Distributed Energy Resource Management System (DERMS) Cybersecurity Scenarios, Trends, and Potential Technologies: A Review

Niroop Sugunaraj[1], Shree Ram Abayankar Balaji[1], Barathwaja Subash Chandar[1], Prashanth Rajagopalan[1], Utku Kose[2], David Charles Loper[1], Tanzim Mahfuz[3], Prabuddha Chakraborty[3], Seerin Ahmad[4], Taesic Kim[5], Giovanni Apruzzese[6], Anamika Dubey[7], Luka Strezoski[8], Benjamin Blakely[9], Subhojit Ghosh[10], Maddikara Jaya Bharata Reddy[11], Harsha Vardhan Padullaparti[12], and Prakash Ranganathan[1]

[1]Center for Cyber Security Research (C2SR), University of North Dakota, Grand Forks, ND 58201, USA
[2]Suleyman Demirel University, 32260, Isparta/Turkey
[3]University of Maine, Orono, ME 04469, USA
[4]Texas A&M University-Kingsville, Kingsville, TX 38363, USA
[5]University of Missouri, MO 65211, USA
[6]Liechtenstein Business School, University of Liechtenstein, 9490 Vaduz, Liechtenstein
[7]Washington State University, Pullman, WA 99164, USA
[8]University of Novi Sad, Faculty of Technical Sciences, Department for Power, Electronics, and Telecommunication Engineering
[9]Argonne National Laboratory, Lemont, IL 60439 USA
[10]National Institute of Technology, Raipur, IN
[11]National Institute of Technology, Tiruchirapalli, IN
[12]National Renewable Energy Laboratory (NREL), Golden, CO 80401, USA

Abstract – Critical infrastructures like the power grid are at risk from increasing cyber threats due to high penetration of interconnected distributed energy resources (DER). Compromised DER endpoints can cause events, data breaches, communication loss, intentional device failures, and even cascading outages. To address these challenges, this paper explores cybersecurity issues in DER management systems (DERMS), including state-of-the-art reviews on architectures, communication protocols, access control privileges, data breaches, identity management policies, attacks such as false data injection, denial of service, distributed denial of service, malware, threats affecting data integrity, and network vulnerabilities. Realistic threat scenarios are outlined, followed by discussions on futuristic solutions like the zero trust framework. The paper presents new architectural patterns for recently released multi-level hierarchical framework as per IEEE 1547.3 standard to handle DERMS data and assets. The paper also discusses potential threats compromising the Confidentiality, Integrity, Availability, and Accountability (CIAA) properties at each level of the IEEE 1547.3 framework. This review is unique and comprehensive, as it covers existing research on cybersecurity challenges in DER-related assets and outlines the necessary capabilities to equip Intrusion Diagnostic Units (IDUs) in future DERMS technologies, all while ensuring compliance with IEEE 1547.3 standard requirements.

***Index Terms*—advanced distribution management systems, cybersecurity, distributed energy resources, distributed energy resource management systems.**

I. Introduction

MODERN power grids (or smart grids) have many sub-systems managing multi-tiered functions. These tiers can be classified as generation, transmission, distribution, and consumption of the electric power. Examples of such sub-systems include supervisory control and data acquisition (SCADA) system, demand response management system (DRMS), distributed control system (DCS), and the advanced distribution management system (ADMS). While high penetration of DERs has the potential for grid stability and is seen as a green alternative to power generation, it also opens doors for cybersecurity vulnerabilities. DERs are defined as renewable energy-based generation, storage, or controllable load units that may interact with local electric power systems (EPS) or microgrids to provide power. DER fleets such as wind, solar photovoltaic (PV), electric vehicle (EV) charging stations, and energy storage systems (ESS) have significant energy footprints. According to the Energy Information Administration (EIA), renewable energy (RE) sources (i.e., wind, solar PV, etc.) contributed to 913 million MW of electricity in 2022 across the United States [1]. Similarly, the Alliance for Automotive Innovation and the U.S. Department of Energy (DoE) [2] states that roughly 80% of all EV charging infrastructure is home-based and as of March 2024 in the U.S., there are 64,641 publicly available charging locations and 168,388 available and unavailable legacy, Level 1, Level 2, and direct current (DC) fast charging ports [3]. Publicly available infrastructure is expected to increase with the signing of the bipartisan Infrastructure Investment and Jobs Act of 2021. However, DER penetration will also significantly increase the cyber attack surface. An overlooked cybersecurity challenge is the ownership model for DERs. DER types (e.g., wind, solar, ESS, EV) are controlled and owned by a broad pool of private, public, and third-party entities distributed and operate outside the purview of regulated administrative domains [4].

Corresponding author: N. Sugunaraj (email: niroop.sugunaraj@und.edu).

A. DERMS Cybersecurity Challenges

Documented evidence suggests that DER fleet types are vulnerable to multiple cyber attacks. Wind DERs can be compromised indirectly by gaining remote access to the SCADA systems operating them [5], launching worms to issue malicious command and control messages [6], and compromised credentials allow privilege escalation (PE) permitting changes to critical configurations and settings [7]. Similarly, solar PV vulnerabilities like poor credential management, weak software supply chains (e.g., code bugs), and default configurations can be exploited due to lack of standardized security policies (e.g., public key infrastructure) [8]. EVs and their infrastructure (e.g., charging stations, supply equipment, operator interfaces) are susceptible to session hijacking, brokenwire attacks, poorly secured smart phone applications, and credit card skimming on supply equipment. These vulnerabilities can lead to personally identifiable information (PII) theft, power grid disruptions, and vehicle battery damage [9].

The increase in DERs has brought the need for additional monitoring and its control systems called DERMS. DERMS is a hardware (i.e., shown through the integration of edge devices, gateways) and software platform designed to manage and optimize DERs. The main functions of a DERMS are: to aggregate individual DERs, load management, market integration, coordinate demand response programs, provide metrics (e.g., load consumption, usage patterns), and monitor grid assets. However, DERMS' digital ecosystem presents unique cybersecurity challenges.

DERMS and its multiple DER endpoints (e.g., remote terminal units (RTUs), intelligent electronic devices (IEDs), smart meters) are vulnerable to attacks such as spoofing and denial of service (DoS) to compromise the integrity and availability of asset(s). For example, a threat actor can gain unauthorized access to DER gateways or inverters by presenting a spoofed access mechanism (e.g., public certificates) to modify data before they are sent. DERMS can have multiple architecture types based on deployment topology (e.g., networked microgrids, nanogrids): centralized, decentralized, distributed, or (more recently) federated [10] (see Fig. 1).

Centralized architectures represent single-point computation where DER endpoints (e.g., controllers, sensing devices) do not communicate with one another but relay all collected data to a central compute node. The latency and real-time response capabilities required (i.e., due to the rapid integration of DERs to the grid) [12] of a centralized architecture are largely dependent on the communication protocol(s) used to handle data between endpoints and the central compute node. The benefit to a centralized approach is that it controls demand-side and generation-side units from one location, and it has authority to integrate or shed non-critical loads based on need [13]; therefore, autonomy is a key aspect of this architecture type. However, it is also generally accepted that the centralized control of DERs presents a single point of failure that can significantly disrupt grid stability and operation.

Decentralized architectures represent DER endpoints that may be geographically dispersed and contain endpoints that do not communicate with one another (i.e., non-cooperative). Small levels of autonomy are advantageous in this architecture although a certain level of supervision is required. Data from these endpoints are relayed to aggregators that participate in data exchange. The bottlenecks in this architecture type is the bandwidth size required to handle large-scale communication as there is a linear increase in network size and the fact that decentralized DERs may be challenging to implement at the control level (i.e., management and control of the system to maintain power balance) since there is a lack of cooperation [14].

Distributed architectures, like decentralized architectures, are dispersed but contain DER endpoints that are cooperative in exchanging collected data and assignment of roles. Distributed architectures are fault-tolerant i.e., failure of a communication link or endpoint will not significantly affect the system as a whole. From a control perspective, distributed endpoints can be integrated into the system with little hassle (i.e., plug-in and plug-out of DERs) [15] but from a communication standpoint and with endpoints being at the same hierarchical level (i.e., no aggregator or centralized compute nodes), the support for many communication links is required and this presents a scalability issue. Other aspects to consider are design complexity, implementation, performance indices (e.g., convergence), and consensus variables to achieve a certain objective (e.g., frequency restoration). Generally DERs have relatively low system inertia, cyber attacks on endpoints in distributed architecture types will have more impacts on the stability of a bulk power system [16].

The federated architecture is a concept first presented by the Electric Power Research Institute (EPRI) [10][17] in 2020 and later supported by four U.S. National Laboratories [18] to allow for computation at two levels on a need basis: at the edge (i.e., locally federated or distributed) or at a single centralized (i.e., centrally federated) location; these two networks can consolidate their networks and their data to share certain services and to maintain adequate and consistent policy enforcement. This architecture is semi-autonomous and decision-making capabilities are given to devices at both these levels - this is not seen in the other architecture types. The obvious challenges to this architecture is related to privacy - globally (i.e., model updates at the global authority) and locally (i.e., model updates are kept private only with the global authority) and concept drift due to cyber attacks or diurnal/nocturnal variations [19].

We propose a Hierarchical Hybrid DERMS Federated Learning (FL) Framework as shown in Fig. 2. "Group 0" contains inverter-based resources (IBRs) and their edge devices (e.g., smart meters, remote terminal units (RTU)). Data are exchanged from/to these edge devices through IEC 61850/Modbus protocols through a device-level interface that acts as a gateway to upper-level entities. The distributed (i.e., co-operative and dispersed edge devices) and locally federated (i.e., co-operative with device-level authority) architecture types align well with this group due to their high fault-tolerance and ability to island without significant

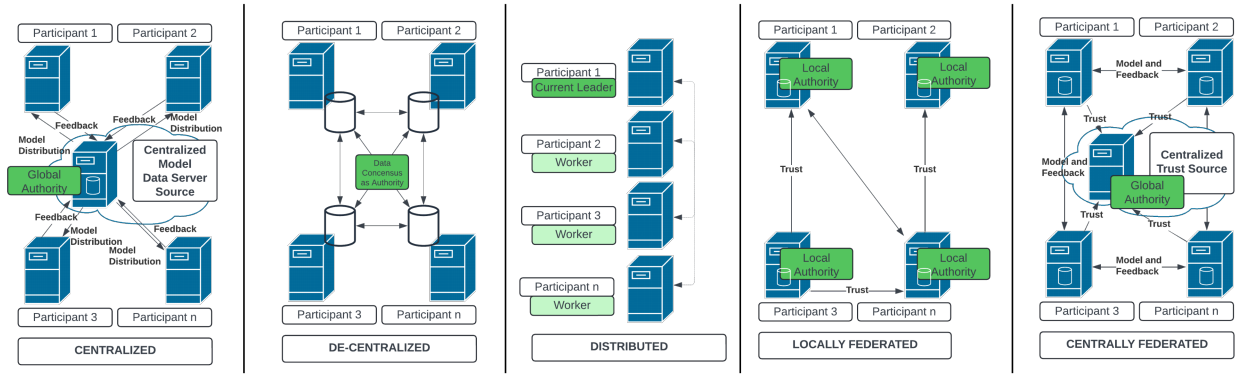


Fig. 1. **Different DERMS architecture types.** The centralized, de-centralized, distributed, locally federated, and centrally federated types are most applicable to DERMS due to distinct modes of operation (e.g., latency, topology), latency, scalability, and robustness to cyber-physical threats.

disruptions to Level 2 and Level 3 entities (i.e., distribution system, power grids).

"Groups 1-3" entities refer to local aggregators (i.e., utility-owned or third-party owned) that aggregate data from IBRs' edge devices to inform higher-level decisions such as grid support functions (e.g., voltage regulation, demand response, load shedding, etc.) We define local aggregators to belong to smaller-scale distribution sites such as microgrids, nanogrids, and macrogrids. The additional interface that local aggregators exchange data is with the cloud. This refers to hardware or software infrastructure that acts as a support for various services such as forecasting, data analytics, and to offload data for remote storage. Centralized or decentralized architecture types are recommended for these groups due to the relatively large amounts of data that are collected and used to inform grid-level decisions. Since aggregators exercise a degree of local control over distribution sites, they interface with our proposed Customized FL Framework through the IEEE 2030.5 standard (i.e., Smart Energy Profile) for various grid support functions.

Finally, "Group 4" supports distributed energy management system (DERMS), advanced distribution management system (ADMS), and other market-relevant authorities such as virtual power plants (VPP) to render data from Group 3 to manage, control, and dispatch resources through the lower-levels to individual or aggregate DERs. The centrally federated architecture type is most applicable – since Group 4 interfaces with Independent System Operators (ISOs) and Regional Transmission Operators (RTOs), a degree of co-operation is required between Group 4 entities to appropriately schedule resources such as generators, loads, and manage bids/energy trading tariffs, or update grid topologies for Groups 1- 3 while still functioning with a degree of autonomy and privacy. We regard VPPs to provide energy management and bidding services to prosumers through the final decision-making from the utility DERMS. We leverage the cloud interface at this group as well for the same benefits offered to Groups 1 – 3. The primary flow modality at this group is control signals, whereas Group 1, 2, 3 and Group 0 entities exchange data and power flows.

We now use the Hierarchical Five-level Architecture specified by IEEE 1547.3-2023 [11] as shown in Fig. 3 to map high-value entities, highlight relevant attacks, and security properties requirements at each level. While accountability (i.e., tracing malicious or benign actions uniquely to an entity [20], the denial that an action took place [21], or uniquely tracing actions to an entity to support non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action [22]) and availability (i.e., denial or prevention of authorized access) are the primary requirements that are compromised at the transmission/distribution and market levels, the lower levels (i.e., DER process and field systems, management systems, and third parties) are more likely to be compromised through attack vectors such as physical intrusions and integrity violations, and attacks such as spoofing, eavesdropping, and man in the middle. We will expand further on these in Section IV.

Additionally, there are several communication standard protocols including Modbus, Distributed Network Protocol 3 (DNP3), and Smart Energy Profile 2 (SEP2) that offer a networking bedrock for DER devices but lack effective in-built security mechanisms. Attacks such as DoS and malware are evolving against smart grids and DERs due to the critical nature of these resources and as such, the sophistication and operation of malware are of rising concern. Eder-Neuhauser and colleagues [23] list communication patterns for nineteen malware types and key findings indicate that recent implementations of malware traffic blend into normal network traffic to obfuscate their presence, and that on internet protocol (IP) networks malware prefers transmission control protocol (TCP) over the user datagram protocol (UDP) for compromised devices. Indicators of compromise (IoCs) that are presented in literature are: 1) forbidden or restricted communication attempts that are unsolicited, and 2) the presence of communication protocols (e.g., TCP, Hypertext Transfer Protocol (HTTP), or Server Message Block (SMB)) that are not ordinarily present in DERMS communications, posing a threat to DERMS and other smart grid control systems (e.g., advanced distribution management systems (ADMS)).

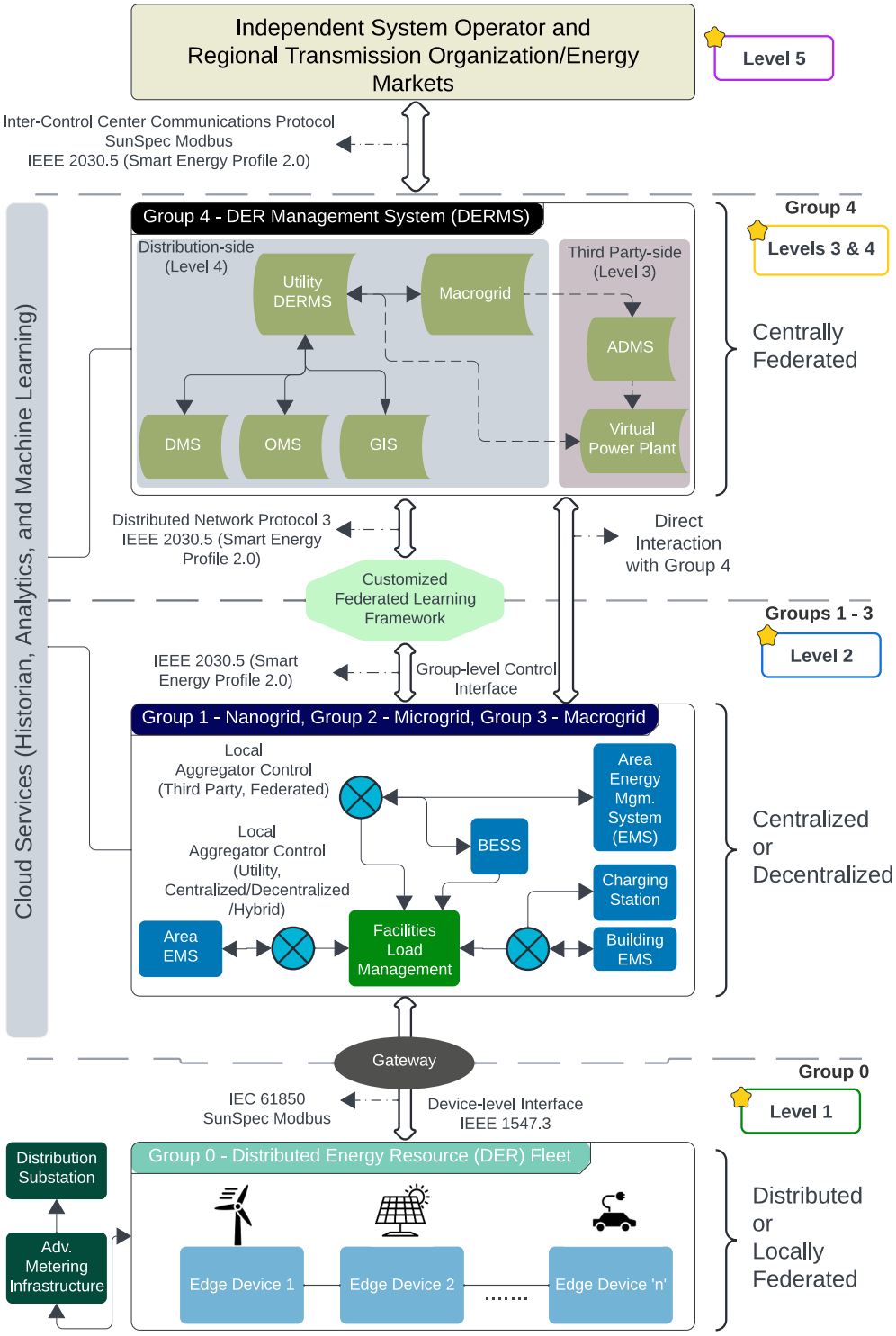


Fig. 2. **Hierarchical Hybrid DERMS Federated Learning framework.** Each level starting from Level 1 (bottom-most) to Level 5 (top-most) interacts with other levels through multiple protocols (e.g., Modbus, SEP) and accommodates different DERMS architecture types based on the factors unique to each architecture type.

B. ADMS Cybersecurity Challenges

ADMS provide cutting-edge control capabilities to a power grid when compared to the traditional distribution management system (DMS). Some of these capabilities include fault location, isolation, and service restoration (FLISR), real-time optimization of voltage and VAR (VVO), and outage management in addition to providing real-time analytics of system processes. Architecturally, a typical ADMS consists of DMS, an outage management system (OMS), and energy management system (EMS). Dubey and colleagues [24] categorize and characterize ADMS according to their current, near-term, and long-term use-cases. Near-term applications of

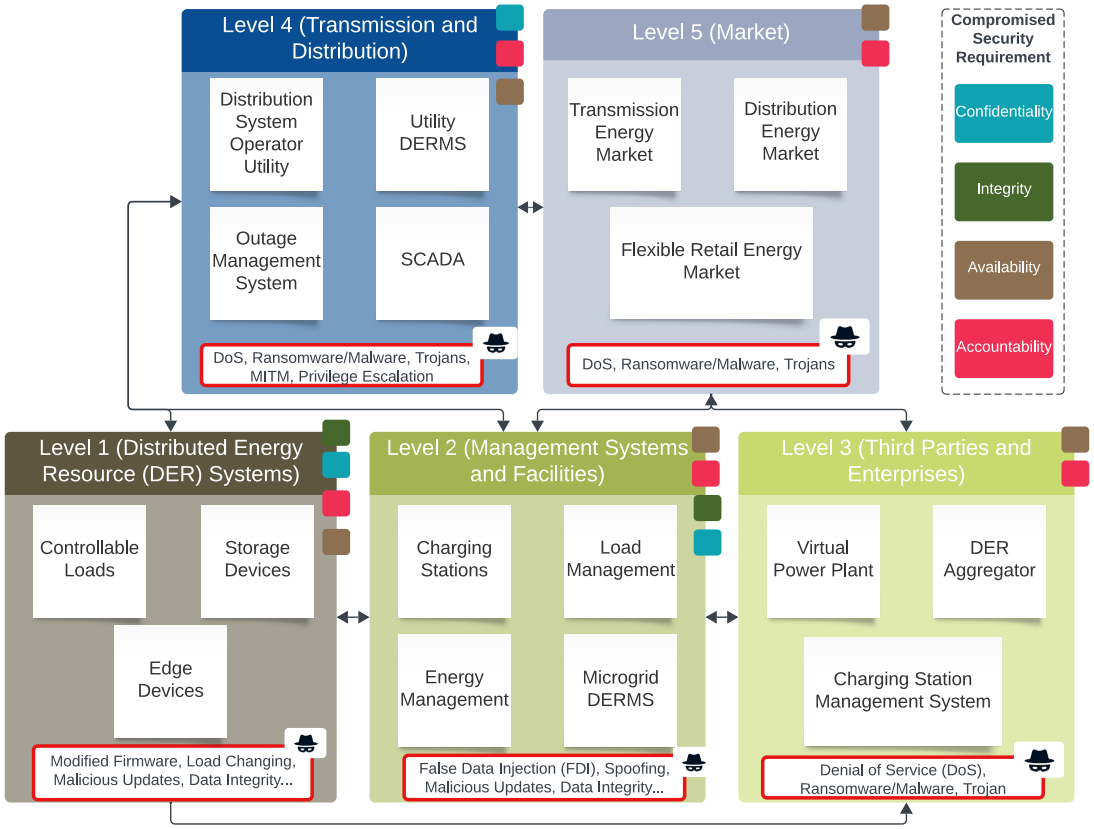


Fig. 3. **Hierarchical Five-level Architecture specified by IEEE 1547.3-2023.** Attack are given at the bottom of each level and compromised security requirements for each level are represented at the top right of each level differentiated by colors: blue (confidentiality), green (integrity), brown (availability), and red (accountability) [11].

ADMS focus on rendering services such as proactive demand response (DR), optimal DER control and coordination, and restoration from outages with intentional islanding through a centralized network while long-term use-cases include data-driven situational awareness and adaptive protection through a distributed architecture. However, ADMS are known to have challenges such as integration of multiple information technology (IT) and operational technology (OT) modules and a dedicated cross-functional team for operations and management [25]. Compared to other aspects within the smart grid, such as SCADA systems and communication networks, studies related to the security of ADMS are scant and require further analyses. However, cyber threats such as: 1) unencrypted communications from monitoring endpoints; 2) unsecured access to the ADMS from non-ADMS or external systems [26]; 3) lack of data validation; 4) unauthorized and privileged access; and 5) inadequate security audits of monitoring logs, can be carried over from the traditional DMS and risk the security of the larger DERMS. Additionally many DER devices (e.g., smart appliances) may be controlled from a cloud- or vendor-hosted centralized application. This creates the potential for a single security compromise to impact a large number of DER devices which could create grid instability.

C. Related Studies

1) Smart Grid Security

Several surveys have been conducted on the smart grid and its sub-entities such as the wide-area monitoring, protection, and control (WAMPAC) systems, smart grid metering networks, and cyber-physical system (CPS) testbeds [30][36][29]. For example, Kumar et al. [32] cover cybersecurity aspects such as privacy and threat modeling with regards to endpoints such as AMI and smart metering infrastructure (SMI). Specifically, the authors address threats and mitigation measures related to SMI system-level security (i.e., SMI networks), SMI services (e.g., demand response), and utility/consumer privacy and confidentiality (e.g., billing information). The paper briefly references attacks on RE resources, but this isn't the focus of this survey and therefore lacks much needed detail on larger threat surface(s) brought in by distributed generation units and DERs. A survey by Yan and colleagues [27] addresses security for smart grid communication infrastructures. There is important information mentioned for DERs and DER security such as stakeholders, standards (e.g., IEC 61850), security requirements (e.g., Federal Information Processing Standard (FIPS) 201), and deploying security technologies (e.g., symmetric encryption, key management). However, the addition of new standards, updates in security protocols, and integration of novel systems and threat models make this information in the study dated and need detailed analyses by looking at the current smart

TABLE I
COMPARING EXISTING WORKS.

Survey	**Scope**	**IEEE 1547.3 5–level Architecture Map [11]**	**IEEE 1547.3 Grid Entities Interaction [11]**	**Security Aspects**				**Year**
				TB	**HS**	**SS**	**ST**	
A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges [27].	Major Requirements for Smart Grid Communication Infrastructures (e.g., Scalability, Resilience) and Challenges (e.g., Security Threats, Cost/Investment, and Standardization).	Level 1 (IEDs and RTUs) and Level4 (Substations).	(1) DER/Customer Premises (Field, Process) (2) Transmission (3) Distribution.	×	×	×	✓	2013
Cybersecurity for DERs and Smart Inverters [28].	DERs and Inverters.	Level 1 (DER Controllers), Level 3 (Aggregators), and Level 4. (ISO/RTO).	(1) DER / Customer Premises (Process, Field, Station) (2) Transmission.	×	✓	✓	×	2016
A Survey on Smart Grid Cyber-Physical System Testbeds [29].	Testbeds. The Smart Grid System's Diversity Needs Scalable, Flexible, and Multi-domain Capable Testbeds that Support Robust Performance Analysis and Vulnerability Assessment.	Level 1 and Level 4.	(1) Distribution (2) DER / Customer Premises (Process, Field) (3) Transmission	✓	×	×	✓	2017
Middleware Architectures for the Smart Grid: A Survey on the State-of-the-Art, Taxonomy and Main Open Issues [30].	Middleware Architectures. Architectures Evaluated Based on Features, Suitability, and Performance. Future Research Directions Include Interoperability and Security.	Level 1 and Level 4.	(1) Distribution, (2) DER / Customer Premises (Field).	✓	×	×	✓	2018
A Survey of Protocol-Level Challenges and Solutions for Distributed Energy Resource Cyber-Physical Security [31].	Protocol-level Mechanisms and Security for Communication Layer Protocols (e.g., Ethernet, ICMP).	Level 1 (Edge, Field, Network).	(1) Transmission (2) Distribution.	×	×	✓	×	2018
Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues [32].	Metering Networks. Security for Smart Metering Infrastructure Considering Aspects such as Heterogeneous Devices, Vulnerability Management, and Data Sensitivity.	Level 1 (Smart Meters), Level 2, and Level 5 (Markets).	(1) Distribution (2) DER / Customer Premises (Station, Field) (3) Transmission.	×	✓	✓	×	2019
Industrial and Critical Infrastructure Security: Technical Analysis of Real-Life Security Incidents [33].	Industrial and Critical Infrastructure.	Level 1, Level 2, Level 3, and Level 4.	(1) Transmission (2) Distribution (3) DER/Customer Premises (Field/Process/Station).	×	✓	✓	×	2021
Cybersecurity Challenges in Distributed Energy Resources for Smart Cities [34].	DER for Smart Cities	Level 1 and Level 2.	(1) Distribution (2) DER / Customer Premises (Field, Process, Station).	×	×	✓	×	2022
DER Communication Networks and Their Security Issues [35].	Communication Networks	Level 1 (DER Devices), Level 2 (Substations)	1) Distribution (2) DER/Customer Premises (Process, Field, Station).	×	×	✓	✓	2022
Federated Architecture for Secure and Transactive Distributed Energy Resource Management Solutions (FAST-DERMS) [18].	DERMS in General	Level 1, Level 3, Level 4, and Level 5	(1) Transmission (2) Distribution. (3) DER / Customer Premises (Station).	×	×	✓	×	2022
Security of Wide-Area Monitoring, Protection, and Control (WAMPAC) Systems of the Smart Grid: A Survey on Challenges and Opportunities [36].	Wide-Area Monitoring, Protection, and Control (WAMPAC).	Level 1, Level 2, and Level 4.	(1) Distribution, (2) DER/Customer Premises (Field, Process).	×	✓	✓	✓	2023
Distributed Energy Resources Cybersecurity Outlook: Vulnerabilities, Attacks, Impacts, and Mitigations [37].	DERs in General	Level 1, Level 2, Level 3, and Level 4.	(1) DER/Customer Premises (Field/Process) (2) Transmission (3) Distribution.	×	✓	✓	×	2023
Our Survey	**DERMS in General.**	**Level 1, Level 2, Level 3, Level 4, and Level 5.**	**(1) Transmission (2) Distribution (3) DER / Customer Premises (Field, Process, Station)**.	✓	✓	✓	✓	**2024**

grid landscape.

While these surveys have gathered valuable information on important areas, there is little to no consideration of DERs and sub-systems such as ADMS, EMS, OMS, etc. and the studies offer high-level information without offering technical insights for cyber vulnerabilities or cyber threat models. Overall, these existing surveys do not consider in sufficient detail the addition and security implications of DERs and their control technologies (e.g., DERMS) to the modern power grid.

2) DER Security

There are works that specifically tackle DER security (i.e., cyber and physical security) such as [34][35][31][28]. Chan et al. [35] specifically address DER communication protocols such as Modbus, Distributed Network Protocol (DNP), and Smart Energy Profile (SEP), and DER cybersecurity attacks and vulnerabilities (e.g., zero-day attacks), and mitigation measures. Similarly, Sundarajan et al. [31] have detailed cybersecurity vulnerabilities and attacks for DER communication architectures at the edge, network, field, and utility command/control centers levels by mapping the Open Systems Interconnection (OSI) model to DER communication protocols. One of the key contributions of this study is highlighting National Renewable Energy Laboratory's (NREL) layered defense strategy for DER systems (e.g., photovoltaic inverters, wind farms) through security controls (e.g., Transport Layer Security (TLS)) for DER communication protocols. Qi and colleagues [28] address DER security through four "domains" - DER devices, distribution utilities, third parties, and transmission operations. Additionally, attack scenarios for DERs are described and an attack-resilient framework for cyber resiliency is detailed at the cyber, physical device, and utility levels. There is significant value in the finer details of this study, such as identifying patterns in DER systems that propagate faults, the recommendation of data-driven approaches for state estimation and anomaly detection, and coordinated hierarchical control to improve transient performance and corrective control to restore system stability. However, rapid developments in the power grid are showing a system of systems trend and reviews in this area need to be robust and comprehensive; high-risk possibilities and robust prevention/mitigation frameworks that leverage advanced technologies such as federated learning, cloud and fog-based computing, and orchestration platforms are viable options that were not considered.

The conventional power system, based on fossil fuels, allows uni-directional power flow (PF). However, with the incorporation of DERs in the systems, the PF has been altered to be bi-directional. Most protection schemes are designed for uni-directional power flow. This may prove futile in case of reverse PF caused by a lightning event; hence, the protection scheme should be redesigned to ensure a safe and reliable network for different distribution grids (e.g., radial) with constraints (e.g., minimum number of micro-phasor measurement units (μPMUs) [38]) for different voltage levels [39]. It is also important to have complete observability for the monitoring of the system. State-of-the-art methods have explored the optimal deployment of μPMUs in a distribution network operation in multiple configurations [40][41][42]. A comprehensive review on PMUs, μPMUs, and their optimal placement in the power system to enhance situation awareness, control, event identification and data mining was performed in [43][44].

Fault detection and system protection (i.e., physical security) can be improved with the aid of PMUs and μPMUs [45]. Techniques to detect symmetrical and asymmetrical faults in distribution systems and microgrids using time series measurements from μPMUs at various locations were proposed in [46][47][48][49]. The impact of DERs on transient stability has been a subject of interest and it is necessary to synchronize the DERs with the main grid for stable operation [50][51]. Linear and non-linear variants of the Kalman filter were implemented and tested for Dynamic State Estimation in [52], which would help access the internal states of distributed generators, for control and monitoring of real-time microgrid.

While these works contain information (i.e., cyber and physical studies) that are relevant to our work, they lack comprehensiveness and adequate scenario modeling for DER risks at multiple levels (e.g., aggregators, endpoints). Furthermore, there is little to no information about how DERMS at the sensing (e.g., endpoints) and control levels (e.g., transmission) can be compromised to cause cascading failures at the transmission-side and distribution-side. The importance of securing the cyber aspect of an integrated CPS like the smart grid with technologies like DERMS is overlooked and we intend to address that in this survey.

3) SCADA/Industrial control System (ICS) Security

ICS is a broad term that refers to control systems such as SCADA and is used to control industrial processes in various industries (e.g., water, transportation, electrical). There are notable survey papers when it comes to SCADA/ICS security [33][53][54][55]. These works have power grid-relevant areas such as communication protocols, survivability and resilience, future trends (e.g., virtualization, software defined networking), studies of major critical infrastructure incidents (e.g., Havex), SCADA/ICS device vulnerabilities (e.g., buffer overflows, insecure hardware/software supply chains), security standards (e.g., NIST SP800-82, Guide for SCADA and ICS Security), control and mitigation strategies for compromised SCADA systems, and SCADA testbeds for security testing.

As SCADA and IED systems connect to open internet networks and possibly the cloud, they are susceptible to cyber threats. Communication based on TCP/IP simplifies the system for fast data transfer but opens the way for worms, viruses, and internet attacks. Cyber attacks types can be of many types such as ARP poisoning, false data injection (FDI), replay, flooding, and DoS. Malicious attacks against SCADA networks cause severe damage to utilities, such as the incorrect triggering of switches, sudden shutdowns of DERs, topological misconfiguration, FDI attacks, protocol vulnerabilities, etc. Thus, the entire DMS collapses resulting in blackouts.

RE-based DERs have gained popularity for several reasons, including clean energy availability, reduced transmission losses, and flexibility. According to the Renewable Capacity Statistics 2024 [56] published by the International Renewable Energy Agency (IRENA), there has almost been a 115% growth in renewable-based power generation in the last decade

(2014-2024). A proper monitoring and control scheme is required to integrate the DERs into the existing distribution system, and SCADA serves this purpose efficiently.

Similar to DERMS and DERs, SCADA/ICS systems are components within the power grid and as such, surveys and review papers in SCADA do not adequately address our topic area simply because it wasn't the research focus for these studies; therefore, we intend to add to the existing body of knowledge through a survey of multiple components in addition to ICS security.

D. Research Questions & Contributions

This review paper draws on the insights from notable works [30]-[55] but attempts to add to the existing body of knowledge by addressing the following research questions:

1) What are the cybersecurity research challenges and threat model scenarios in existing DER-/DERMS-related surveys?
2) How do we map cyber threats that affect the CIAA properties in the IEEE 1547.3 standard?
3) How to select the optimal architecture types across each mapped level according to the IEEE 1547.3 standard?
4) What are the potential emerging intrusion detection unit (IDU) technologies to harden DERMS against cyber threats?

More specifically, our contributions relative to the current state-of-the-art papers are summarized as follows:

1) Our survey proposes a novel intrusion detection framework called the Integrated AI-ready DERMS Edge Testbed that can be integrated with DERs and DERMS, specifically for DER aggregators. We propose integrating service orchestration (i.e., Kubernetes), cloud services, and pre-trained FL models for edge intelligence.
2) As part of our efforts to enhance DER/DERMS security, we put forward zero trust security principles across multiple layers within a DERMS architecture i.e., sensing, communication, and control. We emphasize the importance of shifting from perimeter-based defenses (e.g., physical security, firewalls) to zero trust capabilities (e.g., policy engines, least access privileges).
3) We provide threat models for DERs across multiple layers i.e., sensing, communication, and control that are derived from real-world incidents and actively researched by leading institutions such as the DoE.

Table I compares existing studies to our survey. "Scope" refers to the general focus area and "Security Aspects" specifies cybersecurity topic areas covered within the general focus area; while most of the state-of-the-art surveys present some form of these, they do not comprehensively consider all these aspects, especially with the integration of systems such as ADMS and DERMS to the power system. Additionally, the "IEEE 1547.3 5-level Architecture Map" and "IEEE 1547.3 Grid Entities Interaction" columns map the respective survey paper to the tiered architecture proposed by the IEEE Power and Energy Society and grid entities (e.g., transmission, distribution) within the architecture, respectively. We've used the following four criteria to compare each work for the "Security Aspects" column: (1) are there DER and power grid security-related testbeds ("TB") listed/detailed? (2) are novel hardware solutions ("HS") or software solution ("SS") proposed by the authors? (3) have the authors considered security standards ("ST", for example, NIST Internal Report (IR) 7628) that can be applied to the power grid?

E. Paper Organization

The paper is organized as follows: Section II offers background information relevant to DERMS, Section III introduces a novel system called Hybrid DERMS and considers the most likely cyber threats to this system, Section IV presents three emerging threat models for DERs and offers mitigative/prevention measures for each threat model. Section V explores the hardware security aspect for DERs and DERMS by considering reverse engineering, hardware trojan, and side channel attacks. Section VI presents four potential technologies for DERMS security, and Sections VII and VIII collectively propose the Intrusion Detection and Federated Framework (IDFF) by looking at FL, edge intelligence, and containerization. Section IX discusses threats and mitigations related to the deployment of machine-learning methods in DERMS, Section X identifies cyber threats to vehicular DER assets (i.e., EVs) and proposes an architecture to coordinate grid services from edge DER devices. Finally, Section XI presents lessons learned, Section XII offers technical challenges and future directions, and Section XIII concludes our manuscript.

II. Background for DERMS Security Evaluation

This section lists various test beds currently being used by US National Laboratories and organizations for industrial control systems (ICS)-, SCADA-, and DERMS-based testing, and offers readers a glimpse into how six testbeds are used by leading research and development institutions (e.g., Pacific Northwest National Laboratory (PNNL)) to model and solve challenges (e.g., evolving attack/threat models) relevant to the current cyber landscape. Similarly, a brief listing of seven well-known communication protocols is provided and segregated based on the primary entities (e.g., substations, RTUs) using said protocols.

A. SCADA/DERMS Test Beds

1) GridAPPS-D: PNNL is developing an open-source ADMS platform called GridAPPS-D [57] that is designed to address the operational challenges faced by distribution utilities. GridAPPS-D provides a reference architecture that can be used by researchers in this field to implement existing state-of-the-art tools, adapt existing systems, or create new systems that are compliant with standards.
2) National SCADA Test Bed (NSTB) – The NSTB is a joint initiative by Argonne, Idaho, Lawrence Berkeley, Los Alamos, Oak Ridge, Pacific Northwest, and Sandia National Laboratories [58]. Albeit being a slightly

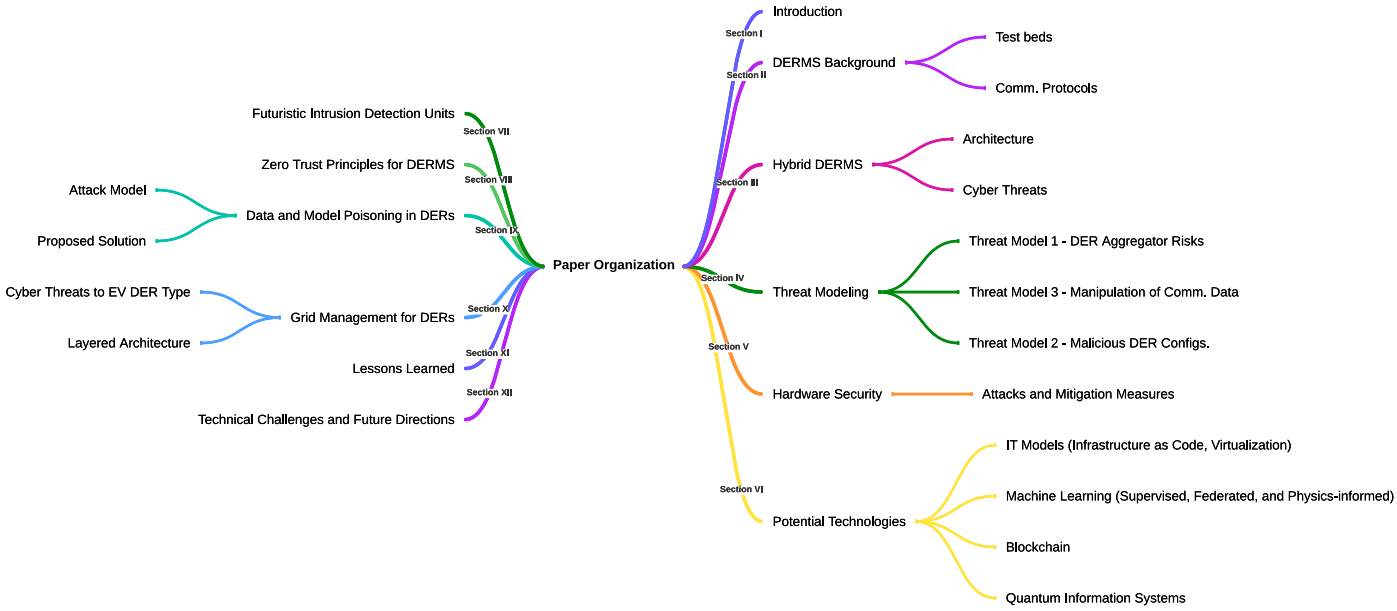


Fig. 4. **Roadmap to navigate the paper.** This paper is divided into thirteen sections with Sections II – XII as the main body.

older test bed being first released in 2008, NSTB is used for cybersecurity applications; for example, Los Alamos National Laboratory has research expertise in the role quantum key distribution (QKD) to exchange cryptographic keys that are then used in traditional algorithms to encrypt energy sector information such as smart grid data.

