Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X
Volume 3, Issue 8, 2025

TOWARD SECURE AND PRIVACY-PRESERVING SMART GRIDS: COMMUNICATION ARCHITECTURES, CYBERSECURITY INNOVATIONS, AND POLICY FRAMEWORKS

Ibraheem Salim[1], Usama Ahmad Mughal[*2], Omer Naveed[3], Sohaib Hafeez[4]

[1]Knowledge Unit of Systems &Technology, University of Management and Technology, Sialkot, Pakistan.
*[*2]Department of Cyber Security, NASTP Institute of Information Technology Lahore, Pakistan.*
[3]Plant Manager, Oursun Pakistan Ltd, 50MWp Solar Power Generation Power Plant, Senior Member ISA USA, Member IEEE USA & PMI USA.
[4]Department of Mechatronics Engineering, Huazhong University of Science and Technology, China.

[1]isaleem7@gmail.com, [*2]usamaahmad@niit.edu.pk, [3]onaveed@yahoo.com, [4]sohaib.hafeez@hotmail.com

DOI: https://doi.org/10.5281/zenodo.17033942

Keywords
Smart grid communication, cybersecurity, data privacy, resilient power systems, ICT, blockchain, machine learning, policy frameworks, secure architectures, privacy-preserving technologies.

Article History
Received: 30 May, 2025
Accepted: 05 August, 2025
Published: 30 August, 2025

Copyright @Author
Corresponding Author: *
Usama Ahmad Mughal

Abstract

The modernization of power systems into smart grids has introduced unprecedented opportunities for efficiency, automation, and sustainability. By leveraging advanced communication architectures and information technologies, smart grids enable real-time data exchange between generation units, transmission systems, distribution networks, and end-users, thereby optimizing energy management and facilitating the integration of renewable resources. However, the reliance on interconnected digital infrastructures exposes smart grids to significant vulnerabilities, including cyberattacks, unauthorized data access, and privacy breaches, which threaten the stability and resilience of critical energy infrastructures. Addressing these challenges requires a holistic approach that combines technological innovation, secure communication frameworks, and policy-driven governance. This paper presents a comprehensive analysis of secure and privacy-preserving smart grids with a focus on communication architectures, cybersecurity mechanisms, and policy frameworks. Emerging technologies such as blockchain-based energy transactions, federated learning for distributed data analytics, and lightweight cryptographic protocols for resource-constrained devices are explored as enablers of resilient and secure smart grid operations. Additionally, machine learning and artificial intelligence techniques for intrusion detection, anomaly detection, and predictive risk management are highlighted as essential tools for safeguarding grid infrastructures against evolving cyber threats. From a privacy standpoint, privacy-preserving data aggregation, differential privacy methods, and decentralized communication models are discussed to protect sensitive *consumer data while ensuring system efficiency. Beyond technological solutions, this study emphasizes the critical role of coherent policies, international standards, and cross-border regulatory frameworks in shaping the secure adoption of smart grid technologies. The interplay between innovation and governance is examined to illustrate how cybersecurity laws, data protection regulations, and industry standards can mitigate risks while fostering trust among stakeholders. By integrating perspectives from communication technologies, cybersecurity innovations, and policy frameworks, this work not only underscores the challenges inherent in deploying secure and privacy-aware smart grids but also identifies pathways for future research and practical implementation. The findings aim to guide researchers, policymakers, and industry stakeholders toward the development of resilient, adaptive, and trustworthy smart grid ecosystems capable of addressing the evolving demands of modern power systems.*

INTRODUCTION

The transformation of traditional power systems into intelligent and interconnected smart grids represents one of the most significant technological shifts in modern energy infrastructures. Smart grids combine power engineering with advanced information and communication technologies to achieve real-time monitoring, efficient energy management, and seamless integration of renewable energy sources. According to recent reports from the International Energy Agency, global investments in smart grid deployments have already exceeded hundreds of billions of dollars, underscoring their central role in meeting future energy demands while advancing sustainability goals. Unlike conventional grids, which operated largely as unidirectional energy delivery systems, smart grids enable bidirectional flows of electricity and information, bringing consumers into the energy ecosystem as active participants through distributed generation, electric vehicle integration, and demand-response programs [1]. At the foundation of this new paradigm lies a sophisticated communication architecture that interconnects sensors, smart meters, supervisory control systems, and advanced metering infrastructures. These cyber–physical interactions extend across generation plants, transmission systems, distribution networks, and consumer endpoints. While this interconnectedness enables operational intelligence and optimization, it also creates unprecedented vulnerabilities. The expansion of digital interfaces increases the attack surface, exposing grid infrastructures to malicious actors capable of compromising confidentiality, integrity, and availability of critical services. Recent cyber incidents, such as the malware-induced blackouts in Ukraine in 2015 and the Colonial Pipeline ransomware attack in 2021, have demonstrated that energy infrastructures are prime targets for adversaries and that disruptions in this sector can lead to cascading failures, economic instability, and threats to public safety [2]. Moreover, privacy risks are rising sharply as the collection of high-resolution consumer energy data can reveal sensitive information about household occupancy, appliance usage, and personal behavior, thereby raising ethical and regulatory concerns regarding data misuse and surveillance. The spectrum of security and privacy challenges in smart grids is broad and multifaceted. Confidentiality breaches may occur through eavesdropping on advanced metering infrastructures, while false data injection attacks can compromise the integrity of supervisory control and data acquisition systems. Denial-of-service attacks on utility backhaul networks or AMI head-ends threaten system availability, and adversarial inference from smart meter readings directly compromises consumer privacy [3]. These representative threats, along with their potential consequences, are summarized in Table 1, which illustrates the diverse vulnerabilities that smart grids must address in order to achieve reliable and resilient operation.

