SJIF Impact Factor (2026): 8.863| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 3 | March 2026 - Peer Reviewed Journal

SECURING THE SMART GRID: A REVIEW OF ENCRYPTION, AUTHENTICATION, AND AI-POWERED INTRUSION DETECTION IN DISTRIBUTED ENERGY RESOURCES

Benjamin Panful[1], Barnabas Apaflo[2], Eunice Abena Lettu[3]
[1]*Lake Land College, USA;*
[2]*Texas A&M University, USA*
[3]*Kwame Nkrumah University of Science and Technology, Ghana*

Article DOI: https://doi.org/10.36713/epra26773
DOI No: 10.36713/epra26773

ABSTRACT

Digitalizing the electric grid has caused distributed energy resources (DERs) to increase in cyber- attack across the surface of utilities, aggregators, vendors, customer premises, and cloud-connected control platforms. This narrative review is a synthesis of the state of practice and research on three security pillars that are interdependent to achieve the objective of Distributed Energy Resources (DER)-enabled smart grids which are encryption, authentication, and AI-powered intrusion detection system (IDS) as applied to the U.S. deployment realities. This review study puts into perspective how the DER interoperability specifications and operational interfaces condition the expectations of cybersecurity and allow us to explore the impact power-system security standards and implementation profiles may have on cryptographic protection and key management, as well as on the operation of secure protocols. It also evaluates authentication and authorization issues in DER ecosystems with multi-stakeholders, in which the scalability of device identity, lifecycle management of credits, and secure remote access are likely to dictate the potential to guarantee control integrity. Lastly, this research outlines AI-based IDS solutions, including protocol and process-sensitive detection, realistic dataset model, and tradeoffs in operation that dictate the adoption of this field, such as tolerance to latency and burden of false alarms. Through these themes, the review combines technical processes with resilience intent, indicating how multiple defenses can be used to sustain continuity of critical grid processes during attacks. The paper ends with gaps informed by deployment and a research agenda consisting of interoperable identity on a scale, robust key management and operationally credible IDS evaluation.

KEYWORDS: *Smart Grid; Distributed Energy Resources; Encryption; Authentication; Intrusion Detection Systems*

1. INTRODUCTION

Inverter-based solar PV, storage, controllable loads and new interface between vehicles and the grid are changing grid operations to the distribution edge through distributed energy resources (DERs). In the United States, this change is accompanied by the interoperability expectations aimed at providing that DER could connect and work effectively with the area electric power systems (Photovoltaics and Storage, 2018). This interoperability and connectivity that is necessary to provide the DER value that is visibility, dispatchability, coordination) also increases the cyber-attack surface, as the operational decisions of the implementation increasingly hinge on networks, software-defined control logic, and third-party service ecosystems, instead of isolated electromechanical behavior (Stouffer *et al*., 2015). Intelligent-grid cybersecurity recommendations have traditionally pointed out that power systems are not like traditional IT since safety, high availability, and time-sensitive control capabilities limit the way security controls may be designed and utilized (Stouffer *et al*., 2015). Regarding the concept of smart grid, National Institute of Standards and Technology (NIST) approaches cybersecurity as an analytical, risk-based process, which must be grid-specific and adaptable to current-day threats, instead of being a checklist (Pillitteri and Brewer, 2014). All these limitations become even more intense in DER environments, and trust limits frequently cut across utilities, aggregators, equipment vendors, installers, cloud platforms, and equipment owned by customers classes of authority that are complex chains of control determining who is allowed to view, command, and update fielded equipment (DOE, 2022).

In this research, we concentrate on three security pillars that rely on each other to understand whether the DER-enabled smart grids are able to maintain the integrity of their operations under adverse conditions. These pillars are encryption, authentication, and AI-powered intrusion detection (IDS). Encryption, which is also known as confidentiality and more importantly in control systems, integrity protection is aimed at ensuring that there are no adversarial eavesdropping and manipulation of operational communications (Ghosal and Conti, 2019). Nevertheless, grid environments do not support encryption as a "set and forget" concept, cryptography protection is only as reliable as the key management and lifecycle credential procedures that underpin it. Key management has been continuously identified as a requirement and a challenge in Advanced Metering Infrastructure (AMI) and larger-scale smart grid implementations

SJIF Impact Factor (2026): 8.863| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 3 | March 2026 - Peer Reviewed Journal