3) ADMS Test Bed – Pratt and Baggu from NREL [59] have proposed the idea of a vendor-neutral national "ADMS Test Bed" that provides a realistic laboratory test setting (e.g., utility management systems and field systems) with controller hardware-in-loop (CHIL) [60], power HIL (PHIL), and remote HIL (RHIL) capabilities in addition to multi-timescale simulation, multi-vendor platforms, and an integrated data collection and management system. Using these features, the test bed can be used to inform field deployment decisions, evaluate performance of ADMS VVO applications, and to evaluate the feasibility and performance of peak load management across multiple systems (e.g., ADMS, DERMS, EMS).
4) Software-defined Intelligent Grid Research Integration and Development (SI-GRID) – Developed by the Oak Ridge National Laboratory (ORNL) [61], SI-GRID test bed provides researchers an open research platform to evaluate the operation and cybersecurity of equipment that are used to support microgrids such as DER equipment (e.g., solar panels and batteries). The platform was used to develop and prototype technologies such as power electronics, generation technologies, energy storage, optimization, etc. All system components in SI-GRID operate under 100 volts but mimic the physics behind higher-voltage components.
5) PowerCyber – Researchers at the Iowa State University (ISU) [62] are currently developing a high-fidelity and open-access test bed to secure the power grid by providing features such as vulnerability analyses at the substation and control center levels, impact analysis quantification, and risk modelling and mitigation. This CPS security test bed interfaces with industry-grade SCADA systems with a real-time digital simulator (RTDS) and EMS software to conduct cyber attack/defense evaluations and cyber training.
6) CyberStrike STORMCLOUD - Sandia National Laboratory's (SNL) DER Cybersecurity Worksgroup (founded in 2017) provides recommendations and best practices for DER cybersecurity and is resposible for developing this testbed. CyberStrike STORMCLOUD [63] in particular is geared towards EV supply equipment (EVSE), solar, and wind DERs and will assist stakeholders in understanding the cyber risks in OT. Simulated equipment in this testbed are focused on providing authentication/authorization, integrity, availability, and encryption technologies to secure DERs. STORMCLOUD is currently not publicly available and requires attendees to participate in workshops and lectures/lessons covering topics such as open-source intelligence (OSINT), DoS attacks, web exploitation, etc.

B. Communication Protocols

The primary communication protocols relevant to substations are as follows:

1) Generic Object Oriented Substation Event (GOOSE) is a protocol that enables the transfer of multicast messages that relay substation event data issued by IEDs to other IEDs and is based on Ethernet (IEEE

802.3). For more information on GOOSE, please refer to [64][65][66][67][68][69][70][71][72].

2) Inter-control Center Communication Protocol (ICCP) was first introduced by the Electric Power Research Institute (EPRI) in 2001 to accommodate communications between control centers, substations, and operators [73] (e.g., Transmission System Operator (TSO), Independent System Operator (ISO)). For more information on ICCP, please refer to [74][75][76].
3) Distributed Network Protocol (DNP) (i.e., IEEE 1815) is used to handle data and control communications between substations and their operating devices such as RTUs and IEDs, and the master control station or control center [77]. For more information on DNP, please refer to [78][79][80][81][82][83][84][85][86].

The primary communication protocols used by endpoints such as RTUs, inverter-based resources (IBRs), and DERs are as follows:

1) Smart Energy Profile (SEP) 2.0 (i.e., IEEE 2030.5) is specified to allow interoperability between multiple smart energy devices in a customer's home to the power grid and is primarily built using TCP/IP [87]. For more information on SEP (e.g., threats, attacks, primary functions), please refer to the following resources [87][88][89][90][91][92].
2) Modbus is the most long-standing and widely used protocol for automation devices such as DER endpoints (e.g., smart inverters) regardless of network or bus types (i.e., architecture agnostic) [93]. It enables communication through a client/server architecture for intra-device communication using TCP/IP, serial, or through the User Datagram Protocol (UDP) [94]. For more information on Modbus, please refer to the following resources [95][96][97][98][99][100].
3) Manufacturing Message Specification (MMS) (i.e., (IEC) 61850) was initially designed to provide remote access or control to field devices. For more information on MMS, please refer to the following resources [101][102][103][104][105] [106][107][108].
4) Building Automation Control Network (BACnet) is a data communication protocol that enables interoperation and compatibility between multiple devices and device types within building automation and control environments. Though not directly related to DERMS, a microgrid that handles multiple energy resources such as solar, wind, or geothermal heat pumps (GHP) can power a smart building that uses BACnet. For more information on BACnet, please refer to the following resources [109][110][111].

III. Hybrid DERMS – A Security Perspective

While Section II has provided an overview of testbeds and communication protocols relevant to DER/DERMS security, we will continue the discussion in this section by proposing a conceptual diagram of Hybrid DERMS and listing five of the most likely cyber threats facing this concept architecture. Hybrid DERMS is designed to accommodate the high penetration of DERs in terms of smooth market operations, flexible resource scheduling, and accurate forecasting.

As discussed by Strezoski et al. [12][112], there are multiple DER management solutions, all frequently called DERMS, but aimed to achieve completely different goals for different stakeholders. They range from centralized software solutions, called Utility/Grid DERMS, aimed for Distribution System Operators (DSOs) and distribution grid planners and engineers to completely decentralized solutions for aggregation of DERs or EVs, and providing basic programs, such as demand response, energy efficiency, or offering aggregated DER power on wholesale markets. These solutions are called DER/EV Aggregators. Generally, DERMS architecture types are classified under centralized or decentralized types, and have DER management solutions that have unique aims and a body of stakeholders that benefit from using them. Stakeholders that benefit from centralized architecture types are DSOs and planning/innovation departments in distribution utilities and typical objectives for centralized types are to relieve congestion problems, secure grid edge stability, and optimize existing and new assets. Similarly, market participants, prosumers and DER aggregators are stakeholders that use the decentralized architecture which provides aggregate DERs for local energy management, optimizes energy portfolios, minimizes imbalance costs, and integrates distributed generators (DGs). Further details on these architecture types are given in [12]. However, none of these solutions alone can fully address the challenges posed by integration of high amount of DERs. To accurately plan for the integration of DERs, forecast their impact on the distribution grid, defer capital investments in grid assets, utilize DERs as flexible resources, harness their aggregated potential, and monetize their flexibility, a concept of "Hybrid DERMS" is proposed in [12].

As shown in Fig. 5, a Hybrid DERMS comprises of a Utility DERMS, DER and EV Aggregators, Microgrid Controllers, and Electricity Market Operators, integrated into a unique solution for managing emerging distribution grids with DERs dispersed all over the grid, and across different voltage levels. By integrating DER and EV Aggregators and Microgrid Controllers through a Utility DERMS, DSOs can enhance their awareness of small-scale, dispersed DERs and EVs. The Utility DERMS enables operators and grid engineers to have real-time visibility into the grid, including the impact of behind-the-meter (BTM) DERs and EV chargers. This integration allows DSOs to utilize the flexibility of all available resources, communicate with large-scale DERs and level 3 EV chargers, and leverage small-scale resources through aggregators to optimize the grid and avoid technical violations. Furthermore, if or when, regulations permit aggregated DERs to participate in electricity markets, the integration of a Utility DERMS with DER Aggregators and Local Electricity Market Operators becomes of a high importance. Namely, the Utility DERMS validates and checks the schedules of DERs and DER Aggregators against technical grid constraints, a task that only a grid-aware software can perform effectively, and in that way keeps the grid in an optimal operational condition, while utilizing DERs in the most effective way.

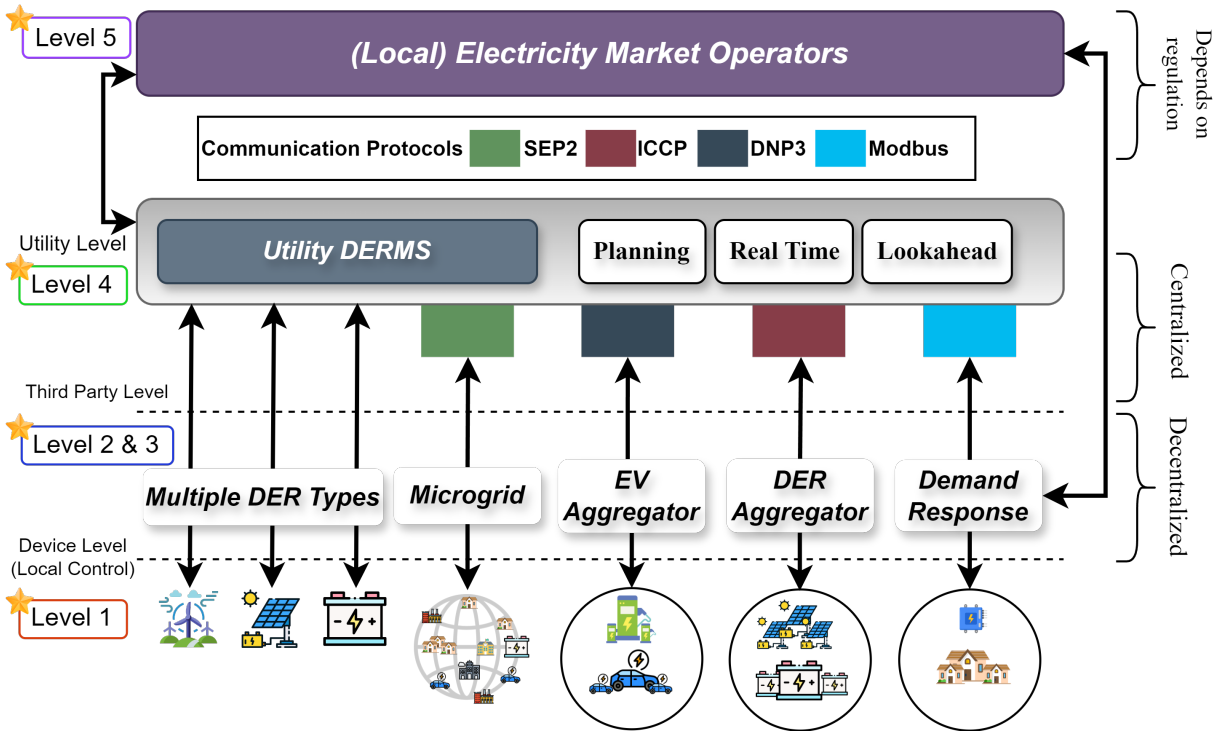


Fig. 5. **Hybrid DERMS.** In addition to the flexibility (i.e., DER scalability, communication) this architecture supports, the integration of centralized and decentralized operation provides broader functionalities (e.g., management and optimization of DERs) across multiple levels [12].

There is no doubt that a Hybrid DERMS concept is the future of DER management, as all of these separate solutions are tremendously more effective when integrate together, and there have already been various pilot projects with highly promising results [12][112]. However, a Hybrid DERMS concept carries a fair share of challenges as well, and cyber attacks are probably the most challenging aspect. As described previously, to work effectively and efficiently, a Hybrid DERMS assumes proper communication on several levels. First, a Utility DERMS should communicate downstream with DER and EV Aggregators, Microgrid Controllers, as well as with large-scale DERs. Second, DER Aggregators and Microgrid Controllers should communicate downstream with small-scale DERs, building management systems, and EV chargers, and upstream with a Utility DERMS. Finally, both a Utility DERMS and Aggregators should be able to communicate with Electricity Market Operators. This complicated communication infrastructure introduces new points of vulnerability and potential cyber threats. The main cyber threats that shall be considered before deploying a Hybrid DERMS are as follows:

- **Resource availability**: Hackers may attempt to overwhelm the Hybrid DERMS system (either through aggregators or through multiplying communication signals directly to/from DERs) with numerous unnecessary information flows, causing service disruptions and rendering the system (at least temporarily) unavailable. These attacks directly endanger grid operations, market transactions, and/or customer services, but may also endanger signals from Hybrid DERMS to protective equipment, causing unnecessary tripping, blackouts, and/or disruptions to entire areas of a distribution grid.
- **Interoperability and integration risks**: As Hybrid DERMS integrate multiple systems (i.e. Utility DERMS, DER and EV Aggregators, Microgrid Controllers, local DER automation, etc.), that can be developed by different vendors, ensuring secure and safe data flow and exchange is a significant challenge. Incompatibilities, vulnerabilities in different interfaces, or improper configuration of the communication infrastructure can be exploited by hackers to gain unauthorized access and/or manipulate the data. This can consequently threaten to endanger both grid operations as well as customer services.
- **Supply chain risks**: Similar to the previous threat, as Hybrid DERMS rely on various software and communication components developed mostly by different vendors, compromised components introduced through the supply chain can lead to security threats and system breaches. It would cause a domino effect, threatening to endanger the entire system causing damages to entire distribution grid infrastructure.
- **Unauthorized access**: Hackers may try to gain access to the Hybrid DERMS system (either through breaching a Utility DERMS' security, or through gaining unauthorized access to aggregators'/microgrids' managing software), endangering the security of sensitive data, control functions, or communication channels. This can lead to unauthorized manipulation of DERs,

grid operations, and/or market transactions, as well as endangering the safety and security of the entire distribution grid, by manipulating data in key applications such as SCADA, State Estimation, and relay protection screening.

- **Data breaches**: A Hybrid DERMS handles a huge amount of data, including customer information, energy usage data, and distribution grid protection settings and information. A data breach can lead to exposure of sensitive information, privacy violations, misuse of customer data, and even malfunction of protective devices leading to massive blackouts.

IV. Threat Modeling for DERs

This section will discuss three threat scenarios, and their respective preventive (i.e., steps taken prior to an attack) and mitigative (i.e., steps taken after an attack to reduce impact) measures based on the threat models presented by the DoE [113]. Subsection 1 covers DER aggregation risks, Subsection 2 details malicious DER configurations, and Subsection 3 covers manipulation of communication data, all with their respective threat models (e.g., indicators of compromise (IoC), vulnerabilities, risk, attacks, and mapping to Microsoft's STRIDE) and prevention/mitigation measures. FDI attacks are a significant part of threat scenario 3 (i.e., Subsection 3) as there is significant research done to model, remediate, and prevent FDI attacks due to its practicality. These measures can be combined with the core framework principles outlined in the NIST Framework for Improving Critical Infrastructure Cybersecurity [114] to manage cyber risk to DERMS and DERs. The core framework principles are identify, protect, detect, respond, and recover. For instance, preventive measures like encryption or firewall implementations would be classified under the "protect" principle; this is because they function as safeguards to ensure the reliable delivery and maintenance of critical services such as power distribution, demand response management, and load shedding.

A DERMS can be broken down into three layers - sensing, communication, and control layers- similar to the framework initially proposed by El Rewini et al. [115][116] for automotive environments. The sensing layer consists of monitoring devices (e.g., IEDs, RTUs, phasor measurement units (PMUs)) and DER smart metering equipment that remotely monitors system states, transmit data about physical events (e.g., line-to-ground or line-to-line faults), and measure DER power contribution to the grid. Secondly, the communication layer consists of protocols that enable inter- and intra-system communication (e.g., device to device, device to substation, substation to Regional Transmission Organizations (RTOs)). This layer acts as a bridge between the sensing and the third layer (i.e., control layer) so there is bidirectional communication between remotely deployed sensors and the main stations that aggregate data from these sensors. Finally, the control layer is responsible for translating digital commands issued from a centralized entity (e.g., substation or control center) into real-time process control to operate sensors' actuators, change switching capabilities, or manipulate overcurrent or fault protection settings.

Various threat scenarios exist at multiple levels of a DERMS system. For instance, threats to the DERMS aggregator may cause widespread disruption due to cascading outages. Similarly, spoofed DER data and man in the middle attacks can impact monitoring and state estimation systems leading to misinformed decision-making or even more drastic failures during periods of high demand. When evaluating threats, it is important to consider features such as likelihood of a successful compromise (including various threat vectors such as unsolicited emails, malicious attachments, unencrypted communications, etc.), severity of the consequences of those compromises across different dimensions (e.g., grid resilience, economic impact, safety, cascading impacts to other critical infrastructures). Enumerating these requires developing an understanding of potential sources of threats and their nature (e.g., insider, nation-state, non-adversarial) using threat modeling.

Threats are defined as the potential for a threat agent (e.g., black hat hackers) to exploit information system vulnerabilities or a threat vector to be exploited (e.g., unauthenticated communication sessions) due to vulnerabilities [117]. As we will see later in this section, depending on the vulnerability types and exploitation methods, different attacks are possible. Threat modeling as defined by the National Institute of Standards and Technology (NIST) [118] is "a form of risk assessment that models aspects of the attack and defense sides of a logical entity, such as a piece of data, an application, a host, a system, or an environment". Threat modeling subsequently allows for the prioritization of the mitigation measures and controls that are most likely to bring risk levels within organizational tolerances. For the purposes of this paper, threats to any cyber-physical energy system are considered as threats also to DERMS and DERs.

A. Threat Scenario 1 – DER Aggregation Risks

1) Threat Model

A DERMS consists of multiple DERs (e.g., solar, wind, battery energy storage systems, EVs) that can either be connected to a utility grid or can function as part of a separate microgrid. A DER aggregator combines real-time data from numerous BTM DER units to inform decisions at the DSO level. DER aggregators may have bidirectional communication with both load (i.e., energy supply) and DER generation units, and may exercise some control over demand response needs. If one of these DERs is compromised, the utility or microgrid it supports can still be made stable through the other DERs. However, large-scale outages or instabilities in the grid at device/aggregator levels could occur when multiple large-scale DERs or DER aggregators are attacked simultaneously through various cyber attacks (e.g., denial-of-service, self-propagating malware). These attacks can exploit vulnerabilities in multiple DERs, significantly increasing the impact of the attack. For example, the smart inverter/DER control parameters can be compromised to modify specific values by configuration change patch methods. As mentioned earlier in this section, this threat scenario is aggregator-centric and market operations-centric. Since DER

TABLE II
POSSIBLE ATTACKS, PREVENTION/MITIGATION MEASURES, AND IMPACTS FOR DER AGGREGATION RISKS THREAT SCENARIO.

Attack	**Vulnerabilities**	**IoC**	**LoA/Risk**	**IEEE 1547.3 Impact**	**Prevention or Mitigation**	**Primary Compromised Property**	**STRIDE Mapping**	**Refs.**
DoS	Unauthorized Physical Access, and Weak Credentials	System Shutdowns, Unusually High Network Traffic	Medium/⇑	Levels 3, 4, & 5	Network Monitoring, Access Control Mechanisms, OT Firewalls	Availability	(D)	[119], [120], [121], [122]
Ransomware or Malware	Unverified Email Payloads, Unauthorized Physical Access, Poorly Written Code	Suspicious Network Traffic, Unauthorized System Operations, System Shutdowns	High/⇑	Levels 3, 4, & 5	Backup Systems/Data	Availability Accountability	(D)	[123], [124], [125]
Load-changing or Load-altering	Access to System Topology via OSINT, Compromised EV/EVCS	Unexpected Variations in Power in Voltage or Frequency, Changes in Electricity Demand	Low/ ⟺	Levels 1 & 2	Isolate or Disconnect Compromised DER Devices	Confidentiality	(E)	[126], [120], [127]
Modified Firmware	Unauthorized Physical/Remote Access or Poor Config. Settings	Frequency Fluctuations or Voltage Sags	Medium/⇑	Levels 1 & 2	Trusted Supply Chain Vendors, Access Control, Firmware Rollbacks	Integrity	(T)	[126], [128], [129], [130]
Trojan	Unverified Email Payloads, Unauthorized Physical Access, Compromised Supply Chain Components	Overworked Systems, Unauthorized Control Operations, System Shutdowns	High/⇑	Levels 3, 4, and 5	Demilitarized Zones, Intrusion Detection Systems	Confidentiality Availability	(I)	[131], [132], [133], [134], [135]

aggregators inform decisions at the system-level (e.g., DSOs, TSOs), operations such as short-term energy forecasting and generator availability, energy trading, dispatching adequate generation to meet daily demands, etc. will suffer unfavourable consequences. According to the reliability rules set by the North American Electric Reliability Corporation (NERC) for power systems [136], steps should be taken to anticipate multiple contingencies (e.g., overloads, inadequate transmission line capacities) and deploy prevention/mitigation measures to keep the grid stable.

It should be noted that these attacks may not be mutually exclusive of one another. For example, attackers can install malware in a DERMS system that could cause DERs and DERs loads to malfunction or shutdown (e.g., the BlackEnergy attack in Ukraine [137]), could execute stealthy FDI attacks to deceive state estimators by changing power system variables to remain within thresholds thus contributing to a load changing attack [120], or could penetrate the system through hardware trojans to enable additional attacks. Furthermore, Konstantinou et al. performed a firmware modification attack by reverse-engineering a relay controller (i.e., a sensing-layer device) to show that modifications to its boot level configurations can make it operate abnormally or even disable it (eg. DoS). Table II lists the attacks, vulnerabilities, indicators of compromise (IoC), impact, and mitigation strategies for this threat scenario. To assess the consequence of these attacks, we utilize likelihood of attack (LoA), risk, and impact as qualitiative metrics. LoA is the likelihood of occurrence of an attack (high, medium, or low) and the primary level of impact is categorized according to the "Hierarchical DER System Five-level Architecture" as specified by IEEE 1547.3 [11] (also see Fig. 3). Level 1 entities include AMI and DER edge devices, Level 2 refers to load and energy management systems, Level 3 covers third party systems such as ADMS and aggregators, Level 4 refers to ISOs/TSOs, and Level 5 handles energy market interactions. Impacts are designated based on findings from the average attack for each scenario and does not specifically consider the worst-case scenario. The STRIDE mapping (i.e., Spoofing, Tampering, Repudiation, Information Disclosure, DoS, and Elevation of Privilege) is applied to the threat models in this section to demonstrate that IT threat models can be adapted to OT threat scenarios. We use the definition of risk outlined by NIST - "The extent to which an entity is threatened by a potential circumstance or event" and is categorized by arrows (double-sided, down, or up). For instance, trojan attacks have a higher likelihood of occurrence as nation-state level threats have launched remote access trojan (RAT) attacks on utilities (e.g., poetRAT) and a high risk of threatening the operational capabilities of power systems through denial-of-service attacks. Also, since Trojan attacks (e.g., BlackEnergy) primarily compromise confidentiality and availability, they will have secondary or tertiary consequences on existing energy suppliers, immediate industrial processes (e.g., level 3 - load management systems, level 4 - outage management systems), and macro-level entities such as in level 5 (i.e., energy markets). The primary STRIDE mapping category for Trojan attacks is Information Disclosure (I) since sensitive information can be obtained through whale-phishing [138] and side-channel leakages (e.g., overt channel, covert channel [139]). Similarly, levels 3, 4, and 5 are also at medium to high likelihoods of being compromised by DoS and ransomware attacks and the primary STRIDE mapping for these attacks is Denial of Service (D).

2) Prevention & Mitigation Measures

Multiple preventive and mitigative measures exist for attacks in Threat Scenario 1. Deploying demilitarized zones (DMZs) or firewalls can limit threats by preventing lateral movement within a target network. DMZs work hand-in-hand with firewalls in defining security policies, functionalities, and optimal placements [140]. Servers that communicate with external networks can be placed within DMZs to provide

isolation and protection of internal networks. Similarly, functionalities such as stateful inspection of network traffic, packet filtering, and circuit-level gateways can be implemented within a next-generation firewall (NGFW) tailored for OT networks. NGFWs can incorporate additional context beyond traditional firewalls, such as application-level context, context about the communicating device or user, or corporate policies regarding acceptable content. A similar mitigation measure at the physical level is to disconnect or otherwise isolate compromised DER devices from the rest of the distribution grid.

A major issue being faced by different industries such as IT, telecommunications, and the energy sector is the deployment of unsecured or untested hardware that have supply chain weaknesses. For instance, hardware, software, or firmware backdoors can be inserted by malicious threat actors or suppliers during manufacturing to exploit devices after they are deployed for various applications. Therefore, it is essential to work with trusted supply chain vendors and third parties that have exercise adequate cyber hygiene to ensure device-level security. Supply chain risk management (SCRM) will enable utilities/aggregators to safeguard critical systems from compromises that may arise due to suppliers, supply chains, products, or their services. According to NIST's Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations publication [141], the following measures will help in controlling supply chain risks: access enforcement (all entities in a supply chain have appropriate access mechanisms in place), accountability management (traceability of actions and actors in a supply chain), information flow (communication of information to various participating entities), secure remote access mechanisms, and auditing/monitoring of external systems (systems outside the networks of the acquirer).

B. Threat Scenario 2 – Malicious DER Configurations and Control Requests

1) Threat Model

Like computing and telecommunications equipment, devices integrated with DERs (e.g., programmable logic controllers can be misconfigured and this can lead to compromised DERs. This misconfiguration can be done unintentionally (e.g., default settings, lack of training or awareness of best practices) or intentionally (manipulation of settings such as firewall rules and timeout settings [4]) during factory shipments, servicing schedules, installation of new equipment, or through unverified system patches. This can either cause the DER device(s) to be non-functional or operate erroneously (e.g., execute malicious control commands from compromised aggregators or utility personnel). Control settings for DER endpoints can be compromised through Edit Parameters or Parameter File updates by malicious grid operators in DER control servers. This attack is a DER control misconfiguration attack leveraging the new required grid support functions defined in IEEE 1547-2018, such as DER ride-through and trip threshold settings, causing inverter tripping during a grid disturbance. The nefarious control setting of multiple inverter-based DER sites can result in a regional blackout. One way malicious updates can be installed is through malicious and stealthy control software that modifies the control logic for DER control devices [143]. It is important to note that PE is considered as an attack in this threat scenario and not as a vulnerability [147]. As stated by Sen and colleagues [142], privilege escalation attacks can be carried out by exploiting PE vulnerabilities. This attack ranks high in risk as once access privileges are escalated to the root level, the threat actor can move laterally across other network assets to carry out other attacks such as DoS and FDI to disrupt grid operation. This threat scenario is device-centric and communication protocol-centric as physical access to devices and unsecured hardware/software supply chains provide fairly easy avenues for threats to tamper with DER assets and access sensitive information. Privilege escalation and malicious update attacks map to Elevation of Privilege (E) in STRIDE but impact different levels of IEEE 1547.3 framework; for example, malicious updates can be targeted at grid support functions (e.g., power factor) of DER edge devices (e.g., solar inverters) to violate the parameters that are defined for these grid support functions to cause undesirable behaviors or make the devices operate outside the limits specified by the parameters [148]. Since privilege escalation attacks primarily gain access to privileged local accounts (e.g., compromising the confidentiality of account passwords and usernames) before progressing to move within internal networks, gaining access to entities in levels 2, 3, and 4 will be most lucrative to retrieve sensitive information such as operational knowledge of the grid [149] as the entities in these levels are responsible for important functions such as grid protection schemes (i.e., level 2), aggregation (i.e., level 3), and outage management (i.e., level 4).

Table III lists three attacks that are relevant to this threat scenario.

2) Prevention & Mitigation Measures

Cryptography remains a viable method for defense through encryption, message authentication codes, hashing, or the exchange of proper cryptographic keys [144]. However, there is a tradeoff between adequate security mechanisms and the computational requirements and energy usage required to support said mechanisms. In consumer and enterprise IT, this tradeoff is often negligible, but it becomes more significant when considering low-power embedded devices.

A preventive measure to detect suspicious behaviour from DER endpoints is through side-channel analysis of power variables to "fingerprint" the behavior of the device during normal (baseline) and suspicious operation. Acceptable threshold and tolerances during baseline operation are measured and then compared to detect anomalous behaviour due to, for example, malicious updates [145].

C. Threat Scenario 3 – Manipulation of Communication Data

1) Threat Model

DERs and their operating devices can be considered as part of the internet of things (IoT) paradigm and are thus equipped

TABLE III
POSSIBLE ATTACKS, PREVENTION/MITIGATION MEASURES, AND IMPACTS FOR MALICIOUS DER CONFIGURATIONS AND CONTROL REQUESTS THREAT SCENARIO.

Attack	**Vulnerabilities**	**IoC**	**LoA/Risk**	**IEEE 1547.3 Impacts**	**Prevention or Mitigation**	**Primary Compromised Property**	**STRIDE Mapping**	**Refs.**
Privilege Escalation/Elevation	Unauthorized Physical or Remote Access, Hardware or Software Backdoors, Unencrypted Communications	Uninitiated Remote Code Execution, Change in Program Flow, Unsolicited Customer DER Messages	Medium/$\Uparrow$	Levels 2, 3, & 4	Access Control Mechanisms, Traffic Monitoring	Confidentiality Accountability	(E)	[119], [125], [142]
Malicious Updates or Malicious Software		Disconnected or Disabled DER Devices	Low/ $\Longleftrightarrow$	Levels 1 & 2	Update Monitoring, Software Integrity Checks/Code-signing, Cryptography, Side Channel Analysis	Confidentiality Integrity	(E)	[121], [143], [144], [145], [130]
Data Modification & Data Alteration		Manipulated System Data	High/ $\Longleftrightarrow$	Levels 1 & 2	Real-time State Estimation, Min. Device Protection, ML-based Anomaly Detection	Integrity	(T)	[126], [146]

TABLE IV
POSSIBLE ATTACKS, PREVENTION/MITIGATION MEASURES, AND IMPACTS FOR MANIPULATION OF COMMUNICATION DATA THREAT SCENARIO.

Attack	**Vulnerabilities**	**IoC**	**LoA/Risk**	**IEEE 1547.3 Impacts**	**Prevention or Mitigation**	**Primary Compromised Property**	**STRIDE Mapping**	**Refs.**
Spoofing	Unauthorized Access to Security Certificates	ARP Poisoning, System Variables Operating Beyond Thresholds	Medium/ $\Longleftrightarrow$	Levels 1 & 2	TLS Security, Certificate Management	Confidentiality Accountability	(S)	[146][150]
MITM	Unencrypted Communications, Legacy Devices and Open Ports	ARP Poisoning, Stolen Ports	Medium/ $\Longleftrightarrow$	Levels 3 & 4	TLS Security, Certificate Management, Session Renegotiation	Confidentiality Accountability	(E)	[146], [151], [152]
FDI	Legacy or Poorly Secured Devices	Erroneous Decisions by Automation Devices, DER Outage	High/$\Uparrow$	Levels 1, 2, & 3	Encryption, Statistical, Temporal, or Distance-based Anomaly Detectors	Integrity	(T)	[153], [154], [155], [156], [157]

TABLE V
REVIEW OF EXISTING FDIA MODELING APPROACHES IN THE ENERGY SECTOR (1).

Attack Vectors on Targeted Features and Devices/Systems	**Countermeasure(s)**	**Remarks**	**Ref.**
Stealthy Attacks on Buses and Superbuses w/ Knowledge of Susceptance.	Securing Meter Measurements & Obscuring Susceptance from Adversaries.	Limited Knowledge of Jacobian Matrix. FDI Successful Only If Transmission Line Susceptances are Known.	[158]
Attacks Possible on Smart (e.g., voltage angles) and Traditional System Variables (e.g., current flows or bus voltages).	DSP-based Thresholding.	Assumed That FDI Attacks Classify as Anomalies in High-frequency Fourier Coefficients Than Regular Measurements.	[159]
Attacks Carried out on AMI or SCADA Communication Channels and Endpoints.	Lightweight Watermarking and Thresholding.	Data Streams from Meters are Watermarked and Passed Through a Threshold to Identify Tampering.	[160]
Hack Endpoints and DC Power Flow Linear Approximation to Model Stealthy Attacks.	Semi-supervised ML for Classification.	Detection Based on Autoencoders and GAN.	[161]
Attacker Types Based on Minimal, Moderate, and Maximum Knowledge of Attacked Devices.	Signature- and Anomaly-based IDS.	Detections Possible for Illegal Read/Write Operations From/To Smart Meters (Tampering).	[162]
"Generalized" DC Power Flow Linear Approximation.	State Forecasting-based Anomaly Detection.	Autoregressive (AR) Models for One-step Ahead Prediction. Two Thresholds Used to Validate Hypothesis Tests.	[163]
FDI Modeled with Limited Network Information.	Increase Attack Cost and Ensure Protection for Pre-determined No. of Compromised Measurements.	Validation Performed on IEEE 14-bus System using a Load Redistribution (LR) Attack Model. Inputs: Network Topology, Network Parameters, and Connected Load Information. Considered Stealthy as the FDI Vector is Always Kept Under Residual.	[164]
Intrusion On Frequency And Voltage Control Inputs Of The Droop Controller In AC Microgrid.	Proposed Distributed Adaptive Secondary Control Strategy To Restore Rated Voltages And Frequency Post-FDI Attacks.	Two Case Studies for When One and All DGs are Attacked are Adopted. Results Indicate that the Proposed Control Strategy Returns Frequency and Voltage Values to Stable Measurements. Validated Through Matlab/HIL Simulations.	[165]
Disruption Of Voltage Stability And Internal Power Balance.	Distributed Control Strategy Based On Consensus Theory For Attack Detection, Localization And Improved Resilience Against FDI Attacks.	Primary and Secondary Control Loops Tested During Attacked Frequency/Voltage Measurements. Consensus Solution Shows Gradual Stabilization to Reference Value ($<$ 3 seconds) for Attacked Measurements.	[166]
Disruption of Voltage Regulation And Current Sharing Among DGs In DC Microgrids.	Multi-agent System Based Extended State Observer And Fault Tolerant Controller For Maintaining Asymptotic Stability Post-attack.	Five Test Scenarios Deployed to Validate Resiliency. FDI Attacks Test Scenario Validated Using Step and Sinusoidal Attacks. Results Indicate Little to No Fluctuation and Fast Recovery to Nominal Value.	[167]
Manipulation Of Voltage And Current Measurement To Disrupt The Primary And Secondary Central Loop Of Each DG In DC Microgrids.	Two-Layer ANN Based Approach For Mitigating Impact Of FDI Attacks On Voltage Regulation Followed By Ensuring Proper Load Distribution Among DGs.	Modeled FDI Attacks Types were Sequential, Random, and Simultaneous for Current/Voltage Measurements.	[168]

TABLE VI
REVIEW OF EXISTING FDIA MODELING APPROACHES IN THE ENERGY SECTOR (2).

Attack Vectors on Targeted Features and Devices/Systems	**Countermeasure(s)**	**Remarks**	**Ref.**
Disturbing The Operation Of The Secondary Control Layer By Manipulating Bus Voltage Of The DC-DC Converter.	AI-based (ANN) Approach For Immediate Detection And Mitigation Under Communication Delay And Time Varying FDI Attacks.	Modeled FDI Attacks Types were Random, Simultaneous, Non-simultaneous, and Time-varying. Results Indicate ANN has Errors $< 5\%$ in Estimating Injected Values for All Types.	[169]
Simultaneous Attack On The Local Measurements And Sensor Information Transmitted Through The Communication Channels To The Controllers.	Energy Based Detection Using Intrinsic Mode Function And Event Driven Mitigation Strategy For Reconstruction Of The Falsified Signals.	Three FDI Attacks Types (Concurrent, Communication Link, Control Input) Were Tested. Authors Propose a "Detection Index" to Detect Anomalies Based on Energy Usage Ratios Between Distributed Agents. Erratic Increases in Energy Usages Indicate FDI Attacks.	[170]
Falsification Of Sensor Measurement To Disrupt The Electricity Market Operation Thereby Causing Loss/Profit To A Particular Utility/Consumer.	Blockchain-based Approach For Secured Peer-to-peer Energy Market Operation.	FDI Attacks Shows Effective Consensus Price Cannot be Reached Even After a High No. of Iterations, Therefore Disrupting the Energy Market. However, the Success Probability of this FDI Attack is 1%.	[171]
Attack On The Advanced Metering Infrastructure (AMI) Of Hybrid Microgrid.	Deep-Learning Based Intrusion Detection And Prediction Of Power, Energy Market Price And Load Demand.	LSTM Used as an IDS and for Load Forecasting and Forecast Error Estimation. If Error Lies Outside LSTM's Prediction Interval, FDI Attacks is Suspected. Results Indicate that Increasing LSTM's Prediction Interval Reduces Its Sensitivity to FDI Attacks.	[172]
Manipulation of The Voltage and Current Information of The Power Converters to Disrupt Load Sharing Among DERs And Voltage Regulation at Interfacing Buses.	Recurrent Neural Network (RNN)-Based Scheme For FDI Attacks Detection and Localising The Targeted DERs.	The Non-linear Autoregressive Exogenous (NARX) Model Used Can Effectively Distinguish between Fluctuations in Measurements Due to Transient Load Changes and FDI Attacks. Performance Validated Through OPAL-RTDS HIL Testing.	[173]
Manipulation Of The Reference Frequency And Voltage Signals To The Droop Controller.	Detection Of FDI Attacks On The Droop Control Using Local Information Of Deviation In Voltage And Frequency Followed By Differentiating Between Cyber Intrusion And Physical Faults.	Proposed Method Validated for IEEE and CIGRE LV Distribution/Bus Systems. Results Indicate a Detection Rate of 20 Samples/Cycle (5 ms).	[174]
Injection Of False Data On The Output Current Of The Distributed Generation Units In Collaborative DC Microgrids.	Adaptive Nonlinear Observer For FDI Attacks Detection And Mitigation While Considering Communication Delay, Uncertainty, And Sensor Noise.	Valid For 2 Scenarios with 4–agent and 8–agent DG units. FDI Attacks Modeled as Time-delayed, Sinusoidal, and Ramp Functions.	[175]
Manipulation of the Reactive Power Data of Individual DGs to Change The Reference Values Of the Secondary Controller.	Mitigation And Imparting Resiliency Against FDI Attacks Using A Credibility-based Synchronous Framework Based on Local Data.	Data from an Attacked DG Unit is Detected and Verified Based on a Threshold through Local/ Neighboring DG Units. Attacked DG Unit and Its Data are Isolated Post-detection.	[176]
Intrusion of the Communication Link Among the Microgrid Agents to Manipulate the Voltage Output of Individual Agents Thereby Disturbing the Voltage Distribution and the Global Reference Voltage Level of the Overall Microgrid.	Distributed Bank of Sliding Mode Observers Used to Replace Corrupted Voltage Information of Converter With Actual Ones.	Superior to the Conventional Consensus Algorithm Due to its Capability of Reducing Voltage Fluctuations in the Presence of FDI Attacks.	[177]
Malicious Propagation of False Data Malware in the Load Bus Communication Network of DC Microgrid.	Defense Mechanism Based On Game Theory Model Between the Attacker and the Defender. Propagation of the Data Malware On System Operation Reduced By Solving the Game Theory Problem Using Evolutionary Algorithms.	Attacker's Objective is to Maximize Benefit and Defender's Objective is to Minimize Total Loss. Natural Aggregation Algorithm (NAA) is Used to Find the Optimal Strategy for Attacker/Defender.	[178]

with networking capabilities primarily supported by the protocols mentioned in Section II. As a result, communicated data may be intercepted, manipulated, or injected to misinform system operators or automation systems. These compromises are known as data integrity attacks and can directly impact grid health by causing operators to respond in an inappropriate manner. The impact of such attacks is becoming ever more relevant as artificial intelligence or machine learning (AI/ML) approaches are leveraged to enable automated responses and advanced analytics. General AI approaches may be able to collaboratively (with each other and human operators) determine optimal actions that can be taken to stop, mitigate, or even retaliate against a cyber attack, and can incorporate much more contextual knowledge that can aid in identifying threats that might otherwise be missed. This is the approach being taken at Argonne National Laboratory in work such as [179].

