shen, and J.-J. Hwang, "A secure one-time password authentication scheme using smart cards," *IEICE Trans. Commun.*, vol. 85, no. 11, pp. 2515–2518, 2002.

[184] Z. Xiang, H. Guangyu, and W. Zhigong, "Masquerade detection using support vector machines in the smart grid," in *Proc. 7th Int. Joint Conf. Comput. Sci. Optim.*, Jul. 2014, pp. 30–34.

[185] P. Risbud, N. Gatsis, and A. Taha, "Vulnerability analysis of smart grids to GPS spoofing," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3535–3548, Jul. 2018.

[186] R. Prasad and V. Rohokale, *Cyber Security: The Lifeline of Information and Communication Technology*. Cham, Switzerland: Springer, 2020.

[187] R. Alabdan, "Phishing attacks survey: Types, vectors, and technical approaches," *Future Internet*, vol. 12, no. 10, p. 168, Sep. 2020.

[188] H. Holm, W. R. Flores, and G. Ericsson, "Cyber security for a smart grid–what about phishing?" in *Proc. IEEE PES ISGT Eur.*, Oct. 2013, pp. 1–5.

[189] D. U. Case, "Analysis of the cyber attack on the Ukrainian power grid," *Electr. Inf. Sharing Anal. Center*, vol. 388, pp. 1–29, Mar. 2016.

[190] I.-C. Alert, "Cyber-attack against Ukrainian critical infrastructure," Cybersecurity Infrastruct. Secur. Agency, Washington, DC, USA, Tech. Rep. ICS Alert (IR-ALERT-H-16-056-01), 2016.

[191] Z. Wang, "An identity-based data aggregation protocol for the smart grid," *IEEE Trans. Ind. Informat.*, vol. 13, no. 5, pp. 2428–2435, Oct. 2017.

[192] G. Kalogridis, M. Sooriyabandara, Z. Fan, and M. A. Mustafa, "Toward unified security and privacy protection for smart meter networks," *IEEE Syst. J.*, vol. 8, no. 2, pp. 641–654, Jun. 2013.

[193] S. Finster and I. Baumgart, "Elderberry: A peer-to-peer, privacy-aware smart metering protocol," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 37–42.

[194] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "PASS: Privacy-preserving authentication scheme for smart grid network," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Oct. 2011, pp. 196–201.

[195] F. Siddiqui, S. Zeadally, C. Alcaraz, and S. Galvao, "Smart grid privacy: Issues and solutions," in *Proc. 21st Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul. 2012, pp. 1–5.

[196] W. Kong, J. Shen, P. Vijayakumar, Y. Cho, and V. Chang, "A practical group blind signature scheme for privacy protection in smart grid," *J. Parallel Distrib. Comput.*, vol. 136, pp. 29–39, Feb. 2020.

[197] W. Zhang, Z. Guo, N. Li, M. Li, Q. Fan, and M. Luo, "A blind signature-aided privacy-preserving power request scheme for smart grid," *Wireless Commun. Mobile Comput.*, vol. 2021, pp. 1–10, Jun. 2021.

[198] J. Zhao, T. Jung, Y. Wang, and X. Li, "Achieving differential privacy of data disclosure in the smart grid," in *Proc. IEEE Conf. Comput. Commun. (IEEE INFOCOM)*, Apr. 2014, pp. 504–512.

[199] V. Arzamasov, R. Schwerdt, S. Karrari, K. Böhm, and T. B. Nguyen, "Privacy measures and storage technologies for battery-based load hiding—An overview and experimental study," in *Proc. 11th ACM Int. Conf. Future Energy Syst.*, Jun. 2020, pp. 178–195.

[200] G. Ács and C. Castelluccia, "I have a DREAM! (Differentially private smart metering)," in *Proc. Int. Workshop Inf. Hiding*. Cham, Switzerland: Springer, 2011, pp. 118–132.

[201] J. Marks, B. Montano, J. Chong, M. Raavi, R. Islam, T. Cerny, and D. Shin, "Differential privacy applied to smart meters: A mapping study," in *Proc. 36th Annu. ACM Symp. Appl. Comput.*, Mar. 2021, pp. 761–770.

[202] H. Bao and R. Lu, "A new differentially private data aggregation with fault tolerance for smart grid communications," *IEEE Internet Things J.*, vol. 2, no. 3, pp. 248–258, Jun. 2015.

[203] H. Cao, S. Liu, R. Zhao, and X. Xiong, "IFed: A novel federated learning framework for local differential privacy in power Internet of Things," *Int. J. Distrib. Sensor Netw.*, vol. 16, no. 5, 2020, Art. no. 1550147720919698.