since it is difficult to reliably perform the operations of securely generating, distributing, rotating and revocation keys due to the operational scale and device limitations (Ghosal and Conti, 2019; Hernandez-Alvarez *et al*., 2025). The smart grid guidance by NIST also emphasizes the use of systemic fragility that is driven by use of common or default credentials and recommends the use of device-specific credentials and strong lifecycle adoption to prevent break-once everywhere effects (Pillitteri and Brewer, 2014). Authentication is a complement to cryptography that answers the fundamental question that determines the security of DER which asks, to whom does an issuer of commands, a modifier of configurations or an attester of state grant authorization. A review of smart-grid authentication methods indicates that authentication is considered one of the key controls in defending smart grid communications and avoiding unauthorized access, although proposed methods are highly diverse in their assumptions of threat model, computational feasibility, and deployment environment (Qasaimeh *et al*., 2019). Authentication in real deployment is not just confined to the device-to-device based authentication, but also human operator, vendor service accounts, aggregator interfaces and machine identities in multi-organization ecosystems. This is especially relevant to DER, where privileged avenues of high impact in terms of credential theft or misuse of privileges can emerge due to remote access points, maintenance platforms and third-party orchestration platforms (DOE, 2022; Stouffer *et al*., 2015). Despite the use of encryption and strong authentication, the smart-grid environments can still be compromised by misconfigurations, credential theft, supply-chain tampering, and new pathways into attack systems that avoid perimeter protection. Therefore, the IDS and anomaly detection are currently being discussed as the necessary complements to the preventive controls (DOE, 2022; Yang *et al*., 2016). Prior work in Independent Examinations Committee (IEC 61850) environments concludes that the context of the grid traffic is typically overlooked, as grid traffic tends to be structured and time-constrained, thus the protocol knowledge and system behavior constraints were introduced into the most promising operational IDS archetypes (Yang *et al*., 2016). Recent studies also examine AI and edge, or fog-based IDS designs that are designed to enhance detection performance and are also controlled by latency and bandwidth limitations that tend to restrict centralized monitoring in Operational Technology (OT) networks (Alsirhani *et al*., 2025). Adding to these developments of models, smart-grid IDS studies also emphasize the significance of plausible evaluation and data realism such as high-fidelity datasets and test-bed-generated traces, which model the attack behavior and operational effects (Elmasry, 2024; Tan *et al*., 2024). The U.S. DER cybersecurity discourse progressively view this technical control through resilience lens that is more focused on continuity of essential functions than localized "prevent all breaches" goals. According to U.S.-oriented DER guidance, the objective of the DER planners is to establish the cyber fortifications as such that will help to survive the attack without losing the most important functions. (DOE, 2022). This framing is consequential to the current review since it requires encryption, authentication, and IDS to be evaluated not only in terms of its abstract security characteristics, but also for real-world practicability, which includes device capability constraints, field lifecycle constraints, interoperability constraints, and false-alarm costs that can undermine operator trust in detection technologies (Stouffer *et al*., 2015; Pillitteri & Brewer, 2014).

2. SMART GRID AND DER CYBER CONTEXT

The distributed energy resources (DER) such as inverter-based solar PV, storage, controllable load and emerging vehicle-grid interface are moving the operations of the grid to the distribution level. Interoperability expectations in the United are meant to provide a means that the DER would be able to be integrated with area electric power systems to offer visibility, dispatchability, and coordination. Connectivity also increases the size of the cyber-attack surface since operations decisions grow, based on networks, software-defined control logic, and third-party ecosystems as opposed to solitary electromechanical activity (Photovoltaics and Storage, 2018; Stouffer *et al*., 2015; DOE, 2022).

DERs are cyber networked nodes, the behavior of which is equally defined by both software and communications as by hardware. U.S. Department of Energy (DOE) guidance identifies DER as small scale generation, flexible load or storage, and is generally 1-10,000 kW or smaller, which can be located on utility systems or at customer meter encompassing EVs with charging equipment (DOE, 2022). As a result, DER control and visibility frequently penetrate the customer networks and third-party platforms forming multi-stakeholder trust dependencies.

The NIST smart grid logical reference defines the smart grid as a system of interacting domains (Transmission, Distribution, Operations, Generation, Markets, Customer, Service Provider) with DER in the customer domain connected to controllers, energy management systems, EV/EVSE elements and gateways to be involved in the grid operations (Pillitteri and Brewer, 2014). In operational terms, this brings out the fact that DER security is not a utility issue only, as the control paths cut across customer and service-provider networks.

Institute of Electrical and Electronics Engineers (IEEE) 1547-2018 standard which establishes criteria and requirements for interconnection (DER) with electric power systems (EPS) and associated interfaces also requires the use of local DER communication interfaces to ensure interoperability and standardize the information models and non-proprietary encodings which encompass the read/write access to the nameplate, configuration, monitoring, and management data (Photovoltaics & Storage, 2018). Those interactions are directly correlated with the cybersecurity priorities like read access can be used to detect operational states, whereas write access can be used to alter modes and setpoints which require strong authentication, authorization and audit systems.

SJIF Impact Factor (2026): 8.863| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 3 | March 2026 - Peer Reviewed Journal

Integration by DER is also currently moving into mobility-linked assets, including V2G interfaces, growing multi-modal communications across home networks, utility networks and EVSE/PEV pathways (SunSpec, 2025). In this regard, security engineering would have to strike a balance between the operational continuity, latency and maintainability requirements that are inherent to industrial control systems (ICS), which do not fully resemble regular IT systems (Stouffer *et al*., 2015). The fact that the attackers can integrate digital activities with physical consequences exacerbates cyber risk since they may also use the manipulation of the DER commands to influence grid stability (Pillitteri and Brewer, 2014).

3. THREAT LANDSCAPE AND ATTACK SURFACE FOR DER-ENABLED SMART GRIDS

DER enlarges the area of attack and a possible impact. Common deployments in the U.S. involve DER field devices, optional aggregators, and utility systems, forming several trust boundaries and compromising the measurements, control intent, or protective measures (DOE, 2022). The spread of operational errors through integrity attacks on DER measurements, and the ability to perform coordinated small-scale manipulations through the significant DER penetration to produce power swings at the system level (DOE, 2022).

The extremes of adversary goals include mis-operation, which involves an attack on the computer system, and cyber compounding, where the physical manipulations are performed before an occurrence, e.g. by changing protective relay settings, or with availability attacks (Pillitteri and Brewer, 2014). Spoofing, man-in-the-middle, replay, and message modification are examples of communication-based attacks, and they exploit local interface, field network or aggregator link vulnerabilities (Stouffer *et al*., 2015; Cremers *et al*., 2019).