However, these approaches can be undermined by improper data such as during online training, where the data may be poisoned [180][181]. One way by which in-transit data can be poisoned is through man-in-the-middle attacks, which affect the address resolution protocol (ARP) [146][150][182]. The adversary changes their media access control (MAC) to match the victim's IP address or through stolen ports, where open ports are used to steal network traffic to perform active or passive attacks. SunSpec Modbus is vulnerable to this attack when X509 certificates are used (IEEE 2030.5 (SEP2), IEEE 1815 (DNP3-SA, which is a new version mandating IEC 62351-5)). Two additional means by which man-in-the-middle attacks are carried out are through address resolution protocol (ARP) poisoning where the adversary changes his/her media access control (MAC) to match the IP address of the victim, and through stolen ports where open ports are used to steal network traffic to carry out active or passive attacks [151]. FDI attacks can be carried out with full or partial system knowledge by modifying system variables such as meter readings, control commands, and state estimates. Such attacks can lead to critical failures especially in times of peak demand or extreme stress (e.g., natural disasters), or misinform utilities and customers of demand and supply needs through what is known as an "energy deceiving" attack [183]. Park and colleagues [152] provide an example of a

firmware modification attack using Lockheed Martin's Cyber Kill Chain (CKC) model. The first five steps of CKC (initial access, execution, persistence, evasion, and discovery) are assumed to have been achieved through backdoor injection, while the authors validate a man-in-the-middle attack through the access of the network layer of a smart inverter through TCP/IP. According to de Carvalho and Saleem [146], SunSpec Modbus and DNP3 are vulnerable to man-in-the-middle and spoofing attacks, in addition to denial-of-service and data modification attacks as these protocols lack adequate security measures. SEP2 implements cryptography and is considered a more resilient protocol, although it is still susceptible to DoS attacks. This threat scenario is primarily communication protocol-centric simply due to the nature of the threat surfaces - if data in transit is intercepted with minimal resistance (i.e., lack of session/device authentication or encryption), there is inadequate security features that are enabled/configured by the respective communication protocol. Table IV lists the respective attacks and their corresponding vulnerabilities and IoCs for this threat scenario.

There might be ambiguity behind data modification/data alteration, FDI, and man-in-the-middle attacks which can be clarified as follows. FDI attacks are different from data modification attacks in that they cause state estimators to output erroneous values and can be modeled in multiple ways [191] whereas data modification attacks modify data in transit before they arrive at a destination [192] and do not typically have a modeling approach. Data modification attacks are usually active (i.e., compromise integrity) while man-in-the-middle can be active or passive in nature (i.e., compromise confidentiality) [81], therefore respectively mapping to the Tampering (T) and Elevation of Privilege (E) categories of STRIDE.

DER operation can be manipulated through FDI attacks that inject falsified data on top of the actual signal/information at different stages i.e., (i) information shared among the DERs; (ii) switching signals generated by the controller for maintaining the required voltage/current profile; (iii) voltage/current signals fed back from the interfacing buses/observer; (iv) data transmitted to the IEDs for representing the status of the switches; and (v) reference signal for the primary current loop controller for the DER(s). As detailed earlier, the wider usage of DERs of varying types and sizes and the threat surface of microgrids is increased due to the high volumes data being transmitted through the communication infrastructure. In the distributed architecture, any false data injected in the communication layer between the DERs has a cascading effect on the DERs and may ultimately lead to deploying contingencies. The notable works carried out on disturbing the DER operation through FDI attacks has been elaborated in Tables V and VI. FDI attacks are primarily detected by using statistical or distance-based models [154]. The former is done by using Chi-squared tests and other statistical measures (e.g., kurtosis, skew) within state estimation processes to identify potentially anomalous data points. The latter measures the Euclidean distance between the estimated and the observed data obtained through state estimation variables (e.g., frequency, amplitude, and sampling frequency).

2) Prevention & Mitigation Measures

Examples of prevention/mitigation measures to spoofing and man-in-the middle attacks include implementing the TLS handshake and cryptography mechanism to ensure data integrity, confidentiality, and authentication, and to deny-list any revoked certificates that are fake or have expired. TLS secures communication between servers and clients using symmetric encryption techniques (private key encryption) though this adds overhead to the communication channel and the server. As of TLS 1.3 (released in 2018), there is reduced latency and enhanced security through reduced round-trip TLS handshake time and advanced cryptographic algorithms respectively.

Certificates from devices requesting a connection to the server can be managed by a certification authority (CA). The server can periodically publish lists of certificates that are deemed invalid or fake through certificate deny-listing. In IP-based networking, this is typically called as certification revocation lists (CRLs). Although this mitigation measure has not been widely applied in power systems, it is still a viable method for authenticating DER endpoints.

These threat scenarios can be mapped to the 3-layered sensing, communication, and control layers as shown in Fig. 6. The most significant threat vectors (i.e., the means by which a threat actor can infiltrate the DER system) for each layer are listed. Threats from scenarios 1 and 2 can be mapped to the sensing and communication layers as they primarily involve the compromise of a large number of DER endpoint devices and their respective device settings/configurations. Attacks at these endpoints can then propagate to other devices in the same network or area through communication-layer protocols like DNP3 or Modbus. These compromised devices can eventually have consequences in the control layer but the layers primarily compromised are the sensing and communication layers. Similarly, threat scenario 3 has more to do with exploiting the communication link between the endpoints and their commanding entity (e.g., control center). Compromising these layers can eventually let a threat actor access endpoint devices in the sensing layer but this is considered as a consequence and not a root cause.

Table VII captures a literature review related to cybersecurity attacks associated with SCADA that captures attacks relevant to all three threat models in this section. The "Attacks/Vulnerability" column lists the main attacks tackled by the proposed solution and the "Existing Correlation" column captures how the proposed solution is relevant to our context, i.e., DERMS security and the power grid.

V. Hardware Security

DERMS heavily rely on electronic hardware to facilitate data collection and sensing, processing, automation, and communication. These electronic devices can be vulnerable to a wide range of cyber attacks that can compromise sensitive data, cause catastrophic system failures, endanger human lives, and lead to massive financial loss. Hence, it is important to safeguard DERMS against these hardware

TABLE VII
REVIEW OF NOTABLE SCADA CYBERSECURITY PROBLEMS, ATTACKS, AND PROPOSED SOLUTIONS.

Problem	Proposed Solution	Attacks/Vulnerability	Correlation	Ref.
Detecting Natural (i.e., Faults) and Malicious (i.e., Cyber Attacks) Power System Events Using a 37-event Oak Ridge National Laboratory (ORNL) Dataset [184].	**Detection Algorithm** – Deep Learning (i.e., Artificial Neural Network (ANN)/Convolutional Neural Network (CNN)) and Support Vector Machine (SVM). **Data Processing** – Restricted Boltzmann Machine (RBM). **Testbed** – Three Bus and Two Line Transmission System with Four Relays and Four Circuit Breakers.	**Attacks** – (1) Relay Settings Change; (2) Data Injection; (3) Tripping Command Injection; **Vulnerability** – Unrestricted Access Privileges to Operators.	The Attacks are Widely Researched and Relevant to Distribution- (e.g., DERMS) and Generation-side Entities (e.g., DERs) as They're Stealthy and Target Protective Devices (e.g., Circuit Breakers)/Control Systems to Disrupt Normal Power Grid Operation and/or Damage Protective Equipment.	[185]
Endpoints Such as RTUs and IEDs Have Security Defenses such as Restricted Perimeters but Do Not Meet Secure Point-to-Point and Real-time Communication Requirements (i.e., Session Authentication) Due to Deployment Constraints (e.g., Resources, Legacy Devices).	**Cryptographic Architecture** – Symmetric Encryption for Key Generation, Asymmetric Encryption for Session Authentication, and Hashing Algorithm for Communication Integrity. **Test Framework** – Point-to-point Architecture with Master Terminal Units (MTUs), Sub-MTUs, RTUs, Broadcast Communication, and Multicast Communication Types. Additionally, the Avalanche Effect (i.e., Diffusion) and Authentication Properties (e.g., Non-injective Synchronisation) were Considered to Formally Evaluate The Proposed Solution.	**Hash Function Attacks** – (1) Collision; (2) Preimage Resistance; (3) Length Extension.	Field-control Devices Typically used in SCADA Systems Relay Sensitive Monitoring and Control Information to Operators in Control Centers and DERMS for Advanced Functions (e.g., Adaptive Protection, Generation Dispatch). Remote Operation of Such Devices Makes Them Easy Targets for Attackers to Intercept and Modify Information.	[186]
Power Grids Primarily Deliver Active and Reactive Power Flows Captured Through Measurement Data. Manipulation of Measurement or Command Data is Called False Data/Command Injection (FDI/FCI) Respectively. FDI Attacks Can be Modeled in Multiple Ways and There is a Lack of Generalized FDI Detection Based on Robust Detection Indices.	**Detection Algorithm** – The Detection Algorithm Computes Covariance Matrices for Different Measurement Variables in Normal and Attack Scenarios. The Matrices Work on the Following Key Sufficient Conditions: (1) The Eigenspace for FDI/FCI Scenarios Combines Standard Measurement Vectors + Injected Vectors in Affected Measurements and Varies Significantly from Normal Scenarios; and (2) The Sum of Eigenvalues (i.e., Trace) for FDI/FCI Scenarios is Significantly Higher than Normal Scenarios. These Conditions are Used to Compute Indices to Create the Detection Metric. A Threshold is Chosen Based on Multiple Test Cases. Algorithm was Evaluated with the Accuracy Metric. **Testbed** – IEEE 118-Bus-Based Power System with SCADA Control Equipment (e.g., On Load Tap Changing Transformers) Tested with Three Scenarios – FCI only, FDI only, and FDI + FCI.	**Attacks** – False Data Injection (FDI) and False Command Injection.	Manipulating Each Flow Type Leads to Undesirable Effects such as Grid Instability, Erroneous Control Operations, and Voltage Overflows. Attacks Through Manipulation Lead to Malfunctioning of SCADA Control Equipment and Faulty Data is Relayed from RTUs at the Substation-level to the Control Plane at the Transmission-level.	[187]
Detecting Malicious Attacks on SCADA Networks Based on State Estimation (e.g., Voltage Phasors) is Primarily Done Through Actual Measurement Data, System Topology, Redundant Measurements, and Measurement Errors. Therefore, There is a Need to Minimize Assumptions and the Data Required to Perform Robust Detection.	**Detection Algorithm** – The Researchers Use Benford's Law to Identify Illicit Data Injected by Hackers. Benford's Law Works Under Only One Assumption i.e., Malicious Data Injected by Hackers are Distributed Uniformly. This Assumption is Supported by the Law of Anomalous Numbers Which States that Smaller Leading Digits (e.g., 1 or 2) in a Set of Measurements Have a Higher Probability of Occurrence than Greater Leading Digits (e.g., 8 or 9). **Testbeds** – Detection Algorithm was Tested on WSCC 9-bus System, IEEE 14-bus System, New England 39-bus System, and 21,177-bus ENTSO-E System.	**Attack** – Generic Malicious Attacks that Manipulate System States.	Application of Benford's Law to Multiple Testbeds Shows that Predictions (i.e., "Fingerprints") Made by Benford's Law Matches Well with a Deviation Index of Less than 0.05 for All Testbeds. Malicious Attacks will Corrupt these Fingerprints and Can Therefore be Detected. Introducing this Detection Algorithm can be Done at Multiple Levels (e.g., Generation, Distribution) as DERs can Also Generate and Distribute Power Back to the Grid.	[188]
FDI Attacks on System Variables are Typically Addressed in the Context of Detection and Prevention, But Are Not Considered To Recover Actual (i.e., Pre-attack) Values of System Variables.	**Recovery Algorithm** – The Recovery Algorithm Requires Identifying an "Optimization Region" That Identifies Subgraphs within a Power System Where the Nodes are Buses and the Edges are Lines Connecting the Buses. The End Result is a Set of Subgraph Nodes that are Detected to be Attacked. The Recovery Algorithm Solves an Objective Function That Considers Voltage Phasors (i.e., Magnitude/Phase Angle) Subject to Active and Reactive Power Flows Constraints at Lines and Buses. Results from the Optimization Algorithm Restores Detected Attack Grid Variable Values to a Range Defined by the Three-sigma Rule. **Testbeds** – IEEE 118- and 14-bus Systems with Seven Attackable Zones. Three Case Studies were Identified (i.e., FDI with Incomplete System Information, FDI with Complete System Information, and FDI on Systems with High Renewables Penetration.	**Attacks** – FDI.	Case Study Three (i.e., High Renewables Penetration) is Particularly Relevant to Economies that Have High DER Penetration. Depending on the Resolution of Data Available to the Detection Algorithm (e.g., Hourly, 5-minute Intervals) and the DER Share to Grid Load Supply, High Detection and Recovery Rates are Produced.	[189]
Phase Shifting Transformers (PSTs) Manipulate Power Flows Between Two Ends of a Power Line Before Dispatching Power Back to the Grid. Manipulating PSTs to Cause Disruptions in Line Power Flows is Done by Sending False Commands to RTUs that Control PSTs, and There is a Lack of Detection Algorithms that Consider Compromised PSTs.	**Detection Algorithm** – Phase Shift and Voltages are Tracked for All Nodes (i.e., Generators, Phase Shifters) to Create a Reference Threshold. Measurements from PSTs $>$ Threshold are Considered as Attacked Measurements. **Testbed** – A Set Of Phase Shifting Transformers Placed in the Power System Based on IEEE 118-Bus System. Multiple (i.e., Four) Case Studies are Considered.	**Attacks** – FDI and Stealthy Phase Shift Command Injection.	The Increase of Variable Renewable Generation and DERs Faciliate the Need for PSTs as They Can Reduce Power Flow Congestion, Optimize Power Flows, and Improve Grid Capacity at Peak Demand Hours at the Transmission-level. Effective PST Operation can be Coupled with DERMS to Facilitate Effective Market Power Flows and Reduce Grid Disruptions by Controlling Power Overflows.	[190]

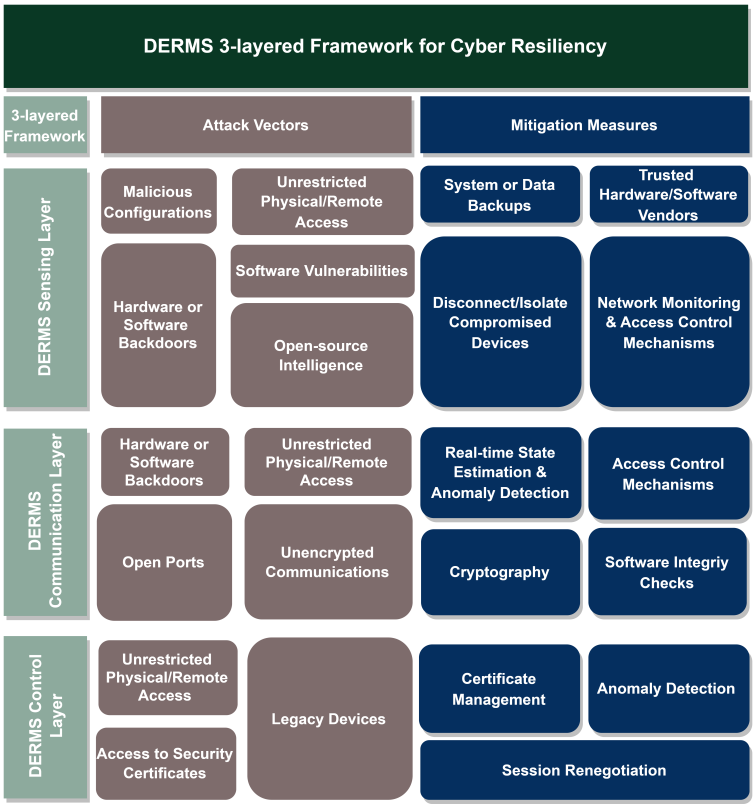


Fig. 6. **Layered framework representing DER threat vectors and mitigation measures.** Sensing, communication, and control layers have unique attack vector types (e.g., hardware backdoors, physical access, unencrypted communications). Attack vectors cannot be eliminated completely but certain mitigation measures (e.g., access control mechanisms, anomaly detection) are effective in removing attack vectors across multiple layers.

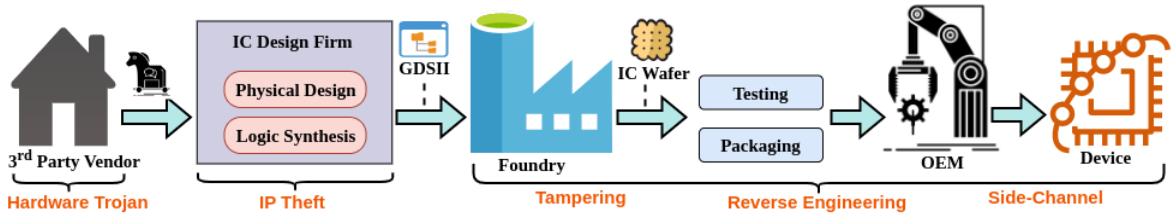


Fig. 7. The semiconductor supply chain and associated security threats.

security threat vectors such as hardware Trojans, tampering attacks, side channel attacks, and fault injection attacks. This is an active area of research and some of the more prominent state-of-the-art solutions involve inserting diverse design-for-security (DFS) constructs into the electronic hardware to deter/detect such attacks.

Most modern power grid systems routinely employ smart meters, sensors, data communication infrastructures, distributed computation units, and management modules to increase the overall efficiency of the system. All these electronic and computation modules typically use diverse integrated circuits (ICs), system-on-chip (SoC), artificial intelligence (AI) hardware, and printed circuit boards (PCB) towards managing and optimizing the grid performance or realizing the desired functionalities. However, the increasing reliance on complex hardware components in modern grids also introduces new security risks [193]. The production model for digital system has changed over the past two decades as a result of the rising cost of semiconductor fabrication and the increasing complexity of contemporary ICs [194]. Many important steps of the digital system manufacturing process (including fabrication, testing, assembly) are outsourced rather than being completely executed internally to save cost and decrease time-to-market. However, such a horizontal and distributed semiconductor manufacturing model introduces diverse vulnerabilities arising from the involvement of malicious entities and rogue employees. Fig. 7 depicts the horizontal semiconductor supply chain and prominent threats arising from all the entities involved. These threats include malicious design modifications (hardware Trojan), intellectual property (IP) theft, reverse engineering to uncover design intent, and tampering to disable security measures which can compromise grid reliability and safety easily. The fabricated digital component is also vulnerable to diverse threats, even

after being deployed (in-the-field), such as side-channel attacks and tampering where attackers glean sensitive information by analyzing physical emissions or power consumption patterns and exploit vulnerabilities in firmware update processes to install malicious firmware respectively. The fabricated digital component is also vulnerable to diverse threats, even after being deployed (in-the-field), such as side-channel attacks and tampering. A compromised hardware can in-turn compromise any system it is part of (including modern grid systems). Compromised hardware making its way into smart grid cloud facilitates can also hamper the decision making capabilities necessary to ensure the safety of the entire system. It is also important to note that many prominent hardware vulnerabilities can also be exploited remotely without requiring physical access to the system, making attacks easier to execute [195]. According to the "Big Hack" article published on 2018 [196], [197], almost 30 U.S. companies such as Amazon and Apple were compromised by maliciously tampered server motherboards supplied by Supermicro. Allegedly, these motherboards had a small (size of sharpened pencil tip) microchip attached to them that can leak sensitive information to adversaries. This is an example of a PCB-level hardware Trojan. Below we discuss, in greater detail, several hardware security threats that pose significant challenges towards securing smart grid electronics.

A. Reverse Engineering

Reverse engineering (RE) involves identifying the design details of an electronic hardware (integrated chip (IC), system on chip (SoC), PCB) by a techniques such as imaging, structural analysis, and functional profiling. By utilizing the reverse engineering knowledge, one can perform a variety of secondary attacks such as: (1) intellectual property (IP) theft, that is, stealing/replicating the design without going through the expensive research & development process [201], [202], [207], [206], [198] and (2) tampering the design easily leading to a hardware Trojan attack [208], [209]. To mitigate this vulnerability, the research community is currently investigating different techniques (e.g. ALMOST, SFLL, LeGO) that can encrypt the digital design through inserting a set of logic gates connected to certain key inputs (logic locking and obfuscation) [210], [200], [211], [212]. These additional insertions: (1) corrupt the output of the digital designs unless the right secret key is provided making it hard to extract the functionality by observing the outputs and (2) bring about structural changes in the design making it difficult for an attacker to guess the design intent through structural analysis. To bypass logic locking and obfuscation, several attacks have been proposed as illustrated in Table VIII. Functional attacks analyze the digital design purely based on its input-output behavior without knowledge of its internal structure. The attacker treats the circuit as a 'black box', supplying inputs and observing outputs to infer the correct key or to deduce a functional equivalent of the circuit [198], [199], [200]. Structural attacks involve analyzing the internal gate-level or transistor-level structure of the circuit. The attacker can inspect its components and connections to extract the key or bypass the obfuscation mechanisms [201], [202], [203], [204], [205]. A joint structural functional attack was also proposed (SURF) that can leverage the advantages of both worlds [206]. These attacks either attempt to retrieve the logic locking key (e.g. SAT) or expose the design for a subsequent structural RE (e.g. SAIL). Many of the older attacks (e.g. SAT) relies on having access to an "Unlocked" design for unlocking a locked design. However, these attacks can also be used as metrics to develop more robust logic locking techniques as demonstrated in LeGO [211]. Explainable Artificial Intelligence (XAI) can also play a crucial role in securing microelectronics for DERMS. Recent works such as X-DFS have used XAI techniques to create human-understandable rules that can mitigate reverse engineering vulnerabilities in electronic hardware [213].

B. Hardware Trojan

Hardware Trojans are malicious modifications inserted into the digital design, by a malicious actor, at any stage of the hardware designing/manufacturing process [208], [209]. Hardware Trojans can be subtle and difficult to detect, making them a significant threat to hardware security. Such modifications typically lead to denial-of-service attacks, create hidden backdoors, allowing unauthorized access to a system and information leakage. In modern power grid system, hardware Trojans can disrupt equipment operation or induce failures, leading to blackouts and destabilization of the grid. It can send the operational parameters and network configurations to unauthorized users.

A hardware Trojan is made up of two components: (1) A trigger circuit that starts the malicious act; (2) A payload circuit that carries our a malicious act. The trigger logic can be based on a digital counter, a set of sequential transitions, a set of combinational logic values, or an external signal. For example, a hardware Trojan may trigger when a specific address appears on the address bus or when a specific input is provided by the user/network [222]. The Trojans are designed in a way to prevent triggering during normal functional testing of an electronic system making them hard to detect during the normal manufacturing process.

A hardware Trojan differs from a software Trojan in that it is installed within the device or, in most cases, directly at the hardware, and it is not affected by any software layers that are operating on the specific hardware [222].

Synchronized hardware Trojans (a special variant) are distributed across multiple devices and get triggered at the same time based on a predetermined timeline or based on some external communication. These, Synchronized hardware Trojans, have been shown to be particularly problematic for modern grids as they can cause large scale power outage [223].

Hardware Trojans are inserted judiciously to avoid detection via normal design testing, making it hard to deal with this threat. The sophisticated concealment techniques used in hardware Trojans necessitate the development of advanced detection mechanisms. However, several techniques are being explored to potentially mitigate this issue, prominent among those are machine learning based techniques [224], [214], [221], [220], self-referencing methods [219], and a newly

TABLE VIII
KEY EXTRACTION ATTACKS FROM HARDWARE OBFUSCATED DESIGNS.

Attacks/Metrics	Type	Focus	Oracle
SAT [198]	Functional	Retrieve Exact Keys	Needed
AppSat [199]	Functional	Retrieve Approx. Keys	Needed
KSA [200]	Functional	Iteratively Retrieve Keys	Needed
SAIL [201], [202]	Structural	Retrieve Original Design	Not Needed
OMLA [203]	Structural	Retrieve Approx. Keys	Not Needed
GNNUnlock [204]	Structural	Extract Protection Logic	Not Needed
SnapShot [205]	Structural	Retrieve Approx. Keys	Not Needed
SIVA [202]	Structural	Quantify Structural Security	Not Needed
SURF [206]	Func.+Struct.	Retrieve Approx. Keys	Needed

TABLE IX
FRAMEWORKS FOR AI–BASED HARDWARE TROJAN DETECTION.

Framework	Benchmarks	Methods	Efficiency/Usability
VIPR [214]	Pre-Fabrication (Gate Level)	SVM, RF, AdaBoost	High
TrojanSAINT [215]	Pre-Fabrication (Gate Level)	Graph Convolution NN	High
NHTD-GL [216]	Pre-Fabrication (Gate Level)	Graph Attention NN	High
GNN4TJ [217]	Pre-Fabrication (RTL)	Graph Convolution NN	Medium
FAST-GO [218]	Pre-Fabrication (Gate Level)	Graph Convolution NN	High
Yang et. al. 2022 [219]	Post Fabrication	Self Referencing	Medium
Yang et. al. 2021 ISQED[220]	Post Fabrication	Unsupervised Learning	High
Yang et. al. 2021 ITC India[221]	Post Fabrication	SVM, NB, DT, KNN	Medium

developed software-variant approach [225]. Graph neural networks (GNNs) have also shown exceptional performance in identifying hardware Trojans because a digital design can be organically represented as a hypergraph [215], [216], [217]. The DFS strategy can be effectively employed in this context because it has been generalized to provide defense mechanisms against such threats [213]. Implementing the DFS strategy in this context provides a generalized defense mechanism against such threats. It is practical for power grids because it can automatically learn from the specific/previous threats targeting the grid's digital infrastructure and offer solutions that are easily understandable by human operators.

Table IX presents prominent frameworks for detecting hardware Trojans at both the pre-fabrication and the post-fabrication stages. The efficiency/usability is estimated based on hardware Trojan detection accuracy, speed of detection, and the practicality of the approach. Several machine learning techniques such as support vector machine (SVM), Random Forest (RF), AdaBoost, Neural Networks (NN), Naive Bayes (NB), Decision Tree (DT), and K-nearest Neighbour (KNN) have been widely used for this purpose.

C. Side Channel Analysis

Side channel attacks on smart grids involve the exploitation of information leaked from the physical characteristics or behaviors of smart grid devices, such as smart meters, sensors, or other critical infrastructure [234]. Side channel information can be used to extract cryptography keys, determine values of secret assets, and predict system behavior among other concerns which can lead to serious problems like load imbalances, equipment damage, or widespread blackouts. Notable related works on side-channel attacks in hardware security are presented in Table X categorized by the type of attack. There are three main sources of side channel leakage and they are discussed below.

- Power Leakage: Power analysis attacks exploit the power consumption patterns of a device to infer sensitive information [235]. Power side-channel attacks are passive and do not leave obvious traces, making them difficult to detect with standard security monitoring tools. Cryptography algorithms have shown to exhibit specific power consumption behaviour dependent on the encryption key values and the input message. By using analysis techniques such as DPA (Differential Power Analysis) and CPA (Correlational Power Analysis), an attacker might be able to extract the encryption keys making data communication over insecure channels highly vulnerable [236], [235], [237]. Test Vector Leakage Assessment (TVLA) [227] is a widely recognized method for power side-channel analysis based on Welch's t-test. Power side channel can also leak the functioning of AI models, which are being widely used in smart grid systems [238], [239]. Defenses involve providing a moving target [240], detecting leaky nets [241], replacing leaky nets [242] (using trichina [243], DOM [244]), and camouflaging [245].
- Electromagnetic (EM) Emissions: EM signals that are generated by electronic circuits (due to switching activities) can also be used to infer sensitive information [246], [247], [248]. EM side channel can also be combined with radio carrier to create what is called a 'Screaming Channel' which is much easier to detect [249]. Defenses such as camouflaging and shielding have been proposed to defend against EM side channel attacks [250], [251].
- Timing Profile: Timing side channel attacks relies on

TABLE X
SIDE-CHANNEL ATTACKS IN HARDWARE SECURITY.

Research Work	Mode of Attack	Description
Kocher et al. [226]	Power Side Channel	Introduced DPA, a form of side-channel attack that uses power consumption measurements
Goodwill et al. [227]	Power Side Channel	Demonstrates power side channel analysis based on Welch's t-test.
Mangard et al. [228]	Power/EM Side Channel	Discusses improvements in power and electromagnetic side-channel attacks.
Chari et al. [229]	Power/EM Side Channel	Introduces template attacks, which use detailed profiling of a device's side-channel leakage.
Quisquater et al. [230]	EM Side Channel	Focuses on using electromagnetic emissions to perform side-channel attacks.
Kocher [231]	Timing Side Channel	Describes timing attacks and how they can compromise cryptographic implementations
Bonneau et al. [232]	Timing Side Channel	Demonstrates timing attacks based on cache-collision information leaks in AES implementations.
Chakraborty et al. [233]	Timing Side Channel	Demonstrates hardware-aware timing side channel analysis

measuring the execution time of a given process to infer sensitive information. In modern power grids, which heavily rely on digital components and cryptographic protocols for secure communication and control, attackers can measure the time it takes for certain processes to execute and use this data to infer the secret system states. This can lead to the compromise of authentication mechanisms and allowing adversaries to manipulate the control signals [252]. Timing side channel techniques been extremely successful towards breaking quantum-key distributions [253], undermining kernel space Address Space Layout Randomization (ASLR) [254], and leaking neural network information through GPU timing [255] among other things. Chakraborty et al. [256] mentions traditional mitigation methods, focused solely on software-level-analysis may be inadequate due to the tight coupling of hardware and software in IoT systems and also compares different types of timing side analysis channel frameworks. Several techniques have been proposed to defend against timing side channel attacks including live detection techniques [257], intelligent scheduling techniques [258], and constant time coding [259]. Timing side channel signatures heavily rely on both the software and the underlying hardware on which the execution takes place [233]. Hence, a joint hardware-software security approach is essential towards mitigating this concern.

VI. POTENTIAL TECHNOLOGIES FOR DERMS SECURITY

This section will highlight four technologies - IT models, machine learning (i.e., supervised, federated, and physics-informed), blockchain, and quantum computing - that we anticipate to play a key role in facilitating automation, peer-to-peer transactions among DER entities, and DER security. Particularly, we lend support to the fact that IT models, machine learning, and quantum computing technologies are relevant to IDUs. We will discuss practical methods to integrate containerization, smart grid services, and DERMS in Section VII.

A. IT Models

Infrastructure as code (IaC) - Typical IT infrastructure requires manual installation and setup of servers, networks, and host machines. Leveraging infrastructure as code enables virtualization of such infrastructure resources in addition to providing a documented and automated methodology to enable fast setups and repeatable executions. Examples of popular IaC tools are Chef, Puppet, Terraform, and Ansible. Brief descriptions for Ansible and Terraform are given below.

- Ansible is a collection of open-source infrastructure as code tools initially developed by Red Hat and used by IT experts to automate various operations such as deployment of code and configuration management [260]. Ansible works in what is known as a push configuration where software is deployed to connected machines (also called nodes or virtual machines such as web or database servers) through an Ansible Engine (control machine) without the need for clients or daemons to be installed on those devices [261]. Communications between an Ansible Engine and its nodes are done through secure shell (SSH). Instructions to execute on these nodes are written in a "playbook" in YAML Aint Markup Language (YAML). Since Ansible is largely community-driven (not to be mistaken for open-source), there is a repository of playbooks in Ansible Galaxy that developers can leverage to easily deploy Ansible.
- Terraform is declarative IT provisioning tool that provides a framework for automation, compliance, and management of infrastructure. Declarative programming is a paradigm that allows users to specify (on a high-level) what should be achieved. Terraform requires configuration files (written in HashiCorp Configuration Language (HCL)) to be provided so execution files can be generated. Execution files are used to reach a target state (or end goal). Terraform can manage higher level IT resources such as servers and also low-level components such as storage [262].

The most efficient methods for researching actual issues that will aid in understanding complex interactions in CPS are simulations and modeling. The most widely

used technique for modeling is agent-based modeling (ABM) which involves simulating the actions of several micro-level agents to understand how they perform and affect the macro-level. Cloud computing offers a broader range of solutions by distributing the computational loads and decreasing the execution time [263][264]. There is support in academic literature that cloud computing [265][266][267] and containzerization [268] can be integrated with the power grid to render services such as data processing (e.g., data anonymization to protect privacy), data storage, machine learning applications (e.g., household occupancy/usage patterns, control strategies to mitigate current/voltage overloading), and forecasting [269] based device-level data (e.g., smart meter data). Though not directly related to DERMS, containerization can be used as conduits for DER/DERMS security due to inherent security features such as mandatory/role-based access control policies and sandboxing for service isolation [270].

B. Machine Learning

Machine learning is a class of mathematical algorithms that analyze a set of data to identify useful patterns. These could be known patterns, where a supervised training approach is used to tell the "model" (the mathematical parameters used by the algorithm) what the pattern looks like, could be unknown patterns where the algorithm attempts to group similar points together or determine boundaries between classes of data, or could be based on continual feedback where reinforcement from an objective function is used to continually modify a algorithmic policy to improve its responses.

Machine learning models for power systems can be classified based on tree-based, neural-network based, hybrid ML models, statistical-based, and fuzzy-logic models [271]. Typical applications for ML models in power systems and DERMS are [272]:

- Optimization and prediction of RE resources (e.g., wind, solar).
- Prediction of levelized cost of electricity (LCOE).
- Forecasting for wind and solar generative units.
- Estimation of power consumption for each individual appliance in a large distribution system
- Short-term and long-term load forecasting (e.g., day-ahead, month-ahead)

Supervised learning approaches can be used for load forecasting, detection of previously seen or common cyber threat activity, or early warning of potential grid failures. Unsupervised approaches are useful for detecting anomalous cyber or grid readings that might indicate something unusual is happening. Supervised learning augmented with physics-informed approaches has been used to solve security problems such as anomaly detection (e.g., bad data detection, faults) and localization [273]. Physics-informed approaches use knowledge about the system and its physical constraints (e.g., network topology, states) to model the system through partial different equations and mixed integer linear programming problems. Physics-informed models offer benefits to ML such as accurate decision-making and modeling, faster computation times to estimate system inputs (e.g., frequency, angle) [274], and meaningful solutions that system operators can implement due to rigorous theoretical foundations, assuming a-priori knowledge is available [275].

Federated learning (FL) is a concept introduced by Google Inc. where ML training is deployed to collections of edge devices or nodes which train a local machine learning model to improve its inference, and then share the learned model parameters with a centralized or hierarchical superior that combines many subordinate models together to redistribute the new "global" model. The core idea is to take the training algorithm to the data, and not bring data to a centralized location for training.

A lesser discussed but prevalent problem in FL is the problem of **fairness** (i.e., bias towards predicting an outcome based on a correlative rather than causative feature) which can be tackled by an FL approach that is based for target distributions that are not biased towards any single or group of client distributions (i.e., client-agnostic) [276]. FL models must also be resilient to poisoning or manipulation by a malicious client, which can be achieved in part by differential privacy methods but additionally by clipping gradients in model updates received from clients to limit the influence of any particular node. FL recently gained interest in the smart grid community for overcoming data-centralization challenges and has been applied to several smart grid problems that tie in with DER integration/DERMS. Some areas include solar irradiation forecasting [277], DER management [278], and synthetic feeder generation [279]. FML can be applied to the smart grid field with various applications such as learning appliance-level usage patterns (e.g., for findings tradeoffs between resource consumption and usage) and forecasting. Smart grid applications are being increasingly IoT-driven and the data transmitted by endpoints to third parties (e.g., utilities) can be secured using FL and to combat cyber attacks at the edge-level [280]. These cyber attacks are well known and include anomaly detection [281], FDI detection [282] (i.e., creating device-level local clients that model FDI attacks based on measurement data and updating the weights of the global detector until there is convergence), and multiple cyber attack models (e.g., stealthy, electricity theft) [283].

General AI approaches to intrusion detection and mitigation in grid infrastructures may also be useful. Blakely et al. [284] incorporated simple distribution grid model into a cybersecurity exercise for the North Atlantic Treaty Organization (NATO) where operators had to maintain both IT and OT networks, while also trying to disrupt the networks of other teams. While the agent built for this did not explicitly incorporate readings from or responses to the simulated grid, the general approach used – transforming all environmental observations into a "world model" knowledge graph – could easily be extended to do so. In the paradigm, graph neural networks can be used to classify hosts on the network as malicious or benign, or network communications can be determined to be anomalous or ordinary, based on graph embeddings of the knowledge graph. A similar approach can be taken using cognitive/symbolic-based AI models such as Soar and ACT-R [285][286]. These models make the reasoning

and learning steps implicit but require instruction from an expert to give them initial objectives and procedures to follow. Argonne National Laboratory is investigating both approaches for use in grid and other cybersecurity contexts.

C. Blockchain

Blockchain is a promising solution to secure interactions and transactions between energy assets. It is highly secure and can be an excellent solution for not only the cybersecurity issue in the energy sector, but also for other critical infrastructure sectors (e.g., water, manufacturing). Blockchain leverages cryptography, public key infrastructure (PKI), consensus algorithms, and access control mechanisms to maintain a distributed ledger [287]. The distributed ledger is scalable and contains a growing list of data records that should be protected against tampering and revision. Smart contracts are used with blockchain technology for DER and smart grid applications. These applications include access control [288], securing supply chain [289], detecting MITM attacks [290], updating DER firmware [291], energy trading [292][293], and controlling inverters [294]. To standardize blockchain use, the IEEE Blockchain Technical Committee has laid out a fundamental framework and principles of IEEE Blockchain-enabled Transactive Energy (BCTE) to deploy BCs in power and energy domains [295]. Authors in [296] developed a reliable decentralized management system for DERs using blockchain technology and smart contracts in order to integrate them to aggregators. In [297], the author proposed an integrated energy management and aggregation platform based on blockchain and smart contracts that optimizes energy flows (i.e., OPF) in a microgrid with different DERs while implementing a bilateral trading mechanism. In [298], author introduces a potential vulnerability of a single point of failure of the centralized DERMS by cyber attacks and proposes a BC-integrated resilient DERMS framework. A multi-channel BC governance system is designed to build a cooperative security ecosystem in a multiple stakeholder involved DER system where DER devices are blockchain client nodes and participating multi-party are blockchain clients. Overall, blockchain has the potential to revolutionize the way that energy is produced, traded, and consumed in DERMS, by providing a secure and transparent platform for energy transactions and enabling greater decentralization of the energy grid.

D. Quantum Information Systems

Quantum information systems (QIS) are technologies that make use of quantum mechanics to communicate, sense, or perform complex calculations quadratically faster than "classical" (non-quantum) computing processors [299]. Processing devices made specifically to perform such computations are known as quantum computers. These have the potential to drastically impact the types of problems that can be solved computationally, but also create security risks. For example, the 2048-bit variant of RSA key was factored in 8 hours using noisy qubits[300]. Quantum communications leverage the ability to entangle pairs of photons to exchange information in a provably secure manner. Quantum sensors are devices with the ability to perform measurements at much higher resolutions and sensitivities than classical measurement devices.

1) Role of QIS in DERs

Quantum computers with their ability to perform multiple calculations simultaneously, can speed up the optimization process for power systems. In addition, quantum computers can potentially be used to simulate power systems behaviors under different conditions (e.g., different load patterns or the integration of RE sources), allowing for more accurate forecasting and planning. However, deployment of quantum computers outside of centralized, highly-controlled environments is a very distant reality, and even today quantum computers outside of laboratory environments are rare and limited in their computational capabilities by challenges ensuring coherence and preventing interference during computations.

2) Quantum computing for DER Power Optimization

Quantum computers have the potential to be used in the optimization of power systems, as they can potentially solve certain types of optimization problems much faster than classical computers. Optimization problems in power systems often involve finding the best configuration of a system, such as the optimal placement and sizing of generators, transmission lines, and other components, to meet certain performance criteria, such as minimizing costs or maximizing reliability [301]. These problems can be extraordinarily complex, as they may involve thousands of variables and constraints, and finding the optimal solution can take a significant amount of time using classical computers.

3) Quantum–secured DERs Communications

While quantum computing provides the space to solve optimization problems, it also poses potential threats to the security of the communications that happen between DERMS elements as secure communication algorithms such as RSA and Diffie-Hellman key exchange rely on heavy computational complexity, which can be cracked by quantum computing within hours using several qubits. The solution to this problem is quantum communication [302]. Quantum computing has the potential to secure communications happening between DERs. These protocols can ensure the confidentiality and integrity of the information transmitted between DERs and the electric grid, protecting against attacks from malicious actors. Advancements in cryptanalytically relevant quantum computers will make it capable of breaking public key cryptographic techniques [303] that are widely used around in various operating units, including DERs.

To enhance secure communications, quantum key distribution (QKD) [304] can be used. In QKD, a quantum communication channel (e.g., fiber optic cable, free space laser) is used for Alice and Bob to exchange their secret keys via photons and based on the quantum state of each photon. Due to the nature of quantum entanglement, if anyone eavesdrops and observes these photons in transit, their quantum state will collapse, and an error will occur when the intended recipient attempts to observe them. Alice and Bob simply build a key out of a sequence of photons

that did not result in an error. This key can then be used for classical encryption ciphers such as the Advanced Encryption Standard (AES). While the threat of prime factorization still exists, Alice and Bob can exchange keys as often as they like to minimize the window for such an attack. However, this requires Alice and Bob to have a quantum channel, which currently means they must be in close physical proximity (e.g., 100km for fiber optics due to signal attenuation) or have line of sight for a free space transmission. This limitation might not be an issue for distribution grids that only span a local region, or even transmission grids where secure and trusted facilities can be conveniently located. However, the equipment to send and receive photons to enable QKD is currently not readibly adaptable to consumer or low-powered edge devices.