Table 1: Representative Threats to Smart Grid Ecosystem

Threat Category	Example Attack	Potential Impact
Confidentiality	Data eavesdropping on AMI	Leakage of customer usage patterns; privacy violations
Integrity	False data injection in SCADA	Incorrect dispatch, cascading failures
Availability	DoS on AMI head-end or control center	Service disruption, delayed response
Privacy	Inference from smart meter data	Household behavior profiling, surveillance risks
Supply Chain	Malicious firmware update	Persistent backdoor in devices

Although significant progress has been made in securing power networks, existing approaches often remain fragmented and insufficient. Much of the literature focuses on isolated solutions such as encryption, intrusion detection, or blockchain-based energy trading without integrating these mechanisms into a coherent framework that simultaneously addresses scalability, privacy preservation, and regulatory compliance. For instance, advanced cryptographic schemes are often too computationally expensive for resource-constrained devices deployed at the grid edge, while machine learning–based anomaly detection systems frequently struggle to balance accuracy with explainability and energy efficiency [4]. Similarly, although privacy-enhancing technologies such as differential privacy and federated learning have been proposed, their large-scale deployment in heterogeneous smart grid environments remains limited. At the same time, the regulatory landscape is evolving rapidly, with instruments such as the European General Data Protection Regulation (GDPR), the North American NERC Critical Infrastructure Protection (CIP) standards, and international norms such as ISO/IEC 27019 introducing new compliance requirements that are not always aligned with the pace of technological innovation [5]. Addressing these shortcomings requires a holistic and interdisciplinary approach that integrates secure communication architectures, advanced cybersecurity mechanisms, and coherent governance frameworks. This paper contributes to the field by analyzing smart grid security and privacy from three complementary dimensions. The first is the communication infrastructure, where emphasis is placed on the architectural backbone that ensures interoperability and trustworthiness across heterogeneous components. The second dimension is cybersecurity innovation, where emerging technologies such as blockchain-enabled energy transactions, lightweight cryptographic protocols, and artificial intelligence–driven intrusion detection are explored in terms of their practical feasibility and resilience [6]. The third dimension is the role of policies, standards, and governance, which are shown to be essential in shaping the secure adoption of technologies while fostering trust among international stakeholders. The integration of these dimensions into a single analytical framework is depicted in Figure 1, which highlights how communication, technological defense, and policy mechanisms converge to build resilient and privacy-aware smart grids.

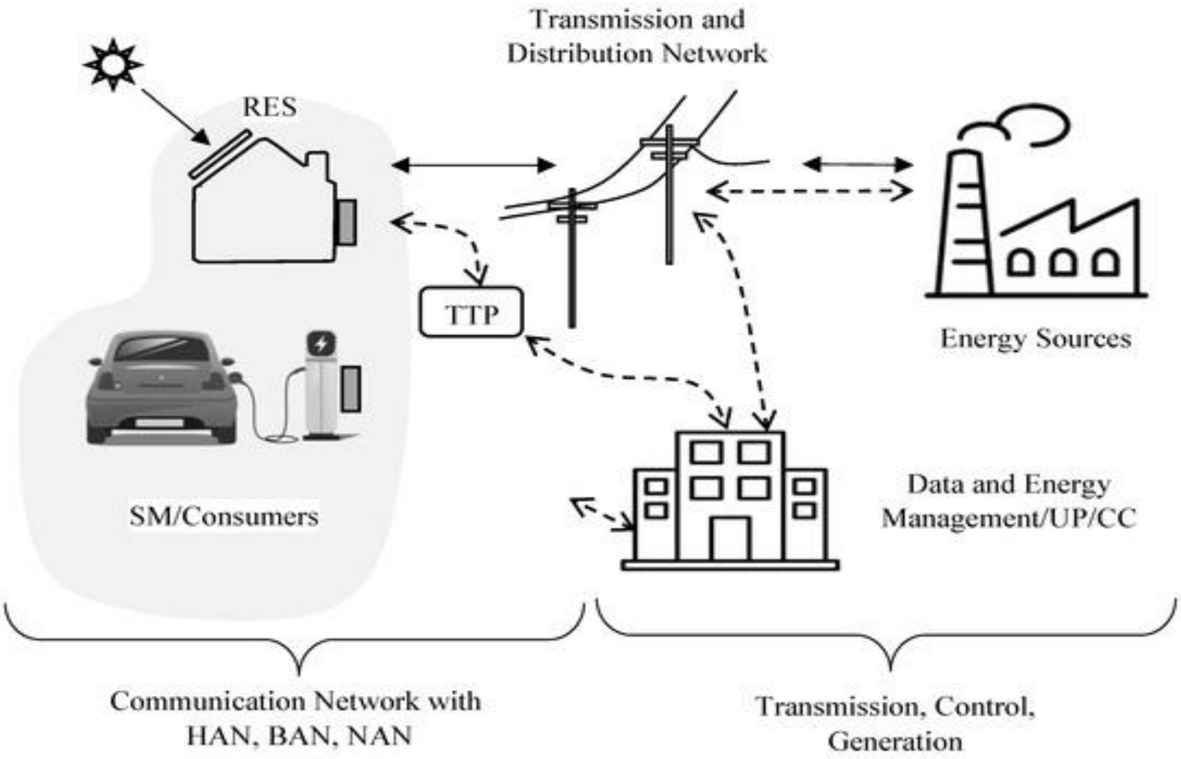
Transmission and Distribution Network
RES
TTP
Energy Sources
SM/Consumers
Data and Energy Management/UP/CC
Communication Network with HAN, BAN, NAN
Transmission, Control, Generation

Figure 1: Conceptual Framework for Secure and Privacy-Preserving Smart Grids

This integrated perspective also reveals persistent gaps in existing research, which this paper seeks to address. As summarized in Table 2, these include the lack of scalable security solutions for low-resource devices, the absence of comprehensive evaluation metrics that jointly consider resilience, latency, and privacy, and the insufficient mapping between technical innovations and regulatory requirements.