[204] H. Liu, X. Zhang, X. Shen, and H. Sun, "A federated learning framework for smart grids: Securing power traces in collaborative learning," 2021, *arXiv:2103.11870*.

[205] P. H. Mirzaee, M. Shojafar, Z. Pooranian, P. Asef, H. Cruickshank, and R. Tafazolli, "FIDS: A federated intrusion detection system for 5G smart metering network," in *Proc. 17th Int. Conf. Mobility, Sens. Netw.*, 2021, pp. 215–222.

[206] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Proc. Annu. Int. Cryptol. Conf.* Cham, Switzerland: Springer, 2001, pp. 213–229.

[207] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, and R. Cepeda, "Privacy for smart meters: Towards undetectable appliance load signatures," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, Oct. 2010, pp. 232–237.

[208] E. L. Quinn, "Privacy and the new energy infrastructure," *Social Sci. Res. Netw.*, 2009, doi: 10.2139/ssrn.1370731.

[209] K. Chaudhuri and C. Monteleoni, "Privacy-preserving logistic regression," in *Proc. NIPS*, vol. 8, 2008, pp. 289–296.

[210] S. Finster and I. Baumgart, "Pseudonymous smart metering without a trusted third party," in *Proc. 12th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Jul. 2013, pp. 1723–1728.

[211] D. Chaum, "Blind signatures for untraceable payments," in *Advances in Cryptology*. Cham, Switzerland: Springer, 1983, pp. 199–203.

[212] J. C. L. Cheung, T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "Credential-based privacy-preserving power request scheme for smart grid network," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Dec. 2011, pp. 1–5.

[213] C. Dwork, "Differential privacy: A survey of results," in *Proc. Int. Conf. Appl. Models Comput.* Cham, Switzerland: Springer, 2008, pp. 1–19.

[214] D. Boneh, E.-J. Goh, and K. Nissim, "Evaluating 2-DNF formulas on ciphertexts," in *Proc. Theory Cryptogr. Conf.* Cham, Switzerland: Springer, 2005, pp. 325–341.

[215] J.-M. Bohli, C. Sorge, and O. Ugus, "A privacy model for smart metering," in *Proc. IEEE Int. Conf. Commun. Workshops*, May 2010, pp. 1–5.

[216] J. Konečnỳ, H. Brendan McMahan, F. X. Yu, P. Richtárik, A. Theertha Suresh, and D. Bacon, "Federated learning: Strategies for improving communication efficiency," 2016, *arXiv:1610.05492*.

[217] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 2, pp. 1–19, 2019.

[218] S. Alam, M. F. Sohail, S. A. Ghauri, I. M. Qureshi, and N. Aqdas, "Cognitive radio based smart grid communication network," *Renew. Sustain. Energy Rev.*, vol. 72, pp. 535–548, May 2017.

[219] S. Farhang, Y. Hayel, and Q. Zhu, "PHY-layer location privacy-preserving access point selection mechanism in next-generation wireless networks," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Sep. 2015, pp. 263–271.

[220] Y. Song, P.-Y. Kong, Y. Kim, S. Baek, and Y. Choi, "Cellular-assisted D2D communications for advanced metering infrastructure in smart gird," *IEEE Syst. J.*, vol. 13, no. 2, pp. 1347–1358, Jun. 2019.

[221] D. Fang, Y. Qian, and R. Q. Hu, "Security for 5G mobile wireless networks," *IEEE Access*, vol. 6, pp. 4850–4874, 2017.

[222] Y. O. Basciftci, C. E. Koksal, and A. Ashikhmin, "Securing massive MIMO at the physical layer," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Sep. 2015, pp. 272–280.

[223] J. Jiang, H. Sun, and W.-Y. Chiu, "Energy efficient massive MIMO system design for smart grid communications," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC)*, May 2016, pp. 337–341.

[224] Y. Deng, L. Wang, K.-K. Wong, A. Nallanathan, M. Elkashlan, and S. Lambotharan, "Safeguarding massive MIMO aided hetnets using physical layer security," in *Proc. Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Oct. 2015, pp. 1–5.

[225] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21–27, Jun. 2015.

[226] R. Chaudhary, G. S. Aujla, S. Garg, N. Kumar, and J. J. P. C. Rodrigues, "SDN-enabled multi-attribute-based secure communication for smart grid in IIoT environment," *IEEE Trans. Ind. Informat.*, vol. 14, no. 6, pp. 2629–2640, Jun. 2018.

[227] U. Ghosh, P. Chatterjee, and S. Shetty, "A security framework for SDN-enabled smart power grids," in *Proc. IEEE 37th Int. Conf. Distrib. Comput. Syst. Workshops (ICDCSW)*, Jun. 2017, pp. 113–118.