VII. Futuristic Intrusion Detection Units for DERMS

Monitoring the traffic moving on the network, searching for suspicious activity and known threats across the network to report them to the concerned security team for thorough inspection, and removal of threats using either hardware or software appliance is called intrusion detection system (IDS). The IDS often resides between an organization network and the internet or between segments of an internal network to continuously monitor and report any found threats to the administrator and forensic analysis team for deep analysis. IDSs include network IDS (NIDS) and host-based IDS (HIDS). NIDS monitors the traffic on individual networks or subnets and comparing it with known attack patterns. On the other hand, HIDS works on individual systems where the network connection, process activity, and/or filesystem activity are continuously monitored. System files are regularly audited, and the administrator will be alerted when discrepancies are found [305]. Blakely [306] considers how different types of information may be useful for IDS purposes as an analogy of biological senses and studies Netflow as an exemplar case study. Valenzuela and colleagues in [307] develop an algorithm using principal component analysis (PCA) to perform intrusion detection on the power flow variability by analyzing the information in the subspace to determine whether an intruder has compromised the power system data. In [308], the authors presented a test bed for developing an intrusion detection system for power systems modeled on a real-time digital simulator. The proposed testbed provides Hardware-in-loop (HIL) simulation, power system attacks, and helps generate data for security researchers. Yang et al. [309] proposed a multilayer security framework based on IDS specific for SCADA and a security testbed to investigate the simulated attacks. The IDS proposed is used to monitor the SCADA systems to protect them from cyber attacks inside or outside the SCADA systems. It uses allow-listing and a behavior-based approach to detect intrusions in DER systems. As SCADA is an integrated level within the DERMS hierarchy, deploying multiple intrusion detection pods at the different hierarchical levels of the DERMS from the DER level to the DERMS operator level ensures intrusion detection at all levels of the DERMS.

With the increasing rates of cyber attacks [310], there is a need for new security concepts and futuristic frameworks that can increase the security of the DERMS. Threats to the OT infrastructure can have a much more significant adverse effect on a business, potentially disrupting operations, demanding ransom payments, and even shutting down the entire industry for brief periods. Hence, there is a need for a lightweight layered framework that combines container-based virtualization technologies and microservice architectures to maximize efficiency and scalability along with real-time monitoring for OT and IT systems - this is what we call the Integrated AI-ready DERMS Edge Testbed at the University of North Dakota (UND). UND has a DoE award from the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) with partners such as ANL and Iowa State University to establish an edge environment for DERs. As part of this grant, UND has established an AI-ready ML library for DERMS. Currently, the solution is to stream solar inverter data streams to NVIDIA's Nano and AGX devices in a federated learning environment. The testbed is scalable and hosts several IDU algorithms and zero trust solutions that could be useful to model threats at multiple levels of the hierarchy presented in Fig. 2. In OT cybersecurity, asset visibility is crucial. Strong asset visibility makes finding vulnerabilities and unsafe configurations on OT networks easier. Hence, DER device and network data should be collected and monitored in near-real time. Open-source software like Apache Kafka and Spark can be used to build data streaming. Because DER data schemas are polymorphic, these near-real-time streaming data can be kept in persistent storage (e.g., MongoDB). Containerization of applications provides broader benefits such as fine-grained resilience, eliminating single points of failure, scalability and infrastructure optimization, quicker rolling upgrades and rollbacks, logging, monitoring, and security. Due to the need for a scalable environment, Kubernetes and Docker containers are used to run some software-in-loop ancillary services, including intrusion diagnostics and quantum-based applications that use cutting-edge machine learning technology to identify attacks on the OT system quickly. The futuristic IDS framework for increasing the security and optimization of DERMS can be conceptualized by adding container-based services like Kubernetes, which has tremendous applications, to host and scale the IDS pods across network infrastructure as needed. Fig. 8 shows a conceptual framework using Kubernetes where multiple IDU members are deployed through container-based services to monitor for intrusions in the network. This scalability through container-based services gives the advantage of monitoring and detecting intrusions like trojan, malware, and anomaly signatures in real-time data at multiple endpoints of the DERMS network. With multi-cloud platforms gaining attention with reliable use cases and the vision to develop and host functional algorithms and services in container pods like Kubernetes for better consumer scalability for maintaining normal operating conditions, academic and industrial researchers should investigate the benefits leveraging the DER usage optimization and security of DERMS through new futuristic frameworks. These architectures are also intended for delivering reliable products

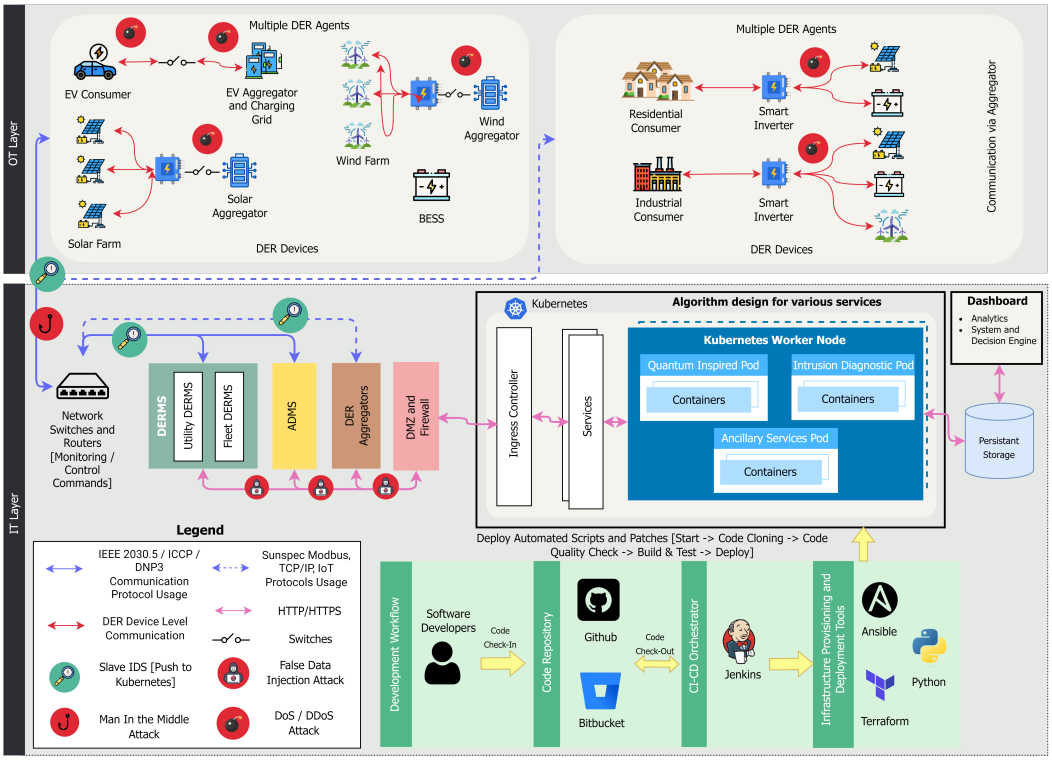


Fig. 8. **Integrated AI-ready DERMS Edge Testbed at the University of North Dakota.** Interactions between the IT and OT layers warrants a flexible and scalable framework that can support large deployments across any region (i.e., through Kubernetes), cater to lightweight edge computing hardware, and anticipate common cyber threats (e.g., DoS, MiTM) at each layer.

quickly while streamlining the workflows for development and deployment. This workflow will aid in increasing agility and reveal software flaws early in the development cycle. To incorporate code changes as frequently as possible, a continuous integration workflow uses build automation; as a result, using a distributed version control system can speed up project tracking and development. One of the well-known open-source automation servers, Jenkins helps automate continuous integration and continuous delivery processes. Each updated piece of software is automatically built into a Jenkins image (package) and spun up as a container. A continuous delivery workflow is started after the code has been integrated and packaged to release updated code into the environment using automated tests securely. The tests verify the build's code quality by advancing through various build stages. After being correctly tested, these packages should be delivered across different environments; as a result, Ansible can deploy the code without requiring the installation of any software on the client machine. Terraform improves management and orchestration for large-scale, multi-cloud infrastructures by making it easier to manage and scale the entire Kubernetes cluster.

In addition to our proposed framework in Fig. 8, we introduce a DER trustworthy engine within the entire framework (see Fig. 9) where the trustworthiness of the DER client is determined. The concept of IDS incorporates FL for deploying machine learning applications to preserve the data privacy aspect at the local DER level. This method improves the overall security, privacy, and localization of the DER data. The trustworthy engine is fed with real-time DER data from the whole DERMS network to check the presence of malware, anomaly signatures, and trojans to determine the overall trustworthiness status of the connected DER in the DERMS network. When a DER in the DERMS network is determined as compromised, fail-safe methods should be triggered to safeguard the other DERs and the DERMS network, leading to the quarantine of the compromised DER. This process of determining the trustworthiness of the DER regularly through the IDS helps in knowing whether the DER is compromised or still trustworthy, easing the operator's ability to switch between the trusted DERs. Research studies should be conducted with the vision of creating combinational IDU designs for any third-party DER aggregators which can lead to numerous innovations and applications, including classification between trusted DERs and the compromised DERs for hardening the security of DERMS. The frameworks and recommendations presented in Figs. 8 and 9 are collectively called the Intrusion Detection Federated Framework (IDFF) for DER security.

VIII. Zero Trust Principles for DERMS

While the proposed IDFF framework in Section VII addresses scalability, privacy, and integrates FL to improve the overall security posture of DERs and DER-dependent entities (e.g., DERMS), additional security considerations should consider the dynamic, diverse, and dispersed nature of the power grid. For example: (1) security policies should be configured to enable power and network flows only among regularly audited and approved systems, regardless

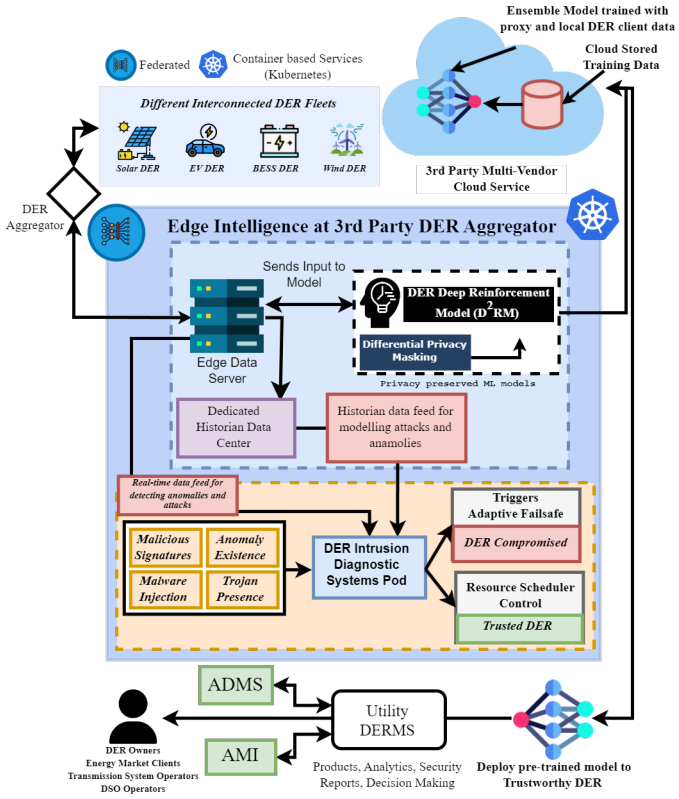


Fig. 9. **Edge intelligence within Integrated AI–ready DERMS Edge Testbed at the University of North Dakota.** Input data from DER edge devices are ingested by a trustworthy engine that is built using Kubernetes (i.e., as a worker node) and the centrally federated architecture type to validate DER trustworthiness at the aggregator level.

of stakeholder type (e.g., utilities, virtual power plants); (2) implement strict access control mechanisms to verify every asset (i.e., newly-joined endpoints, stakeholders) before granting access. These principles are fundamental to what is known as the zero trust paradigm. Implementing this paradigm at multiple layers of the power grid (e.g., network, device) is recommended to adaptively authenticate, perform threat discovery, and implement emergency response measures [311]. We will now outline zero trust principles and recommendations to implement these principles at different layers i.e., sensing, communication, and control of the grid.

Multiple sub-components such as Customer Information System (CIS), virtual power plants (VPP), building energy management system (BEMS), SCADA, etc. interact with DERMS to handle various functions at the generation, transmission, and distribution layers. All such sub-components are rarely provided by a single vendor; this widens the potential for multiple vendors to contribute subsystems that are capable of handling such functions. As such, threat vectors (e.g., software backdoors) are significantly enhanced due to the system inheriting the susceptibilities and inherent weaknesses of each individual technology [312] to compromise the sensing, communication, and control layers.

Moreover, perimeter-based defenses are no longer sufficient due to the constantly evolving digital ecosystem in power systems (e.g., shift from legacy infrastructure to IoT) and are obsolete at least for the following reasons:

1) Increased data transfer not just through ingress and egress tracepoints (i.e., north-south communications) but also among intra-network components (i.e., east-west communications). This presents the potential for zero-day vulnerabilities that originate internally.
2) A reliance on real-time data from a large volume of geographically dispersed endpoints, particularly considering devices that store and process data locally in addition to communicating with other distributed entities and cloud infrastructure. This implies that there isn't a well-demarcated perimeter of defense.

Therefore, there is a need to shift to a zero trust security paradigm that can dynamically and simultaneously oversee assets, users, and resources. Fig. 10 provides an overview of the proposed zero trust framework for DERMS. Before proceeding, the property of cyber resiliency will be discussed.

Resiliency is prevalent across a multitude of scientific disciplines and though standardized definitions may vary based on domain, we define resiliency as the ability to recover from or adjust easily to adversity or change. With the increase in the digital footprint across sub-entities in a power system (e.g., DERs, DERMS), this definition can be applied to a parallel principle called cyber resiliency. As defined by NIST [313], cyber resiliency is "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources". The fundamental concept of cyber resilience is the acknowledgment that a cyber attack is likely to occur and that the system will be impacted as a result. The emphasis here is on the system's ability to not just resist an attack (i.e., robustness), but to recover and adapt [314]. Cyber resilience for power systems has been associated with other concepts relevant to systems engineering such as robustness, durability, accessibility, stability, and flexibility [315][316]. For the purposes of this study, we will constrain resilience to only consider its relationship with efficiency.

For the purposes of this study, efficiency is defined as the ability to produce desired outcomes with the least amount of investment (e.g., time, effort, capital). Now consider two similar but separate sub-systems within the distribution function (e.g., EMS and ADMS). An outage in either of these sub-systems can cause broader implications to the stability of the power grid. Therefore, a cyber resiliency tactic for these sub-systems should focus on long-term rather than short-term benefits [317] and should achieve the primary objective of proactive investments (e.g., financial, technical) that focus on enhancing cyber resiliency before or during the early stages of operation. Though this objective may reflect a lower short-term efficiency due to the allocation of additional resources (e.g., security audits, backups), these sub-systems will be more resilient to cyber attacks. Therefore, sub-systems will have lower costs per unit time thereby reducing long-term operational and technical resource commitments. This example also implies a positive correlation between long-term efficiency and resiliency: Serdar and Ghamdi [318]

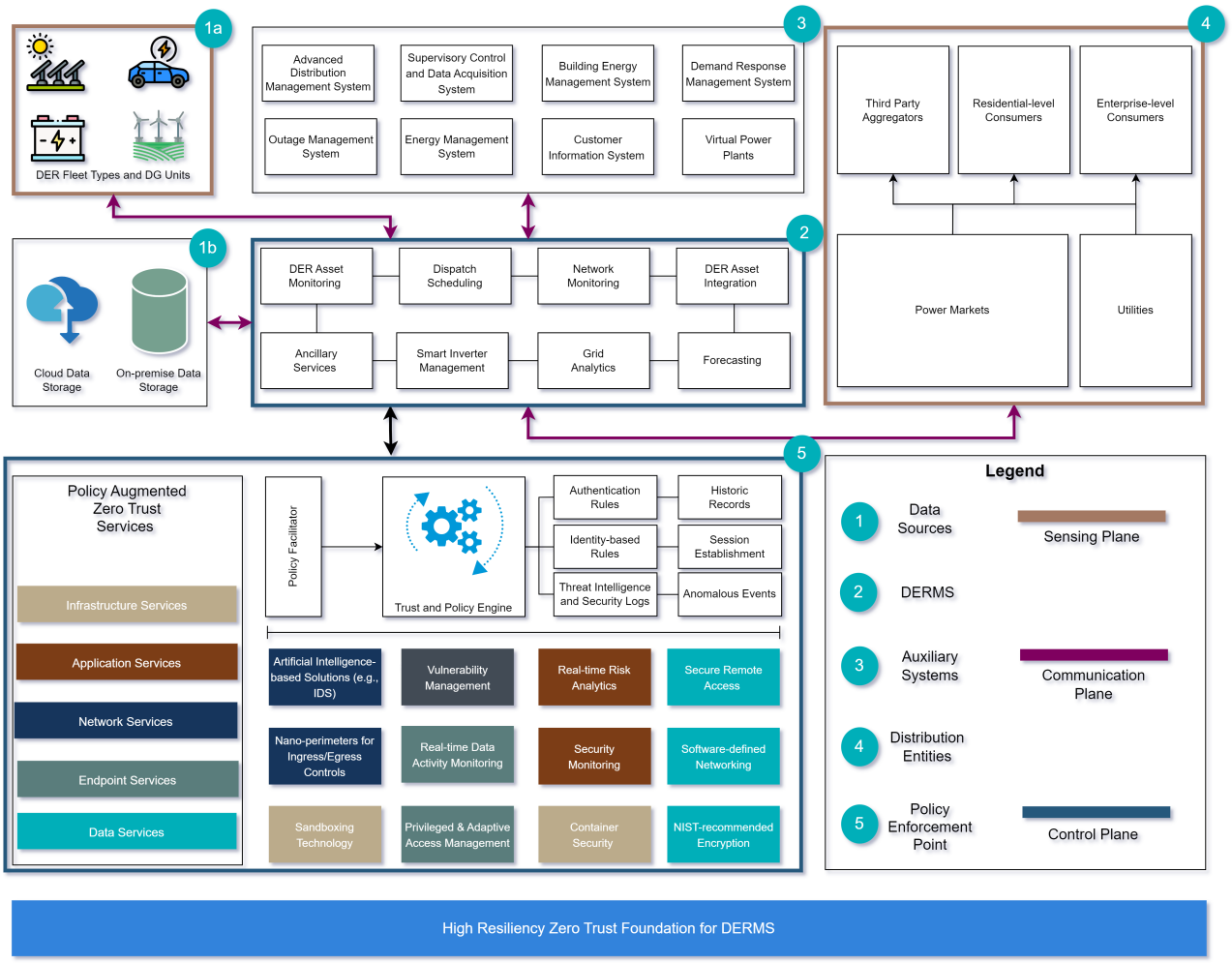


Fig. 10. **Zero trust foundation for DERMS.** We identify multiple data sources (e.g., DER fleets, data–at–rest in cloud), distribution entities (e.g., power markets), and the role of DERMS in managing the communication and control planes. Zero trust entities (e.g., policy engine) are implemented in the back-end and can render different service types (e.g., data, application) based on need.

support this inference by noting that upgrades to legacy infrastructure in power systems are necessary to prevent them from deteriorating (i.e., both physically and cyber-wise), and that the cost of long-term efficiency is far less than the cost of a disaster.

Consider a scenario where a specific device assigned to an aggregator has conflicting roles or attributes in access control. For example, the conflicting attribute is "Control Over Dispatch Instructions." The system operator will be able to provide dispatch instructions to aggregators, directing them on how to operate and control the aggregated DERs. Aggregators are responsible for implementing the dispatch instructions received from the system operator and controlling the operation of individual DERs accordingly. The specific device assigned to an aggregator also has local control capabilities, enabling it to make decisions regarding its operation and dispatch based on local conditions. In this scenario, a conflict arises when the system operator provides dispatch instructions to the aggregator. However, due to its local control capabilities, the device deviates from those instructions and operates differently. This conflicting scenario can lead to inconsistencies and sub-optimal system operations. Zero trust can be made use of to address such conflicts. The conceptualized framework to mitigate these conflicts would be incorporating FL aspects and access control policies into zero trust to deploy a federated zero-trust-based access control structure. This control structure can be made to optimize control decisions and resolve conflicts in access control by leveraging the least privilege principle, Role Based Access Controls (RBAC), Separation of Duties (SoD), and Regular Access Reviews. In such scenarios, a combination of the local and final deep learning-based model can be deployed along with the federated settings to review access policies, preserving the privacy of the DERMS hierarchy for participating third-party DER owners, vendors, or DERMS fleets.

Table XI lists 9 standards from standards bodies such as IEEE, IEC, etc., and DER security recommendations based on the clauses within each standard. We will now look at zero trust recommendations for the three layers introduced in Section IV i.e., sensing, communication, and control.

TABLE XI
STANDARDS FOR DER CYBERSECURITY.

Standard Number	Standard Name	Organization(s)	Recommendations	Ref.
ISO/IEC 27002	Information Security, Cybersecurity, and Privacy Protection	International Organization for Standards (ISO)	Threat Intelligence Capabilities to Mitigate Insider (e.g., Impersonation) and External Attacks (e.g., Phishing). Security Requirements for the Acquisition, Use, Management, and Exit from Cloud Services. Secure Development Life cycle for all Digital Assets (e.g., CI/CD Integration, IAM). Applicable to Communication Layer.	[319]
ISA/IEC 62443	Security of Industrial Automation and Control Systems (IACS)	International Society of Automation	Physical and Digital Assets in Industrial Systems Must Conform to Zones. Each Zone Should Have an Adequate Security Level and Define Logical and Physical Boundaries for all Inter– and Intra–system Communications. Conduits are Security Mediators that Enable Inter-system Communications between Two or More Zones, and Has a Unique Set of Security Requirements. Applicable to Communication and Control Layers.	[320]
NISTIR 7628 (Vols. 1 and 2)	Guidelines for Smart Grid Cybersecurity	National Institute for Standards and Technology (NIST)	Smart Grid Information System Maintenance and Repairs – Digital Sanitization, Backups, Removal of Smart Grid Information System Components. Applicable to Communication Layer.	[321]
C2M2	Cybersecurity Capability Maturity Model	Multiple Private/Public Sector Organizations	Asset and Inventory Management for OT. Deploy Grid– and Plant–level Situational Awareness Measures (e.g., Real–time Data Aggregation and Correlation, Periodic Reviews of Log Trails). Applicable to Communication and Control Layers.	[322]
ISO 22301	Security and Resilience – Business Continuity	International Organization for Standards (ISO)	Deploy Quantitative Measures of Performance (e.g., Maximum Acceptable Outage, Recovery Time Objective, Recovery Point Objective). Applicable to Communication and Control Layers.	
IEEE 1686–2022	Intelligent Electronic Devices Cybersecurity Capabilities	Institute of Electrical and Electronics Engineers (IEEE)	RBACs for IEDs based on IEC 62351–8. Authorizations to record all user actions and accesses. Audit Trails for Cybersecurity Events Accessed on Read–only Basis. Auto-recovery to a Known Secure State After Unexpected Failure. Applicable to Sensing Layer.	[323]
IEEE 1547.3 (Draft 12)	Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems	Institute of Electrical and Electronics Engineers (IEEE)	Adequate Network Segregation Between Internal (e.g., DER controllers, DERMS) and External (e.g., AMI) Network Topologies. Baselines are Established for Network Traffic Based on Source/Destination Addresses, Ports, Protocols, etc. Security for Data-in-transit Through TLS v1.3, Digital Certificates, and Deep Packet Inspection. Applicable to Sensing, Communication, and Control Layers.	[21]

1) Sensing–layer Zero Trust Recommendations

Sensing layer devices contain monitoring units such as IEDs and RE smart inverters to measure faults such as, say, due to overflow currents. Such devices can also be part of wireless sensor networks (WSN) [324] that contain protective devices (e.g., primary or backup relays) that are responsible for comparing the measured power flow variables (e.g., current, voltage) to a threshold that the protective device(s) are given. The protective device can issue responses (e.g., tripping circuit breakers) to protect the network or service from any harms (e.g., power surges). One of the key developments in sensing layer devices is that it allows for remote management of device to issue adaptive protection capabilities [325], although the adaptive parameters should be adjusted routinely by a control center based on a situation's requirements. Utilities can use pseudonyms for end-user smart meters to obscure and protect the identity of their customers. However, de-pseudonymization of these data compromises users' privacy and can reveal sensitive information such as households' usage patterns and appliances being used.

Recommendations to enhance security at this layer is based on Microsoft's Maturity Model [326] and is adapted to OT and IT systems in critical infrastructure. The diversity in endpoint device types expands the threat vector and therefore requires security principles to secure the threat vector to an acceptable level where any compromise or failure does not have large-scale impacts (e.g., outages, financial losses). These security principles can be divided into three broad areas: dynamic endpoint status monitoring, policy-based configuration management, and compliance controls.

Endpoint status monitoring mechanisms must be enforced in real-time to continuously gather and evaluate endpoint device behaviors to identify potential IoCs. Device behaviors and health parameters such as data flow rates, reporting intervals, switch status (if applicable), power parameters, packet losses, and device energy consumption patterns are key parameters that should be monitored to get an accurate reading on device health [324]. Such monitoring mechanisms should also consider the customers' lack of awareness when a smart meter is compromised and is non-functional or doesn't operate properly to produce erroneous readings.

1) Additionally, endpoint detection and response (EDR) capabilities can identify viruses at the kernel-level (software) and micro-processor/micro-controller-level (hardware) to disconnect and quarantine infected devices or segments. There is a steady rise in the research produced in the EDR field [327] specifically exploring the application of ML to EDR. Due to the large number of endpoints, it's necessary to perform EDR at scale (i.e., automation) and limit manual intervention as much as possible. Ensemble models like Random Forest [327] seem to be widely employed for EDR tasks.
2) Security incident and event management (SIEM) functionality offers interactive and user-friendly dashboards to encapsulate the previously mentioned capabilities to enable a convenient, one-stop applications for dynamic monitoring and response. SIEM's notable functions of event logging, report and alert functions, and event correlation can be performed but due to the high penetration of DER endpoints, the number of logs and alerts a SIEM has to process grows exponentially and can benefit from a system that lowers the computational workload by allowing only anomalous alerts/logs to be considered [328]. SIEM solutions such as OpenSearch and Wazuh can accommodate monitoring at scale. For example, OpenSearch's distributed control paradigm across multiple clusters (i.e., nodes and "shards") allows:

(1) simultaneous deployment on multiple control-level nodes (e.g., PDCs, substations) to prevent single-point failures; (2) monitoring of real-time data from shards (i.e., sensing-layer endpoints) for logging, merging, search, and analysis; (3) cross-cluster queries which are applicable for clusters setup by utilities monitoring micro- and nano-grids; (4) secure authentication for customers to access their data (e.g., usage patterns, billing information) through OpenID; (5) ease of access using a REpresentational State Transfer (REST) API regardless of the operating environment (e.g., Linux, Windows).

Policy-based configuration management techniques (e.g., authentication for source nodes, broadcast management) enable administrator-defined capabilities to enforce mechanisms to authenticate and secure participating entities and data (e.g., encryption, key management).

1) Symmetric encryption algorithms (e.g., triple data encryption standard (3DES), AES) enable the encryption of large-scale real-time data and are regarded as computationally efficient relative to asymmetric encryption algorithms.
2) One of the other aspects of policy-based controls is to adequately enforce sufficient trust management using rulebooks to provide least-privilege access to endpoint devices and enforce dynamic trust distribution [329] to such devices based on cyber events, natural disasters, or physical compromises.
3) Data aggregation from deployed endpoints in a DERMS can be considered multi-modal and can provide greater insights into the nature of the system when such data are combined together into a data lake. These insights produce various parameters such as identity, device health status, resource usages, anomalies, etc. and will aid in driving security decisions.

Compliance control mechanisms help in protecting data and improving the security model by adopting industry-specific policies. Compliance is usually done sequentially through risk analysis, developing policies and procedures, implementation, validation, and enforcement [330]. Setting up constraints on what a user can do directly and the programs that they are allowed to execute are defined by access control policies. To set up access control policies, the organization should look into three factors: identification (user base), authentication (user authentication), and authorization (user permissions). Access control policies can be designed in different variations such as discretionary access controls (DAC), RBAC, attribute-based access controls (ABAC), and hybrid access controls. Discretionary access control is the least restrictive model, allowing an individual user control over any assigned objects. ABAC scans the attributes of the requesting user to determine whether they match the existing policies to provide the requested access [331]. In the context of zero trust, these access control policies make sure that all the users are not given access by default, thus creating a trustless environment. This gives access to users only depending on the set of rules that are set up by the organization to secure and restrict access to the organization's data, tools, and devices [332][333]. This ensures that the DERMS operators only with the right level of security clearance can have access to the controls and data. For example, RBAC policies may not permit device-level operators to access higher levels of DERMS which includes energy management services and microgrid controllers as they restrict device-level operators only to the installation and operational maintenance of DER devices.

2) Communication–layer Zero Trust Recommendations

Communications between critical infrastructure assets (e.g., AMI, DERs) are currently shifting from remote and segregated units to systems that are network-capable. Commonly used protocols for industrial control systems (ICS) and SCADA systems used in power infrastructure are SEP and DNP, among others (detailed in Section II). It is important to reiterate that there is an increased attack surface due to the distributed aspect of the modern power grid by what can really be considered data-driven reliance.

Firstly, we recommend performing a gap analysis to enable utilities and other entities involved in the energy lifecycle to identify: (a) physical assets (i.e., control stations, PMUs, RTUs) and other internet-facing sensing and control devices, and (b) digital assets such as licensed or unlicensed software such as ADMS, DERMS, and cloud infrastructure (e.g., Microsoft Azure for log audits and data storage). Having a thorough listing of physical and cyber assets provides the necessary insights to identify tracepoints [334] (i.e., ingress and egress interfaces) and therefore a broader view of the threat landscape. This can then be followed-up by implementing access control, incident response and planning, and configuration management control mechanisms.

Access control policies (e.g., DAC, mandatory access control, RBAC, ABAC, time-based, context-based, and hybrid access control) can also be applied to this layer. From a zero trust standpoint, this can be implemented as a software-defined perimeter (SDP). For example, if we consider a self-sustaining microgrid i.e., all the functions in the energy lifecycle are handled solely by the microgrid, less emphasis can be placed on the location and the function of the networks and more significance can be given to dynamically and logically allocating resources to networks requesting the resources and the nodes within those networks. Additionally, recall that the endpoints in distributed and federated DERMS types (see Fig. 1) exchange data amongst themselves and with a centralized entity to provide real-time insights; this increases the visibility that each endpoint receives because of the broadcasted full-duplex data exchange.

3) Control–layer Zero Trust Recommendations

Control-layer entities such as operator workstations and control centers can be breached to issue unauthorized commands to critical infrastructure. For instance, the Kemuri Water Company hack in 2016 was carried out by hackers who compromised an internet-facing workstation to operate programmable logic controllers (PLCs) that manage water flow rates and water treatment methods. The attack was primarily due to outdated IT and OT infrastructure (i.e., the IBM AS/400 and legacy operating systems) that were compromised due to a vulnerability in the company web server's payment

application [335]. Though not explicitly stated by Kemuri, this is an example of a man-in-the-middle attack where systems were breached (remotely in this case) to manipulate control subsystems.

Control systems should be equipped with digital forensics functions such as process and memory captures to analyze data and processing health of multiple DERs at the system- and device-levels to identify potential IoCs before there are cascading consequences. User and entity behaviour analytics (UEBA) can be performed to further capture device or user behaviors that deviate from established baselines. For example, Yip and colleagues [336] model the electricity consumption of households using a system of linear equations where a coefficient ('a') (called anomaly coefficient) is used to determine whether consumers are under-, over-, or correctly reporting their consumption patterns. Similarly, Fenza et al. [337] use a LSTM and k-means algorithm to capture historical usage patterns by clustering raw data and extracting features such as day/week/month and average consumptions. The real consumption is used as the target label by which the LSTM regression output is evaluated through the root mean squared error (RMSE). Anomalous user behaviour or patterns are not looked at a single event but rather as a trend over a historical period (e.g., past week) and are captured by using the RMSE and checking whether this value is between the range of (-2σ, 2σ) where σ is the standard deviation for the RMSE in the preceding week; if the RMSE is not in this range, the authors consider that as the presence of anomalies. The limitation to such an approach is that it relies on a week's time horizon to make accurate predictions about current usage patterns and therefore any anomalies; if such a model has to adapt to varying consumption patterns and new environments, it needs to be fine-tuned appropriately to handle concepts drifts.

There are other related works that address anomalies from a user behaviour perspective [338][339] that may be of interest to readers. It should be noted that most emerging works with supervised and unsupervised algorithms (e.g., DNNs) solve this problem and this presents a challenge on the quality of data going into these algorithms, specifically from an adversarial standpoint. Understanding adversarial attacks against machine learning models will help in detecting bad data (e.g., poisoned data) but also improve model robustness to adversarial attacks [340].

IX. ML–SPECIFIC SECURITY RISKS IN DERS

Recall that, in Section VI-B, we introduced the many ways in which ML can further enhance the efficiency of DERs. However, it is now acknowledged that ML, despite providing many technological benefits, also presents various security risks [341]. This section extends our previous threat-modeling analysis (in Section IV) so as to explain how deployment of ML in DER should take into account potential adversarial threats. Specifically, we will first summarize the most relevant threats to ML, outline how they can be staged in the DER context, and provide some mitigations drawn from prior work. We will conclude this section with a description of a defense tailored for data-perturbation–based attacks.

A. Evasion Attacks

The simplest form of security threat that can befall a ML model embedded in a DERMS are evasion attacks, i.e., erroneous predictions (e.g., misclassifications) of the ML model due to the so-called "adversarial perturbations" [341]. The fundamental principle of these attacks is to introduce a small manipulation in a given input so that the ML model is induced to produce a wrong output—ideally, one that favors the attacker. The most common case is a malicious event that is misclassified as a benign event, thereby "evading" a detection mechanism and allowing an hypothetical attacker to persist in their malicious actions.[1]

Abundant prior work has showcased that similar evasion attacks can be staged in many settings—including those envisioned in a DERMS. For instance, there is evidence of successful attacks against telecommunication systems [343], network-management systems [344], industrial control systems [345], fault detection systems [346], power allocation systems [347], intrusion detection systems [348], or even systems for solar/wind power forecasting [349], [350].

There are many countermeasures that have been proposed to mitigate these attacks, but many works have shown contrasting results [351] with defenses being invalidated quickly after publication (e.g., the defensive distillation case [352]). The only technique which is known to produce good results is *adversarial training* [353], which relies on training an ML model on those samples that would otherwise evade such a model: in this way, the model will be able to recognize such "adversarial examples" and produce a correct output. The problem, however, is that such a method only works by predicting the attacks beforehand, and ensuring protection against all conceivable evasion attacks is not possible [347]. Moreover, there are concerns about the degradation in terms of baseline performance of the ML model, since the retraining procedure may yield an ML model with an inferior performance—albeit some works have shown how to mitigate such an issue [354].

Nevertheless, we recommend future works considering deployment of ML models in DERMS to scrutinize how an hypothetical attacker can interact with such ML models. Indeed, staging evasion attacks typically requires knowledge of the model or the capability of querying the model and observing its output: if this is not possible, then launching a successful evasion attack is much harder for a real-world attacker [355]. For instance, consider a DERMS using ML for fault detection: to have a "faulty" event be misclassified as "normal", an attacker may attempt an evasion attack; however, doing so in practice is not simple because the attacker would require some form of access to the ML model, which should be accessible only to users with elevated privileges. Hence,

[1]It is important to note that the term "evasion attack" in the ML-security domain has a different connotation with respect to the cyber-security domain [342]. In ML security, an "evasion attack" denotes a misclassification at test time, i.e., after the ML model has been trained and deployed to fulfill any given task. In cyber security, the term "evasion attack" refers to an attempt that bypasses a security system (see also the cyber-kill chain discussed in Section IV-C). In this section (i.e., Section IX) we use the term "evasion attack" as is used in the ML-security domain.

some evasion attacks can be effectively countered by denying access to unauthorized people to the ML model [342].

B. Data Poisoning

While most security threats to ML (including "evasion attacks") occur during the inference phase of the ML model, there is a form of security risks that specifically affect the training phase of the ML model: data poisoning.[2]

The fundamental principle of "data-poisoning" is that a given piece of data, after its acquisition by any given source, is subject to some change. Then, when such a piece of data is used to train (or re-train) any given ML model, such an ML model may be "poisoned" and exhibit an incorrect behavior during its inference (or operational) phase [341]. For instance, such a poisoned datapoint may lead to, e.g., an overall lower performance of the entire system over multiple inputs [357]; or to the creation of a "backdoor" that can be exploited by an attacker by sending specific inputs that, e.g., bypass an ML-based detector [358].

What makes data poisoning subtle, however, is that these effects can also occur due to natural events—e.g., it is entirely possible that some data that is used to train an ML model is corrupted, or faulty, or wrongly labelled: in these cases, the model will be negatively affected during its operational phase [347]. Such an occurrence is not unlikely in the DERMS context, given that the range of application of ML is vast and, in some cases, large amounts of data are collected every day by thousands of sensors. Historically, there have been works covering poisoning in diverse domains that are envisioned in DERMS, such as intrusion detection [359], industrial control systems [360], fault detection [361], or load forecasting [362]. Given the complexity of DERMS, it is expected that one or more ML components may be subject to poisoning—which is something that practitioners in the field are concerned about [363]. Moreover, the issue of data poisoning in DERMS also encompasses all those use cases which leverage federated learning (such as, e.g., power system applications). Recall from Section VI that federated machine learning deploys a global model to edge nodes to locally train models with the objective to improve the global model. Model weights contributed by each of the locally trained models can be maliciously perturbed before they are sent to the global model, thereby leading to "poisoning" the global model. In the context of DERMS and power systems, the IoT paradigm and the volume of data contributed from geographically dispersed sensing devices fits the description for a canonical federated machine learning application [19] (e.g., energy prediction to prevent grid instability and congestion [364]).

Defenses against poisoning are well-studied in the academic sphere [365], [366], [367], [368], [369], [370]. However, the best approach to mitigate the problem of poisoning is to prevent the generation of poisoned data in the first place. For instance, this may entail input verification/sanitization whenever some sensor produces an output [371]; or more accurate labeling duties [372]. Moreover, to protect against poisoning attacks (and not that induced by natural phenomena or negligence), the best way to do so is to prevent unauthorized people from accessing the training datasets of an ML model. However, similar solutions may not be applicable in some contexts: for instance, an attacker can control a sensor in a network, and such a network uses the data produced by the sensors to train some ML model. In these cases, it is possible to apply some of the previously mentioned solutions (e.g., [365], [366], [367], [368], [369], [370]). We also mention the existence of defenses that are specifically tailored for mitigating poisoning attacks in federated learning contexts [373], [374].

[2]In the ML-security domain, a "poisoning attack" is a term used to denote adversarial manipulations of the training data—or that, more broadly, seek to mislead any given ML model by tampering with the training data used to train the ML model. Such a connotation is different from that used in other security domains [356], for which there is no notion of "training" (which is intrinsic of ML). For instance, as we discussed in Section IV-C, ARP poisoning is an attack that has no nothing to do about "manipulating training data".

C. Model Inversion/Stealing

A concern that is becoming increasingly popular among ML developers is the risk of having an ML model to be "stolen" [375], thereby leading a third-party to cheaply obtain a copy of a model that may have taken years to develop. The first "model stealing" attack was carried out by Tramér et al. in 2016 [376]. Since then, a plethora of papers have been focusing on this problem [375].

In the context of DERMS, possibilities of model stealing can arise when taking into account that DERMS are not always managed by a single entity. Potentially, some tasks are outsourced to other companies—and these channels enable one to stealthily obtain information that can be used to "clone" a given ML model, leading to loss of intellectual property from the rightful owners of the model.

Nevertheless, the ways to carry out model stealing attacks are diverse. It is possible to do so via power side channel [377], or by operating at the hardware level [378], or even by querying a model and see its output [379]. Defenses can involve the usage of deception [380] or obfuscation [381], as well as detection of stealing attempts [382]. However, when the attack is carried out at the hardware level or via side channel, developing a "general" defense is a potentially unfeasible goal [375].

An orthogonal line of defense can entail the usage of watermarking: [383]: by embedding a watermark on a model, it is possible to at least "prove" if your model has been stolen by revealing the watermark in the stolen model. However, such a mechanism may not be simple to stage in the DERMS context, since it would require the rightful owners of a model to figure out that their model is being used somewhere else.

D. Membership Inference

The last type of ML-specific security risk is a type of *privacy* attack denoted "membership inference". The idea is to determine if a given piece of data is included in the training set used to develop a given ML model [384]. Such a threat is typically envisioned in healthcare contexts: in principle, it is possible to determine if (the data of) a given patient was used to train a model for, e.g., diagnosing cancer—which is

clearly a privacy violation. As a result, many defenses have been proposed to counter such a threat [385], [386].