Table 2: Research Gaps and Contributions of this Paper

Research Gap	Contribution of this Paper
Fragmented treatment of technical vs. policy	Provides an integrated analysis of communication, security, policy
Scalability limitations of cryptographic tools	Reviews lightweight and efficient protocols for AMI and DER nodes
Narrow evaluation metrics	Proposes resilience–latency–privacy rubric for performance analysis
Weak regulatory alignment	Maps technical controls to GDPR, NIST, and ISO/IEC

	standards

The introduction establishes the dual nature of smart grids as both enablers of energy modernization and potential sources of vulnerability. It positions the present study as a comprehensive exploration of secure and privacy-preserving smart grids, integrating communication technologies, cybersecurity innovations, and policy frameworks into a unified discussion [7]. By providing this interdisciplinary perspective, the paper not only underscores the urgency of addressing cyber and privacy risks but also charts a forward-looking research agenda for building resilient, adaptive, and trustworthy smart grid ecosystems.

2- Smart Grid Communication Infrastructures:

The modern smart grid represents a convergence of electrical power systems with advanced information and communication technologies, designed to meet the dual challenges of energy sustainability and infrastructure resilience. At its core, the smart grid is more than an upgraded distribution network; it is a cyber–physical system where communication infrastructures orchestrate interactions among generators, substations, utilities, and end-users. These infrastructures ensure the bidirectional exchange of information necessary for real-time control, demand-side management, and integration of renewable and distributed energy resources (DERs). Without robust and interoperable communication backbones, the vision of a secure, adaptive, and efficient smart grid cannot be realized. Globally, smart grid deployments have scaled rapidly. According to the International Energy Agency, by 2023 more than 1.2 billion smart meters had been installed worldwide, generating continuous streams of consumption and operational data [8]. This data must traverse multi-layered communication networks that extend from households to national transmission systems. Unlike traditional grids, which relied primarily on one-way supervisory telemetry and manual control, smart grids depend on layered, interoperable, and low-latency data exchange. This architectural shift brings enormous opportunities but simultaneously introduces a broad spectrum of vulnerabilities [9]. A smart grid communication infrastructure is typically conceptualized in three interconnected domains: the Home Area Network (HAN), the Neighborhood/Field Area Network (NAN/FAN), and the Wide Area Network (WAN). Each of these domains is distinguished by its scale, underlying technologies, performance requirements, and security considerations, yet all must interoperate seamlessly to ensure reliable grid functionality.

2.1- Home Area Network (HAN):

The Home Area Network (HAN) forms the consumer-facing edge of the smart grid and constitutes the most immediate interface between end-users and advanced energy infrastructures. Situated within the confines of a household or small building, it brings together a diverse collection of components including smart appliances, electric vehicle charging stations, rooftop solar inverters, home batteries, and, most critically, the smart meter that serves as both a data aggregation hub and the primary gateway to the wider utility network. Through this integration, the HAN enables two-way communication that not only provides consumers with detailed information about their energy usage but also facilitates their participation in demand-response programs, dynamic pricing, and distributed energy resource management [10]. The technological foundation of HANs is built on short-range communication standards optimized for in-home environments. ZigBee remains one of the most widely adopted protocols because of its low-power operation and mesh networking capabilities, making it suitable for connecting meters and appliances across a household. Wi-Fi, by contrast, offers higher data throughput and is often employed for home gateways and advanced smart appliances that require richer communication. Bluetooth Low Energy (BLE) has gained popularity in recent years because of its seamless integration with smartphones and home assistants, enabling intuitive control of energy-aware devices [11]. Power line communication (PLC), which uses existing electrical wiring for data transmission, is another alternative that minimizes the need for new infrastructure and is commonly applied to smart metering and EV charging contexts. A comparative overview of these technologies is presented in **Table 3**, which outlines their range, data rates, advantages, and typical applications. This comparison underscores the diversity of HAN deployments and illustrates how no single technology satisfies all requirements, thereby necessitating hybrid communication approaches in modern households.

Table 3: Common Communication Technologies in Home Area Networks

Technology	Range	Data Rate	Advantages	Limitations	Typical Use Cases
ZigBee	10–100 m	20–250 kbps	Low power, mesh networking	Limited throughput, early security flaws	Smart meters, appliance control
Wi-Fi	30–100 m	Up to 1 Gbps	High data rate, ubiquitous deployment	Higher power consumption, interference	Smart appliances, gateways
Bluetooth Low Energy (BLE)	5–30 m	125 kbps–2 Mbps	Ultra-low power, smartphone integration	Short range, scalability limits	Smart appliances, wearables
Power Line Communication (PLC)	Household wiring	2–200 Mbps	No new wiring required	Noise sensitivity, variable reliability	Smart meters, EV chargers

While HANs bring consumers closer to the operation of the grid, they simultaneously expose a number of vulnerabilities. One of the most pressing concerns relates to **privacy**, since smart meters often record consumption data at very fine-grained intervals, sometimes as frequently as every fifteen seconds. Such high-resolution measurements can be analyzed to infer personal routines, appliance usage, occupancy patterns, and even socio-economic behavior. Without strong safeguards, the risk of consumer surveillance or unauthorized exploitation of this data is significant [12]. The issue of privacy in HANs is further compounded by the fact that data collection is continuous and unavoidable, making consumer trust a crucial factor in the widespread adoption of smart grid technologies. From a **security perspective**, HANs are particularly vulnerable because many of the devices deployed at this level are resource-constrained and operate with limited processing power, memory, or firmware support. As a result, they often cannot support computationally expensive cryptographic operations or frequent security updates. Devices such as smart plugs, sensors, and even some low-cost smart meters may therefore become easy entry points for adversaries [13]. Once compromised, these devices can serve as footholds for launching more sophisticated attacks against higher-level networks such as neighborhood or wide-area infrastructures. For example, poorly secured Wi-Fi connected appliances could be hijacked as part of a botnet or used to inject false data into the utility's billing or control systems. The role of HANs in grid reliability is not only limited to data privacy and security but also extends to performance and latency. Although most household applications can tolerate seconds of delay, certain scenarios such as electric vehicle charging coordination or inverter control for rooftop solar installations require much tighter timing to maintain balance with the wider grid. Similarly, demand-response systems rely on communication latencies of only a few seconds in order to adjust household consumption effectively in response to utility signals. These latency requirements are summarized in **Table 4**, which provides a comparison of typical HAN applications, their performance expectations, and the risks they face.