[228] C. Bekara, "Security issues and challenges for the IoT-based smart grid," in *Proc. FNC/MobiSPC*, 2014, pp. 532–537.

[229] L. Strous, S. von Solms, and A. Zúquete, "Security and privacy of the Internet of Things," *Comput. Secur.*, vol. 102, May 2021, Art. no. 102148.

[230] H. Hui, Y. Ding, Q. Shi, F. Li, Y. Song, and J. Yan, "5G network-based Internet of Things for demand response in smart grid: A survey on application potential," *Appl. Energy*, vol. 257, Jan. 2020, Art. no. 113972.

[231] S. Bera, S. Misra, and J. J. P. C. Rodrigues, "Cloud computing applications for smart grid: A survey," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 5, pp. 1477–1494, May 2015.

[232] S. A. Hashmi, C. F. Ali, and S. Zafar, "Internet of Things and cloud computing-based energy management system for demand side management in smart grid," *Int. J. Energy Res.*, vol. 45, no. 1, pp. 1007–1022, Jan. 2021.

[233] A. Mondal, S. Misra, and A. Chakraborty, "Dynamic price-enabled strategic energy management scheme in cloud-enabled smart grid," *IEEE Trans. Cloud Comput.*, vol. 10, no. 1, pp. 111–122, Jan. 2022.

[234] M. R. Momeni, F. Haghighat, and M. Haghighat, "An efficient and cloud based architecture for smart grid security," *Int. J. Wireless Microw. Technol.*, vol. 5, pp. 35–42, Oct. 2021. [Online]. Available: http://www.mecs-press.org/, doi: 10.5815/ijwmt.2021.05.05.

[235] N. Kulkarni, S. V. N. L. Lalitha, and S. A. Deokar, "Real time control and monitoring of grid power systems using cloud computing," *Int. J. Electr. Comput. Eng.*, vol. 9, no. 2, p. 941, Apr. 2019.

[236] H. Suo, Z. Liu, J. Wan, and K. Zhou, "Security and privacy in mobile cloud computing," in *Proc. 9th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jul. 2013, pp. 655–659.

[237] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2322–2358, 4th Quart., 2017.

[238] Y. Huang, Y. Lu, F. Wang, X. Fan, J. Liu, and V. C. M. Leung, "An edge computing framework for real-time monitoring in smart grid," in *Proc. IEEE Int. Conf. Ind. Internet (ICII)*, Oct. 2018, pp. 99–108.

[239] M. Chiang and T. Zhang, "Fog and IoT: An overview of research opportunities," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 854–864, Dec. 2016.

[240] J. Hu and A. V. Vasilakos, "Energy big data analytics and security: Challenges and opportunities," *IEEE Trans. Smart Grid*, vol. 7, no. 5, pp. 2423–2436, Sep. 2016.

[241] W.-L. Chin, W. Li, and H.-H. Chen, "Energy big data security threats in IoT-based smart grid communications," *IEEE Commun. Mag.*, vol. 55, no. 10, pp. 70–75, Oct. 2017.

[242] H. Lasi, P. Fettke, H. G. Kemper, T. Feld, and M. Hoffmann, "Industry 4.0," *Bus. Inf. Syst. Eng.*, vol. 6, no. 4, pp. 239–242, 2014.

[243] M. Faheem and V. C. Gungor, "Energy efficient and QoS-aware routing protocol for wireless sensor network-based smart grid applications in the context of Industry 4.0," *Appl. Soft Comput.*, vol. 68, pp. 910–922, Jul. 2018.

[244] M. Faheem, S. B. H. Shah, R. A. Butt, B. Raza, M. Anwar, M. W. Ashraf, M. A. Ngadi, and V. C. Gungor, "Smart grid communication and information technologies in the perspective of Industry 4.0: Opportunities and challenges," *Comput. Sci. Rev.*, vol. 30, pp. 1–30, Nov. 2018.

[245] T. Kotsiopoulos, P. Sarigiannidis, D. Ioannidis, and D. Tzovaras, "Machine learning and deep learning in smart manufacturing: The smart grid paradigm," *Comput. Sci. Rev.*, vol. 40, May 2021, Art. no. 100341.

[246] S. K. Rao and R. Prasad, "Impact of 5G technologies on Industry 4.0," *Wireless Pers. Commun.*, vol. 100, no. 1, pp. 145–159, May 2018.

[247] P. K. Singh, S. K. Nandi, and S. Nandi, "A tutorial survey on vehicular communication state of the art, and future research directions," *Veh. Commun.*, vol. 18, Aug. 2019, Art. no. 100164.