Nonetheless, to the best of our knowledge, there are no practical use cases of membership inference attacks in the DERMS context [387]. This is because, even under the assumption that an attacker is able to carry out a membership inference attack, the use cases in which ML can be deployed in DERMS do not enable a straightforward profit for an attacker. Indeed, it is important to stress that a membership inference attack *does not allow one to steal the training dataset*: it merely serves to determine if, given a datapoint, such a datapoint was included in the training dataset of the ML model. Hence, an attacker first needs to obtain a datapoint, and then gain some profit by the attack.

A potential application, however, of a membership attack in a DERMS context may be one considering a *billing* system. For instance, an ML model may be used to automatically determine when is the best moment to send a billing notification to a given client. Therefore, such a training dataset must contain details of the clients of a given company. Via a membership inference attack, an attacker can infer (assuming that the attacker meets the requirements to launch such an attack) if a given entity is a client of the company owning the model.

Hence, we advocate ML engineers and DERMS developers to consider the possibility of membership inference attacks, too, and apply proper countermeasures if deemed necessary.

E. A Potential Defense Against Data Perturbations

In what follows, we now provide a high-level overview of a defensive mechanism against malicious data perturbations that relies on the principle of "quarantining" those inputs that are not properly analysed by an ML model (similarly to, e.g., [388]).

The intuition is that the output of any given ML model should not be trusted a-priori. Rather, it should be scrutinized, and potentially used to identify instances of data-poisoning—either at inference- or at training-stage. Such a goal can be achieved through methods based on uncertainty estimation [389], [390], [391]. For instance, by computing the confidence of the prediction of a given ML model, it is possible to ignore some of its outputs, putting them in a dedicated quarantine that will be further scrutinized (either by experts or by dedicated systems [392]). The decision to "accept" or "reject" a given prediction will depend on a confidence threshold θ: predictions above θ will be used by the DERMS, whereas those below θ will be put in quarantine [393]. The triaging of the events in quarantine will occur depending on various factors such as when there is a substantial number of events generated by the same source; potentially, such triaging may entail the development and application of automated mechanisms (e.g., [394]). The confidence threshold θ should be set so as to balance the tradeoff between usability and security.

The use-case we consider is one where an ML model M analyzes the traffic produced by the DERMS in the form of communication flows, depicted in Fig. 11. The ML model M is a binary classifier: given an input flow f, the ML model classifies it as benign (b) or malicious (m):

$$M(f) = (m \vee b) \tag{1}$$

This input flow can be considered as being drawn from a data lake whose individual datapoints originate from various sensing layer endpoints such as RTUs, smart metering devices, smart inverters, PMUs, etc. The ML model is obtained by fitting any ML algorithm on a training dataset T. With respect to data perturbations, we consider two scenarios: S1 (i.e., training-stage "poisoning" perturbation) wherein some perturbed samples f are put in T leading to future versions of M to exhibit a poor performance; S2 (i.e., inference-stage "evasive" perturbations) wherein a given set of samples f have been purportedly manipulated so as to produce an incorrect output by M.

Note that both S1 and S2 can stem from three diverse sources, i.e., a deliberate attack (e.g., FDI), a natural fault of the DERMS (e.g., system outage), or poor management by the DERMS' developers. For example, S1 can be a product of a FDI attacks and data integrity compromise i.e., incorrect labeling (clean or dirty) for binary classification problems. Membership functions used during the FDI attack phase can decrease detection likelihoods and alter a fraction of the training data only marginally to remain unnoticed (e.g., partial reduction of continuous variables by a constant factor [395]). Such a training-stage poisoning attack can lead ML models to misclassify anomalous behavior (e.g., electricity theft) or produce erroneous predictions (e.g., load forecasting errors).

In the considered defensive mechanism, the ML model will not only provide the classification output to a given input, but will also provide the confidence of such output, which we denote as $C_M(f)$. Then (given the confidence threshold 'θ') the actual prediction $M(f)$ will be accepted i.i.f $C_M(f) > \theta$: in this case, the DERMS will act upon such predictions (e.g., if $M(f) = m$, then it may raise an alert to investigate the components involved in the input flow 'f'); otherwise, if $C_M(f) < \theta$, the sample f will be put in quarantine, Q. The samples in Q will be periodically reviewed (e.g., by a human analyst), in an attempt to understand the reason that led M to produce a particular confidence level. Such an analysis may reveal that, e.g., a component may have been subject to FDI attacks, or some natural fault (both of which are discernible if there are many flows f from the same source). Moreover, as an additional benefit of such an approach, by comparing the samples in Q with those in T, it is possible to determine if the ML model M must be updated (i.e., due to concept drift [392]). We note that the mitigation above may fail in the event of "clean label poisoning" [396], [397], as well as in other attacks which require an adversary to have precise control of T (e.g., backdoors [398]).

X. Grid Service Management for DERs

Section IX has briefly defined an adversarial machine learning method (i.e., data poisoning) and details a robust mechanism to identify poisoned data with a certain degree of confidence. We will now shift our focus to looking at

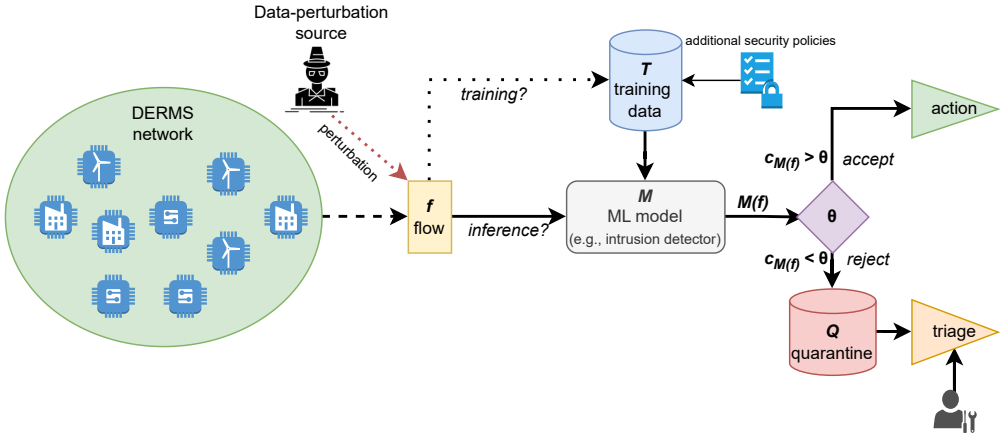


Fig. 11. **Data–perturbation scenario and a potential defense.** We consider adversarial perturbations that can "poison" (i.e., negatively affect) the output of the ML model either during its training stage (i.e., when such perturbations are put in the training data) or during its inference stage (i.e., when the perturbations only entail samples analysed by the model during its operational phase). An exemplary use-case is an ML model for intrusion detection.

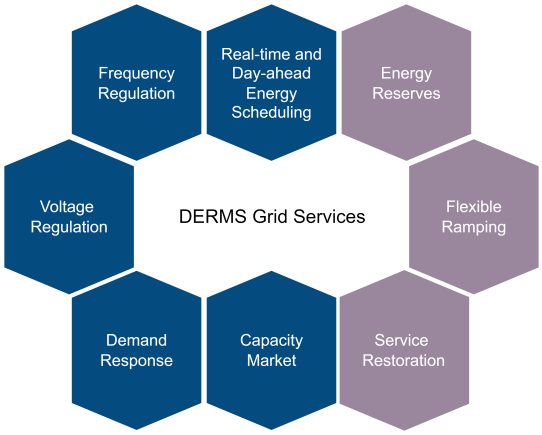


Fig. 12. Grid services supported by DERMS – Flexible load compatible (blue) and PV/BESS compatible (beige).

grid service management practices for increasing penetration of certain DER types (i.e., electric vehicles) from cyber and distributed architecture perspectives to improve the resiliency and decision-making at levels 1, 2, and 3 of the IEEE 1547.3-2023 standard. The first part of this section will summarize cyber threats for the EV DER asset type and make two recommendations for securing V2G infrastructure. Secondly, a layered architecture to support grid resiliency and offer distributed decision-making to prevent single-point failures (i.e., similar to the distributed and decentralized architecture types) is proposed for general DER applications.

Electric system planners and operators use demand response (DR) programs as resource options for balancing supply and demand. In the United States, demand response was primarily used to provide peak load management, specifically load reduction during contingency events [399]. DR allows consumers to play an important role in grid operation by reducing or shifting their electricity usage during peak periods in response to time-based rates or other forms of financial incentives [399]. In the future, DR services will be offered with greater flexibility in the renewables integration of variable resources and new technologies such as electric vehicles such as bidirectional charging capability using Vehicle-to-Grid (V2G) technologies.

DR services are actively bidding energy for capacity-based generation from various resources such as solar photovoltaic (PV), as well as other ancillary services in the form of wholesale and retail markets under dynamic pricing programs. These services are still emerging advances in communications and control technology because they allow for maximum resource value without insight into future market structures.

To avoid curtailment based on the DR scenarios such as low and high DR, the DR end-users are categorized as commercial, industrial, municipal, and residential sectors, for purposes such as cooling, heating, and ventilation. With this rapid development, the use of AC/DC hybrid multi-microgrid (MMG) concepts is gaining popularity [400]. As a part of DR responses, these MMGs will be used in both commercial and residential sectors, integrating small-scale solar PV, wind, and renewable distributed generators. Energy storage systems, such as the battery energy storage system (BESS), can store energy from bidirectional charging from V2G services as well as renewable generation. Fig. 12 offers a non-exhaustive list of grid services that serve flexible loads (e.g., EVs) and fixed loads.

The massive interaction of data within and outside the DR management system present unique cyber threats [401][402].

A. Cyber Threats for Vehicular Grid Assets

The utilization of V2G technology enhances the grid flexibility by balancing the demand and supply scenario by harnessing the bidirectional capability from the charging stations. In terms of grid stabilization, the V2G system also facilitates the peak load management, during the load demand period and maintains the grid resiliency with a reduced infrastructural cost [403] [404]. In common, V2G contributes to reduction in carbon emission by utilizing renewable resources [405].

The integration of V2G systems to the grids causes potential vulnerabilities and is susceptible to cyber attacks. In a V2G

system, several modules can be targeted for attacks based on their system architecture and design.

1) Mobility of data packets: The functionality of vehicle-to-home (V2H) and vehicle-to-building (V2B) systems aims to connect several smart devices through mobile and web applications facilitating efficient charging scenarios and user's decision in contribution to its storage unit or to a designated aggregator.
2) Meters and monitoring systems: The V2G ecosystem includes several metering and monitoring systems such as AMI, Smart Meters, and aggregators. There are many security challenges involved in considering these modules to be protected. The EV charging sites follow Open Charge Point Protocol (OCPP) for their charging operations which ensures the efficiency and quality of services (QoS) between the charge points and central management systems [406]. The attack in AMIs includes the intrusion detection system (IDS), monitoring abnormalities that deal with energy theft by grid overloading.
3) Edge device tampering: Common attacks on the electric vehicle supply equipment (EVSE) are physical access attacks through the interfaces in EV charging stations. According to a report from NREL on vehicular security threats, the on-board diagnostics (OBD) which provides access to external networks and devices is the most commonly used port for exploitation, in terms of the physical access risk [407]. Their mitigation approach includes preventing unauthorized access, reducing the number of external interfaces, and monitoring vehicles for signs of physical access. In addition, the charging stations demand the use of RFID to schedule the charge. According to the report from Kaspersky, these RFIDs are vulnerable to attacks through replication that turn out to be MiTM attacks. This RFID includes the critical data logs such as charging duration, and payment details and can lead to malicious firmware when communicating with the vehicle and the charging station [408].

The key factor in securing V2G infrastructure includes the privacy-sensitive continuous data exchange, monitoring the infrastructure for anomalies, and AI-driven solutions based on DL:

1) Blockchain and consensus scheme: In the context of vehicular communication, channeling wireless networks requires real-time data authentication through blockchain technology. The Internet of Vehicles and its architecture can be protected from cyber risks with the characteristics of decentralization. A consensus algorithm enables a network of nodes to validate data added to the blockchain. According to Xu et al., the Practical Byzantine Fault Tolerance consensus algorithm is popular in recent research studies, although it's not suitable for dynamic networks due to its large communication overhead [426]. The wireless communication between the vehicles and other corresponding nodes is vulnerable to cyber attacks such as injecting false data and tampering with the information transferred [427]. Thus, securing and validating the data blocks with a consensus algorithm can resist malicious attacks in addition to securing communication nodes such as roadside units (RSUs) and charging service providers [428].
2) AI for securing vehicular communication: An approach of intrusion detection and diagnostics systems (IDDS) enhances vehicular communication by authentication and encryption. Research efforts exploring ensemble learning and several optimization frameworks offer diverse functionalities and services. Within the network-controlled vehicles, various attacks including DoS, spoofing, and malicious messages have been observed within the network packets [429]. The progression of ML and DL techniques can process these packets by classifier-based IDDS thereby reducing the vulnerability of cyber threats in the vehicular ecosystem [430].

An overview of cyber risks involved in the context of V2X, and related technologies is illustrated in Table XII. They are categorized based on the assets and their associated attack vectors. The likelihood and impact of certain assets and their impacts are assessed based on the attack types discussed in the existing literature. V2G services can either be centralized (i.e., aggregator is responsible for managing and optimizing EV contributions) or decentralized (i.e., local entities autonomously manage EVs) and our assessment in Table XII refers to both these architecture types. Each of these types have their advantages/disadvantages [431] and at least from the perspective of grid services (e.g., voltage regulation) provided by edge resources such as EVs, a better solution to integrate such edge resources with systems such as ADMS and DERMS is through a laminar architecture that we will discuss in the following subsection.

B. Layered Architecture for Grid Services

Traditionally, centralized decision support located at ADMS is employed to coordinate the grid's many distributed resources to extract different grid services [24]. However, the centralized decision-support system is vulnerable to communication and single-point failures either due to cyber attacks or natural events, is slow in response, and poses scalability challenges when required to coordinate a large number of controllable agents. This has led to an interest in distributed decision-making paradigms for the active distribution systems that (1) reduce the computational requirements on a single decision-making unit by distributing the problem into several smaller sub-problems that are computationally simpler; (2) result in a decision-making paradigm with multiple interacting agents that is robust to single-point failures; and (3) relax the need for communication between the central controller and all connected controllable/non-controllable assets thus better manage data privacy considerations [57][432]. Due to these advantages, distributed optimization in power distribution systems has gained significant attention lately, with several contributions related to algorithm development and their applications for optimizing operations [433]. Furthermore,

TABLE XII
THREATS IN V2X ECOSYSTEM: ASSETS, ATTACK VECTORS AND COUNTERMEASURES.

Assets	Attack Vectors	Likelihood (High/Medium/Low); Impact (↑, ↓, ↔)			Framework & Countermeasures	Refs.
		Confidentiality	Integrity	Availability		
V2G & G2V	Mobility of Data Packets, AMI, Smart Meters Charging Stations and EVSE: OBUs, Charging Service Provider Authority (CSPA).	Side Channel Attack (High, ↓).	Replay Attacks (Medium, ↔).	DDoS (Low, ↑), Tampering (High, ↔).	Blockchain-based distributed ledger technology (DLT): Consensus Algorithm – RAFT and PBFT Efficient Cryptographic Primitives Enabling Mutual Authentication, Key Derivation, Hash Function.	[409], [410], [411], [412], [413], [414], [415], [416]
In–Vehicle & V2X	In-Vehicle: EV Charging Port, OBD, CAN, ECU V2X: Keyless Entry, BLE, DSRC, WiFi, Road Side Units (RSUs).	MiTM (Low, ↑), Eavesdropping (Low, ↓).	Malware (High, ↑), Spoofing (Medium,↔), Packet Replay (Medium, ↔).	DoS (Low, ↑), Cloning (Low, ↔), Tampering (High, ↔).	AI-based framework for Intrusion Detection System and Vehicular Ad Hoc Network: Deep Transfer Learning, CNN.; Blockchain Assisted Authentication Protocol.	[417], [418], [419], [420], [421]
Renewables & BESS	PV System at Microgrid Level.	Phishing (Low, ↓), MiTM (Low, ↑), FDI (High, ↑).	Spoofing (Low, ↔), Replay Attacks (Medium, ↔).	Scaling and Ramping (High, ↑), DoS (Low, ↑).	Fuzzy Modeling and Identification Approach; Singular Value Decomposition (SVD) and Disturbance Decoupling.	[422], [423], [424], [425]

the increasing deployment of non-utility DERs is forcing a transition away from the purely centralized approach [434]. To this end, a laminar/layered architecture for decision support that synergistically combines distributed and edge-control paradigms is emerging as a viable architecture for grid-edge coordination [435]. A layered architecture typically recruits an ADMS that is centralized, and many distributed decision-making agents to coordinate a large number of controllable grid-edge resources including grid-interactive buildings, DERs, and other legacy devices to extract grid services. An example framework is shown in Fig. 13. The description of the control levels is briefly explained here for general applications.

- Level 1 controller is located at the DMS/ADMS and has access to the full distribution system model. However, measurement data from edge devices are available less frequently. This agent is responsible for only observing the control decisions or making decisions at coarser time-scale.
- Level 2 controller is located at several distributed agents throughout the distribution feeder. These agents have partial access to the distribution network model and are responsible for controlling one or a group of active nodes (controllable assets). The distributed agents solve a distributed optimization problem to maximize either system-level utility or individual utilities (in the case of greedy/private stakeholders). These agents use peer-to-peer (P2P) communication to exchange a minimum set of information among their trusted neighbors to achieve their respective goals. Then, they coordinate the agreed-upon decision on their controllable assets in Level-3.
- Level-3 controllers are located at individual controllable nodes. They communicate with the Level-2 controller that they are affiliated with. Level-3 controllers can either include purely local control modes or peer-to-peer control, as in Level 2. In most cases, Level-3 agents will have limited computing capability and limited access to the distribution system model and parameters.

The application of layered architecture has been demonstrated to coordinate grid services from DERs. One such application includes using layered architectures for power distribution system restoration for enhanced resilience [436]. This work develops a distributed decision-making paradigm that deploys multiple agents to solve a global/network-level objective by solving smaller sub-problems and jointly coordinating their individual decisions. This architecture enables a bottom-up distribution system restoration by using all available resources (e.g., DG units) through local awareness and limited data exchange with neighboring agents/regions. It enables system autonomy through distributed algorithms, preserves privacy, has reduced computational costs relative to other centralized solutions, and is robust to single-point failures.

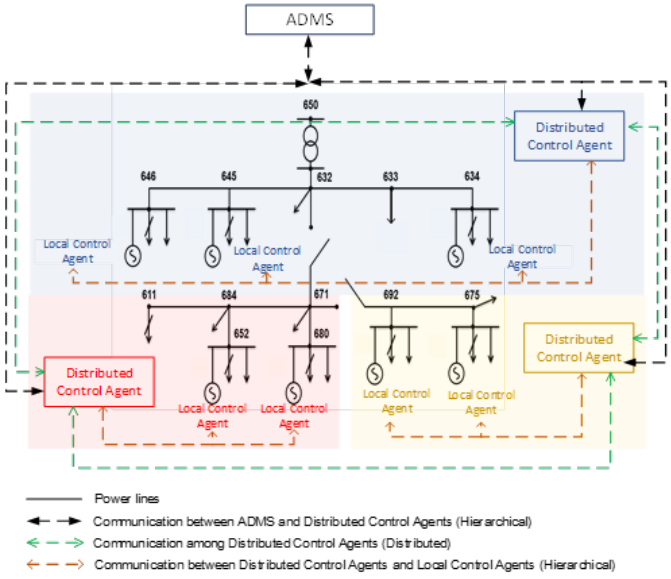


Fig. 13. Layered architecture mapped for distributed applications.

To systematically deploy advanced decision-making architectures, the following important questions need to be answered: (1) what information (model and measurement data) should be exchanged among agents at different levels and those within the same levels? (2) how are control and optimization algorithms distributed for different levels of a given application? The two questions are strongly coupled; a different information structure leads

to a different optimization/control paradigm and related algorithmic challenges. Moreover, the attributes of the communication network dictate the reliability and applicability of the distributed algorithms for real-time operations. This necessitates evaluating the algorithm performance with a realistic communication system model. Lately, co-simulation platforms such as HELICS have emerged as a viable means to co-simulate cyber and physical layers [437]. In a recent work, this platform is used to co-simulate power, communication, and control layers to evaluate the effects of communication delays, latency, and topology on the performance of distribution optimization algorithms for grid operations [438].

XI. Lessons Learned

As was seen in the previous sections, cybersecurity for DERMS requires thoughtful consideration of multiple aspects such as architecture types, test beds, threat models, etc. We expect the digital ecosystem to evolve with increasing vendor products (e.g., ADMS software) and product integrations (e.g., DERMS augmented with AI) in the market, and this presents unique cyber-physical challenges and threat scenarios; however, this survey has provided notable trends, threat models (i.e., hardware and software), and IT technologies that will remain applicable to the future's DER-focused grid. In this section, we will highlight lessons learned on: (1) existing test bed capabilities, (2) threat models, (3) hardware security, (4) our proposed solutions for intrusion detection technology/(5) zero trust security, (6) and machine learning applications to the power grid.

A. Stress Testing

Stress testing is important when deploying SCADA/ADMS test beds. Performance metrics for stress testing such as System Average Interruption Duration Index (SAIDI), Momentary Average Interruption Frequency Index (MAIFI), etc. only evaluate the reliability of a power system [439] and not a power system's stability, efficiency, or resiliency against cyber attacks. The evolving nature of adversarial threat models warrants fine-grained insights into a power system's behavior through analyzing voltage/frequency stability (e.g., deviations), power quality (e.g., distortion), and response-time (e.g., fault tolerance) to identify anomalous behavior and deploy remediation measures. Other related test beds environments include the Real-time Immersive Network Simulation Environment (RINSE), Internet-Scale Event and Attack Generation Environment (ISEAGE) by ISU [440], and the Defense technology experimental research (DETER) project supported by the Department of Homeland Security (DHS), National Science Foundation (NSF), and the Department of Defense (DoD) [441]. Details on these test beds are provided because: 1) they do not create platform testing specific to DERMS, or 2) are dated and do not comprehend emerging innovations. Nevertheless, these test beds offer wide capabilities to perform stress tests.

The protocols mentioned offer native security features although the "hardness" of these features can be questioned. Though the properties of authentication, authorization, and confidentiality are theoretically provided by Modbus, Modbus can still be compromised through packet sniffing to extract confidential information and DoS can be used to interrupt data flow [119]. Standardized protocols, interoperable devices, and appropriate cybersecurity measures must be set in place to facilitate the feasible incorporation of PMUs and μPMUs into the grid. Native security features only serve as capabilities and do not guarantee security when these features are not enabled or properly configured by system operators. Also, variations within protocols require additional security considerations especially when they are integrated with different systems. One counter-strategy is to establish security benchmarks at the time of design and development.

B. Threat Modeling

Findings indicate that Threat Scenario 1 ("DER Aggregation Risks") poses a large threat to system-level and large-scale entities such as DER aggregators and market operations. Threat Scenarios 2 and 3 pose significant threats to DERs at device-level and communication protocol-levels. Threat models targeting specific layers may exploit critical security problems and critically affect DERMS' functionality (e.g., outages). Data science techniques (e.g., statistical models) and AI (e.g., generative models) can be used to create synthetic data for threat modeling. Deploying AI-powered security components that can be trained to prevent concept drift and adapt to evolving threats provide more innovation avenues. Future DERs are at risk for AI-generated attacks, so the best solution lies in protective and watcher AI components.

Based on the FDI attacks detailed in Tables V and VI, we notice that FDI attacks are primarily constructed to disrupt the control of power electronics devices (e.g., converters, inverters) as they rely heavily on the voltage/current information at the interfacing buses and on the power demanded from the different DERs. FDIs can be modeled in multiple ways - for example, FDI attacks can assume full network, limited, or even no network topology information, recruit various membership functions (e.g., random, time-varying, ramp), target assets at the sensing and communication layers, or incorporate falsified state estimation measurements or malware. Along with directly manipulating the control signals that are fed to power switches, FDI attacks on these control signals provide an opportunity for the intruder to manipulate the switching action of power electronics, thereby disturbing grid-reliant processes (e.g., automatic generation control, voltage stabilization, load dispatch) typically executed at energy management systems (EMS). Beyond the switching signals, FDI attacks on the data corresponding to the switching status (ON/OFF) results in hiding a converter/inverter fault scenario as a normal scenario or vice versa. Any manipulation of the grid voltage signal not only hinders attainment of the control objectives at the individual DER level but has a detrimental impact on the stability of the entire grid.

C. Hardware Security

Compromised electronics can significantly hamper privacy, security, safety, and resiliency of DERMS and other smart

grid systems. Incidents such as the "Big Hack" [196][197] have large scale devastating societal impacts. Hence, it is important to recognize these security concerns in the context of smart grid so that effective security solutions can be developed through broad collaborations. Demonstrated threats such as hardware Trojans, side channel attacks, and reverse engineering must be thoroughly explored. Furthermore, awareness of hardware security threats among smart grid professionals and students must be enhanced to properly support this area of research and engineering. A strong consensus between software and hardware developers for DERMS should also be established. Standards and regulations for securing DER hardware must be enforced along production cycles. Commercial concerns may keep hardware developers from revealing details for their products; therefore, regulations should require that DER hardware be produced in accordance with pre-defined security best practices.

D. Intrusion Detection

Building continuous integration/continuous delivery (CI/CD) pipelines provides rapid development and reliably to deliver services while streamlining development and deployment workflows. Our proposed IDFF framework is an example of this and will aid in increasing agility and reveal software flaws early in the development cycle. A continuous integration workflow uses build automation to incorporate frequent code changes. Each piece of software code that is changed is automatically built into an image and spun up as a container. Containerization of applications provides broader benefits such as fine-grained resilience, eliminating single points of failure, scalability, infrastructure optimization, rolling upgrades/rollbacks, logging, monitoring, and security. Upon integration and packaging of the code, a continuous delivery workflow is initiated. CI/CD aims to safely deliver integrated code changes into environments by using automated tests. Moving through various stages of the build process, tests validate the code quality and ensure secure deployment.

E. Zero Trust Security

Simple defense strategies to secure endpoints and perimeter devices are not viable due to the complex nature of power infrastructure and the integration of technologies like the cloud. Old models include measures such as locking down networks and user access for varied periods of time to restrict unauthorized movement; this hinders interoperability and collaboration, especially in heterogeneous and multi-entity systems like power grids. Zero trust principles based on access control policies (e.g., privileged access management, identity access management), real-time endpoint monitoring (e.g., endpoint detection and response), incident management solutions (e.g., SIEM), edge frameworks (e.g, secure access service edge), SDPs, and digital forensics reduce the likelihood of cyber attacks in addition to improving the resiliency of the systems. This is made possible by the reduction of attack surface and implementing risk-based security policies compatible with cloud technologies, DERMS, DER endpoints, and system-level entities such as TSOs. One major bottleneck of zero trust application to power grids is the abundance of legacy infrastructure. Legacy systems may not justify a complete zero trust shift in all cases, and custom security controls must be designed and enforced to remediate emerging cyber-physical attack vectors. Our proposed frameworks in Section VII and Section VIII support the pillars of the Zero Trust Strategy proposed by the Department of Defense (DoD) [442] - (1) Users (2) Devices (3) Applications and Workloads (4) Data (5) Network and Environment (6) Automation and Orchestration (7) Visibility and Analytics.

F. Machine Learning

From our discussion on ML-specific security issues in Section IX, we emphasize the importance of assessing the security risks of ML before deploying such technologies in DERMS. Even though some attacks proposed by prior literature may seem far-fetched in the DERMS context, DERMS are a critical infrastructure and hence they should expect to face even highly skilled and motivated adversaries. Nonetheless, as long as fundamental security precautions are taken (e.g., preventing access to the model by unauthorized parties) then the majority of security threats to ML would be prevented. However, attackers may still leverage blind spots such as side channel, or insider threats, or may even compromise the supply chain so as to gain some form of access to the model. In these cases, it is necessary to rely on proper defensive techniques that enable to withstand, e.g., evasion attempts, or data poisoning (which can also happen "naturally"), or model stealing, or even privacy violations via membership inference attacks. Therefore, it is crucial to identify the weakest link in a DERMS that is powered by an ML model, and then invest enough resources to ensure the DERMS continuity of operation even if it is subject by adversarial ML attacks.

XII. Technical Challenges and Future Directions

Finally, we provide important technical challenges and future directions that should be discussed in the context of DERMS security. For this study, we look at control parameter optimization, advanced persistent threats, application of cyber kill chains, and recommended security practices.

A. Control Parameter Optimization

It is well established that utility operators have to deal with a large number of parameters that operators can tune to optimize grid support functions such as power factor control, frequency/voltage ride through, power curtailment, voltage regulation, among others [443]. Considering this and the heterogeneity of DERs, the control parameter space for distribution entities and serviceable endpoints starts to expand. Work is done to optimize these grid support functions to improve grid stability [444][445][446]. For example, automatic voltage ride-through or dynamic voltage/VAR grid support functions can be implemented by DERs through an ADMS to minimize voltage deviations from a set

target voltage so there is a reduction in unnecessary power consumption and/or voltage reduction [447] (i.e. putting the "smart" in smart inverter-based DERs). However, recent works in this area (2021 onwards) use statistical and optimization algorithms without leveraging AI/ML; this presents novel research directions given the scalability of DERs and grid support functions. As stated by EPRI [448], determining parameters for grid support functions has different levels of complexity and the highest levels of complexity (i.e., based on DER type) should consider parameters such as feeder model topology, location, transformer impedance, load levels, etc. Once the optimal parameter set is chosen, the information is relayed through remote communication or firmware updates both of which are viable threat vectors [449]. We expect FDI, data modification/alteration [450], and DoS attacks to be targeted at such grid support functions to create sub-optimal conditions (e.g., unexpected reactive power due to manipulated voltage), small but permanent damage to transformers and power lines, and malicious islanding of DERs [451].

B. Advanced Persistent Threats and Cybersecurity Kill Chain Methods

Advanced Persistent Threats (APTs) require "diligent surveillance" and constantly adaptive cybersecurity responses [452] and because the energy sector is a principal target for cybersecurity attacks [453], we must employ effective methodologies like CKC. Attacks in Ukraine, Saudi Arabia, and South Africa illustrate the need for heightened vigilance against APTs [454]. A common kill chain methodology addresses 7 levels of resolution for cybersecurity threats [455]:

1) Reconnaissance
2) Weaponization
3) Delivery
4) Exploitation
5) Installation
6) Command and Control
7) Action on Objectives (AoO)

These levels represent objectives by a threat actor in an APT scenario. The degree of hostility that may be encountered with a cybersecurity adversary considers the Opportunity Triad which measures persistence and drive of the threat actor as a product of their Capability, Intent, and Opportunity [456].

Energy grid cyber safety is relevant when the defense exceeds the product of a threat actor's capability, intent, and opportunity. Since it is impossible to control the intent of a threat actor, and the control of threat actors' capability is limited, controlling opportunities effectively stops attackers before they reach their AoO. If the opportunity is brought to zero, no attack is possible. This principle stresses the need for grid infrastructure to remain up-to-date with fixes that address security issues, adherence to best security practices, and the need for rigorous testing of new features.

While postmortem analysis from the following victims does not provide all permutations of the CKC in all situations, we address the points at which a CKC could have stopped energy sector attacks on Ukraine in 2015 and 2016 (BlackEnergy), the Shamoon attack on Saudi Arabia oil interests in 2012 (Aramco), and the 2022 ransomware attack against South Africa's state electrical provider (Eskom). Ukraine and Aramco appear to have politically motivated intent [457][458] while Eskom's woes appear to be financially motivated [459].

The Pyramid of Pain (PoP) spots indicators of attack that are key for unraveling the APT and implementing your kill chain before AoO is accomplished [460]. Not all of these indicators are equally valuable and are ranked according to utility i.e., from least valuable to most valuable:

1) **Hash values (applicable at the communication layer)**: Antivirus programs, Threat Intelligence Platforms, and SIEM systems can all leverage known threat hash values to find malware items and specific patterns on systems. Within energy grids, hashes for threat activity (e.g., viruses) and for allow-listed software, firmware, and devices can greatly improve security. For example, batches of data sent from smart meters can be monitored as processes that are used to generate n-bit hash functions (e.g., n = 128, 256) [461]. Since smart meters operate according to a fixed environment specified by the manufacturer, an allow list of legal processes is feasible (i.e., memory-wise) and hashes can be used to monitor for any modifications due to malware in these processes. Similarly, security recommendations from NREL for IBRs and edge devices [462] list a test (i.e., "Test 5: Message Authentication Code") to validate if MACs exist for DER communication protocols that use TLS (e.g., Modbus) for for MACs that integrate hash functions. While a secure channel is recommended for two-way communication (e.g., between DER devices and gateways) to implement MACs, this may not be necessary in all cases as shown by Aghapour et al. [463].
2) **IP addresses (applicable at the sensing layer)**: Knowledge of known malicious addresses can cut off communications before they begin. Tight IP control is useful against reconnaissance phases of the kill chain or as a response against later phases. For example, IEEE 2030.5 calls for IP addresses as part of provisioning of DER endpoints as part of the Common Smart Inverter Profile (CSIP) [464]. Helpful tools include IP allow lists based on authentication, integration with dynamic DNS, firewalls, IDS/IPS systems, and Threat Intelligence Feeds which list hacker-controlled systems.
3) **Domain names (applicable at the sensing layer)**: Provisioning DNS is also included in CSIP [464]. Additionally, knowledge of compromised domains used by threat actors can be used to prevent endpoints/customers from accessing known threats. These domain names can be resolved in proxy systems, DNS filtering systems, and as part of a SIEM.
4) **Network and host artifacts (applicable at the sensing and communication layers)**: Grid devices creating logs and histories should be analyzed to reveal threat actors. Tools like Endpoint Detection and Response (EDR), Log Analysis, Network Monitoring/Analyzers and Behavioral Analysis analyze Smart GRID artifacts

to determine compromise. Increasingly, AI tools like clustering and large language models (LLMs) are useful in blocking threats using past network and host artifact data. To adapt security systems to newer cybersecurity tools, semantic understanding of edge devices nomenclature will benefit from systems like the Open Energy Data Initiative's Energy Language Model (ELM) [465].

5) **Tools (applicable at the control layer)**: Cybersecurity-specific tools (e.g., virtualization, sandboxing, group policy management) can be used to identify compromises or contain your environment deterministically, lowering hacking opportunities. Tooling can be difficult on endpoint DERs except when provided by the manufacturer. In situations where endpoints are not using encryption, switches should compensate by creating encryption layers on behalf of the endpoint. For other systems, like aggregators, sandboxing via containers, message authentication codes, and application allow-listing is necessary for secure environments.
6) **Tactics, techniques, and procedures (applicable at the control layer)**: Behavioral analysis, Threat Hunting, and implementing the MITRE ATT&CK Framework proactively protects networks. The MITRE ATT&CK Framework presents fourteen adversarial tactics (e.g., reconnaissance, lateral movement) and various techniques (e.g., account manipulation, log enumeration). Each tactic can applied to different technology domains (e.g., ICS, enterprises) [466]. This facilitates personalized use-cases like threat intelligence and adversarial emulation/red-teaming exercises, or to profile global threats (e.g., APTs). A tool called "Decider" [467] has been developed by the Cybersecurity and Infrastructure Security Agency (CISA) to assist security personnel in categorizing adversarial behaviors to ATT&CK. These generic tools, when leveraged with energy sector-specific reports from CISA, directly address successful tactics, techniques, and procedures [468][469] by providing actionable solutions to security deficits. ATT&CK holds promise for smart grid applications especially given the rise in APTs. This requires a thorough understanding of the framework and target systems. These approaches often take human capital to implement but are increasingly enabled by AI resources.

C. Applying Cyber Kill Chains at Grid–edge

Organizations need to implement kill chain response by create automation and orchestration, setup comprehensive monitoring, create incident response plans, regularly update and patch systems and processes, and provide training to address the social engineering issues. These activities address the Opportunity Triad and address ongoing technical challenges for securing grid networks. When prior failures are taken as lessons for future responses, addressable gaps are revealed in the implementation of CKCs.

Ukraine's systems were heavily surveilled before the attacker's AoO. In this incident, deficiency exists between reconnaissance activity and the acquisition of administrative rights by hackers [457]. This shows weakness in the PoP tooling in weaponization analysis, delivery logging, and exploitation accounting layers. Post-attack analysis showed that spear-phishing emails with Microsoft Word, PowerPoint, Excel, or Rich Text Format (RTF) attachments were used to deliver malicious payloads. When executed, these attachments were used to continue reconnaissance with network discovery and password stealers. A file containing an Excel macro deployed 'BlackEnergy' and installed agents typically used by Russians hackers called 'Sandworm' to perform additional internal analysis. The attacks on Ukraine's grid in 2016 was linked to the same APT as in the 2015 attack. The success of similar phishing techniques used to deliver payloads showed lack in subsequent training. Knowledge of the domain names used by this threat actor and timely action could have deny-listing intelligence and may have blocked this threat vector. Attackers were eventually able to access an operator's workstation to deploy 'Radmin', a RAT, further exploits within the network. Because much is known about this attack, we see exceptional accountability and the existence of significant tooling for certain phases of the attack and gaps in others.

The Shamoon Aramco attack also began as a phishing email that was opened by an information systems employee [470]. The malware was able to spread worm-like on the network and exploited vulnerabilities which had known fixes at the time. This points to gaps in the deployment of hash-based tools, timely updates, and TTPs within the organization.

Eskom sustained multiple events after this ransomware illustrating the longevity of APTs. These recurrences illustrate broad gaps within their infrastructure. The rate of occurrence between attacks suggests that attackers are able to build upon previous compromises and gaps in accountability [459][471]. The ransomware event was a result of gaps in user training and should have been controlled by common cybersecurity tools which prevent anomalous application installation [472].

D. Grid–Relevant Security Practices

To meet gaps, AI promises the ability to find gaps and anomalies in data, on networks, and infrastructure. The implementation of AI Trust, Risk and Security Management (AI TRiSM) to support grids in implementing their kill chains are heavily trending in industry as an answer to automation challenges and dealing with big data within the CKC [473]. These should be adopted as cyber-criminals are increasingly using AI for their own purposes [474].

Coordination is increasing as the information exchanged between multiple DER vendors, DER owners, aggregators, and DER-related assets requires the exploration of new technologies such as zero-trust or perimeter-less based security frameworks. Such methods will need to warrant continuous authentication and verification during TCP connection sessions. Future work should include self-healing models, adversarial threat modeling, quantum-resistant cryptography, blockchain, moving target defense (MTD), secure digital twin,

integration of 5G security features in DER communication, and deep packet inspection (DPI) methods (e.g, pattern matching, protocol/behavior analysis, statistical flow analysis) [475] as endpoint data need to be encrypted. It is also equally important to reassess secure operator actions such as DSOs, RTOs, TSOs, and ISOs market interactions. Other areas to improve timely detection of events or anomalies, and corresponding proactive response actions to mitigate risks. This may require pilot security drills, audits and risk assessment on recovery mechanisms or planning within utilities or organizations that can compromise CIAA properties. We also recommend DER/DERMS stakeholders follow the NIST Cybersecurity Framework (CSF) [476]: Identify, Protect, Detect, Respond, Recover functionalities. Utilities should ensure network topologies are properly documented with their bandwidth and traffic size expectations, and latency and trust requirements for anticipated recovery phases during ransomware or DDoS attacks. As there is a mixed opinion on where DERMS textcolorbluetechnologies reside, whether ADMS, AMI or stand-alone DERMS network, it is critical to consider these suggestions and recommendations from the IEEE 1547.3-2023 standard [11].

XIII. Conclusion

Securing power infrastructure is crucial against both intentional (e.g., cyber attacks) and unintentional (e.g., natural disasters) outages. To effectively integrate Distributed Energy Resource Management Systems (DERMS) into Advanced Metering Infrastructure (AMI) or Advanced Distribution Management Systems (ADMS), it's essential to incorporate an Intrusion Diagnostic Federated Framework (IDFF) for DERs. The choice of DERMS architecture is pivotal in addressing cyber threats, including configuration errors, data manipulation, and DER aggregation. This paper offers an in-depth examination of DERMS frameworks, attack types, use cases, and cybersecurity challenges. It emphasizes the necessity of a federated DERMS that operates with a zero trust framework to secure grid-related services.

Acknowledgment

The work presented in this paper was partially supported by the U.S. DoE, Office of Science under DoE contract number DE-AC02-06CH11357. The submitted manuscript has been created by UChicago Argonne, LLC, operator of Argonne National Laboratory. Argonne, a DoE Office of Science laboratory, is operated under Contract No. DE-AC02-06CH11357. The work for this manuscript was supported by the U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response under contract TL0401010-05907-4219031 (Agreement # 51582). The U.S. Government retains for itself, and others acting on its behalf, a paid-up nonexclusive, irrevocable worldwide license in said article to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, by or on behalf of the Government.