Table 4: **Representative Applications and Requirements in HANs**

Application	Latency Tolerance	Bandwidth Requirement	Key Risks
Smart Metering	Seconds to minutes	Low	Data leakage, profiling
Demand Response	1–10 seconds	Low–Medium	Manipulation of signals
EV Charging	Sub-second to seconds	Medium–High	Unauthorized access, billing fraud
Rooftop Solar Integration	Sub-second to seconds	Medium	Malicious inverter control
Appliance Automation	Seconds	Low	Unauthorized control, denial of service

The architectural complexity of HANs and their centrality to consumer interaction with the smart grid is illustrated in **Figure 2**, which depicts a household network connecting diverse devices through various communication standards to a smart meter gateway. The figure highlights both the opportunities and vulnerabilities inherent in HANs, including data aggregation, bidirectional control flows, and multiple points where security breaches or privacy violations may occur.

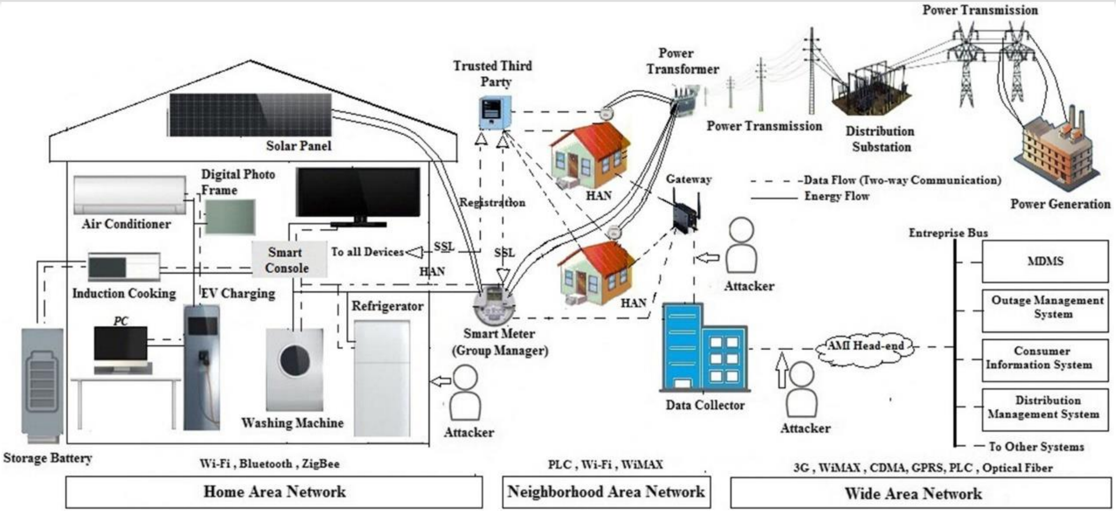

Figure 2: Home Area Network Architecture and Security/Privacy Concerns

In light of these opportunities and risks, it is evident that securing the HAN requires a multifaceted strategy. Lightweight cryptographic algorithms, capable of running efficiently on constrained devices, form a critical foundation. At the same time, the deployment of secure key management protocols and mutual authentication schemes between appliances and gateways is vital to mitigate the risk of unauthorized access. From a privacy standpoint, data aggregation techniques that minimize exposure of individual usage patterns, as well as differential privacy mechanisms that obfuscate identifiable traces in energy profiles, are emerging as practical solutions. Additionally, new paradigms such as federated learning show promise by enabling the training of anomaly detection models directly within HAN devices without centralizing raw data. Taken together, the Home Area Network exemplifies both the strengths and vulnerabilities of the smart grid [14]. It empowers consumers to play an active role in energy management, yet simultaneously exposes highly sensitive data and relatively insecure devices to potential compromise. The success of the smart grid vision therefore depends, to a large extent, on embedding robust, privacy-preserving communication within HANs, supported not only by technological innovation but also by coherent regulatory frameworks and consumer trust.

2.2- Mid-Scale Communication Layers in Smart Grids:

While the Home Area Network (HAN) represents the consumer-facing edge of the smart grid, the Neighborhood Area Network (NAN) and Field Area Network (FAN) together form the mid-scale communication layers that bridge local households and devices to the utility's backbone. These domains are responsible for aggregating data from thousands of consumers, coordinating distributed energy resources (DERs), and enabling feeder-level automation. As such, they play a pivotal role in scaling smart grid intelligence beyond the individual home toward community and regional infrastructures. The NAN typically interconnects hundreds to thousands of HANs within a neighborhood or distribution zone, consolidating metering data, demand-response signals, and control instructions [15]. FANs operate at a slightly broader scope, linking substations, feeder automation equipment, and field sensors with utility control centers. Together, NANs and FANs extend the communication reach of the grid across distances ranging from a few kilometers to tens of kilometers, functioning as the intermediate layer between localized HANs and the mission-critical Wide Area Network (WAN). Technological diversity defines these mid-scale layers. Cellular technologies such as 4G LTE and emerging 5G are increasingly favored for their reliability, bandwidth, and wide coverage. In rural or semi-urban deployments, WiMAX and proprietary radio systems continue to provide flexible solutions. Power Line Communication (PLC) also remains attractive for medium-range data aggregation, though its reliability can be hindered by noise and electromagnetic interference. Fiber-optic links and microwave transmission are sometimes deployed in FANs where higher throughput is required. Each of these technologies introduces trade-offs in terms of cost, latency, resilience, and security. For example, 5G offers ultra-reliable low-latency communication that is well-suited for distributed automation but depends on robust infrastructure investments and consistent coverage. The data exchanged across NAN/FAN infrastructures is more time-sensitive than typical HAN traffic. Demand-response coordination, feeder protection, and voltage stability monitoring often require sub-second to second-level responsiveness [16]. Latency constraints are particularly strict for fault detection and isolation, where delays can jeopardize system reliability. In addition, NAN/FAN infrastructures must handle larger volumes of data than HANs, as they collect aggregated consumption data, DER status reports, and control messages for entire communities or feeder circuits. Security requirements in these layers are correspondingly elevated. Since NAN/FANs serve as aggregation points, compromising a single node can expose data from thousands of consumers or disrupt feeder-level operations. Mutual authentication between meters and data concentrators, integrity verification of control messages, and deployment of intrusion detection systems at gateways are critical safeguards. Moreover, these networks are vulnerable to denial-of-service (DoS) attacks on head-end systems, replay attacks on demand-response messages, and privacy leakage through aggregated data traffic. A comparative perspective is provided in Table 5, which summarizes the characteristics of NAN and FAN infrastructures, including their technologies, latency expectations, and security challenges.