[248] P. H. Mirzaee, M. Shojafar, H. Bagheri, T. H. Chan, H. Cruickshank, and R. Tafazolli, "A two-layer collaborative vehicle-edge intrusion detection system for vehicular communications," in *Proc. IEEE 94th Veh. Technol. Conf. (VTC-Fall)*, Sep. 2021, pp. 1–6.

[249] F. Calise, F. L. Cappiello, M. Dentice d'Accadia, and M. Vicidomini, "Smart grid energy district based on the integration of electric vehicles and combined heat and power generation," *Energy Convers. Manage.*, vol. 234, Apr. 2021, Art. no. 113932.

[250] N. Piperigkos and A. S. Lalos, "Impact of false data injection attacks on decentralized electric vehicle charging protocols," *Transp. Res. Proc.*, vol. 52, pp. 331–338, Jan. 2021.

[251] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Gener. Comput. Syst.*, vol. 107, pp. 841–853, Jun. 2020.

[252] A. S. Musleh, G. Yao, and S. M. Muyeen, "Blockchain applications in smart grid–review and frameworks," *IEEE Access*, vol. 7, pp. 86746–86757, 2019.

[253] C. Pop, T. Cioara, M. Antal, I. Anghel, I. Salomie, and M. Bertoncini, "Blockchain based decentralized management of demand response programs in smart energy grids," *Sensors*, vol. 18, no. 1, p. 162, Jan. 2018.

[254] A. Maw, S. Adepu, and A. Mathur, "ICS-BlockOpS: Blockchain for operational data security in industrial control system," *Pervas. Mobile Comput.*, vol. 59, Oct. 2019, Art. no. 101048.

[255] S. Magare, A. Dudhgaonkar, and S. Kondekar, "Security and privacy issues in smart city: Threats and their countermeasures," in *Security and Privacy Applications for Smart City Development*. Cham, Switzerland: Springer, 2021, pp. 37–52.

**PARYA HAJI MIRZAEE** (Member, IEEE) received the master's degree in communication engineering from the University of Kurdistan Hewlêr, Iran, in 2016. She is a Ph.D. Researcher in information and communication systems with the 5GIC/6GIC Innovation Centre, University of Surrey, U.K. Her research interests include applied ML and information and communication systems security and privacy.

**MOHAMMAD SHOJAFAR** (Senior Member, IEEE) received the Ph.D. degree (Hons.) in ICT from the Sapienza University of Rome, Rome, Italy, in 2016. He is a Senior Lecturer (Associate Professor) in the networks security, an Intel Innovator, and a Marie Curie Alumni, working with the 5G and 6G Innovation Centre (5GIC and 6GIC), Institute for Communication Systems (ICS), University of Surrey, U.K. Before joining 5GIC/6GIC, he was a Senior Researcher and a Marie Curie Fellow with the SPRITZ Security and Privacy Research Group, University of Padua, Italy. He is a PI of AutoTrust, a 750k euro 5G secure autonomous vehicular communication project supported by European Space Agency (ESA), in 2021, and was a PI of PRISENODE Project, a 275k euro Horizon 2020 Marie Curie global fellowship project in the areas of fog/cloud security collaborating at the University of Padua. He also was a PI on an Italian SDN security and privacy (60k euro) supported by the University of Padua, in 2018. He was contributed to some Italian projects in telecommunications like GAUChO, SAMMClouds, and SC2. He is a Professional Member and a Distinguished Speaker of ACM. He is an Associate Editor of IEEE Transactions on Network and Service Management, IEEE Transactions on Consumer Electronics, IEEE Systems Journal, and *Computer Networks*. For additional information, please visit his website (http://mshojafar.com).

**HAITHAM CRUICKSHANK** (Senior Member, IEEE) has been working with the ICS (formerly CCSR), since January 1996, on several European research projects in the ACTS, ESPRIT, Ten-Telecom, and IST programs. He is currently working in several FP6 projects, such as SATLIFE, EuroNGI, and SATNEX. He also teaches the data and internet networking and satellite communication courses at the University of Surrey. His main research interests include networks security, satellite networks architectures, and VoIP and IP conferencing over satellites. He is a Chartered Engineer. He is a member of the Satellite and Space Communications Committee of the IEEE ComSoc. He is active in the ETSI Broadband Satellite Multimedia (BSM) and the IETF MSEC groups. He is the Vice Chair of the COST 272 Activity, which is part of the European COST Research Program.

**RAHIM TAFAZOLLI** (Senior Member, IEEE) is the Regius Professor and a Professor of mobile and satellite communications. He is the Director of ICS and the Founder and the Director of world's first 5G innovation centre at the University of Surrey, U.K. He is regularly invited by many governments for advise on mobile communications and in particular 5G technologies. He has given many interviews to international media in the form of television, radio interviews, and articles in international press.