This material is based upon work partially supported by the National Science Foundation (NSF) under Grant No. 2350363, Grant No. 2316399, and Grant No. CNS-2219733.

Giovanni Apruzzese would like to acknowledge the Hilti Foundation for funding part of this research.

Appendix A
Abbreviations

Please see Tables XIII and XIV for the list of acronyms and their definitions.

References

[1] "What is u.s. electricity generation by energy source?," Jun 2023. https://www.eia.gov/tools/faqs/faq.php?id=427&t=4.
[2] . Alliance for Automotive Innovation, "Electric Vehicle Quarterly Report," tech. rep., 2022.
[3] Mar. 2024.
[4] C. Powell, K. Hauck, A. D. Sanghvi, A. Hasandka, J. Van Natta, and T. L. Reynolds, "Guide to the distributed energy resources cybersecurity framework," tech. rep., National Renewable Energy Lab.(NREL), Golden, CO (United States), 2019.
[5] A. Zabetian-Hosseini, A. Mehrizi-Sani, and C.-C. Liu, "Cyberattack to cyber-physical model of wind farm scada," in *IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society*, pp. 4929–4934, IEEE, 2018.
[6] J. Staggs, D. Ferlemann, and S. Shenoi, "Wind farm security: attack surface, targets, scenarios and mitigation," *International Journal of Critical Infrastructure Protection*, vol. 17, pp. 3–14, 2017.
[7] Aug 2018. https://www.cisa.gov/news-events/ics-advisories/icsa-15-162-01a.
[8] J. Johnson, "Roadmap for photovoltaic cyber security," *Sandia National Laboratories*, 2017.
[9] J. Johnson, T. Berg, B. Anderson, and B. Wright, "Review of electric vehicle charger cybersecurity vulnerabilities, potential impacts, and defenses," *Energies*, vol. 15, no. 11, p. 3931, 2022.
[10] . Gerald Gray, "DERMS, Federated Architecture for DER, And the Enabling Standards," Oct. 2020. https://shorturl.at/KtJUW.
[11] "Ieee guide for cybersecurity of distributed energy resources interconnected with electric power systems," *IEEE Std 1547.3-2023 (Revision of IEEE Std 1547.3-2007)*, pp. 1–183, 2023.
[12] L. Strezoski, "Distributed energy resource management systems—derms: State of the art and how to move forward," *Wiley Interdisciplinary Reviews: Energy and Environment*, vol. 12, no. 1, p. e460, 2023.
[13] S. Garip, M. Bilgen, N. Altin, S. Ozdemir, and İ. Sefa, "Reliability analysis of centralized and decentralized controls of microgrid," in *2022 11th International Conference on Renewable Energy Research and Application (ICRERA)*, pp. 557–561, IEEE, 2022.
[14] B. N. Alhasnawi, B. H. Jasim, B. E. Sedhom, E. Hossain, and J. M. Guerrero, "A new decentralized control strategy of microgrids in the internet of energy paradigm," *Energies*, vol. 14, no. 8, p. 2183, 2021.
[15] E. Espina, J. Llanos, C. Burgos-Mellado, R. Cardenas-Dobson, M. Martinez-Gomez, and D. Saez, "Distributed control strategies for microgrids: An overview," *IEEE Access*, vol. 8, pp. 193412–193448, 2020.
[16] Q. Zhou, M. Shahidehpour, A. Paaso, S. Bahramirad, A. Alabdulwahab, and A. Abusorrah, "Distributed control and communication strategies in networked microgrids," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2586–2633, 2020.
[17] B. Seal, "Understanding derms," *EPRI Journal*, vol. 2018, 2018.
[18] F. Ding, W. Liu, J. MacDonald, J. Ogle, A. Pratt, and M. Baggu, "Federated architecture for secure and transactive distributed energy resource management solutions (fast-derms)," tech. rep., National Renewable Energy Lab.(NREL), Golden, CO (United States), 2022.
[19] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated learning: Challenges, methods, and future directions," *IEEE signal processing magazine*, vol. 37, no. 3, pp. 50–60, 2020.
[20] E. Barker, W. C. Barker, U. D. of Commerce, N. I. of Standards, Technology, C. S. Division, D. Consulting, N. S. Agency, Venafi, T. Polk, B. Burr, and M. Smid, *NIST Special Publication 800-57 Part 2 Revision 1 Recommendation for Key Management: Part 2 – Best Practices for Key Management Organizations*. revision 1 ed., May 2019.

[21] IEEE, "Ieee approved draft guide for cybersecurity of distributed energy resources interconnected with electric power systems," *IEEE P1547.3/D3.12, March 2023*, pp. 1–158, 2023.

[22] C. on National Security Systems (CNSS), "Committee on national security systems (cnss) glossary," Mar. 2022.

[23] P. Eder-Neuhauser, T. Zseby, J. Fabini, and G. Vormayr, "Cyber attack models for smart grid environments," *Sustainable Energy, Grids and Networks*, vol. 12, pp. 10–29, 2017.

[24] A. Dubey, A. Bose, M. Liu, and L. N. Ochoa, "Paving the way for advanced distribution management systems applications: Making the most of models and data," *IEEE Power and Energy Magazine*, vol. 18, no. 1, pp. 63–75, 2020.

[25] . National Renewable Energy Laboratory (NREL), "Insights into Advanced Distribution Management Systems," 2015.

[26] N. Dizdar, "Using Data Diodes to Secure Your ADMS Data Transfer," August 2021.

[27] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on smart grid communication infrastructures: Motivations, requirements and challenges," *IEEE communications surveys & tutorials*, vol. 15, no. 1, pp. 5–20, 2012.

[28] J. Qi, A. Hahn, X. Lu, J. Wang, and C.-C. Liu, "Cybersecurity for distributed energy resources and smart inverters," *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 28–39, 2016.

[29] M. H. Cintuglu, O. A. Mohammed, K. Akkaya, and A. S. Uluagac, "A survey on smart grid cyber-physical system testbeds," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 446–464, 2016.

[30] J. Rodríguez-Molina and D. M. Kammen, "Middleware architectures for the smart grid: A survey on the state-of-the-art, taxonomy and main open issues," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 2992–3033, 2018.

[31] A. Sundararajan, A. Chavan, D. Saleem, and A. I. Sarwat, "A survey of protocol-level challenges and solutions for distributed energy resource cyber-physical security," *Energies*, vol. 11, no. 9, p. 2360, 2018.

[32] 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 Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2886–2927, 2019.

[33] G. M. Makrakis, C. Kolias, G. Kambourakis, C. Rieger, and J. Benjamin, "Industrial and critical infrastructure security: Technical analysis of real-life security incidents," *IEEE Access*, vol. 9, pp. 165295–165325, 2021.

[34] T. Himdi, M. Ishaque, and M. J. Ikram, "Cyber security challenges in distributed energy resources for smart cities," in *2022 9th international conference on computing for sustainable global development (INDIACom)*, pp. 788–792, IEEE, 2022.

[35] K. Chan, Y. Kim, and J.-Y. Jo, "Der communication networks and their security issues," in *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 0785–0790, IEEE, 2022.

[36] S. Vahidi, M. Ghafouri, M. Au, M. Kassouf, A. Mohammadi, and M. Debbabi, "Security of wide-area monitoring, protection, and control (wampac) systems of the smart grid: A survey on challenges and opportunities," *IEEE Communications Surveys & Tutorials*, 2023.

[37] I. Zografopoulos, N. D. Hatziargyriou, and C. Konstantinou, "Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations," *IEEE Systems Journal*, 2023.

[38] M. D. Lal and R. Varadarajan, "A review of machine learning approaches in synchrophasor technology," *IEEE Access*, vol. 11, p. 33520–33541, Jul 2023.

[39] W. Ahmed, M. Nayel, and M. T. El-Mohandes, "A μpmu full observation algorithm for balanced radial distribution grid with pv integration," in *2021 22nd International Middle East Power Systems Conference (MEPCON)*, IEEE, Dec. 2021.

[40] G. S. Dua, B. Tyagi, and V. Kumar, "Deploying micro-pmus with channel limit in reconfigurable distribution systems," *IEEE Systems Journal*, vol. 16, p. 832–843, Mar. 2022.

[41] N. Constandache, D. M. Stanescu, M. Sanduleac, C. Stanescu, I. Tristiu, and A. Mandis, "Smart meters, pmu and pq data analysis in active distribution grids – case studies in mv networks," in *2018 International Conference on Applied and Theoretical Electricity (ICATE)*, IEEE, Oct. 2018.

[42] Z. Soltani and M. Khorsand, "Real-time topology detection and state estimation in distribution systems using micro-pmu and smart meter data," *IEEE Systems Journal*, vol. 16, p. 3554–3565, Sept. 2022.

[43] A. Meydani, H. Shahinzadeh, H. Nafisi, and G. B. Gharehpetian, "Synchrophasor technology applications and optimal placement of micro-phasor measurement unit (upmu): Part i," in *2024 28th International Electrical Power Distribution Conference (EPDC)*, IEEE, Apr. 2024.

[44] A. Meydani, H. Shahinzadeh, H. Nafisi, and G. B. Gharehpetian, "Synchrophasor technology applications and optimal placement of micro-phasor measurement unit (upmu): Part ii," in *2024 28th International Electrical Power Distribution Conference (EPDC)*, IEEE, Apr. 2024.

[45] A. Shahsavari, M. Farajollahi, E. Stewart, C. Roberts, and H. Mohsenian-Rad, "A data-driven analysis of lightning-initiated contingencies at a distribution grid with a pv farm using micro-pmu data," in *2017 North American Power Symposium (NAPS)*, IEEE, Sept. 2017.

[46] G. S. Dua, B. Tyagi, and V. Kumar, "Fault detection technique for distribution networks and microgrids using synchrophasor data," *IEEE Transactions on Industry Applications*, vol. 59, p. 7368–7381, Nov. 2023.

[47] D. Dwivedi, P. K. Yemula, and M. Pal, "Dynamopmu: A physics informed anomaly detection, clustering and prediction method using non-linear dynamics on μpmu measurements," *IEEE Transactions on Instrumentation and Measurement*, 2023.

[48] R. Chandrakar, R. K. Dubey, and B. K. Panigrahi, "Deep-learning based multiple class events detection and classification using micro-pmu data," in *2024 8th International Conference on Green Energy and Applications (ICGEA)*, IEEE, Mar. 2024.

[49] A. Srivastava and S. Parida, "A robust fault detection and location prediction module using support vector machine and gaussian process regression for ac microgrid," *IEEE Transactions on Industry Applications*, vol. 58, p. 930–939, Jan. 2022.

[50] M. Tsebia, H. Bentarzi, and A. Ratni, "Micro-grids integration using remote synchronisation based on micro-pmu," in *2024 2nd International Conference on Electrical Engineering and Automatic Control (ICEEAC)*, IEEE, May 2024.

[51] M. Baudette, L. Vanfretti, G. Del-Rosario, A. Ruiz-Alvarez, J. L. Dominguez-Garcia, I. Al-Khatib, M. Shoaib Almas, I. Cairo, and J. O. Gjerde, "Validating a real-time pmu-based application for monitoring of sub-synchronous wind farm oscillations," in *ISGT 2014*, IEEE, Feb. 2014.

[52] S. V. Hareesh and K. Shanti Swarup, "Dynamic state estimation of synchronous generator based distributed energy resource in autonomous microgrid," in *2019 8th International Conference on Power Systems (ICPS)*, IEEE, Dec. 2019.

[53] D. Pliatsios, P. Sarigiannidis, T. Lagkas, and A. G. Sarigiannidis, "A survey on scada systems: secure protocols, incidents, threats and tactics," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1942–1976, 2020.

[54] M. Alanazi, A. Mahmood, and M. J. M. Chowdhury, "Scada vulnerabilities and attacks: A review of the state-of-the-art and open issues," *Computers & security*, vol. 125, p. 103028, 2023.

[55] D. Upadhyay and S. Sampalli, "Scada (supervisory control and data acquisition) systems: Vulnerability assessment and security recommendations," *Computers & Security*, vol. 89, p. 101666, 2020.

[56] IRENA, "Renewable capacity statistics 2023 - 2024." Available Online: https://www.irena.org/Publications/2024/Mar/Renewable-capacity-statistics-2024, title = Renewable Capacity Statistics 2024, Mar 2024.

[57] R. B. Melton, K. P. Schneider, E. Lightner, T. E. Mcdermott, P. Sharma, Y. Zhang, F. Ding, S. Vadari, R. Podmore, A. Dubey, *et al.*, "Leveraging standards to create an open platform for the development of advanced distribution applications," *IEEE Access*, vol. 6, pp. 37361–37370, 2018.

[58] . Department of Energy, "National SCADA Test Bed," 2022.

[59] A. Pratt, M. Baggu, F. Ding, S. Veda, I. Mendoza, and E. Lightner, "A test bed to evaluate advanced distribution management systems for modern power systems," in *IEEE EUROCON 2019-18th International Conference on Smart Technologies*, pp. 1–6, IEEE, 2019.

[60] H. Padullaparti, A. Pratt, I. Mendoza, S. Tiwari, M. Baggu, C. Bilby, and Y. Ngo, "Peak load management in distribution systems using legacy utility equipment and distributed energy resources," in *2021 IEEE Green Technologies Conference (GreenTech)*, pp. 435–441, IEEE, 2021.

[61] O. R. N. L. O. , "Advancing grid resiliency, security with a microgrid test bed: SI-GRID | ORNL," June 2017.

[62] M. Govindarasu, V. Ajjarapu, D. Jacobson, and U. Vaidya, "PowerCyber: A Cyber- Physical Security Testbed for Smart Grid."

[63] J. Johnson, "SunSpec Alliance Annual Meeting," *Sandia National Laboratories*, Dec. 2022.

[64] . iGrid T & D, "What is GOOSE Messaging?," 2022.

[65] H. T. Reda, B. Ray, P. Peidaee, A. Anwar, A. Mahmood, A. Kalam, and N. Islam, "Vulnerability and impact analysis of the iec 61850 goose protocol in the smart grid," *Sensors 2021, Vol. 21, Page 1554*, vol. 21, p. 1554, 2 2021.

[66] J. Hoyos, M. Dehus, and T. X. Brown, "Exploiting the goose protocol: A practical attack on cyber-infrastructure," *2012 IEEE Globecom Workshops, GC Wkshps 2012*, pp. 1508–1513, 2012.

[67] J. Noce, Y. A. P. A. on Cyber-InfrastructureLopes, N. C. Fernandes, C. V. Albuquerque, and D. C. Muchaluat-Saade, "Identifying vulnerabilities in smart gric communication networks of electrical substations using geese 2.0," *IEEE International Symposium on Industrial Electronics*, pp. 111–116, 8 2017.

[68] M. Chlela, G. Joos, M. Kassouf, and Y. Brissette, "Real-time testing platform for microgrid controllers against false data injection cybersecurity attacks," *IEEE Power and Energy Society General Meeting*, vol. 2016-November, 11 2016.

[69] S. S. M. Reshikeshan and M. S. Illindala, "Systematically encoded polynomial codes to detect and mitigate high-status-number attacks in inter-substation goose communications," *2020 IEEE Industry Applications Society Annual Meeting, IAS 2020*, 10 2020.

[70] S. E. Quincozes, C. Albuquerque, D. Passos, and D. Mossé, "A survey on intrusion detection and prevention systems in digital substations," *Computer Networks*, vol. 184, p. 107679, 2021.

[71] H. León, C. Montez, O. Valle, and F. Vasques, "Real-time analysis of time-critical messages in iec 61850 electrical substation communication systems," *Energies*, vol. 12, no. 12, p. 2272, 2019.

[72] S. Joshi, "Utilization of goose in mv substation," in *16th National power systems conference*, pp. 323–328, 2010.

[73] E. P. R. Institute, "Inter-control center communications protocol (iccp, tase.2): Threats to data security and potential solutions," *Technical Report*, 2001.

[74] N. Malviya, "TASE 2.0 and ICCP." Available Online: https://resources.infosecinstitute.com/topic/tase-2-0-and-iccp/, February 2020.

[75] X. He, X. Liu, and P. Li, "Coordinated false data injection attacks in agc system and its countermeasure," *IEEE Access*, vol. 8, pp. 194640–194651, 2020.

[76] G. Dán, H. Sandberg, M. Ekstedt, and G. Björkman, "Challenges in power system information security," *IEEE Security & Privacy Magazine*, vol. 10, no. 4, pp. 62–70, 2012.

[77] . National Instruments, "Introduction to dnp3." Available Online: https://www.ni.com/en-us/innovations/white-papers/10/introduction-to-dnp3.html, October 2020.

[78] A. Corporation, "DNP 3.0 Communication Protocol," 2004.

[79] V. Kelli, P. Radoglou-Grammatikis, T. Lagkas, E. K. Markakis, and P. Sarigiannidis, "Risk analysis of dnp3 attacks," in *2022 IEEE International Conference on Cyber Security and Resilience (CSR)*, pp. 351–356, IEEE, 2022.

[80] M. Abdelkhalek, G. Ravikumar, and M. Govindarasu, "Ml-based anomaly detection system for der communication in smart grid," in *2022 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, pp. 1–5, IEEE, 2022.

[81] P. Wlazlo, A. Sahu, Z. Mao, H. Huang, A. Goulart, K. Davis, and S. Zonouz, "Man-in-the-middle attacks and defence in a power system cyber-physical testbed," *IET Cyber-Physical Systems: Theory & Applications*, vol. 6, no. 3, pp. 164–177, 2021.

[82] I. Darwish, O. Igbe, and T. Saadawi, "Experimental and theoretical modeling of dnp3 attacks in smart grids," in *2015 36th IEEE Sarnoff Symposium*, pp. 155–160, IEEE, 2015.

[83] F. B. Galán, "A machine learning based security analysis of dnp3,"

[84] D. Jin, D. M. Nicol, and G. Yan, "An event buffer flooding attack in dnp3 controlled scada systems," *Proceedings - Winter Simulation Conference*, pp. 2614–2626, 2011.

[85] I. Darwish, O. Igbe, and T. Saadawi, "Experimental and theoretical modeling of dnp3 attacks in smart grids," *2015 36th IEEE Sarnoff Symposium*, pp. 155–160, 11 2015.

[86] F. Burrieza Galán, "A machine learning based security analysis of dnp3," 2021.

[87] . IEEE Communications Society, "IEEE Adoption of Smart Energy Profile 2.0 Application Protocol Standard," *IEEE Std 2030.5-2013*, pp. 1–348, November 2013. Conference Name: IEEE Std 2030.5-2013.

[88] R. Anderson and S. Fuloria, "Smart meter security: a survey," *University of Cambridge Computer Laboratory, United Kingdom*, 2011.

[89] *2030.5-2018 - IEEE Standard for Smart Energy Profile Application Protocol*. IEEE, 2018.

[90] D. J. Sebastian and A. Hahn, "Exploring emerging cybersecurity risks from network-connected der devices," *2017 North American Power Symposium, NAPS 2017*, 11 2017.

[91] G. Ravikumar, B. Hyder, and M. Govindarasu, "Hardware-in-the-loop cps security architecture for der monitoring and control applications," *2020 IEEE Texas Power and Energy Conference, TPEC 2020*, 2 2020.

[92] N. K. Singh and V. Mahajan, "International journal of critical infrastructure protection end-user privacy protection scheme from cyber intrusion in smart grid advanced metering infrastructure," *International Journal of Critical Infrastructure Protection*, vol. 34, p. 100410, 2021.

[93] . Modbus, "Modbus Application Protocol." Available Online: https://modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf.

[94] . National Instruments, "What is the Modbus Protocol & How Does It Work?." Available Online: https://www.ni.com/en-us/innovations/white-papers/14/the-modbus-protocol-in-depth.html, December 2022.

[95] "MODBUS/TCP Security," July 2018.

[96] O. N. Nyasore, P. Zavarsky, B. Swar, R. Naiyeju, and S. Dabra, "Deep packet inspection in industrial automation control system to mitigate attacks exploiting modbus/tcp vulnerabilities," *Proceedings - 2020 IEEE 6th Intl Conference on Big Data Security on Cloud, BigDataSecurity 2020, 2020 IEEE Intl Conference on High Performance and Smart Computing, HPSC 2020 and 2020 IEEE Intl Conference on Intelligent Data and Security, IDS 2020*, pp. 241–245, 5 2020.

[97] D. M. Thomas, N. Pandey, V. K. Shukla, and A. V. Singh, "Attack vectors and susceptibilities of the modbus in tcp/ip model," *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions), ICRITO 2021*, 2021.

[98] A. S. Mohammed, E. Anthi, O. Rana, N. Saxena, and P. Burnap, "Detection and mitigation of field flooding attacks on oil and gas critical infrastructure communication," *Computers & Security*, vol. 124, p. 103007, 1 2023.

[99] P. Radoglou-Grammatikis, P. Sarigiannidis, G. Efstathopoulos, T. Lagkas, A. Sarigiannidis, V. Mladenov, and N. Siaxabanis, "Defending industrial internet of things against modbus/tcp threats: A combined ai-based detection and sdn-based mitigation solution," *SSRN Electronic Journal*, 6 2022.

[100] B. Chen, N. Pattanaik, A. Goulart, K. L. Butler-Purry, and D. Kundur, "Implementing attacks for modbus/tcp protocol in a real-time cyber physical system test bed," *Proceedings - CQR 2015: 2015 IEEE International Workshop Technical Committee on Communications Quality and Reliability*, 6 2015.

[101] J. T. Sørensen and M. G. Jaatun, "An analysis of the manufacturing messaging specification protocol," in *International Conference on Ubiquitous Intelligence and Computing*, pp. 602–615, Springer, 2008.

[102] H. Palahalli, M. Hemmati, and G. Gruosso, "Analysis of cyber security threat of using iec61850 in digital substations involving derms," *2022 International Symposium on Power Electronics, Electrical Drives, Automation and Motion, SPEEDAM 2022*, pp. 948–953, 2022.

[103] M. R. Saifuddin, L. Wei, H. Tan, and B. Chen, "Coordinated network attacks on microgrid dispatch function: An epic case study," 11 2022.

[104] J. Parssinen, P. Raussi, S. Noponen, M. Opas, and J. Salonen, "The digital forensics of cyber-attacks at electrical power grid substation," *10th International Symposium on Digital Forensics and Security, ISDFS 2022*, 2022.

[105] M. Hemmati, M. H. Palahalli, G. S. Gajani, and G. Gruosso, "Impact and vulnerability analysis of iec61850 in smartgrids using multiple hil real-time testbeds," *IEEE Access*, vol. 10, pp. 103275–103285, 2022.

[106] L. Yang, Y. Zhai, Y. Zhang, Y. Zhao, Z. Li, and T. Xu, "A new methodology for anomaly detection of attacks in iec 61850-based substation system," *Journal of Information Security and Applications*, vol. 68, p. 103262, 2022.

[107] S. C. , "Overview and Introduction to the Manufacturing Message Specification (MMS) (Revision 2)," Aug. 1995.

[108] T. S. Ustun, S. S. Hussain, and A. Kalam, "Performance evaluation of iec 61850 mms messages under cybersecurity considerations," *Energy Reports*, vol. 8, pp. 1189–1199, 2022.

[109] T. Agarwal, "BACnet Protocol : Architecture, Working, Types, Objects & Its Applications."

[110] V. Graveto, T. Cruz, and P. Simões, "Security of building automation and control systems: Survey and future research directions," *Computers & Security*, vol. 112, p. 102527, 1 2022.

[111] T. Yimer, E. Smith, P. Harvey, M. Tienteu, and K. Kornegay, "Error correction attacks on bacnet ms/tp," *Proceedings of the 2022 IEEE International Symposium on Hardware Oriented Security and Trust, HOST 2022*, pp. 77–80, 2022.

[112] L. Strezoski, H. Padullaparti, F. Ding, and M. Baggu, "Integration of utility distributed energy resource management system and aggregators for evolving distribution system operators," *Journal of Modern Power Systems and Clean Energy*, vol. 10, no. 2, pp. 277–285, 2022.

[113] . US Department of Energy (DoE), "Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid." https://tinyurl.com/5n6jam5r.

[114] National Institute of Standards and Technology Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," Tech. Rep. NIST CSWP 04162018, National Institute of Standards and Technology, Gaithersburg, MD, Apr. 2018.

[115] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity challenges in vehicular communications," *Vehicular Communications*, vol. 23, p. 100214, 2020.

[116] Z. El-Rewini, K. Sadatsharan, N. Sugunaraj, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity attacks in vehicular sensors," *IEEE Sensors Journal*, vol. 20, no. 22, pp. 13752–13767, 2020.

[117] . Computer Security Resource Center. https://csrc.nist.gov/glossary/term/threat.

[118] Joint Task Force Interagency Working Group, "Security and Privacy Controls for Information Systems and Organizations," tech. rep., National Institute of Standards and Technology, September 2020. Edition: Revision 5.

[119] H. Vallant, B. Stojanović, J. Božić, and K. Hofer-Schmitz, "Threat modelling and beyond-novel approaches to cyber secure the smart energy system," *Applied Sciences*, vol. 11, no. 11, p. 5149, 2021.

[120] H. M. Albunashee, C. Farnell, A. Suchanek, K. Haulmark, R. A. McCann, J. Di, and A. Mantooth, "A test bed for detecting false data injection attacks in systems with distributed energy resources," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 10, no. 1, pp. 1303–1315, 2019.

[121] N. Duan, N. Yee, B. Salazar, J.-Y. Joo, E. Stewart, and E. Cortez, "Cybersecurity analysis of distribution grid operation with distributed energy resources via co-simulation," in *2020 IEEE Power & Energy Society General Meeting (PESGM)*, pp. 1–5, IEEE, 2020.

[122] C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for scada systems," *IEEE Transactions on Power Systems*, vol. 23, no. 4, pp. 1836–1846, 2008.

[123] M. Basnet, S. Poudyal, M. H. Ali, and D. Dasgupta, "Ransomware detection using deep learning in the scada system of electric vehicle charging station," in *2021 IEEE PES Innovative Smart Grid Technologies Conference-Latin America (ISGT Latin America)*, pp. 1–5, IEEE, 2021.

[124] P. Bajpai, R. Enbody, and B. H. Cheng, "Ransomware Targeting Automobiles," in *Proceedings of the Second ACM Workshop on Automotive and Aerial Vehicle Security*, (New Orleans LA USA), pp. 23–29, ACM, Mar. 2020.

[125] O. T. Soyoye and K. C. Stefferud, "Cybersecurity risk assessment for california's smart inverter functions," in *2019 IEEE CyberPELS (CyberPELS)*, pp. 1–5, IEEE, 2019.

[126] I. Zografopoulos, J. Ospina, X. Liu, and C. Konstantinou, "Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies," *IEEE Access*, vol. 9, pp. 29775–29818, 2021.

[127] O. G. M. Khan, E. El-Saadany, A. Youssef, and M. Shaaban, "Impact of electric vehicles botnets on the power grid," in *2019 IEEE Electrical Power and Energy Conference (EPEC)*, pp. 1–5, IEEE, 2019.

[128] C. Carter, I. Onunkwo, P. Cordeiro, and J. Johnson, "Cyber security assessment of distributed energy resources," in *2017 IEEE 44th Photovoltaic Specialist Conference (PVSC)*, pp. 2135–2140, IEEE, 2017.

[129] C. Konstantinou and M. Maniatakos, "Impact of firmware modification attacks on power systems field devices," in *2015 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 283–288, IEEE, 2015.

[130] M. Slowinske and D. Saleem, "U.s department of energy cybersecurity strategy (2018-2020)." Jan. 2022.

[131] Z. Li, M. Shahidehpour, and F. Aminifar, "Cybersecurity in distributed power systems," *Proceedings of the IEEE*, vol. 105, no. 7, pp. 1367–1388, 2017.

[132] D. Tellbach and Y. Li, "A survey on the cyber-security of distributed generation systems," *Proceedings of the ESREL, Portorož, Slovenia*, pp. 18–22, 2017.

[133] P. Paganini, "Blackenergy used as a cyber weapon against ukrainian critical infrastructure — infosec resources," Jan 2016.

[134] C. Osborne, "Poetrat trojan targets energy sector using coronavirus lures," Apr 2020.

[135] . Symantec Security Response Team, "Dragonfly - western energy sector targeted by sophisticated attack group resurgence in energy sector attacks," September 2017.

[136] D. of Energy, *Advanced Transmission Technologies*. Dec. 2020.

[137] C. Miller, "Throwback attack: Blackenergy attacks the ukrainian power grid - industrial cybersecurity pulse," Nov 2021.

[138] M. Geiger, J. Bauer, M. Masuch, and J. Franke, "An analysis of black energy 3, crashoverride, and trisis, three malware approaches targeting operational technology systems," in *2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, vol. 1, pp. 1537–1543, IEEE, 2020.

[139] C. Konstantinou, A. Keliris, and M. Maniatakos, "Taxonomy of firmware trojans in smart grid devices," in *2016 IEEE Power and Energy Society General Meeting (PESGM)*, pp. 1–5, IEEE, 2016.

[140] P. Radoglou-Grammatikis, P. Sarigiannidis, T. Liatifis, T. Apostolakos, and S. Oikonomou, "An overview of the firewall systems in the smart grid paradigm," in *2018 Global information infrastructure and networking symposium (GIIS)*, pp. 1–4, IEEE, 2018.

[141] J. Boyens, A. Smith, N. Bartol, K. Winkler, A. Holbrook, and M. Fallon, "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations," tech. rep., National Institute of Standards and Technology, Oct. 2021.

[142] Ö. Sen, D. van der Velde, S. N. Peters, and M. Henze, "An approach of replicating multi-staged cyber-attacks and countermeasures in a smart grid co-simulation environment," 2021.

[143] D. Cerotti, D. Codetta-Raiteri, G. Dondossola, L. Egidi, G. Franceschinis, L. Portinale, and R. Terruggia, "Evidence-based analysis of cyber attacks to security monitored distributed energy resources," *Applied Sciences*, vol. 10, no. 14, p. 4725, 2020.

[144] J. Jasiūnas, P. D. Lund, and J. Mikkola, "Energy system resilience–a review," *Renewable and Sustainable Energy Reviews*, vol. 150, p. 111476, 2021.

[145] C. Aguayo Gonzalez and A. Hinton, "Detecting malicious software execution in programmable logic controllers using power fingerprinting," in *International Conference on Critical Infrastructure Protection*, pp. 15–27, Springer, 2014.

[146] R. S. de Carvalho and D. Saleem, *Recommended functionalities for improving cybersecurity of distributed energy resources*, vol. 1. IEEE, 2019.

[147] X. Zhong, L. Yu, R. Brooks, and G. K. Venayagamoorthy, "Cyber security in smart dc microgrid operations," in *2015 IEEE First International Conference on DC Microgrids (ICDCM)*, pp. 86–91, 2015.

[148] J. Johnson, J. Quiroz, R. Concepcion, F. Wilches-Bernal, and M. J. Reno, "Power system effects and mitigation recommendations for der cyberattacks," *IET Cyber-Physical Systems: Theory & Applications*, vol. 4, no. 3, pp. 240–249, 2019.

[149] J. Sande-Ríos, J. Canal-Sánchez, C. Manzano-Hernández, and S. Pastrana, "Threat analysis and adversarial model for smart grids," in *2024 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pp. 130–145, IEEE, 2024.

[150] H. J. Liu, M. Backes, R. Macwan, and A. Valdes, "Coordination of ders in microgrids with cybersecure resilient decentralized secondary frequency control," 2018.

[151] C. Carter, C. Lai, N. Jacobs, S. Hossain-McKenzie, P. Cordeiro, I. Onunkwo, and J. Johnson, "Cyber Security Primer for DER Vendors Aggregators and Grid Operators," Tech. Rep. SAND–2017-13113, 1761987, 674083, Sandia National Laboratory, November 2017.

[152] K. Park, B. Ahn, J. Kim, D. Won, Y. Noh, J. Choi, and T. Kim, "An advanced persistent threat (apt)-style cyberattack testbed for distributed energy resources (der)," in *2021 IEEE Design Methodologies Conference (DMC)*, pp. 1–5, IEEE, 2021.

[153] J. M. Taylor and H. R. Sharif, "Security challenges and methods for protecting critical infrastructure cyber-physical systems," in *2017 International Conference on Selected Topics in Mobile and Wireless Networking (MoWNeT)*, pp. 1–6, IEEE, 2017.

[154] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using kalman filter," *IEEE transactions on control of network systems*, vol. 1, no. 4, pp. 370–379, 2014.

[155] D. Jafarigiv, K. Sheshyekani, M. Kassouf, Y. Seyedi, H. Karimi, and J. Mahseredjian, "Countering fdi attacks on ders coordinated control system using fmi-compatible cosimulation," *IEEE Transactions on Smart Grid*, vol. 12, no. 2, pp. 1640–1650, 2020.

[156] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data-injection attacks against power system state estimation: Modeling

and countermeasures," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 3, pp. 717–729, 2013.

[157] S. Acharya, R. Mieth, R. Karri, and Y. Dvorkin, "False data injection attacks on data markets for electric vehicle charging stations," *Advances in Applied Energy*, vol. 7, p. 100098, 2022.

[158] R. Deng and H. Liang, "False data injection attacks with limited susceptance information and new countermeasures in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 3, pp. 1619–1628, 2018.

[159] E. Drayer and T. Routtenberg, "Detection of false data injection attacks in smart grids based on graph signal processing," *IEEE Systems Journal*, vol. 14, no. 2, pp. 1886–1896, 2019.

[160] W. Yu, D. Griffith, L. Ge, S. Bhattarai, and N. Golmie, "An integrated detection system against false data injection attacks in the smart grid," *Security and Communication Networks*, vol. 8, no. 2, pp. 91–109, 2015.

[161] Y. Zhang, J. Wang, and B. Chen, "Detecting false data injection attacks in smart grids: A semi-supervised deep learning approach," *IEEE Transactions on Smart Grid*, vol. 12, no. 1, pp. 623–634, 2020.

[162] X. Liu, P. Zhu, Y. Zhang, and K. Chen, "A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2435–2443, 2015.

[163] J. Zhao, G. Zhang, M. La Scala, Z. Y. Dong, C. Chen, and J. Wang, "Short-term state forecasting-aided method for detection of smart grid general false data injection attacks," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1580–1590, 2015.

[164] X. Liu, Z. Bao, D. Lu, and Z. Li, "Modeling of local false data injection attacks with reduced network information," *IEEE Transactions on Smart Grid*, vol. 6, no. 4, pp. 1686–1696, 2015.

[165] Q. Su, H. Fan, and J. Li, "Distributed adaptive secondary control of ac microgrid under false data injection attack," *Electric Power Systems Research*, vol. 223, p. 109521, 2023.

[166] R. Lu and J. Wang, "Distributed control for ac microgrids with false data injection attacks and time delays," in *E3S Web of Conferences*, vol. 194, p. 03023, EDP Sciences, 2020.

[167] Z. Xie and Z. Wu, "Distributed fault-tolerant secondary control for dc microgrids against false data injection attacks," *International Journal of Electrical Power and Energy Systems*, vol. 144, p. 108599, 2023.

[168] A. H. EL-Ebiary, M. Mokhtar, A. M. Mansour, F. H. Awad, M. I. Marei, and M. A. Attia, "Distributed mitigation layers for voltages and currents cyber-attacks on dc microgrids interfacing converters," *Energies*, vol. 15, no. 24, p. 9426, 2022.

[169] M. R. Habibi, H. R. Baghaee, F. Blaabjerg, and T. Dragičević, "Secure control of dc microgrids for instant detection and mitigation of cyber-attacks based on artificial intelligence," *IEEE Systems Journal*, vol. 16, no. 2, pp. 2580–2591, 2021.

[170] J. Zhang, S. Sahoo, J. C.-H. Peng, and F. Blaabjerg, "Mitigating concurrent false data injection attacks in cooperative dc microgrids," *IEEE Transactions on Power Electronics*, vol. 36, no. 8, pp. 9637–9647, 2021.

[171] A. Kavousi-Fard, A. Almutairi, A. Al-Sumaiti, A. Farughian, and S. Alyami, "An effective secured peer-to-peer energy market based on blockchain architecture for the interconnected microgrid and smart grid," *International Journal of Electrical Power and Energy Systems*, vol. 132, p. 107171, 2021.

[172] T. Cheng, X. Zhu, X. Gu, F. Yang, and M. Mohammadi, "Stochastic energy management and scheduling of microgrids in correlated environment: A deep learning-oriented approach," *Sustainable Cities and Society*, vol. 69, p. 102856, 2021.

[173] M. R. Habibi, H. R. Baghaee, T. Dragičević, and F. Blaabjerg, "Detection of false data injection cyber-attacks in dc microgrids based on recurrent neural networks," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 5, pp. 5294–5310, 2020.

[174] K. Gupta, S. Sahoo, R. Mohanty, B. K. Panigrahi, and F. Blaabjerg, "Distinguishing between cyber attacks and faults in power electronic systems—a noninvasive approach," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 11, no. 2, pp. 1578–1588, 2022.

[175] A. Cecilia, S. Sahoo, T. Dragičević, R. Costa-Castelló, and F. Blaabjerg, "On addressing the security and stability issues due to false data injection attacks in dc microgrids—an adaptive observer approach," *IEEE Transactions on Power Electronics*, vol. 37, no. 3, pp. 2801–2814, 2021.

[176] G. Cao, R. Jia, and J. Dang, "Distributed resilient mitigation strategy for false data injection attack in cyber-physical microgrids," *Frontiers in Energy Research*, vol. 10, p. 845341, 2022.

[177] Y. Barzegari, J. Zarei, R. Razavi-Far, M. Saif, and V. Palade, "Resilient consensus control design for dc microgrids against false data injection attacks using a distributed bank of sliding mode observers," *Sensors*, vol. 22, no. 7, p. 2644, 2022.

[178] J. Bi, F. Luo, S. He, G. Liang, W. Meng, and M. Sun, "False data injection-and propagation-aware game theoretical approach for microgrids," *IEEE Transactions on Smart Grid*, vol. 13, no. 5, pp. 3342–3353, 2022.

[179] B. Blakely, W. Horsthemke, N. Evans, and D. Harkness, "Case study a: A prototype autonomous intelligent cyber-defense agent," in *Autonomous Intelligent Cyber Defense Agent (AICA) A Comprehensive Guide*, pp. 395–408, Springer, 2023.

[180] G. Sun, Y. Cong, J. Dong, Q. Wang, L. Lyu, and J. Liu, "Data poisoning attacks on federated machine learning," *IEEE Internet of Things Journal*, vol. 9, no. 13, pp. 11365–11375, 2021.

[181] Y. Wang and K. Chaudhuri, "Data poisoning attacks against online learning," *arXiv preprint arXiv:1808.08994*, 2018.

[182] C. Lai, N. Jacobs, S. Hossain-McKenzie, C. Carter, P. Cordeiro, I. Onunkwo, and J. Johnson, "Cyber security primer for der vendors, aggregators, and grid operators," *Tech. Rep.*, vol. 12, 2017.

[183] A. Sayghe, Y. Hu, I. Zografopoulos, X. Liu, R. G. Dutta, Y. Jin, and C. Konstantinou, "Survey of machine learning methods for detecting false data injection attacks in power systems," *IET Smart Grid*, vol. 3, no. 5, pp. 581–595, 2020.

[184] T. Morris, "Dataset 1: Power system datasets."

[185] S. Y. Diaba, M. Shafie-Khah, and M. Elmusrati, "Cyber security in power systems using meta-heuristic and deep learning algorithms," *IEEE Access*, vol. 11, pp. 18660–18672, 2023.

[186] D. Upadhyay, M. Zaman, R. Joshi, and S. Sampalli, "An efficient key management and multi-layered security framework for scada systems," *IEEE Transactions on Network and Service Management*, vol. 19, no. 1, pp. 642–660, 2021.

[187] S. Chakrabarty and B. Sikdar, "Unified detection of attacks involving injection of false control commands and measurements in transmission systems of smart grids," *IEEE Transactions on Smart Grid*, vol. 13, no. 2, pp. 1598–1610, 2021.

[188] F. Milano and A. Gomez-Exposito, "Detection of cyber-attacks of power systems through benford's law," *IEEE Transactions on Smart Grid*, vol. 12, no. 3, pp. 2741–2744, 2020.

[189] M. Jorjani, H. Seifi, A. Y. Varjani, and H. Delkhosh, "An optimization-based approach to recover the detected attacked grid variables after false data injection attack," *IEEE Transactions on Smart Grid*, vol. 12, no. 6, pp. 5322–5334, 2021.

[190] S. Chakrabarty and B. Sikdar, "Detection of malicious command injection attacks on phase shifter control in power systems," *IEEE Transactions on Power Systems*, vol. 36, no. 1, pp. 271–280, 2020.

[191] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630–1638, 2016.

[192] T. Bartman and K. Carson, "Securing communications for scada and critical industrial systems," in *2016 69th annual conference for protective relay engineers (CPRE)*, pp. 1–10, IEEE, 2016.

[193] M. Nagata, T. Miki, and N. Miura, "Physical attack protection techniques for ic chip level hardware security," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 30, no. 1, pp. 5–14, 2021.