Table 5: Characteristics of NAN/FAN Communication Layers

Domain	Typical Technologies	Latency Requirement	Data Volume	Security/Privacy Considerations
Neighborhood Area Network (NAN)	Cellular (4G/5G), WiMAX, PLC	Sub-seconds to seconds	Medium (aggregated smart meter data, demand-response signals)	Authentication, anomaly detection, privacy of aggregated data
Field Area Network (FAN)	Cellular, PLC, fiber optics, microwave	Sub-second (fault detection, feeder automation)	Medium–High (sensors, protection devices, DER data)	Integrity of control signals, DoS resilience, secure key management

The importance of mid-scale communication layers extends beyond aggregation. They increasingly support advanced functions such as distributed energy resource orchestration, electric vehicle fleet coordination, and microgrid management. In these contexts, NANs and FANs must not only provide reliable connectivity but also ensure resilience under high stress, such as during peak demand or natural disasters. The ability to prioritize critical traffic for instance, feeder protection messages over routine metering data is a defining requirement of these networks. The architectural organization of these layers is depicted conceptually in Figure 3, which illustrates the role of NAN and FAN as bridges between consumer-level HANs and the utility backbone [17]. The figure emphasizes the bidirectional flow of information: consumer data and DER statuses flow upward toward the utility, while control instructions, demand-response signals, and pricing information flow downward to consumers. Security anchors such as mutual authentication protocols, anomaly detection modules, and identity management systems are shown as overlays across the mid-scale layer, reflecting their central role in ensuring trust.

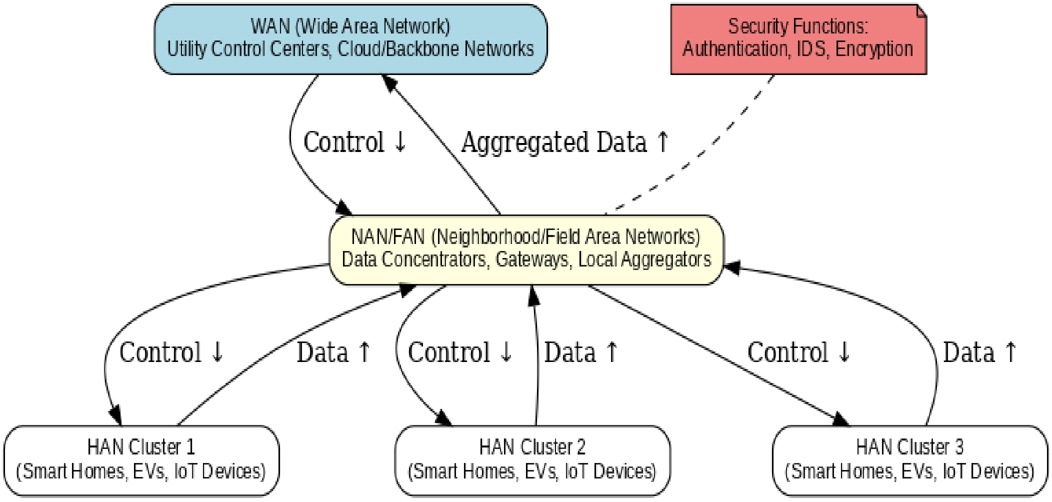
WAN (Wide Area Network)
Utility Control Centers, Cloud/Backbone Networks
Security Functions:
Authentication, IDS, Encryption
Control ↓
Aggregated Data ↑
NAN/FAN (Neighborhood/Field Area Networks)
Data Concentrators, Gateways, Local Aggregators
Control ↓
Data ↑
Control ↓
Data ↑
Control ↓
Data ↑
HAN Cluster 1
(Smart Homes, EVs, IoT Devices)
HAN Cluster 2
(Smart Homes, EVs, IoT Devices)
HAN Cluster 3
(Smart Homes, EVs, IoT Devices)

Figure 3: Conceptual View of Mid-Scale Communication Layers

The mid-scale communication layers of the smart grid represent the critical backbone that scales household intelligence to community-level resilience. By aggregating, securing, and transmitting data between consumers and utilities, NANs and FANs form the indispensable bridge between the edge of the grid and its centralized operations. Their effectiveness determines not only the efficiency of distributed energy management but also the resilience of the entire grid against cyber and physical disruptions. As such, they embody both opportunities for enhanced functionality and vulnerabilities that demand careful attention in the design of secure and privacy-preserving smart grids.