Risks of manipulation have been recorded in DER-related protocols. Independent Examinations Committee (IEC) 61850 Generic Object-Oriented Substation Events (GOOSE) and SV messages may be spoofed, flooded to cause a control or monitoring disruption, and the DNP3 Secure Authentication provides protection against spoofing, modification, and replay instead of full privacy (Hussain *et al*., 2019; Cremers *et al*., 2019). Even safe DER profiles, including SunSpec IEEE 2030.5 V2G-AC have man-in-the-middle risks that remain as residual in case the private keys are compromised or certificates are compromised (SunSpec, 2025). Potential attack vectors are increased by device and lifecycle realities, such as exposure to local interfaces and the inability of vendors to provide support (Photovoltaics and Storage, 2018; DOE, 2022).

4. STANDARDS AND GUIDANCE SHAPING DER SMART-GRID CYBERSECURITY

In the U. S., DER cybersecurity expectations are defined not by a single prescriptive DER security standard, but by a hierarchical series of (i) grid/DER interoperability requirements, (ii) ICS security engineering guidance, and (iii) power-system communications security standards. The guidance of DER by DOE explicitly states the aim in terms of resilience, which is, DER defenses must be able to survive attacks and remain capable of providing important functionality, and DER systems are gradually becoming required to confirm data and take actions in a cryptographically secure way in accordance with standards, testing, and vulnerability analysis (DOE, 2022). Notably, DOE points to the fact that general best practices for multifactor authentication, encryption, and detection/response tooling might have to be refined to meet the DER requirements, and that a DER trust model and clearer separation of roles among the owners, operators, vendors and aggregators are needed (DOE, 2022).

On the interconnection layer, IEEE 1547-2018 makes a more realistic assumption that cybersecurity is inherently system-wide, and the standard does not impose any specific security requirements on the local DER communication interface because overall security is based on architecture, complexity, and testability (Photovoltaics and Storage, 2018). It also clarifies that the network security of DER (the networks connecting DER with remote managing entities) is scoped, which demonstrates the diversity and dynamism of integration networks in practice (Photovoltaics and Storage, 2018). Rather, IEEE 1547-2018 indicates deployment-oriented patterns, including the inclusion of a DER with a secure networking device in such a way an open DER interface can be integrated into a secure communications path, and even recommends default disabling the local communication interface and enabling it only by password-protected local action (Photovoltaics and Storage, 2018). The encryption and authentication implication is that, in practice, utilities must have a coherent, fleet-wide security strategy, which can support heterogeneous DER brands and extended equipment lifetimes, instead of depending on application-specific device security capabilities which can make the system-level governance and maintenance complex (Photovoltaics and Storage, 2018).

The second reference is the NIST guidance on cryptography and ICS security architecture of smart grids. NISTIR 7628, guidelines for Smart Grid Cybersecurity, makes it clear that cryptography can only be reliable when paired with resilient key management, that it should not lead to break-once break-everywhere, that common credentials or shared secret keys create cryptography error, and that key diversity and the ability to rekey and revoke keys is necessary (Pillitteri and Brewer, 2014). It also suggests deploying published, time-tested cryptographic methods (preferably FIPS/NIST validated) since proprietary or minimally vetted ones have been found to be

SJIF Impact Factor (2026): 8.863| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 3 | March 2026 - Peer Reviewed Journal

unsound once revealed but also recognizes that sometimes smart-grid requirements require use of non-standard methods (Pillitteri and Brewer, 2014). In addition to that, NIST SP 800-82 which provides comprehensive guidelines for securing OT systems outlines the architectural floor of most OT environments, it asserts that architectural and boundary protection must separate corporate and control networks, connections must be limited , and patterns of firewall/DMZ must be used so that corporate-reachable services end in a controlled intermediate zone instead of touching control networks (Stouffer *et al*., 2015). Other defense-in-depth segmentation principles suggested by NIST include the principles of least privilege and minimization of unnecessary communications, which is particularly applicable in cases when DER ecosystems open new remote access options and third-party services (Stouffer *et al*., 2015).

Encryption and authentication are operationalized at the protocol layer in power-system communications security standards that were in operation at the time. IEC 62351 is categorically set as a standard to enhance security of the power system automation protocols by ensuring confidentiality, integrity, availability, and non-repudiation, which is mostly achieved by introducing the concept of authentication (Schlegel *et al*., 2017). The most notable one is IEC 62351-3 that recommends Trasport Layer Service (TLS) usage with X.509 certificates on Transmission Control Protocol/Internet Protocol (TCP/IP)-based applications, such as mutual authentication, minimum cryptographic specifications, and certificate revocation policies, in part to prevent man-in-the-middle and replay attacks (Schlegel *et al*., 2017). Nevertheless, the same analysis points to implementation caveats that directly apply to DER and smart-grid activities. Backwards compatibility may lower security posture, certain profiles may accept insecure communication modes or even enable TLS to be disabled, and algorithm selections for example 1024-bit RSA allowances and use of SHA-1 in some profiles may be out of date (Schlegel *et al*., 2017). The authors, however, find that IEC 62351 can be used to enhance security significantly when implemented in a holistic manner, but the security of it is limited by backwards compatibility requirements (Schlegel *et al*., 2017).

The meaning of authentication and encryption in operational terms are also protocol-specific security scopes. The standard's threat list of the specific threats that are being counteracted with the DNP3 Secure Authentication as analyzed in a formal analysis of protocol security framing includes only spoofing, modification, replay, and notably eavesdropping when it comes to cryptographic key exchanges, but not the general confidentiality of data (Cremers *et al*., 2019). Here is an important contextual fact related to DER environments, although a protocol layer is considered secured, it might be focused on authenticity/integrity over confidentiality which influences the interpretation of encryption requirement and the need to compensate it, for instance network segmentation or more secure tunnels).