[194] M. T. Rahman, M. S. Rahman, H. Wang, S. Tajik, W. Khalil, F. Farahmandi, D. Forte, N. Asadizanjani, and M. Tehranipoor, "Defense-in-depth: A recipe for logic locking to prevail," *Integration*, vol. 72, pp. 39–57, 2020.

[195] J. Gravellier, J.-M. Dutertre, Y. Teglia, P. L. Moundi, and F. Olivier, "Remote side-channel attacks on heterogeneous soc," in *Smart Card Research and Advanced Applications: 18th International Conference, CARDIS 2019, Prague, Czech Republic, November 11–13, 2019, Revised Selected Papers 18*, pp. 109–125, Springer, 2020.

[196] "The big hack: How china used a tiny chip to infiltrate u.s. companies."

[197] D. Mehta, H. Lu, O. P. Paradis, M. A. MS, M. T. Rahman, Y. Iskander, P. Chawla, D. L. Woodard, M. Tehranipoor, and N. Asadizanjani, "The big hack explained: Detection and prevention of pcb supply chain implants," *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, vol. 16, no. 4, pp. 1–25, 2020.

[198] P. Subramanyan, S. Ray, and S. Malik, "Evaluating the security of logic encryption algorithms," in *2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pp. 137–143, IEEE, 2015.

[199] K. Shamsi, M. Li, T. Meade, Z. Zhao, D. Z. Pan, and Y. Jin, "Appsat: Approximately deobfuscating integrated circuits," in *2017*

IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pp. 95–100, IEEE, 2017.

[200] M. Yasin, J. J. Rajendran, O. Sinanoglu, and R. Karri, "On improving the security of logic locking," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 35, no. 9, pp. 1411–1424, 2015.

[201] P. Chakraborty, J. Cruz, and S. Bhunia, "Sail: Machine learning guided structural analysis attack on hardware obfuscation," in *2018 Asian Hardware Oriented Security and Trust Symposium (AsianHOST)*, pp. 56–61, IEEE, 2018.

[202] P. Chakraborty, J. Cruz, A. Alaql, and S. Bhunia, "Sail: Analyzing structural artifacts of logic locking using machine learning," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3828–3842, 2021.

[203] L. Alrahis, S. Patnaik, M. Shafique, and O. Sinanoglu, "Omla: An oracle-less machine learning-based attack on logic locking," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 69, no. 3, pp. 1602–1606, 2021.

[204] L. Alrahis, S. Patnaik, F. Khalid, M. A. Hanif, H. Saleh, M. Shafique, and O. Sinanoglu, "Gnnunlock: Graph neural networks-based oracle-less unlocking scheme for provably secure logic locking," in *2021 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pp. 780–785, IEEE, 2021.

[205] D. Sisejkovic, F. Merchant, L. M. Reimann, H. Srivastava, A. Hallawa, and R. Leupers, "Challenging the security of logic locking schemes in the era of deep learning: A neuroevolutionary approach," *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, vol. 17, no. 3, pp. 1–26, 2021.

[206] P. Chakraborty, J. Cruz, and S. Bhunia, "Surf: Joint structural functional attack on logic locking," in *2019 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pp. 181–190, IEEE, 2019.

[207] P. Chakraborty, J. Cruz, R. Almawzan, T. Mahfuz, and S. Bhunia, "Learning your lock: Exploiting structural vulnerabilities in logic locking," *IEEE Design & Test*, 2024.

[208] J. Cruz, Y. Huang, P. Mishra, and S. Bhunia, "An automated configurable trojan insertion framework for dynamic trust benchmarks," in *2018 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pp. 1598–1603, IEEE, 2018.

[209] J. Cruz, P. Gaikwad, A. Nair, P. Chakraborty, and S. Bhunia, "A machine learning based automatic hardware trojan attack space exploration and benchmarking framework," in *2022 Asian Hardware Oriented Security and Trust Symposium (AsianHOST)*, pp. 1–6, IEEE, 2022.

[210] R. S. Chakraborty and S. Bhunia, "Hardware protection and authentication through netlist level obfuscation," in *2008 IEEE/ACM International Conference on Computer-Aided Design*, pp. 674–677, IEEE, 2008.

[211] A. Alaql, S. Chattopadhyay, P. Chakraborty, T. Hoque, and S. Bhunia, "Lego: A learning-guided obfuscation framework for hardware ip protection," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 41, no. 4, pp. 854–867, 2021.

[212] A. B. Chowdhury, L. Alrahis, L. Collini, J. Knechtel, R. Karri, S. Garg, O. Sinanoglu, and B. Tan, "Almost: Adversarial learning to mitigate oracle-less ml attacks via synthesis tuning," in *2023 60th ACM/IEEE Design Automation Conference (DAC)*, pp. 1–6, IEEE, 2023.

[213] T. Mahfuz, S. Bhunia, and P. Chakraborty, "X-dfs: Explainable artificial intelligence guided design-for-security solution space exploration," 2024.

[214] P. Gaikwad, J. Cruz, P. Chakraborty, S. Bhunia, and T. Hoque, "Third-party hardware ip assurance against trojans through supervised learning and post-processing," *arXiv preprint arXiv:2111.14956*, 2021.

[215] H. Lashen, L. Alrahis, J. Knechtel, and O. Sinanoglu, "Trojansaint: Gate-level netlist sampling-based inductive learning for hardware trojan detection," in *2023 IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 1–5, IEEE, 2023.

[216] K. Hasegawa, K. Yamashita, S. Hidano, K. Fukushima, K. Hashimoto, and N. Togawa, "Node-wise hardware trojan detection based on graph learning," *IEEE Transactions on Computers*, 2023.

[217] R. Yasaei, S.-Y. Yu, and M. A. Al Faruque, "Gnn4tj: Graph neural networks for hardware trojan detection at register transfer level," in *2021 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pp. 1504–1509, IEEE, 2021.

[218] A. Imangholi, M. Hashemi, A. Momeni, S. Mohammadi, and T. E. Carlson, "Fast-go: Fast, accurate, and scalable hardware trojan detection using graph convolutional networks," in *2024 25th International Symposium on Quality Electronic Design (ISQED)*, pp. 1–8, IEEE, 2024.

[219] S. Yang, T. Hoque, P. Chakraborty, and S. Bhunia, "Golden-free hardware trojan detection using self-referencing," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 30, no. 3, pp. 325–338, 2022.

[220] S. Yang, P. Chakraborty, P. SLPSK, and S. Bhunia, "Trusted electronic systems with untrusted cots," in *2021 22nd International Symposium on Quality Electronic Design (ISQED)*, pp. 198–203, IEEE, 2021.

[221] S. Yang, P. Chakraborty, and S. Bhunia, "Side-channel analysis for hardware trojan detection using machine learning," in *2021 IEEE International Test Conference India (ITC India)*, pp. 1–6, IEEE, 2021.

[222] D. Mukhopadhyay and R. S. Chakraborty, *Hardware security: design, threats, and safeguards*. CRC Press, 2014.

[223] C. Jin, L. Ren, X. Liu, P. Zhang, and M. van Dijk, "Mitigating synchronized hardware trojan attacks in smart grids," in *Proceedings of the 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids*, pp. 35–40, 2017.

[224] T. Hoque, J. Cruz, P. Chakraborty, and S. Bhunia, "Hardware ip trust validation: Learn (the untrustworthy), and verify," in *2018 IEEE International Test Conference (ITC)*, pp. 1–10, IEEE, 2018.

[225] M. Hasan, J. Cruz, P. Chakraborty, S. Bhunia, and T. Hoque, "Trojan resilient computing in cots processors under zero trust," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 30, no. 10, pp. 1412–1424, 2022.

[226] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology—CRYPTO'99: 19th Annual International Cryptology Conference Santa Barbara, California, USA, August 15–19, 1999 Proceedings 19*, pp. 388–397, Springer, 1999.

[227] B. J. Gilbert Goodwill, J. Jaffe, P. Rohatgi, *et al.*, "A testing methodology for side-channel resistance validation," in *NIST non-invasive attack testing workshop*, vol. 7, pp. 115–136, 2011.

[228] S. Mangard, T. Popp, and B. M. Gammel, "Side-channel leakage of masked cmos gates," in *Cryptographers' Track at the RSA Conference*, pp. 351–365, Springer, 2005.

[229] S. Chari, J. R. Rao, and P. Rohatgi, "Template attacks," in *Cryptographic hardware and embedded systems-CHES 2002: 4th International Workshop Redwood Shores, CA, USA, August 13–15, 2002 Revised Papers 4*, pp. 13–28, Springer, 2003.

[230] J.-J. Quisquater and D. Samyde, "Electromagnetic analysis (ema): Measures and counter-measures for smart cards," in *Smart Card Programming and Security: International Conference on Research in Smart Cards, E-smart 2001 Cannes, France, September 19–21, 2001 Proceedings*, pp. 200–210, Springer, 2001.

[231] P. C. Kocher, "Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems," in *Advances in Cryptology—CRYPTO'96: 16th Annual International Cryptology Conference Santa Barbara, California, USA August 18–22, 1996 Proceedings 16*, pp. 104–113, Springer, 1996.

[232] J. Bonneau and I. Mironov, "Cache-collision timing attacks against aes," in *Cryptographic Hardware and Embedded Systems-CHES 2006: 8th International Workshop, Yokohama, Japan, October 10-13, 2006. Proceedings 8*, pp. 201–215, Springer, 2006.

[233] P. Chakraborty, J. Cruz, C. Posada, S. Ray, and S. Bhunia, "Haste: Software security analysis for timing attacks on clear hardware assumption," *IEEE Embedded Systems Letters*, vol. 14, no. 2, pp. 71–74, 2021.

[234] X. Wang, W. Yueh, D. B. Roy, S. Narasimhan, Y. Zheng, S. Mukhopadhyay, D. Mukhopadhyay, and S. Bhunia, "Role of power grid in side channel attack and power-grid-aware secure design," in *Proceedings of the 50th Annual Design Automation Conference*, DAC '13, (New York, NY, USA), Association for Computing Machinery, 2013.

[235] M. Randolph and W. Diehl, "Power side-channel attack analysis: A review of 20 years of study for the layman," *Cryptography*, vol. 4, no. 2, p. 15, 2020.

[236] Y. Fei, A. A. Ding, J. Lao, and L. Zhang, "A statistics-based success rate model for dpa and cpa," *Journal of Cryptographic Engineering*, vol. 5, pp. 227–243, 2015.

[237] C. O'Flynn and Z. D. Chen, "Side channel power analysis of an aes-256 bootloader," in *2015 IEEE 28th Canadian Conference on Electrical and Computer Engineering (CCECE)*, pp. 750–755, IEEE, 2015.

[238] L. Wei, B. Luo, Y. Li, Y. Liu, and Q. Xu, "I know what you see: Power side-channel attack on convolutional neural network accelerators," in *Proceedings of the 34th Annual Computer Security Applications Conference*, pp. 393–406, 2018.

[239] M. Méndez Real and R. Salvador, "Physical side-channel attacks on embedded neural networks: A survey," *Applied Sciences*, vol. 11, no. 15, p. 6790, 2021.

[240] S. Vuppala, A. E.-D. Mady, and A. Kuenzi, "Moving target defense mechanism for side-channel attacks," *IEEE Systems Journal*, vol. 14, no. 2, pp. 1810–1819, 2019.

[241] S. Maji, U. Banerjee, and A. P. Chandrakasan, "Leaky nets: Recovering embedded neural network models and inputs through simple power and timing side-channels—attacks and defenses," *IEEE Internet of Things Journal*, vol. 8, no. 15, pp. 12079–12092, 2021.

[242] R. Sadhukhan, S. Saha, S. Paria, S. Bhunia, and D. Mukhopadhyay, "Valiant: An eda flow for side-channel leakage evaluation and tailored protection," *IEEE Transactions on Computers*, 2023.

[243] E. Trichina, "Combinational logic design for aes subbyte transformation on masked data," *Cryptology ePrint Archive*, 2003.

[244] H. Groß, S. Mangard, and T. Korak, "Domain-oriented masking: Compact masked hardware implementations with arbitrary protection order," *Cryptology ePrint Archive*, 2016.

[245] B. Erbagci, C. Erbagci, N. E. C. Akkaya, and K. Mai, "A secure camouflaged threshold voltage defined logic family," in *2016 IEEE International symposium on hardware oriented security and trust (HOST)*, pp. 229–235, IEEE, 2016.

[246] J. Longo, E. De Mulder, D. Page, and M. Tunstall, "Soc it to em: electromagnetic side-channel attacks on a complex system-on-chip," in *Cryptographic Hardware and Embedded Systems–CHES 2015: 17th International Workshop, Saint-Malo, France, September 13-16, 2015, Proceedings 17*, pp. 620–640, Springer, 2015.

[247] A. Sayakkara, N.-A. Le-Khac, and M. Scanlon, "A survey of electromagnetic side-channel attacks and discussion on their case-progressing potential for digital forensics," *Digital Investigation*, vol. 29, pp. 43–54, 2019.

[248] R. Jevtic and M. G. Otero, "Methodology for complete decorrelation of power supply em side-channel signal and sensitive data," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 69, no. 4, pp. 2256–2260, 2022.

[249] G. Camurati, S. Poeplau, M. Muench, T. Hayes, and A. Francillon, "Screaming channels: When electromagnetic side channels meet radio transceivers," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pp. 163–177, 2018.

[250] S. Maji, U. Banerjee, S. H. Fuller, and A. P. Chandrakasan, "A threshold implementation-based neural network accelerator with power and electromagnetic side-channel countermeasures," *IEEE Journal of Solid-State Circuits*, vol. 58, no. 1, pp. 141–154, 2022.

[251] Y. Gao, Q. Zhang, H. Ma, J. He, and Y. Zhao, "Eo-shield: A multi-function protection scheme against side channel and focused ion beam attacks," in *Proceedings of the 28th Asia and South Pacific Design Automation Conference*, pp. 670–675, 2023.

[252] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, pp. 1–33, 2011.

[253] A. Lamas-Linares and C. Kurtsiefer, "Breaking a quantum key distribution system through a timing side channel," *Optics express*, vol. 15, no. 15, pp. 9388–9393, 2007.

[254] R. Hund, C. Willems, and T. Holz, "Practical timing side channel attacks against kernel space aslr," in *2013 IEEE Symposium on Security and Privacy*, pp. 191–205, IEEE, 2013.

[255] H. Chabanne, J.-L. Danger, L. Guiga, and U. Kühne, "Side channel attacks for architecture extraction of neural networks," *CAAI Transactions on Intelligence Technology*, vol. 6, no. 1, pp. 3–16, 2021.

[256] P. Chakraborty, T. Suha, and S. Bhunia, "Hardware specification aware timing side channel security analysis," in *2023 IEEE 36th International System-on-Chip Conference (SOCC)*, pp. 1–6, IEEE, 2023.

[257] T. Zhang, Y. Zhang, and R. B. Lee, "Cloudradar: A real-time side-channel attack detection system in clouds," in *Research in Attacks, Intrusions, and Defenses: 19th International Symposium, RAID 2016, Paris, France, September 19-21, 2016, Proceedings 19*, pp. 118–140, Springer, 2016.

[258] V. Varadarajan, T. Ristenpart, and M. Swift, "Scheduler-based defenses against cross-vm side-channels," in *23rd {USENIX} Security Symposium ({USENIX} Security 14)*, pp. 687–702, 2014.

[259] O. Reparaz, J. Balasch, and I. Verbauwhede, "Dude, is my code constant time?," in *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2017*, pp. 1697–1702, IEEE, 2017.

[260] Ansible, "Ansible documentation," Dec 2022. https://docs.ansible.com/ansible/latest/index.html.

[261] P. Finley, Y. Wang, and J. Cropper, "Ansible automation for ibm power systems," May 2020. url: https://developer.ibm.com/tutorials/ansible-automation-for-power/.

[262] RedHat and . Hashicorp, "Hashicorp Terraform and Red Hat Ansible Automation." https://shorturl.at/2s5gL.

[263] S. J. Taylor, A. Anagnostou, T. Kiss, G. Terstyanszky, P. Kacsuk, and N. Fantini, "A tutorial on cloud computing for agent-based modeling i& simulation with repast," vol. 2015-January, pp. 192–206, Institute of Electrical and Electronics Engineers Inc., 1 2015.

[264] D. Zehe, A. Knoll, W. Cai, and H. Aydt, "Semsim cloud service: Large-scale urban systems simulation in the cloud," *Simulation Modelling Practice and Theory*, vol. 58, pp. 157–171, 11 2015.

[265] M. Forcan and M. Maksimović, "Cloud-fog-based approach for smart grid monitoring," *Simulation Modelling Practice and Theory*, vol. 101, p. 101988, 2020.

[266] A. H. Rabie, A. I. Saleh, and H. A. Ali, "Smart electrical grids based on cloud, iot, and big data technologies: state of the art," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 10, pp. 9449–9480, 2021.

[267] S. Zhang, A. Pandey, X. Luo, M. Powell, R. Banerji, L. Fan, A. Parchure, and E. Luzcando, "Practical adoption of cloud computing in power systems—drivers, challenges, guidance, and real-world use cases," *IEEE Transactions on Smart Grid*, vol. 13, no. 3, pp. 2390–2411, 2022.

[268] O. Bentaleb, A. S. Belloum, A. Sebaa, and A. El-Maouhab, "Containerization technologies: Taxonomies, applications and challenges," *The Journal of Supercomputing*, vol. 78, no. 1, pp. 1144–1181, 2022.

[269] Z. Chen, A. M. Amani, X. Yu, and M. Jalili, "Control and optimisation of power grids using smart meter data: A review," *Sensors*, vol. 23, no. 4, p. 2118, 2023.

[270] Y. Yang, W. Shen, B. Ruan, W. Liu, and K. Ren, "Security challenges in the container cloud," in *2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, pp. 137–145, IEEE, 2021.

[271] A. Mosavi, M. Salimi, S. Faizollahzadeh Ardabili, T. Rabczuk, S. Shamshirband, and A. R. Varkonyi-Koczy, "State of the art of machine learning models in energy systems, a systematic review," *Energies*, vol. 12, no. 7, p. 1301, 2019.

[272] A. K. Ozcanli, F. Yaprakdal, and M. Baysal, "Deep learning methods and applications for electrical power systems: A comprehensive review," *International Journal of Energy Research*, vol. 44, no. 9, pp. 7136–7157, 2020.

[273] M. J. Zideh, P. Chatterjee, and A. K. Srivastava, "Physics-informed machine learning for data anomaly detection, classification, localization, and mitigation: A review, challenges, and path forward," *IEEE Access*, 2023.

[274] G. S. Misyris, A. Venzke, and S. Chatzivasileiadis, "Physics-informed neural networks for power systems," in *2020 IEEE power & energy society general meeting (PESGM)*, pp. 1–5, IEEE, 2020.

[275] B. Huang and J. Wang, "Applications of physics-informed neural networks in power systems-a review," *IEEE Transactions on Power Systems*, vol. 38, no. 1, pp. 572–588, 2022.

[276] M. Mohri, G. Sivek, and A. T. Suresh, "Agnostic federated learning," in *International Conference on Machine Learning*, pp. 4615–4625, PMLR, 2019.

[277] X. Zhang, F. Fang, and J. Wang, "Probabilistic solar irradiation forecasting based on variational bayesian inference with secure federated learning," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 7849–7859, 2020.

[278] S. Lee and D.-H. Choi, "Federated reinforcement learning for energy management of multiple smart homes with distributed energy resources," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 1, pp. 488–497, 2020.

[279] M. Liang, Y. Meng, J. Wang, D. L. Lubkeman, and N. Lu, "Feedergan: Synthetic feeder generation via deep graph adversarial nets," *IEEE Transactions on Smart Grid*, vol. 12, no. 2, pp. 1163–1173, 2020.

[280] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, and H. V. Poor, "Federated learning for internet of things: A comprehensive survey," *IEEE Communications Surveys and Tutorials*, vol. 23, no. 3, pp. 1622–1658, 2021.

[281] J. Jithish, B. Alangot, N. Mahalingam, and K. S. Yeo, "Distributed anomaly detection in smart grids: a federated learning-based approach," *IEEE Access*, vol. 11, pp. 7157–7179, 2023.

[282] Y. Li, X. Wei, Y. Li, Z. Dong, and M. Shahidehpour, "Detection of false data injection attacks in smart grid: A secure federated deep

learning approach," *IEEE Transactions on Smart Grid*, vol. 13, no. 6, pp. 4862–4872, 2022.
[283] J. Wang, Y. Si, Y. Zhu, K. Zhang, S. Yin, and B. Liu, "Cyberattack detection for electricity theft in smart grids via stacking ensemble gru optimization algorithm using federated learning framework," *International Journal of Electrical Power & Energy Systems*, vol. 157, p. 109848, 2024.
[284] B. Blakely, H. Billings, N. Evans, A. Landry, and A. Domingo, "Evaluation of an autonomous intelligent cyberdefense agent at nato cyber coalition exercise 2022," in *Disruptive Technologies in Information Sciences VII*, vol. 12542, pp. 80–93, SPIE, 2023.
[285] J. Laird, "Introduction to the soar cognitive architecture," tech. rep., Technical report, Technical Report, 2022.
[286] J. E. Laird, "An analysis and comparison of act-r and soar," *arXiv preprint arXiv:2201.09305*, 2022.
[287] M. News, ""it's like the early days of the internet," blockchain-based brooklyn microgrid tests p2p energy trading - microgrid media," Mar 2016.
[288] Y. Ding, J. Jin, J. Zhang, Z. Wu, and K. Hu, "Sc-rbac: a smart contract based rbac model for dapps," in *Human Centered Computing: 5th International Conference, HCC 2019, Čačak, Serbia, August 5–7, 2019, Revised Selected Papers 5*, pp. 75–85, Springer, 2019.
[289] M. Mylrea, S. N. G. Gourisetti, *et al.*, "Blockchain: Next generation supply chain security for energy infrastructure and nerc critical infrastructure protection (cip) compliance," *Resilience Week*, vol. 16, 2018.
[290] J. Choi, B. Ahn, G. Bere, S. Ahmad, H. A. Mantooth, and T. Kim, "Blockchain-based man-in-the-middle (mitm) attack detection for photovoltaic systems," in *2021 IEEE Design Methodologies Conference (DMC)*, pp. 1–6, IEEE, 2021.
[291] J. Choi, B. Ahn, S. Pedavalli, S. Ahmad, A. Villasenor, and T. Kim, "Secure firmware update and device authentication for smart inverters using blockchain and phyiscally uncloable function (puf)-embedded security module," in *2021 6th IEEE Workshop on the Electronic Grid (eGRID)*, pp. 01–04, IEEE, 2021.
[292] P. Ciampoli, "Blockchain rec trading platform set to launch in the u.s.," Feb 2020.
[293] T. Gaybullaev, H.-Y. Kwon, T. Kim, and M.-K. Lee, "Efficient and privacy-preserving energy trading on blockchain using dual binary encoding for inner product encryption," *Sensors*, vol. 21, no. 6, p. 2024, 2021.
[294] A. Hadi, G. Bere, B. Ahn, and T. Kim, "Smart contract-defined control and co-simulation for smart inverters in a photovoltaic (pv) system and blockchain network," in *Proc. 2020 IEEE CyberPELS Workshop*, pp. 1–6, 2020.
[295] C. Lima, H. Albright, P. D. Heitmann, B. Llc, and T. Martinez, "IEEE BCTE Steering Committee," 2021.
[296] Q. Yang and H. Wang, "Exploring blockchain for the coordination of distributed energy resources," in *2021 55th Annual Conference on Information Sciences and Systems (CISS)*, pp. 1–6, IEEE, 2021.
[297] G. van Leeuwen, T. AlSkaif, M. Gibescu, and W. van Sark, "An integrated blockchain-based energy management platform with bilateral trading for microgrid communities," *Applied Energy*, vol. 263, p. 114613, 2020.
[298] S. Ahmad, B. Ahn, T. Kim, J. Choi, M. Chae, D. Han, and D. Won, "Blockchain-integrated resilient distributed energy resources management system," in *2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, pp. 59–64, IEEE, 2022.
[299] A. Steane, "Quantum computing," *Reports on Progress in Physics*, vol. 61, no. 2, p. 117, 1998.
[300] C. Gidney and M. Ekerå, "How to factor 2048 bit rsa integers in 8 hours using 20 million noisy qubits," *Quantum*, vol. 5, p. 433, 2021.
[301] J. Tangpanitanon, "Use cases of quantum computing in the energy industry," Aug.
[302] Y. Zhou, Z. Tang, N. Nikmehr, P. Babahajiani, F. Feng, T.-C. Wei, H. Zheng, and P. Zhang, "Quantum computing in power systems," *iEnergy*, vol. 1, pp. 170–187, 7 2022.
[303] "National security memorandum on promoting united states leadership in quantum computing while mitigating risks to vulnerable cryptographic systems," May 2022.
[304] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of modern physics*, vol. 74, no. 1, p. 145, 2002.
[305] R. G. Bace, P. Mell, *et al.*, "Intrusion detection systems," 2001.
[306] B. Blakely, "Cyber senses: Modeling network situational awareness after biology," in *2021 Resilience Week (RWS)*, pp. 1–8, IEEE, 2021.
[307] J. Valenzuela, J. Wang, and N. Bissinger, "Real-time intrusion detection in power system operations," *IEEE Transactions on Power Systems*, vol. 28, no. 2, pp. 1052–1062, 2012.
[308] U. Adhikari, T. H. Morris, and S. Pan, "A cyber-physical power system test bed for intrusion detection systems," in *2014 IEEE PES General Meeting— Conference & Exposition*, pp. 1–5, IEEE, 2014.
[309] Y. Yang, K. McLaughlin, S. Sezer, T. Littler, E. G. Im, B. Pranggono, and H. Wang, "Multiattribute scada-specific intrusion detection system for power networks," *IEEE Transactions on Power Delivery*, vol. 29, no. 3, pp. 1092–1102, 2014.
[310] IBM, "X-force threat intelligence index 2022 2," 2022.
[311] D. Bin, S. Ming, C. Yang, H. Fu, and Y. Ling, "Optimization design of zero trust network architecture for new power systems," in *Proceedings of the 2024 3rd International Conference on Cryptography, Network Security and Communication Technology*, pp. 282–286, 2024.
[312] M. M. Pour, A. Anzalchi, and A. Sarwat, "A review on cyber security issues and mitigation methods in smart grid systems," *SoutheastCon 2017*, pp. 1–4, 2017.
[313] N. I. of Standards and Technology, "cyber resiliency - glossary — csrc," Feb 2020.
[314] I. Linkov and A. Kott, "Fundamental concepts of cyber resilience: Introduction and overview," *Cyber resilience of systems and networks*, pp. 1–25, 2019.
[315] M. Izadi, S. H. Hosseinian, S. Dehghan, A. Fakharian, and N. Amjady, "A critical review on definitions, indices, and uncertainty characterization in resiliency-oriented operation of power systems," *International Transactions on Electrical Energy Systems*, vol. 31, no. 1, p. e12680, 2021.
[316] N. Voropai and C. Rehtanz, "Flexibility and resiliency of electric power systems: Analysis of definitions and content," in *EPJ Web of Conferences*, vol. 217, p. 01018, EDP Sciences, 2019.
[317] I. Linkov, A. Ligo, K. Stoddard, B. Perez, A. Strelzoffx, E. Bellini, and A. Kott, "Cyber efficiency and cyber resilience," *Communications of the ACM*, vol. 66, no. 4, pp. 33–37, 2023.
[318] M. Z. Serdar and S. G. Al-Ghamdi, "Preparing for the unpredicted: A resiliency approach in energy system assessment," in *Energy Systems Evaluation (Volume 1) Sustainability Assessment*, pp. 183–201, Springer, 2021.
[319] Rapid7, *How Rapid7 Supports ISO 27002 Controls*. 2023. https://shorturl.at/ZkJ4X.
[320] C. I. S. R. Lab, *Securing industrial networks: What is ISA/IEC 62443?* 2021. https://tinyurl.com/j882dyn3.
[321] *Guidelines for Smart Grid Cybersecurity*. https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf.
[322] D. of Energy, *Cybersecurity Capability Maturity Model*. Jun 2022. https://shorturl.at/oTvQo.
[323] IEEE, "Ieee standard for intelligent electronic devices cybersecurity capabilities," *IEEE Std 1686-2022 (Revision of IEEE Std 1686-2013)*, pp. 1–36, 2023.
[324] D. He, S. Chan, and M. Guizani, "Cyber security analysis and protection of wireless sensor networks for smart grid monitoring," *IEEE Wireless Communications*, vol. 24, no. 6, pp. 98–103, 2017.
[325] M. Alonso, H. Amaris, D. Alcala, and D. M. Florez R, "Smart sensors for smart grid reliability," *Sensors*, vol. 20, no. 8, p. 2187, 2020.
[326] . Microsoft, "Evolving zero trust," Nov 2021.
[327] N. N. A. Sjarif, S. Chuprat, M. N. Mahrin, N. A. Ahmad, A. Ariffin, F. M. Senan, N. A. Zamani, and A. Saupi, "Endpoint detection and response: Why use machine learning?," in *2019 International Conference on Information and Communication Technology Convergence (ICTC)*, pp. 283–288, IEEE, 2019.
[328] S. Perez, "Practical siem tools for scada environment," 2018.
[329] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–physical system security for the electric power grid," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210–224, 2011.
[330] S. S. Kim and Y. J. Kim, "The effect of compliance knowledge and compliance support systems on information security compliance behavior," *Journal of Knowledge Management*, 2017.
[331] R. S. Sandhu and P. Samarati, "Access control: principle and practice," *IEEE communications magazine*, vol. 32, no. 9, pp. 40–48, 1994.
[332] R. Vanickis, P. Jacob, S. Dehghanzadeh, and B. Lee, "Access control policy enforcement for zero-trust-networking," in *2018 29th Irish Signals and Systems Conference (ISSC)*, pp. 1–6, IEEE, 2018.
[333] J. T. Johnson, "Recommendations for distributed energy resource access control," tech. rep., Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), 2021.
[334] R. Chandramouli, *Guide to a Secure Enterprise Network Landscape*. Nov 2022.

[335] G. Cohen, "Throwback attack: Kemuri water company attack puts critical infrastructure at risk - industrial cybersecurity pulse," Feb 2022.

[336] S.-C. Yip, W.-N. Tan, C. Tan, M.-T. Gan, and K. Wong, "An anomaly detection framework for identifying energy theft and defective meters in smart grids," *International Journal of Electrical Power and Energy Systems*, vol. 101, pp. 189–203, 2018.

[337] G. Fenza, M. Gallo, and V. Loia, "Drift-aware methodology for anomaly detection in smart grid," *IEEE Access*, vol. 7, pp. 9645–9657, 2019.

[338] M. Yamauchi, Y. Ohsita, M. Murata, K. Ueda, and Y. Kato, "Anomaly detection in smart home operation from user behaviors and home conditions," *IEEE Transactions on Consumer Electronics*, vol. 66, no. 2, pp. 183–192, 2020.

[339] S.-V. Oprea, A. Bâra, F. C. Puican, and I. C. Radu, "Anomaly detection with machine learning algorithms and big data in electricity consumption," *Sustainability*, vol. 13, no. 19, p. 10963, 2021.

[340] J. Tian, B. Wang, J. Li, and C. Konstantinou, "Adversarial attack and defense methods for neural network based state estimation in smart grid," *IET Renewable Power Generation*, vol. 16, no. 16, pp. 3507–3518, 2022.

[341] B. Biggio and F. Roli, "Wild patterns: Ten years after the rise of adversarial machine learning," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pp. 2154–2156, 2018.

[342] G. Apruzzese, H. S. Anderson, S. Dambra, D. Freeman, F. Pierazzi, and K. Roundy, ""real attackers don't compute gradients": bridging the gap between adversarial ml research and practice," in *2023 IEEE Conference on Secure and Trustworthy Machine Learning (SaTML)*, pp. 339–364, IEEE, 2023.

[343] M. Sadeghi and E. G. Larsson, "Physical adversarial attacks against end-to-end autoencoder communication systems," *IEEE Communications Letters*, vol. 23, no. 5, pp. 847–850, 2019.

[344] A. Ghasemi, E. Zeraatkar, M. Moradikia, and S. R. Zekavat, "Adversarial attacks on resource management in p2p wireless communications," in *2023 IEEE International Conference on Wireless for Space and Extreme Environments (WiSEE)*, pp. 148–153, IEEE, 2023.

[345] E. Anthi, L. Williams, M. Rhode, P. Burnap, and A. Wedgbury, "Adversarial attacks on machine learning cybersecurity defences in industrial control systems," *Journal of Information Security and Applications*, vol. 58, p. 102717, 2021.

[346] A. S. Awad, I. R. Alkhouri, and G. K. Atia, "Adversarial attacks on multi-level fault detection and diagnosis systems," in *2021 IEEE 31st International Workshop on Machine Learning for Signal Processing (MLSP)*, pp. 1–6, IEEE, 2021.

[347] G. Apruzzese, R. Vladimirov, A. Tastemirova, and P. Laskov, "Wild networks: Exposure of 5g network infrastructures to adversarial examples," *IEEE Transactions on Network and Service Management*, vol. 19, no. 4, pp. 5312–5332, 2022.

[348] H. Qiu, T. Dong, T. Zhang, J. Lu, G. Memmi, and M. Qiu, "Adversarial attacks against network intrusion detection in iot systems," *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10327–10335, 2020.

[349] N. Tang, S. Mao, and R. M. Nelms, "Adversarial attacks to solar power forecast," in *2021 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, IEEE, 2021.

[350] R. Heinrich, C. Scholz, S. Vogt, and M. Lehna, "Targeted adversarial attacks on wind power forecasts," *Machine Learning*, vol. 113, no. 2, pp. 863–889, 2024.

[351] M. Pintor, L. Demetrio, A. Sotgiu, A. Demontis, N. Carlini, B. Biggio, and F. Roli, "Indicators of attack failure: Debugging and improving optimization of adversarial examples," *Advances in Neural Information Processing Systems*, vol. 35, pp. 23063–23076, 2022.

[352] N. Carlini and D. Wagner, "Defensive distillation is not robust to adversarial examples," *arXiv preprint arXiv:1607.04311*, 2016.

[353] F. Tramèr, D. Boneh, A. Kurakin, I. Goodfellow, N. Papernot, and P. McDaniel, "Ensemble adversarial training: Attacks and defenses," in *6th International Conference on Learning Representations, ICLR 2018-Conference Track Proceedings*, 2018.

[354] A. Shafahi, M. Najibi, M. A. Ghiasi, Z. Xu, J. Dickerson, C. Studer, L. S. Davis, G. Taylor, and T. Goldstein, "Adversarial training for free!," *Advances in neural information processing systems*, vol. 32, 2019.

[355] G. Apruzzese, M. Andreolini, L. Ferretti, M. Marchetti, and M. Colajanni, "Modeling realistic adversarial attacks against network intrusion detection systems," *Digital Threats: Research and Practice (DTRAP)*, vol. 3, no. 3, pp. 1–19, 2022.

[356] A. Dua, N. Bulusu, W.-C. Feng, and W. Hu, "Towards trustworthy participatory sensing," in *Proceedings of the 4th USENIX Conference on Hot Topics in Security*, 2009.

[357] B. Zhao and Y. Lao, "Clpa: Clean-label poisoning availability attacks using generative adversarial nets," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 36, pp. 9162–9170, 2022.

[358] K. Doan, Y. Lao, W. Zhao, and P. Li, "Lira: Learnable, imperceptible and robust backdoor attacks," in *Proceedings of the IEEE/CVF international conference on computer vision*, pp. 11966–11976, 2021.

[359] G. Severi, S. Boboila, A. Oprea, J. Holodnak, K. Kratkiewicz, and J. Matterer, "Poisoning network flow classifiers," in *Proceedings of the 39th Annual Computer Security Applications Conference*, pp. 337–351, 2023.

[360] M. Kravchik, L. Demetrio, B. Biggio, and A. Shabtai, "Practical evaluation of poisoning attacks on online anomaly detectors in industrial control systems," *Computers & Security*, vol. 122, p. 102901, 2022.

[361] M. Padilla, A. Perera, I. Montoliu, A. Chaudry, K. Persaud, and S. Marco, "Fault detection, identification, and reconstruction of faulty chemical gas sensors under drift conditions, using principal component analysis and multiscale-pca," in *The 2010 International Joint Conference on Neural Networks (IJCNN)*, pp. 1–7, IEEE, 2010.

[362] Y. Liang, D. He, and D. Chen, "Poisoning attack on load forecasting," in *2019 IEEE innovative smart grid technologies-Asia (ISGT Asia)*, pp. 1230–1235, IEEE, 2019.

[363] R. S. S. Kumar, M. Nyström, J. Lambert, A. Marshall, M. Goertzel, A. Comissoneru, M. Swann, and S. Xia, "Adversarial machine learning-industry perspectives," in *2020 IEEE security and privacy workshops (SPW)*, pp. 69–75, IEEE, 2020.

[364] Y. M. Saputra, D. T. Hoang, D. N. Nguyen, E. Dutkiewicz, M. D. Mueck, and S. Srikanteswara, "Energy demand prediction with federated learning for electric vehicle networks," in *2019 IEEE global communications conference (GLOBECOM)*, pp. 1–6, IEEE, 2019.

[365] J. Chen, X. Zhang, R. Zhang, C. Wang, and L. Liu, "De-pois: An attack-agnostic defense against data poisoning attacks," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3412–3425, 2021.

[366] X. Li, Z. Qu, S. Zhao, B. Tang, Z. Lu, and Y. Liu, "Lomar: A local defense against poisoning attack on federated learning," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 1, pp. 437–450, 2021.

[367] C. Wang, J. Chen, Y. Yang, X. Ma, and J. Liu, "Poisoning attacks and countermeasures in intelligent networks: Status quo and prospects," *Digital Communications and Networks*, vol. 8, no. 2, pp. 225–234, 2022.

[368] A. E. Cinà, K. Grosse, A. Demontis, S. Vascon, W. Zellinger, B. A. Moser, A. Oprea, B. Biggio, M. Pelillo, and F. Roli, "Wild patterns reloaded: A survey of machine learning security against training data poisoning," *ACM Computing Surveys*, vol. 55, no. 13s, pp. 1–39, 2023.

[369] K. Huang, Y. Li, B. Wu, Z. Qin, and K. Ren, "Backdoor defense via decoupling the training process," in *International Conference on Learning Representations*, 2022.

[370] W. Chen, B. Wu, and H. Wang, "Effective backdoor defense by exploiting sensitivity of poisoned samples," *Advances in Neural Information Processing Systems*, vol. 35, pp. 9727–9737, 2022.

[371] S. Wang, K. Fan, K. Zhang, H. Li, and Y. Yang, "Data complexity-based batch sanitization method against poison in distributed learning," *Digital Communications and Networks*, vol. 10, no. 2, pp. 416–428, 2024.

[372] T. Braun, I. Pekaric, and G. Apruzzese, "Understanding the process of data labeling in cybersecurity," in *Proceedings of the 39th ACM/SIGAPP Symposium on Applied Computing*, pp. 1596–1605, 2024.

[373] V. Shejwalkar and A. Houmansadr, "Manipulating the byzantine: Optimizing model poisoning attacks and defenses for federated learning," in *NDSS*, 2021.

[374] Y. Wan, Y. Qu, W. Ni, Y. Xiang, L. Gao, and E. Hossain, "Data and model poisoning backdoor attacks on wireless federated learning, and the defense mechanisms: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, 2024.

[375] D. Oliynyk, R. Mayer, and A. Rauber, "I know what you trained last summer: A survey on stealing machine learning models and defences," *ACM Computing Surveys*, vol. 55, no. 14s, pp. 1–41, 2023.

[376] F. Tramèr, F. Zhang, A. Juels, M. K. Reiter, and T. Ristenpart, "Stealing machine learning models via prediction {APIs}," in *25th USENIX security symposium (USENIX Security 16)*, pp. 601–618, 2016.

[377] Y. Gao, H. Qiu, Z. Zhang, B. Wang, H. Ma, A. Abuadbba, M. Xue, A. Fu, and S. Nepal, "Deeptheft: Stealing dnn model architectures through power side channel," in *2024 IEEE Symposium on Security and Privacy (SP)*, pp. 3311–3326, IEEE, 2024.

[378] A. S. Rakin, M. H. I. Chowdhuryy, F. Yao, and D. Fan, "Deepsteal: Advanced model extractions leveraging efficient weight stealing in memories," in *2022 IEEE symposium on security and privacy (SP)*, pp. 1157–1174, IEEE, 2022.

[379] S. Sanyal, S. Addepalli, and R. V. Babu, "Towards data-free model stealing in a hard label setting," in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, pp. 15284–15293, 2022.

[380] T. Lee, B. Edwards, I. Molloy, and D. Su, "Defending against neural network model stealing attacks using deceptive perturbations," in *2019 IEEE Security and Privacy Workshops (SPW)*, pp. 43–49, IEEE, 2019.