2.3- Wide Area Network (WAN):

At the top of the communication hierarchy lies the Wide Area Network (WAN), which serves as the high-capacity backbone interconnecting substations, control centers, market operators, and transmission system operators. The WAN represents the most mission-critical layer of the smart grid communication infrastructure because it carries the data necessary for supervisory control, grid stability, and market coordination across vast geographical areas. Unlike the consumer-focused HAN or the community-oriented NAN/FAN, the WAN is designed to support long-distance, high-bandwidth, and ultra-reliable communication, making it indispensable to the secure and resilient functioning of modern power systems. The WAN typically spans entire cities, regions, or even national grids, linking multiple substations with central utility operations. The types of data exchanged in this layer include supervisory control and data acquisition (SCADA) commands, real-time measurements from phasor measurement units (PMUs), synchrophasor data streams, market and settlement transactions, and aggregated reports from distribution and mid-scale networks [18]. The sensitivity and time-criticality of this information are far greater than in lower layers. For example, PMU measurements are used to detect oscillations, monitor stability margins, and initiate corrective action in near real time. A latency of more than a few tens of milliseconds can impair the effectiveness of these controls, potentially endangering system stability during disturbances. To meet these stringent requirements, WAN infrastructures rely on high-performance technologies. **Fiber-optic communication** is the gold standard, providing gigabit-level throughput, electromagnetic immunity, and very low latency. **Microwave radio links** are frequently used for redundancy and in areas where laying fiber is impractical. Increasingly, utilities are also adopting **IP-based backbones**, which allow convergence with enterprise IT systems but demand careful segmentation to protect critical operations from cyberthreats. In some cases, satellite communication provides coverage for remote substations, although the latency penalties restrict its use to non-time-sensitive applications. Security requirements in WANs are the most stringent of all smart grid domains [19]. The loss or manipulation of WAN traffic can have catastrophic consequences, including cascading outages or blackouts. For this reason, strong end-to-end encryption, digital signatures, and integrity verification are standard practices. Low-latency key exchange and rekeying protocols are critical to ensure that cryptographic operations do not interfere with real-time performance. In addition, WANs must incorporate redundancy mechanisms, fault-tolerant routing, and defense-in-depth architectures to withstand both cyber and physical disruptions. Because WAN infrastructures increasingly converge with general-purpose IP networks, segmentation and isolation become essential to prevent IT-side vulnerabilities from spilling over into operational technology. **Table 6** provides a summary of WAN characteristics compared to lower-layer networks, highlighting the unique requirements that make it both the most powerful and the most vulnerable component of smart grid communications.

Table 6: Characteristics of Wide Area Networks in Smart Grids

Feature	Typical WAN Properties	Comparison to Lower Layers
Technologies	Fiber optics, microwave, IP backbones, limited satellite	HAN uses short-range wireless; NAN/FAN uses cellular/PLC
Latency	Milliseconds to sub-seconds	Stricter than HAN (seconds) and NAN/FAN (sub-seconds)
Data Volume	Very high (SCADA, PMU, synchrophasor data, control commands)	Aggregated data in NAN/FAN; low-volume household data in HAN
Security Needs	Strongest encryption, integrity verification, redundancy, segmentation	More demanding than HAN or NAN/FAN
Criticality	Direct link to grid stability and national energy security	Localized failures in HAN/NAN less catastrophic

A conceptual representation of the WAN is illustrated in **Figure 4**, where substations, transmission lines, and control centers are interconnected via fiber backbones and microwave links. The diagram emphasizes how WANs serve as the nervous system of the grid, transmitting both operational data upward and control commands downward. Security anchors such as redundancy mechanisms, intrusion detection, and integrity verification overlays are highlighted across this domain to underscore the necessity of robustness.

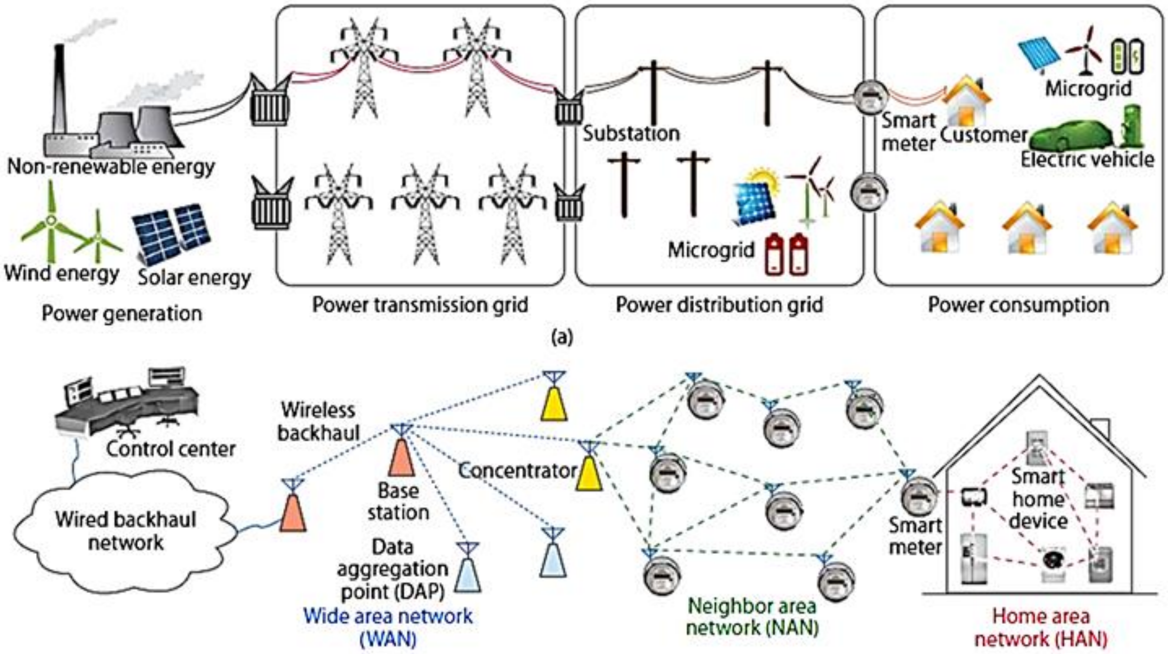

Figure 4: Wide Area Network Architecture in Smart Grids

The Wide Area Network provides the critical backbone without which smart grids could not function as cyber–physical systems. Its ability to deliver vast amounts of data with minimal latency ensures real-time situational awareness and rapid control, while its resilience against failures and attacks safeguards national energy infrastructures [20]. The WAN is therefore both the most advanced and the most exposed layer of the communication hierarchy, demanding uncompromising attention to performance, security, and reliability. As the next section will show, the threat landscape facing these high-stakes communication channels is evolving rapidly, necessitating innovations that go beyond traditional security practices.