Lastly, implementation profiles show how these principles get enforced into requirements in DER ecosystems. The SunSpec IEEE 2030.5 V2G-AC profile states that both terminals must have IEEE 2030.5-compliant certificates and use Hypertext Transfer Protocol Secure (HTTPS) to carry out all communications (SunSpec, 2025). It also records a residual man-in-the-middle threat and relates practical practicability of spoofing with possession of a valid certificate chain and a legitimate private key, without explicitly considering certain mitigations as additional burden to the user experience (SunSpec, 2025). This is a practical demonstration of how DER security is commonly a tradeoff between high cryptographic posture and practical usability, a problem which recurs later in this review when it comes to the topic of authentication workflow and IDS alert load.

5. ENCRYPTION AND KEY MANAGEMENT IN DER SMART-GRID COMMUNICATIONS

In smart grids organized with DER, encryption is mostly used to impose message trusts within conditions of operation, as opposed to the mere assurance of privacy. Its performance is closely bound with strong key management, including safe material of key, key diversity and rekeying or revocation of key periodically. The systems based on the same keys or similar credentials used by a high population of DER systems are susceptible to the so-called break-once, break-everywhere failures, where a single endpoint may spread across the infrastructure when compromised (Pillitteri and Brewer, 2014). One of the main security points of contention is key management at scale. The AMI deployment experience demonstrates that messages may be leaked to attackers and confidentiality and integrity cannot be guaranteed due to poor cryptographic key handling, and the same argument can be applied to the DER fleets, aggregators, and gateways that are expected to manage the provisioning, rotation, and revocation of credentials in a distributed ecosystem (Ghosal and Conti, 2019). Although the cryptographic algorithms recommended by the FIPS and determined by the NIST represent a secure baseline, a real-world DER implementation may be limited, e.g., by computational or protocol constraints, which can compel a different approach or implementation (Pillitteri and Brewer, 2014). This means that utilities and integrators should not only make sure that DER communications are encrypted but also make cryptographic building blocks that are durable, implementable and maintainable throughout the device's operational lifetime. Transport-layer security is a typical method of obtaining security for DER communications. The IEC 62351-3 specifies TLS using X.509 certificates over TCP-based power system protocols and requires mutual authentication and integrity of the message but not confidentiality. It facilitates long-lasting sessions and several certificate authorities per device, which makes DER ecosystems multi-stakeholder (Schlegel *et al*., 2017). Nonetheless, weaker communication channels may co-exist with optional insecure modes, and so backward compatibility and optional insecure modes may permit this provided that it is properly managed. Vendors of DER can also focus on interoperability rather than security and leave potentially insecure paths open in deployed systems (Schlegel et al., 2017).

SJIF Impact Factor (2026): 8.863| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 3 | March 2026 - Peer Reviewed Journal

Strong cryptography at the DER edge is operationalized by implementation profiles like SunSpec IEEE 2030.5 V2G-AC, which requires endpoints to share certificates during handshakes over HTTPS/TLS and to impose allowlists or certificate attributes as an extra authorization criterion (SunSpec, 2025). In this stringent minimum, there is still residual man-in-the-middle risk when the private keys or chains of certificates are compromised, and so TLS needs to be supplemented by extensive identity, credential issuance, and revocation procedures.

The protocol-specific analyses explain how the premises of authentication and integrity are given more importance than confidentiality. To give an example, the DNP3 Secure Authentication v5 framework is largely focused on spoofing, message alteration, and replay protection, whereas eavesdropping is only covered when it comes to key exchanges (Cremers *et al*., 2019). It is also recommended to use more resistant asymmetric cryptography and to use HMAC-SHA-256 instead of HMAC-SHA-1. With these DER deployments using DNP3-like control semantics, secure operation is attained in case messages are authenticated and anti-replay and confidentiality is selectively implemented according to the sensitivity of telemetry and the exposure of underlying networks (Cremers *et al*., 2019).

Encryption also impacts monitoring and intrusion detection. TLS-Protected IEC 61850 traffic does not allow the description of the payload, forcing the detection system to analyze the endpoint behavior, semantics of protocols, and correlated authentication or authorization telemetry (Ustun *et al*., 2022). This further justifies the importance of integrating encryption and key management with IDS policies to ensure observability and allow credible detection of anomalies.

In general, DER encryption must be incorporated into a credential lifecycle system, namely, unique credentials, controlled cryptoperiods, revocation distribution, and domain-scoped trust. Protocol security should be measured against the real guarantees, that is, authenticity and integrity as opposed to confidentiality, instead of the nominal compliance labels (Pillitteri and Brewer, 2014; Cremers *et al*., 2019). This makes sure that DER communications are reliable besides meeting the operational needs, which form the basis to authentication and IDS mechanisms in the further sections.

6 AUTHENTICATION, AUTHORIZATION, AND ACCESS CONTROL FOR DER ECOSYSTEMS

DER security relies on the determination of who is permitted to make commands, make modifications, and attest to device state and the way identity is defined within a multi-entity ecosystem that contains utilities, aggregators, vendors, and customers (DOE, 2022). According to DOE guidance, role/responsibility definitions, DER trust model, and standard practices that is multifactor authentication, certificate-based verification, cryptographically secure access-control policies, and many more are all required (DOE, 2022). Such steps are essential so as to implement accountability, safeguard operational integrity and ensure secure communication in multi-stakeholder deployments of DER.