[381] B. F. Goldstein, V. C. Patil, V. C. Ferreira, A. S. Nery, F. M. França, and S. Kundu, "Preventing dnn model ip theft via hardware obfuscation," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 11, no. 2, pp. 267–277, 2021.

[382] X. Liu, T. Liu, H. Yang, J. Dong, Z. Ying, and Z. Ma, "Model stealing detection for iot services based on multi-dimensional features," *IEEE Internet of Things Journal*, 2024.

[383] H. Zhu, S. Liang, W. Hu, L. Fangqi, J. Jia, and S.-L. Wang, "Reliable model watermarking: Defending against theft without compromising on evasion," in *Proceedings of the 32nd ACM International Conference on Multimedia*, pp. 10124–10133, 2024.

[384] R. Shokri, M. Stronati, C. Song, and V. Shmatikov, "Membership inference attacks against machine learning models," in *2017 IEEE symposium on security and privacy (SP)*, pp. 3–18, IEEE, 2017.

[385] L. Hu, A. Yan, H. Yan, J. Li, T. Huang, Y. Zhang, C. Dong, and C. Yang, "Defenses to membership inference attacks: A survey," *ACM Computing Surveys*, vol. 56, no. 4, pp. 1–34, 2023.

[386] X. Tang, S. Mahloujifar, L. Song, V. Shejwalkar, M. Nasr, A. Houmansadr, and P. Mittal, "Mitigating membership inference attacks by {Self-Distillation} through a novel ensemble architecture," in *31st USENIX Security Symposium (USENIX Security 22)*, pp. 1433–1450, 2022.

[387] H. Hu, Z. Salcic, L. Sun, G. Dobbie, P. S. Yu, and X. Zhang, "Membership inference attacks on machine learning: A survey," *ACM Computing Surveys (CSUR)*, vol. 54, no. 11s, pp. 1–37, 2022.

[388] M. Maabreh, A. Maabreh, B. Qolomany, and A. Al-Fuqaha, "The robustness of popular multiclass machine learning models against poisoning attacks: Lessons and insights," *International Journal of Distributed Sensor Networks*, vol. 18, no. 7, p. 15501329221105159, 2022.

[389] A. Loquercio, M. Segu, and D. Scaramuzza, "A general framework for uncertainty estimation in deep learning," *IEEE Robotics and Automation Letters*, vol. 5, no. 2, pp. 3153–3160, 2020.

[390] U. S. Shanthamallu, J. J. Thiagarajan, and A. Spanias, "Uncertainty-matching graph neural networks to defend against poisoning attacks," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 35, pp. 9524–9532, 2021.

[391] S. Liu, A. C. Cullen, P. Montague, S. M. Erfani, and B. I. Rubinstein, "Enhancing the antidote: improved pointwise certifications against poisoning attacks," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 37, pp. 8861–8869, 2023.

[392] F. Barbero, F. Pendlebury, F. Pierazzi, and L. Cavallaro, "Transcending transcend: Revisiting malware classification in the presence of concept drift," in *2022 IEEE Symposium on Security and Privacy (SP)*, pp. 805–823, IEEE, 2022.

[393] C. Ni, N. Charoenphakdee, J. Honda, and M. Sugiyama, "On the calibration of multiclass classification with rejection," *Advances in Neural Information Processing Systems*, vol. 32, 2019.

[394] C. Zhong, T. Lin, P. Liu, J. Yen, and K. Chen, "A cyber security data triage operation retrieval system," *Computers & Security*, vol. 76, pp. 12–31, 2018.

[395] A. Takiddin, M. Ismail, U. Zafar, and E. Serpedin, "Robust electricity theft detection against data poisoning attacks in smart grids," *IEEE Transactions on Smart Grid*, vol. 12, no. 3, pp. 2675–2684, 2020.

[396] A. Shafahi, W. R. Huang, M. Najibi, O. Suciu, C. Studer, T. Dumitras, and T. Goldstein, "Poison frogs! targeted clean-label poisoning attacks on neural networks," *Advances in neural information processing systems*, vol. 31, 2018.

[397] H. Zeng, Z. Yue, Y. Zhang, L. Shang, and D. Wang, "Manipulating out-domain uncertainty estimation in deep neural networks via targeted clean-label poisoning," in *Proceedings of the 32nd ACM International Conference on Information and Knowledge Management*, pp. 3114–3123, 2023.

[398] M. Goldblum, D. Tsipras, C. Xie, X. Chen, A. Schwarzschild, D. Song, A. Madry, B. Li, and T. Goldstein, "Dataset security for machine learning: Data poisoning, backdoor attacks, and defenses," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 45, no. 2, pp. 1563–1580, 2022.

[399] . Department of Energy, "Demand response," 2023. https://shorturl.at/FFg2V.

[400] A. Nawaz, M. Zhou, J. Wu, and C. Long, "A comprehensive review on energy management, demand response, and coordination schemes utilization in multi-microgrids network," *Applied Energy*, vol. 323, p. 119596, 2022.

[401] L. Zeng, D. Qiu, and M. Sun, "Resilience enhancement of multi-agent reinforcement learning-based demand response against adversarial attacks," *Applied Energy*, vol. 324, p. 119688, 2022.

[402] E. I. Zountouridou, G. C. Kiokes, N. D. Hatziargyriou, and N. K. Uzunoglu, "An evaluation study of wireless access technologies for v2g communications," in *2011 16th International Conference on Intelligent System Applications to Power Systems*, pp. 1–7, IEEE, 2011.

[403] A. Dutta and S. Debbarma, "Frequency regulation in deregulated market using vehicle-to-grid services in residential distribution network," *IEEE Systems Journal*, vol. 12, no. 3, pp. 2812–2820, 2017.

[404] J. Li, R. Xiong, Q. Yang, F. Liang, M. Zhang, and W. Yuan, "Design/test of a hybrid energy storage system for primary frequency control using a dynamic droop method in an isolated microgrid power system," *Applied Energy*, vol. 201, pp. 257–269, 2017.

[405] C. G. Hoehne and M. V. Chester, "Optimizing plug-in electric vehicle and vehicle-to-grid charge scheduling to minimize carbon emissions," *Energy*, vol. 115, pp. 646–657, 2016.

[406] H. T. Mouftah and M. Erol-Kantarci, *Smart grid: networking, data management, and business models*. CRC Press, 2017.

[407] C. Hodge, K. Hauck, S. Gupta, and J. C. Bennett, "Vehicle cybersecurity threats and mitigation approaches," tech. rep., National Renewable Energy Lab.(NREL), Golden, CO (United States), 2019.

[408] Y. Ryabova, J. Esposito, A. Andreev, A. Titterington, and O. Svistunova, "Vulnerabilities of electric car charging."

[409] H. Luo, H. Yu, and J. Luo, "Praft and rpbft: A class of blockchain consensus algorithm and their applications in electric vehicles charging scenarios for v2g networks," *Internet of Things and Cyber-Physical Systems*, vol. 3, pp. 61–70, 2023.

[410] H. Wang, Q. Wang, D. He, Q. Li, and Z. Liu, "Bbars: Blockchain-based anonymous rewarding scheme for v2g networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3676–3687, 2019.

[411] Z. Wan, T. Zhang, W. Liu, M. Wang, and L. Zhu, "Decentralized privacy-preserving fair exchange scheme for v2g based on blockchain," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 4, pp. 2442–2456, 2021.

[412] P. R. Babu, A. G. Reddy, B. Palaniswamy, and S. K. Kommuri, "Ev-auth: Lightweight authentication protocol suite for dynamic charging system of electric vehicles with seamless handover," *IEEE Transactions on Intelligent Vehicles*, vol. 7, no. 3, pp. 734–747, 2022.

[413] T. Bianchi, S. Asokraj, A. Brighente, M. Conti, and R. Poovendran, "Qevsec: Quick electric vehicle secure charging via dynamic wireless power transfer," in *2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring)*, pp. 1–6, IEEE, 2023.

[414] S. Asokraj, T. Bianchi, A. Brighente, M. Conti, and R. Poovendran, "Identity-based authentication for on-demand charging of electric vehicles," *arXiv preprint arXiv:2208.02857*, 2022.

[415] M. Ali, G. Kaddoum, W.-T. Li, C. Yuen, M. Tariq, and H. V. Poor, "A smart digital twin enabled security framework for vehicle-to-grid cyber-physical systems," *IEEE Transactions on Information Forensics and Security*, 2023.

[416] M. E. Kabir, M. Ghafouri, B. Moussa, and C. Assi, "A two-stage protection method for detection and mitigation of coordinated evse switching attacks," *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 4377–4388, 2021.

[417] W. Lo, H. Alqahtani, K. Thakur, A. Almadhor, S. Chander, and G. Kumar, "A hybrid deep learning based intrusion detection system using spatial-temporal representation of in-vehicle network traffic," *Vehicular Communications*, vol. 35, p. 100471, 2022.

[418] S. T. Mehedi, A. Anwar, Z. Rahman, and K. Ahmed, "Deep transfer learning based intrusion detection system for electric vehicular networks," *Sensors*, vol. 21, no. 14, p. 4736, 2021.

[419] A. K. Desta, S. Ohira, I. Arai, and K. Fujikawa, "Rec-cnn: In-vehicle networks intrusion detection using convolutional neural networks

trained on recurrence plots," *Vehicular Communications*, vol. 35, p. 100470, 2022.
[420] J. Zhang, Y. Jiang, J. Cui, D. He, I. Bolodurina, and H. Zhong, "Dbcpa: Dual blockchain-assisted conditional privacy-preserving authentication framework and protocol for vehicular ad hoc networks," *IEEE Transactions on Mobile Computing*, 2022.
[421] C. Lin, X. Huang, and D. He, "Ebcpa: Efficient blockchain-based conditional privacy-preserving authentication for vanets," *IEEE Transactions on Dependable and Secure Computing*, 2022.
[422] S. Jadidi, H. Badihi, and Y. Zhang, "Active cyber-resilient control for a pv system at microgrid level," in *2021 IEEE 4th International Conference on Renewable Energy and Power Engineering (REPE)*, pp. 339–344, IEEE, 2021.
[423] S. Tan, P. Xie, J. M. Guerrero, and J. C. Vasquez, "False data injection cyber-attacks detection for multiple dc microgrid clusters," *Applied Energy*, vol. 310, p. 118425, 2022.
[424] R. Germanà, A. Giuseppi, A. Pietrabissa, and A. Di Giorgio, "Optimal energy storage system placement for robust stabilization of power systems against dynamic load altering attacks," in *2022 30th Mediterranean Conference on Control and Automation (MED)*, pp. 821–828, IEEE, 2022.
[425] V. Katewa and F. Pasqualetti, "Optimal dynamic load-altering attacks against power systems," in *2021 American Control Conference (ACC)*, pp. 4568–4573, IEEE, 2021.
[426] G. Xu, H. Bai, J. Xing, T. Luo, N. N. Xiong, X. Cheng, S. Liu, and X. Zheng, "Sg-pbft: A secure and highly efficient distributed blockchain pbft consensus algorithm for intelligent internet of vehicles," *Journal of Parallel and Distributed Computing*, vol. 164, pp. 1–11, 2022.
[427] C.-F. Cheng, G. Srivastava, J. C.-W. Lin, and Y.-C. Lin, "Fault-tolerance mechanisms for software-defined internet of vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 6, pp. 3859–3868, 2021.
[428] S. M. H. Bamakan, A. Motavali, and A. B. Bondarti, "A survey of blockchain consensus algorithms performance evaluation criteria," *Expert Systems with Applications*, vol. 154, p. 113385, 2020.
[429] L. Yang and A. Shami, "A transfer learning and optimized cnn based intrusion detection system for internet of vehicles," in *ICC 2022-IEEE International Conference on Communications*, pp. 2774–2779, IEEE, 2022.
[430] L. Yang, D. M. Manias, and A. Shami, "Pwpae: An ensemble framework for concept drift adaptation in iot data streams," in *2021 IEEE Global Communications Conference (GLOBECOM)*, pp. 01–06, IEEE, 2021.
[431] S. S. Ravi and M. Aziz, "Utilization of electric vehicles for vehicle-to-grid services: Progress and perspectives," *Energies*, vol. 15, no. 2, p. 589, 2022.
[432] K. P. Schneider, S. Laval, J. Hansen, R. B. Melton, L. Ponder, L. Fox, J. Hart, J. Hambrick, M. Buckner, M. Baggu, *et al.*, "A distributed power system control architecture for improved distribution system resiliency," *IEEE Access*, vol. 7, pp. 9957–9970, 2019.
[433] D. K. Molzahn, F. Dörfler, H. Sandberg, S. H. Low, S. Chakrabarti, R. Baldick, and J. Lavaei, "A survey of distributed optimization and control algorithms for electric power systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 6, pp. 2941–2962, 2017.
[434] R. Sadnan and A. Dubey, "Distributed optimization using reduced network equivalents for radial power distribution systems," *IEEE Transactions on Power Systems*, vol. 36, no. 4, pp. 3645–3656, 2021.
[435] J. D. Taft, "Comparative architecture analysis: Using laminar structure to unify multiple grid architectures," tech. rep., Pacific Northwest National Lab.(PNNL), Richland, WA (United States), 2016.
[436] R. Sadnan, S. Poudel, A. Dubey, and K. P. Schneider, "Layered coordination architecture for resilient restoration of power distribution systems," *IEEE Transactions on Industrial Informatics*, 2022.
[437] B. Palmintier, D. Krishnamurthy, P. Top, S. Smith, J. Daily, and J. Fuller, "Design of the helics high-performance transmission-distribution-communication-market co-simulation framework," in *2017 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, pp. 1–6, IEEE, 2017.
[438] N. Gray, R. Sadnan, A. Bose, and A. Dubey, "Effects of communication network topology on distributed optimal power flow for radial distribution networks," in *2021 North American Power Symposium (NAPS)*, pp. 1–6, IEEE, 2021.
[439] A. P. P. Association, "Evaluation of Data Submitted in APPA's 2018 Distribution System Reliability & Operations Survey." Available Online: https://www.publicpower.org/system/files/documents/2018%20DSRO%20Report_0.pdf, July 2019.
[440] I. S. U. , "ISEAGE," 2022.
[441] N. S. F. , D. o. D. , and D. o. H. S. , "The DETER Project," 2022.
[442] D. of Defense, *DoD Zero Trust Strategy*. Nov. 2022.
[443] X. Zhao, L. Chang, R. Shao, and K. Spence, "Power system support functions provided by smart inverters—a review," *CPSS Transactions on Power Electronics and Applications*, vol. 3, no. 1, pp. 25–35, 2018.
[444] S. Subedi, N. Guruwacharya, R. Fourney, H. M. Rekabdarkolaee, R. Tonkoski, T. M. Hansen, U. Tamrakar, and P. Cicilio, "Computationally efficient partitioned modeling of inverter dynamics with grid support functions," in *IECON 2021 – 47th Annual Conference of the IEEE Industrial Electronics Society*, pp. 1–6, 2021.
[445] L. Li, J. Li, and L. Zhang, "Identification method of control parameters for wind power grid-connected converter based on optimization algorithm," in *IECON 2023- 49th Annual Conference of the IEEE Industrial Electronics Society*, pp. 1–4, 2023.
[446] B. Tang, M. Qian, N. Chen, J. Li, H. Li, and Y. Shi, "Frequency support demand analysis of high non-synchronous resource penetration receiving-end power grid based on system frequency response model," in *2022 IEEE 6th Conference on Energy Internet and Energy System Integration (EI2)*, pp. 858–862, 2022.
[447] I. Stefani, V. Stokic, S. Dzaleta, and B. Brbaklic, "Grid optimization using der grid support functions," in *2022 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, pp. 1–5, 2022.
[448] E. P. R. Institute, *Recommended Smart Inverter Settings for Grid Support and Test Plan*. Apr. 2018.
[449] Y. Li and J. Yan, "Cybersecurity of smart inverters in the smart grid: A survey," *IEEE Transactions on Power Electronics*, vol. 38, no. 2, pp. 2364–2383, 2022.
[450] T. S. Ustun, "Cybersecurity vulnerabilities of smart inverters and their impacts on power system operation," in *2019 International Conference on Power Electronics, Control and Automation (ICPECA)*, pp. 1–4, IEEE, 2019.
[451] S. Sahoo, T. Dragičević, and F. Blaabjerg, "Cyber security in control of grid-tied power electronic converters—challenges and vulnerabilities," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 5, pp. 5326–5340, 2019.
[452] D. Shea, "State Efforts to Protect the Electric Grid," Apr. 2016.
[453] "NCCIC/ICS-CERT FY 2015 Annual Vulnerability Coordination Report,"
[454] "Cybersecurity and the Electric Grid | The State Role in Protecting Critical Infrastructure."
[455] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains,"
[456] A. Rynes and T. Bjornard, "Intent, Capability and Opportunity: A Holistic Approach to Addressing Proliferation as a Risk Management Issue," Tech. Rep. INL/CON-11-20974, Idaho National Lab. (INL), Idaho Falls, ID (United States), July 2011.
[457] "Cyber-Attack Against Ukrainian Critical Infrastructure | CISA," July 2021.
[458] "Connect the Dots on State-Sponsored Cyber Incidents - Compromise of Saudi Aramco and RasGas."
[459] M. Popa, "Everest Gang Puts $200K Price Tag on ESKOM Stolen Data," Oct. 2022.
[460] D. Bianco, "Enterprise Detection & Response: The Pyramid of Pain," Mar. 2013.
[461] Z. Zhongdong, C. Ziwen, Y. Jinfeng, Q. Bin, and X. Yong, "Cloud based cyber security defense of smart meters," in *2020 International Conference on Virtual Reality and Intelligent Systems (ICVRIS)*, pp. 532–535, 2020.
[462] W. Hupp, D. Saleem, J. T. Peterson, N. R. E. Laboratory, K. Boyce, and U. Laboratories, *Cybersecurity Certification Recommendations for Interconnected Grid Edge Devices and Inverter Based Resources*. Nov. 2021.
[463] S. Aghapour, M. Kaveh, M. R. Mosavi, and D. Martín, "An ultra-lightweight mutual authentication scheme for smart grid two-way communications," *IEEE Access*, vol. 9, pp. 74562–74573, 2021.
[464] J. Obert, P. Cordeiro, J. Johnson, G. Lum, T. Tansy, M. Pala, and R. Ih, *Recommendations for Trust and Encryption in DER Interoperability Standards*. No. SAND2019-1490, Feb. 2019.
[465] G. Buster, *Large Language Models (LLMs) for Energy Systems Research*. National Renewable Energy Laboratory, Oct. 2023.
[466] Cybersecurity, I. S. A. (CISA), and MITRE, *Best Practices for MITRE ATT&CK Mapping*. June 2021.
[467] Cybersecurity and C. I. Agency, "Github - cisagov/decider: A web application that assists network defenders, analysts, and researchers

in the process of mapping adversary behaviors to the mitre att&ck framework.."
[468] Cybersecurity and I. S. A. CISA, Mar. 2022.
[469] Cybersecurity and I. S. A. CISA, Oct. 2024.
[470] N. Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," *The New York Times*, Oct. 2012.
[471] C. Owens, "Johannesburg Rocked By Cyberattack," July 2019.
[472] L. Abrams, "Power Company Has Security Breach Due to Downloaded Game," Feb. 2019.
[473] B. Willemsen, "Gartner Top 10 Strategic Technology Trends 2024," 2024.
[474] "FBI Warns of Increasing Threat of Cyber Criminals Utilizing Artificial Intelligence," May 2024.
[475] L. F. Sikos, "Packet analysis for network forensics: A comprehensive survey," *Forensic Science International: Digital Investigation*, vol. 32, p. 200892, 2020.
[476] C. E. Pascoe, "Public draft: The nist cybersecurity framework 2.0," 2023.

Niroop Sugunaraj (Graduate Student Member, IEEE) is a Ph.D. student in the School of Electrical Engineering and Computer Science (SEECS) at the University of North Dakota (UND). His research areas are in cybersecurity and artificial intelligence, specifically for cyber-physical systems (e.g., power grids, automotive networks). He received his M.S. in EE from UND in 2021 and B.E. in Computer Science from the University of Wollongong in Dubai (UOWD) in 2018. He has authored manuscripts for IEEE, Elsevier, MDPI, Springer, and Wiley, and is serving as a reviewer for these publishers.

Shree Ram Abayankar Balaji (Graduate Student Member, IEEE) received his B.E. Degree in Computer Science from the Adhiyamaan College of Engineering (ACE), India, in 2022. He is currently working on his Ph.D. in Computer Science with the University of North Dakota, Grand Forks, ND, USA. Since 2022, he has been a Graduate Research Assistant (GRA) with the Data Energy Cyber and Systems (DECS) Laboratory and the Center for Cyber Security Research (C2SR), UND. He has authored manuscripts published in IEEE. His research interests focus on cybersecurity and the application of machine learning to cyber-physical systems, particularly Distributed Energy Resources (DERs) and Industrial Control Systems (ICS).

Barathwaja Subash Chandar graduated from the University of North Dakota (UND) in 2023 with a Master's degree in Computer Science. He has worked in the DECS Research Laboratory and Cyber Security Research (C2SR) at UND under the guidance of Dr. Prakash Ranganathan on projects related to Unmanned Aerial Vehicles (UAVs) and energy. He has over 5 years of experience as a Software Engineer - Developing Web Applications and Automating manual activities. His areas of interest include machine Learning, federated learning, Continuous Integration and Continuous Delivery (CI-CD) pipelines, and web programming languages.

Prashanth Rajagopalan has graduated from the University of North Dakota (UND) in 2023 with a Master's degree in Electrical Engineering. He served as a Graduate Research Assistant (GRA) at the Data, Energy, Cyber and Systems (DECS) laboratory and Cyber Security Research (C2SR) at UND, led by Dr. Prakash Ranganathan. Prashanth's research interests are around forecasting and optimization of Electric Vehicle-to-Grid (V2G) services using AI and machine learning.

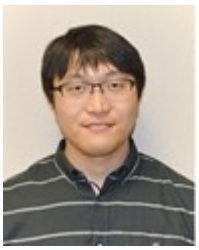
Dr. Utku Kose received the B.S. degree in 2008 from computer education of Gazi University, Turkey as a faculty valedictorian. He received M.S. degree in 2010 from Afyon Kocatepe University, Turkey in the field of computer and D.S. / Ph. D. degree in 2017 from Selcuk University, Turkey in the field of computer engineering. Between 2009 and 2011, he has worked as a Research Assistant in Afyon Kocatepe University. Following this, he has also worked as a Lecturer and Vocational School - Vice Director in Afyon Kocatepe University between 2011 and 2012, as a Lecturer and Research Center Director in Usak University between 2012 and 2017, Assistant Professor in Suleyman Demirel University between 2017 and 2019, and as an Associate Professor in Suleyman Demirel University between 2019 and 2024. Currently, he is a Full Professor in Suleyman Demirel University, Turkey. Kose also gave lectures at other higher education institutions such as Gazi University and Istanbul Arel University. He also worked as a Visiting Researcher at the University of North Dakota, USA (between 2023 and 2024) and holds the Honorary Professor of Artificial Intelligence title at ITM (SLS) Baroda University, India. He has more than 300 publications including articles, authored and edited books, proceedings, and reports. He is also in editorial boards of many scientific journals and serves as one of the editors of the Biomedical and Robotics Healthcare (CRC Press) and Computational Modeling Applications for Existential Risks (Elsevier) book series. His research interests include artificial intelligence, machine ethics, artificial intelligence safety, biomedical applications, optimization, the chaos theory, distance education, e-learning, computer education, and computer science.

David Loper received his master's degree in computer science from the University of North Dakota in 2024. Before returning to school, he worked in key roles in information technology companies as a researcher, principal architect, and lead engineer. He was the co-head of research and development at an industry-leading managed service company before becoming the Vice President of Technology for an award-winning Linux distribution company. He currently lectures full-time at Utah Valley University on Linux and technology topics. He is currently working on his Ph.D. in computer science, where his research focus is using AI for early-phase detection of botnet network negotiation.

Tanzim Mahfuz (Graduate Student Member, IEEE) received his B.Sc. degree from the Jahangirnagar University, Dhaka. He is currently pursuing his Ph.D. degree in Electrical and Computer Engineering from the University of Maine, Orono under the supervision of Dr. Prabuddha Chakraborty. His research focuses on applied artificial intelligence for hardware security and trust.

Prabuddha Chakraborty (Member, IEEE) is an Assistant Professor at the University of Maine. He received his Ph.D. in Electrical and Computer Engineering from the University of Florida. His research interest lies in the intersecting areas of Artificial Intelligence and system security. He is a recipient of the Certificate of Outstanding Merit from the Herbert Wertheim College of Engineering at the University of Florida (2021), for his academic and research excellence. He has also received several awards for his research contributions, including IEEE TTTC's E. J. McCluskey Best Doctoral Thesis Award (2022).

Seerin Ahmad (S'21–M'25) received his B.E. degree from Aligarh Muslim University, Aligarh, India, in 2017, and his M.S. degree from the Budapest University of Technology and Economics, Budapest, Hungary, in 2019, both in Electrical Engineering. He recently completed his Ph.D. in Engineering (Electrical Engineering Specialization) at Texas A&M University-Kingsville, TX in December 2024. He also worked as a summer intern at Oak Ridge National Laboratory (ORNL), Oak Ridge, TN, USA, in 2024. His research interests include cyber-resilient power systems, distributed energy resource management systems, power electronics, and cybersecurity.



Taesic Kim (S'10–M'15–SM'21) received the B.S. degree in Electronics Engineering from Changwon National University, Changwon, Korea in 2008 and the M.S. and Ph.D. degree in Electrical Engineering and Computer Engineering from the University of Nebraska–Lincoln, in 2012 and 2015, respectively. In 2009, He was with the New and Renewable Energy Research Group of Korea Electrotechnology Research Institute, Korea. He was also with Mitsubishi Electric Research Laboratories, Cambridge, MA, USA in 2013. He was an Associate Professor in the Department of Electrical Engineering and Computer Science at Texas A&M University-Kingsville. He is currently an Associate Professor with the Department of Electrical Engineering and Computer Science at the University of Missouri, Columbia. His research interests now cover broad areas of cyber-physical power and energy systems including cyber-physical system security, power electronics and cyber-resilient power systems, quantum security and intelligence, and blockchain. He was a recipient of the 2018 Myron Zucker Student–Faculty Grant Award from IEEE Foundation, the Best Paper Awards in the 2021 IEEE PES Innovative Smart Grid Technologies – Asia and 2017 IEEE International Conference on Electro Information Technology, and the first prize award in the 2013 IEEE Industry Application Society Graduate Student Thesis Contest.

Giovanni Apruzzese is an Assistant Professor within the Hilti Chair of Data and Application Security at the University of Liechtenstein. He obtained the PhD in Information and Communication Technologies at the University of Modena and Reggio Emilia (Italy) in 2020. He authored over 30 peer-reviewed papers at internationally-recognized research venues. His research interests encompass a variety of themes, most of which revolve around cybersecurity and artificial intelligence, but he also appreciates topics within human-computer interaction. His primary expertise lies in network security and in phishing detection. Giovanni also puts a lot of effort in servicing the scientific community, and he was awarded numerous recognitions for his reviewing duties in leading computer-science venues.

Anamika Dubey (SM) received her Ph.D. degree in Electrical and Computer Engineering from the University of Texas at Austin in Dec 2015. She is currently Huie-Rogers Endowed Chair Associate Professor of Electrical Engineering in the School of EECS at Washington State University (WSU), Pullman. She also holds a joint appointment as a Research Scientist at the Pacific Northwest National Laboratory (PNNL) and currently serves as the Co-director for the WSU-PNNL Advanced Grid Institute. Her research focuses on the scalable integration of cross-domain models and data to provide better decision support for increasingly complex electric power grids. Currently, her lab is actively working on climate change adaptation solutions for the power grid via hazard modeling, risk-averse planning, and distributed operations. She is a recipient of the National Science Foundation CAREER Award (2019) and the IEEE PES Outstanding Young Engineer Award (2023).

Luka V. Strezoski received the B.S., M.Sc., and Ph.D. degrees (with honors) in power engineering from the University of Novi Sad, Novi Sad, Serbia, in 2013, 2014, and 2017, respectively. His Ph.D. research was conducted under joint supervision between the University of Novi Sad and Case Western Reserve University, Cleveland, USA. He is currently with the Faculty of Technical Sciences, University of Novi Sad, as an Associate Professor and the Head of the Department of Power Engineering and Applied Software Department and the Director of the Smart Grid Laboratory. He is also a Visiting Affiliate with Case Western Reserve University. His current research interests include distribution system modeling, renewable distribution generation modeling, and integration of distributed energy resources (DER) into the distribution management system (DMS) and distributed energy resource management system (DERMS) applications.

Benjamin Blakely (Ph.D., CISSP, Senior Member, IEEE), is a cybersecurity and artificial intelligence researcher at Argonne National Laboratory, a United States Department of Energy laboratory. He leads the Applied Research group within the Strategic Security Sciences division, driving innovation in critical areas of national security.

With over 20 years of experience across private enterprises, government agencies, and academia, Dr. Blakely has demonstrated expertise in operations, research, and education. He has successfully built and led teams in information security, information technology, and data science, including supporting a software company through its initial public offering (IPO). His professional engagements also include serving as a subject matter expert for various United States departments, such as Energy, Homeland Security, State, and Defense.

Dr. Blakely holds PhD and Bachelor of Science degrees from Iowa State University in computer engineering with minors in psychology and political science. He has contributed to education by designing and teaching courses at Iowa State, including "Legal, Ethical, and Professional Issues in Cybersecurity" and "Formal Methods of Software Verification." Currently, he shares his knowledge by teaching short courses on cybersecurity and artificial intelligence at the University of Chicago.

He is a Certified Information Systems Security Professional (CISSP) through ISC² and a Certified Information Security Manager (CISM) through ISACA (inactive certification). His research interests focus on applying artificial intelligence to risk management, safeguarding critical infrastructure, and developing systems capable of intelligent self-defense.

Subhojit Ghosh (Senior Member, IEEE) received the Ph.D. degree in biomedical control system from the Indian Institute of Technology Kharagpur, Kharagpur, India, in 2010. He has more than 23 years of teaching experience with the Birla Institute of Technology Mesra, National Institute of Technology (NIT) Rourkela, and NIT Raipur. He is currently a Professor with Electrical Engineering Department, NIT Raipur, Raipur, India. His research interests include cyber security in smart grid, optimization techniques, control systems, renewable energy, and power system protection.

Maddikara Jaya Bharata Reddy (Senior Member, IEEE) was born in India, in 1980. He received the B.Tech. degree in Electrical and Electronics Engineering from Acharya Nagarjuna University, Guntur, India, in 2002, and the M.E. degree in electrical engineering and the Ph.D. degree from the Birla Institute of Technology (BIT), Ranchi, India, in 2004 and 2008, respectively.

He has 20 years of experience in teaching and research. He is currently working as a Professor at the Department of Electrical and Electronics Engineering, National Institute of Technology (NIT) Tiruchirappalli, Tiruchirappalli, India. His current research interests include smart grids, substation automation, wide-area protection, digital relaying, soft computing applications in power systems and cyber security in smart grids. Dr. Reddy has published more than 115 journal and conference papers. He holds three patents. He served as an Editor of the Power Components & Systems (Taylor & Francis Publications), Associate Editor of IET High Voltage, Associate Editor of IEEE Access, and now Associate and Subject Editor for IET Generation, Transmission & Distribution.

Harsha Padullaparti (Senior Member, IEEE) received the B.Tech. degree in electrical and electronics engineering from Jawaharlal Nehru Technological University Hyderabad, Hyderabad, India, in 2007, the M.S. degree in electrical engineering from the Indian Institute of Technology Madras, India, in 2010, and the Ph.D. degree in electrical and computer engineering from the University of Texas at Austin, in 2018. He was a Senior Engineer with Power Grid Corporation of India Ltd. (PGCIL), from 2009 to 2014. He is currently a Senior Researcher with the Power Systems Engineering Center, National Renewable Energy Laboratory, Golden, CO, USA. His research interests include data analytics for distribution grid operations, advanced distribution management systems, distributed energy resources management systems, distribution system modeling, and renewable energy integration.

Dr. Prakash Ranganathan (Senior Member, IEEE) is an Associate Professor of Electrical Engineering and Director of the Data Energy Cyber and Systems (DECS) Laboratory at the University of North Dakota (UND). He's a Senior Member of IEEE and an accomplished researcher in areas like smart grids, cybersecurity, data science, and renewable energy. Dr. Ranganathan also serves as the Director for the Center for Cyber Security Research (C2SR) at UND and has received various awards for his outstanding contributions to teaching and research. With 130+ peer-reviewed articles and over 18+ years in higher education, he's a leading figure in engineering and computer science. His extensive grant funding, mentorship, and leadership in cyber educational initiatives further underscore his dedication to advancing the field. Dr. Ranganathan holds a Ph.D. in Software Engineering from North Dakota State University (NDSU) and has actively supporting diversity and inclusivity in STEM education, particularly among involving Native American students.

TABLE XIII
ACRONYMS AND ABBREVIATIONS (1).

Acronym	Definition	Acronym	Definition
3DES	Triple Data Encryption Standard	FLISR	Fault Location, Isolation, and Service Restoration
ABAC	Attribute–based Access Control	FML	Federated ML
ABM	Agent–based Modeling	G2V	Grid to Vehicle
AC	Alternating Current	GAN	Generative Adversarial Network
ADMS	Advanced Distribution Management System	GHP	Geothermal Heat Pumps
ADS	Anomaly Detection System	GOOSE	Generic Object Oriented Substation Event
AES	Advanced Encryption Standard	GPU	Graphics Processing Unit
AI	Artificial Intelligence	HCL	Hashicorp Configuration Language
AMI	Advanced Metering Infrastructure	HELICS	Hierarchical Engine for Large-scale Infrastructure Co-Simulation
ANN	Artificial Neural Network	HIDS	Host IDS
AoC	Action on Objectives	HIL	Hardware–in–loop
API	Application Programming Interface	HS	Hardware Solutions
APT	Advanced Persistent Threat	HTTP	Hypertext Transfer Protocol
AR	Autoregressive	HTTPS	Hypertext Transfer Protocol Secure
ARP	Address Resolution Protocol	IACS	Industrial Automation and Control Systems
ASLR	Address Space Layout	IAM	Identity Access Management
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge	IBM	International Business Machines
BACnet	Building Automation Control Network	IBR	Inverter–Based Resource
BC	Blockchain	IC	Integrated Circuit
BCTE	Blockchain-enabled Transactive Energy	ICCP	Inter-control Center Communication Protocol
BEMS	Building Energy Management System	ICMP	Internet Communication Management Protocol
BESS	Battery Energy Storage System	ICS	Industrial Control System
BTM	Behind–the–meter	IDDS	Intrusion Detection and Diagnostics Systems
CA	Certification Authority	IDFF	Intrusion Detection Federated Framework
CAN	Controller Area Network	IDS	Intrusion Detection System
CHIL	Controller Hardware–in–loop	IDU	Intrusion Diagnostic Unit
CI/CD	Continuous Integration/Continuous Development	IEC	International Electrotechnical Commission
CIAA	Confidentiality, Integrity, Availability, and Accountability	IED	Intelligent Electronic Devices
CIGRE	Council of Large Electric Systems	IEEE	Institute of Electrical and Electronics Engineers
CIS	Customer Information System	IoC	Indicator of Compromise
CISA	Cybersecurity and Infrastructure Security Agency	IoT	Internet of Things
CKC	Cyber Kill Chain	IP	Internet Protocol
CNN	Convolutional Neural Network	IR	Internal Report
CPA	Correlational Power Analysis	IRENA	International Renewable Energy Agency
CPS	Cyber–Physical System	ISEAGE	Internet–scale Event and Attack Generation Environment
CRL	Certification Revocation List	ISO	Independent System Operator
CSIP	Common Smart Inverter Profile	ISU	Iowa State University
CSPA	Charging Service Provider Authority	IT	Information Technology
DAC	Disrectionary Access Control	KNN	K-Nearest Neighbour
DC	Direct Current	LCOE	Levelized Cost of Electricity
DCS	Distributed Control System	LoA	Likelihood of Attack
DER	Distributed Energy Resource	LR	Linear Regression
DERMS	Distributed Energy Resource Management System	LSTM	Long–short Term Memory
DETER	Defense Technology Experimental Research	MAC	Media Access Control
DFS	Design–for–Security	MAIFI	Momentary Average Interruption Frequency Index
DG	Distributed Generation	MitM	Man–in–the–Middle
DHS	Department of Homeland Security	MITRE	MIT Research Establishment
DL	Deep Learning	ML	Machine Learning
DLT	Distributed Ledger Technology	MMG	Multi–microgrid
DMS	Distribution Management System	MMS	Manufacturing Message Specification
DMZ	Demilitarized Zone	MW	Mega Watt
DNP	Distributed Network Protocol	NAA	Natural Aggregation Algorithm
DNS	Domain Name Service	NARX	Nonlinear autoregressive with external input
DoD	Department of Defense	NATO	North Atlantic Treaty Organization
DoS	Denial of Service	NERC	North American Electric Reliability Corporation
DPA	Differential Power Analysis	NGFW	Next Generation Firewall
DR	Demand Response	NIDS	Network IDS
DRMS	Demand Response Management System	NIST	National Institute of Standards and Technology
DSO	Distribution System Operator	NN	Neural Networks
DSP	Digital Signal Processing	NREL	National Renewable Energy Laboratory
DT	Decision Tree	NSF	National Science Foundation
EDR	Endpoint Detection and Response	NSTB	National SCADA Test Bed
EIA	Energy Information Administration	OBD	On–board Diagnostics
EM	Electromagnetic	OCPP	Open Charge Point Protocol
EMS	Energy Management System	OMS	Outage Management System
EPRI	Electric Power Research Institute	OPF	Optimal Energy Flow
EPS	Electric Power Systems	ORNL	Oak Ridge National Laboratory
ESS	Energy Storage Systems	OSI	Open Systems Interconnection
EV	Electric Vehicle	OSINT	Open–source Intelligence
EVSE	EV Supply Equipment	OT	Operational Technology
FAST–DERMS	Federated Architecture for Secure and Transactive Distributed Energy Resource Management System	P2P	Peer–to–peer
FCI	False Command Injection	PCA	Principal Component Analysis
FDI	False Data Injection	PCB	Printed Circuit Board
FIPS	Federal Information Processing Standard	PE	Privilege Escalation
FL	Federated Learning	PF	Power Flow

TABLE XIV
ACRONYMS AND ABBREVIATIONS (2).

Acronym	Definition	Acronym	Definition
PHIL	Power Hardware–in–loop	SIEM	Security Incident and Event Management
PII	Personally Identifiable Information	SI–GRID	Software–defined Intelligent Grid Research Integration and Development
PKI	Public Key Infrastructure	SMB	Server Message Block
PLC	Programmable Logic Controller	SMI	Smart Metering Infrastructure
PMU	Phasor Measurement Unit	SNL	Sandia National Laboratory
PNNL	Pacific Northwest National Laboratory	SoC	System–on–Chip
PQC	Post Quantum Cryptography	SoD	Separation of Duties
PST	Phase Shifting Transformers	SQL	Structured Query Language
PV	Photovoltaic	SS	Software Solution
QIS	Quantum Information Systems	SSH	Secure Shell
QKD	Quantum Key Distribution	ST	Security Standards
RAT	Remote Access Trojan	STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, DoS, and Elevation of Privilege
RBAC	Role–based Access Control	SVD	Singular Value Decomposition
RBM	Restricted Boltzmann Machine	SVM	Support Vector Machine
RE	Renewable Energy	TB	Testbed
REST	Representational State Transfer	TCP	Transmission Control Protocol
RF	Radio Frequency	TLS	Transport Layer Security
RFID	Radio Frequency Identification	TSO	Transmission System Operator
RHIL	Remote Hardware–in–loop	TVLA	Test Vector Leakage Assessment
RINSE	Real-time Immersive Network Simulation Environment	TX	Transmission
RMSE	Root Mean Square Error	UDP	User Datagram Protocol
RNN	Recurrent Neural Network	UEBA	User and Entity Behaviour Analytics
RSA	Rivest—Shamir—Adleman	V2B	Vehicle-to-Building
RTDS	Real-time Digital Simulator	V2G	Vehicle–to–Grid
RTF	Rich Text Format	V2H	Vehicle-to-Home
RTO	Regional Transmission Organization	VPP	Virtual Power Plant
RTU	Remote Terminal Unit	VVO	Voltage Var Optimization
SA	Standards Association	WAMPAC	Wide–Area Monitoring, Protection, and Control
SAIDI	System Average Interruption Duration Index	WSCC	Western System Coordinating Council
SCADA	Supervisory Control and Data Acquisition	WSN	Wireless Sensor Network
SCRM	Supply Chain Risk Management	XAI	Explainable AI
SDP	Software Defined Perimeter	YAML	YAML Aint Markup Language
SEP	Smart Energy Profile		