2.4- Interoperability Frameworks for Smart Grid Networks:

As smart grids evolve into complex cyber–physical ecosystems, their effectiveness increasingly depends on the ability of heterogeneous components to communicate seamlessly. Smart appliances, meters, substations, distributed energy resources, and control centers are often built by different vendors, operate across diverse communication technologies, and follow varying implementation guidelines. Without a robust interoperability framework, this diversity risks fragmenting the grid into isolated silos, undermining efficiency, reliability, and security. Interoperability frameworks therefore emerge as the critical enabler that harmonizes protocols, standards, and architectural designs, ensuring that the smart grid operates as a cohesive, resilient system [21]. At the foundation of interoperability lies a suite of **communication standards** designed specifically for electric power systems. **IEC 61850**, developed for substation automation, defines object-oriented data models and communication services that facilitate rapid protection, control, and monitoring. Its Generic Object-Oriented Substation Event (GOOSE) messaging allows millisecond-level performance, which is indispensable for critical fault detection and isolation. **DNP3,** widely adopted in North America for supervisory control and data acquisition (SCADA), provides robustness over unreliable communication links and supports secure authentication in its enhanced versions [22]. For metering, **DLMS/COSEM** has become the de facto standard, enabling consistent data exchange between smart meters and utility head-end systems across different vendors. Complementing these traditional industrial standards, lightweight protocols such as **MQTT** and **CoAP** have entered the smart grid domain through the integration of Internet of Things (IoT) devices, offering efficient communication for resource-constrained nodes at the edge. Beyond communication protocols, interoperability frameworks must also consider the **semantics of data exchange**. For example, the **Common Information Model (CIM),** standardized under IEC 61970/61968, defines a unified ontology for representing power system components, allowing applications across transmission and distribution to interpret exchanged data consistently. Such semantic interoperability is critical not only for operational coordination but also for integrating advanced applications such as distributed energy resource management systems (DERMS), microgrid controllers, and market platforms [23]. Security is inseparable from interoperability. Inconsistent or poorly implemented standards can create weak links exploitable by adversaries. For instance, legacy deployments of DNP3 without authentication have been targeted for false data injection attacks. Similarly, gateways translating between IEC 61850 and proprietary protocols may introduce vulnerabilities if not hardened. Thus, interoperability frameworks must embed **cybersecurity requirements**, including authentication, encryption, and integrity verification, as first-class design elements rather than optional add-ons. This alignment is increasingly enforced by regulatory guidelines, such as the North American NERC CIP standards, the European Network Codes, and international cybersecurity frameworks like ISO/IEC 27019. The diversity of standards across grid domains is summarized in **Table 7**, which maps key protocols to their primary applications and highlights associated interoperability challenges.

Table 7: Major Standards and Protocols in Smart Grid Communication

Standard/Protocol	Primary Application	Key Features	Interoperability Considerations
IEC 61850	Substation automation	Object-oriented data models; GOOSE messaging	Widely used, but integration with legacy protocols requires gateways
DNP3 (Secure)	SCADA communications	Robust over noisy channels; authentication extensions	Legacy versions lack security; interoperability with IEC standards can be complex

DLMS/COSEM	Smart metering	Standardized data exchange for meters	Widely adopted, but variations across regions complicate integration
CIM (IEC 61970/61968)	System modeling (transmission/distribution)	Unified semantic model for grid assets	Ensures semantic interoperability; requires adoption across vendors
MQTT / CoAP	IoT-enabled devices and DERs	Lightweight, efficient protocols for constrained devices	Not originally grid-specific; integration with traditional standards requires adaptation

To visualize these relationships, **Figure 5** illustrates how interoperability frameworks span the smart grid communication hierarchy. The figure shows HAN, NAN/FAN, and WAN layers, each with representative protocols, and highlights how frameworks such as CIM and PKI-based security overlays provide cross-layer coherence. Interoperability is thus represented not only as vertical consistency within each layer but also as horizontal alignment across the entire ecosystem.