Authentication determines identity and authorization determines what can be performed by an authenticated entity (Stouffer *et al*., 2015). In DER systems, an authenticated device or user can create security incidents even when the authentication policies are correctly configured to permit authenticated users to issue the DER dispatch commands or update the protection settings, e.g., by permitting every authenticated operator to issue the DER dispatch commands. Scale, latency and resource constraints also complicate authentication. DER endpoints, such as inverters, gateways, and controllers, have limited compute capability, extended lifespan, and disconnected connectivity, where efficient and robust authentication strategies are needed (Qasaimeh *et al*., 2019). Challenge/response systems cannot be feasible on the human access path in ICS networks because of latency yet could be applicable in network service authentication (Stouffer *et al*., 2015).

Mutual authentication with the use of certificates is the real-world minimum of DER systems, it allows scalable identity and revocation which is secure. TLS using X.509 certificates and mutual authentication is required in IEC 62351-3, and role-based access control that extends to human and automated agents is defined in IEC 62351-8 (Schlegel *et al*., 2017). DES implementation profiles, including SunSpec IEEE 2030.5 V2G-AC, implement this scheme by requiring endpoints to send and receive certificates during TLS handshakes, imposing allowlists, and adding certificate attributes as extra authorization principles (SunSpec, 2025).

There should also be authenticated local autonomy in the case of compromised connectivity. The NISTIR 7628 emphasizes that the authentication and authorization capabilities should be maintained even when the network is not operational, with the help of the secure key management, ensuring the key uniqueness, lifecycle protection, and alerting on key revocation across the DER fleet (Pillitteri & Brewer, 2014). This operationally demands scalable issuance of certificates, distribution of revocation and contingency modes of fielded devices. Lastly, the nature of OT systems operations implies the need to take into account password-based access, MFA, and the safe processing of human and third-party access (Stouffer *et al*., 2015). IEEE 1547 underlines that DER cybersecurity is systemic, local interfaces should be handled with care, e.g., turned off by default and reachable only with controlled authentication protocols (Photovoltaics and storage, 2018). DER ecosystems authentication is a type of control problem of the ecosystem, that is, it is identity-

SJIF Impact Factor (2026): 8.863| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 3 | March 2026 - Peer Reviewed Journal

based authentication based on certificates, authorization that depends on policies, and OT-safe access control methods based on the realities of the U.S. deployment (DOE, 2022; Photovoltaics and Storage, 2018).

7. ARTIFICIAL INTELLIGENCE-BASED INTRUSION AND ANOMALY DETECTION OF DER-BASED SMART GRIDS

With the use of ICT-enabled monitoring and automated control, intrusion detection and anomaly monitoring are mandatory operational needs instead of optional ones as smart grids are being implemented. ICS guidance emphasizes that the OT setting needs detection solutions that comply with availability and safety limitations, and that the traditional IDS approaches should take into consideration encrypted traffic as well as restricted field devices (Stouffer *et al*., 2015; Reda *et al*., 2021; Pillitteri and Brewer, 2014; Yaacoub *et al*., 2025).

The integration of DER enlarges the attack surface, making the number and variety of endpoints such as inverters, gateways, aggregators, and field controllers more, creating more distributed loops of automation, such as islanding and protection functions, which attackers can use (Elmasry, 2024). AI/ML-based IDS are useful to complement preventive controls including encryption and authentication to detect manipulations, replay attacks and protocol abuse that preventive mechanisms cannot cover entirely. Operationally feasible detection through IDS in IEC 61850/GOOSE deployments may be available when the cryptography is inadequate and lacking on the legacy devices (Elmasry, 2024).

AI-based IDS is a protocol-sensitive feature engineering method that encodes anticipated operational behavior with policy-based operational rules, statistical or machine-learning (supervised, unsupervised, or hybrid) classifiers and statistical or machine-learned features. Multi-dimensional anomaly detection is possible in IEC 61850 networks using high-fidelity datasets, including those of Electric Power and Intelligent Control (EPIC) testbeds, on feature extraction of measurements and control commands (Tan *et al*., 2024; Yang *et al*., 2016; DOE, 2022). Its prevalence, for example, the use of encryption, such as TLS in IEC 62351 makes the payloads invisible, and the IDS must operate based on metadata, behavioral patterns, and protocol-state monitoring (Ustun *et al*., 2022; Reda *et al*., 2021; Pillitteri and Brewer, 2014).

Evaluation and dataset realism are also significant bottlenecks. Decent quality labeled data is limited as it is sensitive to operations, not provided by default, and may compromise security, which forces the generation of data and its simulation and testbed to be validated through IDS models (Tan *et al*., 2024; Elmasry, 2024). The new edge or fog deployment models minimize the latency and bandwidth overheads, yet they also present issues regarding governance, model integrity and resistance to adversarial manipulation (Sanjalawe *et al*., 2025; Alsirhani *et al*., 2025; Yaacoub *et al*., 2025). In U.S. DER deployments, it then follows that IDS should be designed as an operationally aware integrated component, both in detection and evaluation and in adaptation to ensure resiliency across any type of DER system (Stouffer *et al*., 2015; Reda *et al*., 2021; Pillitteri and Brewer, 2014).

8. SYNTHESIS: U.S. DER DEFENSE-IN-DEPTH REFERENCE ARCHITECTURE

One of the key conclusions of U.S. DER cybersecurity studies is that security is not a characteristic of devices, but a characteristic of the system, including utilities, aggregators, vendors, customer networks, and field operations (DOE, 2022; Photovoltaics and Storage, 2018; Pillitteri and Brewer, 2014). Continuing the findings of the earlier sections, deployable defense-in-depth architecture needs to be able to consider the OT limitations, the realities of interoperability in DER, and modern threats such as protocol abuse, credential compromise, and multi-device coordinated manipulation (Stouffer *et al*., 2015; Reda *et al*., 2021; Cremers *et al*., 2019). The general objective is to ensure operational integrity at the time of attack as well as recognize that it is not possible to prevent all intrusions. This practice of resilience is consistent with the recommendation of ICS, where the emphasis on single-point control is avoided and layered defenses are also encouraged. Since IEEE 1547 does not dictate the standardized design of DER cybersecurity, the architecture must be adaptable to support various communication routes and jurisdictional needs (Photovoltaics and Storage, 2018). The initial layer is aimed at reducing the exposure and diminishing pathways. The default-off local communication of DER interfaces should be provided, and secure networking devices must be used to provide controlled access to fielded DERs. Segmentation introduces fewer direct conduits between business and control network, whereas permitted gateways are in control of trust destinations across DER ecosystems (Stouffer *et al*., 2015; DOE, 2022; Pillitteri and Brewer, 2014).

The second layer means secure communications based on profile-driven encryption as opposed to best-effort TLS. DER pathways based on IEEE 2030.5 have rigid baselines, such as HTTPS with mutual certificate authentication. The pathway is resistant to compromising of its private-key or certificate trust failure (SunSpec, 2025). In case of utility automation protocols, the IEC 62351 provides authentication, integrity and optional confidentiality protection. Nevertheless, similarity and mutability (compatibility) between secure and insecure modes can compromise the security unless there is governance that uses secure modes as the default (Schlegel *et al*., 2017; Mekkanen, 2021). Protocol-specific security analysis also explains that certain standards give more weight to integrity/authentication

SJIF Impact Factor (2026): 8.863| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 3 | March 2026 - Peer Reviewed Journal

than to confidentiality and may need extra security where it is required that the information remains secret (Cremers *et al*., 2019; Stouffer *et al*., 2015).

The third layer deals with key management and identity scale. DER fleets must have special credentials, lifecycle management, revocation, local autonomy to operate safely even in the outage (Pillitteri & Brewer, 2014; Ghosal & Conti, 2019; Hernandez-Alvarez et al., 2025). Authentication is accompanied by authorization to apply role-based access and least-privilege policies based on the operations of the organization and functions of the device, especially in cross-organization DER control chains (Schlegel et al., 2017; DOE, 2022).

Protocol and process-aware detection is combined into the fourth layer. Even with intense cryptography and identity, the DER systems are susceptible to credential theft, misconfigurations, compromise of the supply-chain, and semantic protocol abuse. IDS is a safety net, and AI-based IDS is taking advantage of protocol awareness and behavior modeling, as well as high-fidelity datasets to match anomalies and fewer false alarms (Stouffer *et al*., 2015; Yang *et al*., 2016; Reda *et al*., 2021; Hussain *et al*., 2019). The Latency and bandwidth constraints are also dealt with through the edge/fog deployment, and the model robustness and governance are considered (Alsirhani *et al*., 2025; Sanjalawe *et al*., 2025; Yaacoub *et al*., 2025).

These layers shape a unified U.S ready blueprint when they are put together. Exposure is minimized by segmentation, secure gateways and controlled remote access. Data in transit is secured by certificate-backed communications, and protocol-compliant encryptions. Key and identity control on a fleet level ensures there is continuity in operations, whereas AI-based and protocol-conscious IDS offers real-time tracking despite the encryption diminishing face-to-face visibility (Pillitteri & Brewer, 2014; Tan *et al*., 2024; Elmasry, 2024). Lastly, meeting multi-stakeholder trust models would resolve the threat of emergent coordination risks, such as cross-vendor and aggregator interactions (DOE, 2022; Chen *et al*., 2025; Rashid *et al*., 2025; Ajiboye *et al*., 2024). This holistic, multi-layered partnership explains the reason why recent reviews promote hybrid solutions involving the combination of edge analytics, strong identity management, and coordinated governance instead of depending on cryptography or AI only (Yaacoub *et al*., 2025; Rashid *et al*., 2025; Sanjalawe *et al*., 2025).

9. GAPS

There has continually been a discontinuity between standard-level intent and deployment-level enforceability in the framework of DER-enabled smart-grid security. IEEE 1547 recognizes that cybersecurity is a system-wide phenomenon and does not specify a specific security requirement at the DER interface, which is left to utilities and regulators to translate interoperability to operationally testable security is perceived in heterogeneous DER fleets (Photovoltaics and Storage, 2018). Meanwhile, the guidance of the U.S. DER focuses on resilience, which is designing defenses to ensure critical functionality in the face of attack, but the model with respect to trust remains unimplemented uniformly among utilities, aggregators, vendors or customers (DOE, 2022). Recent surveys on DER within the context of the systems perspective further affirm this architecture of multi-stakeholder DER and the necessity to have frameworks of defense-in-depth, as opposed to single control (Chen *et al*., 2025).

The second gap is a key management at scale which is the practical constraint of encryption and authentication. NIST specifically cautions against systemic vulnerability due to shared keys/credentials and stresses key diversity, key revocation and key lifecycle management (Pillitteri and Brewer, 2014). Nonetheless, the AMI-oriented work still reveals that secure two-way communication heavily relies on an effective management of the session keys under storage, processing, and dynamic group-participatory constraints, precisely the type of constraints that also emerge in DER fleets and in coordination by aggregators (Ghosal and Conti, 2019; Hernandez-Alvarez *et al*., 2025; Ajiboye *et al*., 2024; Gupta *et al*., 2022). This is the direction of the research that is not as focused on stronger algorithms, but on operationally viable credential lifecycle engineering, it should be able to provision at deployment scale, revocation distribution that is able to work when connectivity becomes degraded, and governance models that can survive change of vendors and ownership of assets over long asset lifetimes (Pillitteri and Brewer, 2014; Photovoltaics and storage, 2018).

The third gap relates to deterministic security of the time-bound power-system messaging when cryptography is to be undergoing tight latency requirements. The environments of IEC 61850 need to support fast processing of GOOSE/SV messages, and the work shows that the security of the messages is not a problem of cryptography only, but also an architectural concern, and the fixed-latency design approach aims to maintain timing constraints and introduce the protection mechanisms (Rodriguez *et al*., 2021). Simultaneously, the security assessment of IEC 62351 indicates that backward compatibility and optional insecure modes may diminish real-life posture provided that the implementation allows a secure and insecure channel to coexist or falls behind the current cryptographic standards (Schlegel *et al*., 2017; Mekkanen, 2021). The vulnerability and impact analysis of GOOSE also shows that physical operation can be impacted by realistic adversaries through a falsified scenario, which underscores the necessity to protect it in a protocol-conscious and operationally enforceable manner (Reda *et al*., 2021; Hussain *et al*., 2019). The secure-by-default and interoperable profiles with

SJIF Impact Factor (2026): 8.863| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 3 | March 2026 - Peer Reviewed Journal

quantifiable timing and assurance attributes, not the security which is available when inconsistently enabled is also a key research requirement (Schlegel *et al*., 2017; Photovoltaics and Storage, 2018).

The fourth gap is the operational credibility of AI-powered intrusion detection, particularly because the payload is diminished due to encryption. The IEC 61850 traffic work demonstrates that in the case of applying TLS-based protection, monitoring tools no longer have direct access to the content, and they must depend more on behavior, timing, and protocol/process semantics (Ustun *et al*., 2022; Pillitteri and Brewer, 2014). In the meantime, research on IDS has found dataset realism as the fundamental obstacle as high-fidelity datasets are infrequent, labeling is costly, and operators are unwilling to share operational traces to enhance reproducibility and external validity (Tan *et al*., 2024; Elmasry, 2024). The proposed multi-dimensional and protocol-sensitive IDS designs are perspective since they align detection to power-system behavioral features as opposed to generic IT signature but demand assessment regimes that represent actual operational limitations (Yang *et al*., 2016; Reda *et al*., 2021).

Lastly, there is convergence on distributed and edge/fog deployment models of security enforcement and security detection driven by latency, bandwidth and scalability demands. Survey work in smart-grid security and intelligent energy systems has identified the importance of AI-driven monitoring, emerging architectures, and false-positive and robustness management (Sanjalawe *et al.*, 2025; Yaacoub *et al*., 2025). IDS architectures that bring analytics to the grid edge are placed in a position to achieve shorter detection latency and alleviate centralized bottlenecks, but then raise new governance and trust concerns, particularly in cases where learning, updates, and model integrity have to be managed across multiple operators and vendors (Alsirhani *et al*., 2025; Rashid *et al*., 2025; DOE, 2022).

10. RECOMMENDATIONS

The first gap to fill in the standard level and deployment level gap on security is to establish clear operational security baselines of DER by the utilities and the regulators, which have operational policies and audit procedures. The multi-stakeholder trust models are to be formalized, defining the responsibilities among the utilities, aggregators, vendors, and customers, and having integrated defense-in-depth. In the case of the most significant management gap, DER deployments should adopt scalable credential lifecycle management, which consists of unique device credentials, automated revocation, rekeying, and provisioning workflows. Mechanisms such as redundancy, local autonomy, etc. must be designed to ensure security in times of degraded connectivity or switching vendors. A strategy to reduce the time-sensitive messaging gap is through the use of secure-by-default protocols where throughput of fixed-latency guarantees, and timing and integrity checking of GOOSE/SV messages. Profiles should be checked with the reality of time constraints before they are deployed. In the case of the AI-based IDS restrictions, the operators can devise high-fidelity anonymized datasets and simulation testbeds to test them out plus protocol- and process-sensitive IDS that will operate on encrypted traffic. False positives, latency and operational impact should be considered by the IDS tuning. Lastly, as a way of dealing with the difficulties of distributed/ edge/fog deployments, operators should employ well-developed governance models to coordinate learning updates, model integrity and multi-operators' coordination, and ensure that latency, bandwidth and reliability requirements are met.

11. FUTURE DIRECTIONS

Based on these gaps, future research and development needs to work on developing resilient, scalable and operationally feasible DER security systems. This involves coming up with enforceable, interoperable standards and profiles that are in accordance with operational timing limits, secure-by-default settings and multi-actor governance. It also involves the development of credential lifecycle management methods of DER fleets, low-latency cryptographic assessment, and combination of AI-based scale detectors with strong datasets, simulation test beds, and edge/fog deployments. Lastly, the research needs to focus on multi-stakeholder trust modeling and coordinated response systems to be able to assure security and reliability of utilities, aggregators, vendors, and customer arenas.

12. CONCLUSION

DER-enriched smart grids require the design of cybersecurity that is based on operational integrity as opposed to a secondary IT service. This review revealed that encryption can only work as well as scalable key management and profile discipline, authentication should be more than device identity and enforcing least-privilege authority across utilities, aggregators, vendors and customer interfaces, and AI-based intrusion detection is increasingly needed to detect abuse, misconfiguration, and coordinated manipulation which cannot be completely blocked by the protective measures. With a deployment that implements more robust transport protections, detection and response needs to be improved to behavior and protocol-aware monitoring that has been validated using realistic operational data. Defense-in-depth architecture, limiting exposure, imposing cryptographically verifiable trust, and implementing monitoring in the way critical grid functions can safely proceed even in the face of active attack is the most plausible way forward.

SJIF Impact Factor (2026): 8.863| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 3 | March 2026 - Peer Reviewed Journal

REFERENCES

1. *Ajiboye, P. O., Agyekum, K. O. B. O., & Frimpong, E. A. (2024). Privacy and security of advanced metering infrastructure (AMI) data and network: a comprehensive review. Journal of Engineering and Applied Science, 71(1), 91.*
2. *Alsirhani, A., Tariq, N., Humayun, M., Naif Alwakid, G., & Sanaullah, H. (2025). Intrusion detection in smart grids using artificial intelligence-based ensemble modelling. Cluster Computing, 28(4), 238.*
3. *Chen, J., Yan, J., Kemmeugne, A., Kassouf, M., & Debbabi, M. (2025). Cybersecurity of distributed energy resource systems in the smart grid: A survey. Applied Energy, 383, 125364.*
4. *Cremers, C., Dehnel-Wild, M., & Milner, K. (2019). Secure authentication in the grid: A formal analysis of DNP3 SAv5. Journal of Computer Security, 27(2), 203-232.*
5. *DOE, U. (2022). Cybersecurity Considerations for Distributed Energy Resources on the US Electric Grid.*
6. *Elmasry, A. (2024). Developing and Evaluating Simulation Testbeds for IEC61850 GOOSE Protocol: Enhancing Cybersecurity in Substations and Smart Grids (Master's thesis, Hamad Bin Khalifa University (Qatar)).*
7. *Ghosal, A., & Conti, M. (2019). Key management systems for smart grid advanced metering infrastructure: A survey. IEEE Communications Surveys & Tutorials, 21(3), 2831-2848.*
8. *Gupta, K., Kumar, V., & Prakash, R. (2025). An Efficient Approach to Key Management for Bidirectional Communication in AMI System of Smart Grids. Procedia Computer Science, 259, 1179-1188.*
9. *Hussain, S. S., Ustun, T. S., & Kalam, A. (2019). A review of IEC 62351 security mechanisms for IEC 61850 message exchanges. IEEE Transactions on Industrial Informatics, 16(9), 5643-5654.*
10. *Mekkanen, M. (2021). IEC 62351 Data and Communication Security: Power Systems Management and Associated Information Exchange. https://www.uwasa.fi/sites/default/files/2022-11/WP3_TR3.2_0.pdf*
11. *Photovoltaics, D. G., & Storage, E. (2018). IEEE standard for interconnection and interoperability of distributed energy resources with associated electric power systems interfaces. IEEE std, 1547(1547), 2018.*
12. *Pillitteri, V. Y., & Brewer, T. L. (2014). Guidelines for smart grid cybersecurity.*
13. *Qasaimeh, M., Turab, R., & Al-Qassas, R. S. (2019). Authentication techniques in smart grid: a systematic review. TELKOMNIKA (Telecommunication Computing Electronics and Control), 17(3), 1584-1594.*
14. *Rashid, M. M., Mosarat, Z., Habib, A. A., Ghosh, A., Rahman, K. S., Sultan, S. M., ... & Rokonuzzaman, M. (2025). A Comprehensive Review of Cybersecurity Challenges and Resilience Strategies in Renewable Energy Integration with Battery Storage for Sustainable Smart Grids. Results in Engineering, 108557.*
15. *Reda, H. T., Ray, B., Peidaee, P., Anwar, A., Mahmood, A., Kalam, A., & Islam, N. (2021). Vulnerability and impact analysis of the IEC 61850 GOOSE protocol in the smart grid. Sensors, 21(4), 1554.*
16. *Sanjalawe, Y., Fraihat, S., Makhadmeh, S. N., & Alzubi, E. (2025). aI-powered smart grids in the 6G era: A comprehensive survey on security and intelligent energy systems. IEEE Open Journal of the Communications Society.*
17. *Schlegel, R., Obermeier, S., & Schneider, J. (2017). A security evaluation of IEC 62351. Journal of Information Security and Applications, 34, 197-204.*
18. *Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). Guide to Industrial Control Systems (ICS) Security. NIST Special Publication, 800, 82.*
19. *SunSpec, A. (2025). IEEE 2030.5 V2G-AC Profile Implementation Guide for SAE J3072. https://sunspec.org/wp-content/uploads/2009/03/SunSpec-IEEE-2030.5-V2G-AC-Profile-v1.0.pdf*
20. *Tan, H. C., Hossain, M. A., Mashima, D., & Kalbarczyk, Z. (2024, September). High-fidelity Intrusion Detection Datasets for Smart Grid Cybersecurity Research. In 2024 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm) (pp. 340-346). IEEE.*
21. *Ustun, T. S., Hussain, S. S., & Kalam, A. (2022). Performance evaluation of IEC 61850 MMS messages under cybersecurity considerations. Energy Reports, 8, 1189-1199.*
22. *Yaacoub, J. P. A., Noura, H. N., Salman, O., & Chahine, K. (2025). Toward secure smart grid systems: risks, threats, challenges, and future directions. Future Internet, 17(7), 318.*
23. *Yang, Y., Xu, H. Q., Gao, L., Yuan, Y. B., McLaughlin, K., & Sezer, S. (2016). Multidimensional intrusion detection system for IEC 61850-based SCADA networks. IEEE Transactions on Power Delivery, 32(2), 1068-1078.*