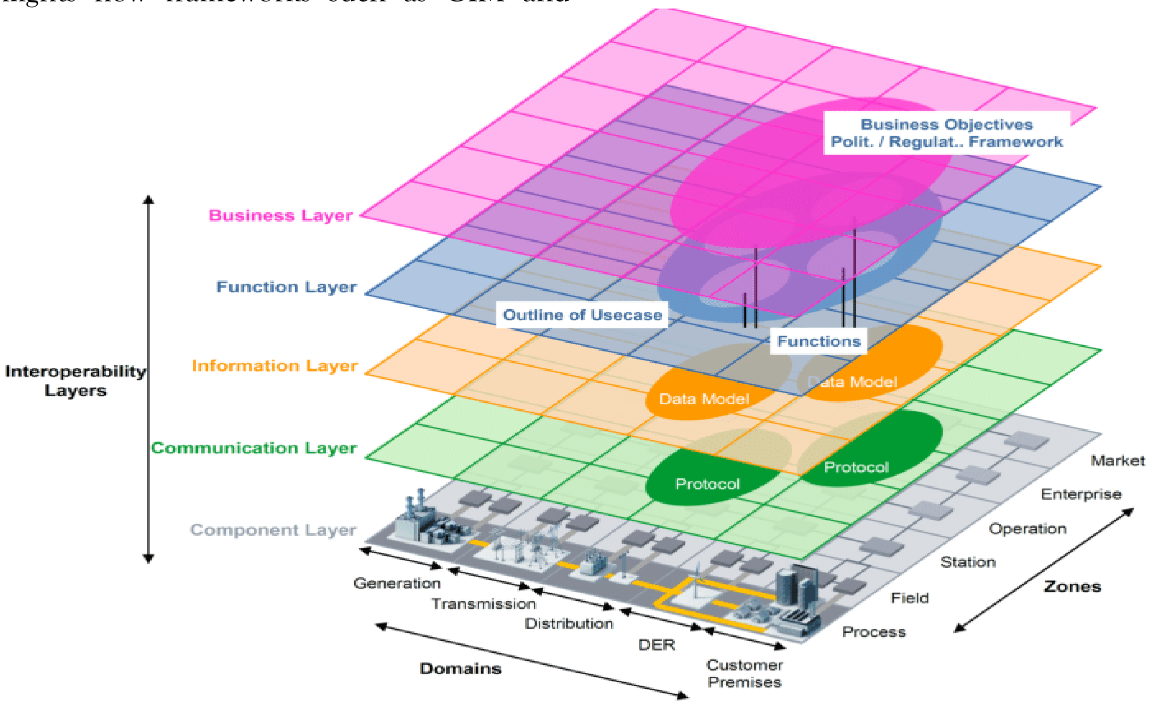

Figure 5: Interoperability Frameworks across Smart Grid Communication Layers

Interoperability frameworks are the invisible architecture that makes the smart grid more than the sum of its parts. By standardizing communication protocols, unifying semantic models, and embedding security requirements, they ensure that technologies from different vendors and regions can interact reliably [24]. However, achieving full interoperability remains an ongoing challenge, requiring continuous alignment between evolving technologies, legacy systems, and regulatory mandates. Addressing this challenge is crucial for realizing the vision of a secure, scalable, and privacy-preserving smart grid.

2.5- Cross-Layer Security Mechanisms in Smart Grids:

Smart grid communication infrastructures are not merely collections of isolated networks but interdependent layers that extend from households through neighborhood and field areas to wide-area utility backbones. Because of this interdependence, security cannot be confined to any single domain or protocol; it must be conceptualized and implemented as a cross-layer framework that safeguards the entire ecosystem. Cross-layer security mechanisms are therefore essential to prevent adversaries from exploiting weak points in one layer to compromise the integrity of the system as a whole. At the core of these mechanisms lies public key infrastructure (PKI), which provides the foundation for authenticating devices, establishing secure sessions, and ensuring trust between disparate entities across all layers. PKI enables smart meters in the Home Area Network (HAN), data concentrators in the Neighborhood Area Network (NAN), and substations in the Wide Area Network (WAN) to verify one another's identities and exchange encrypted information with confidence [25]. Effective deployment of PKI requires not only strong cryptographic algorithms but also scalable key management systems (KMS) capable of distributing, rotating, and revoking credentials at the scale of millions of devices. Another key mechanism is intrusion detection and anomaly monitoring, which must extend across the communication stack. In HANs, lightweight anomaly detection algorithms can identify unusual consumption patterns or malicious firmware behavior. In NANs and FANs, intrusion detection systems (IDS) placed at gateways can monitor aggregated traffic for denial-of-service attempts or replay attacks. At the WAN level, anomaly detection systems equipped with machine learning models can analyze synchrophasor and SCADA traffic in real time to flag deviations that may indicate sophisticated false data injection or coordinated cyber–physical attacks. Identity and access management (IAM) further strengthens the cross-layer defense by regulating which devices and users can interact with specific grid functions. IAM frameworks implement principles of least privilege, ensuring that compromised devices cannot escalate privileges beyond their immediate scope [26]. For example, an IoT sensor in a HAN may be authorized to send metering data but not to issue control commands to substations. Similarly, access to SCADA operations in the WAN is tightly segmented and continuously verified, reducing the risk of insider threats or lateral movement by attackers. These mechanisms must also be supported by secure software and firmware update channels. Supply chain attacks that introduce malicious code during updates can compromise devices at scale. By enforcing cryptographic signing of updates and validating them through trusted execution environments, utilities can maintain integrity across device fleets. Secure updates are particularly crucial for resource-constrained HAN devices, where vulnerabilities often persist due to patching challenges [27]. A structured overview of how these mechanisms apply across different grid layers is presented in Table 8, which highlights their specific functions and importance in HAN, NAN/FAN, and WAN contexts.

Table 8: Cross-Layer Security Mechanisms in Smart Grids

Security Mechanism	Role in HAN	Role in NAN/FAN	Role in WAN
Public Key	Device authentication	Secure sessions between	Authentication of

Infrastructure (PKI)	for smart meters and appliances	meters and data concentrators	substations, PMUs, and control centers
Key Management Systems (KMS)	Lightweight key provisioning and renewal	Key distribution for large-scale meter networks	Fast, low-latency rekeying for mission-critical SCADA/PMU data
Intrusion Detection & Anomaly Monitoring	Detection of abnormal device behavior	IDS at gateways for DoS/replay attack detection	Real-time anomaly detection in SCADA and synchrophasor streams
Identity & Access Management (IAM)	Restriction of appliance/device permissions	Role-based access for field devices and operators	Segmentation of SCADA access; prevention of insider misuse
Secure Firmware/Software Updates	Verification of appliance and meter updates	Validation of concentrator/gateway updates	Cryptographic signing for substation and control center systems

The interdependence of these mechanisms is illustrated in Figure 6, which presents a cross-layer security view of the smart grid. The figure 6 depicts HAN, NAN/FAN, and WAN layers as stacked tiers, with PKI, KMS, IDS, IAM, and secure update channels overlaying all three. Arrows indicate how these mechanisms not only protect within each domain but also establish trust and resilience across the entire communication stack.

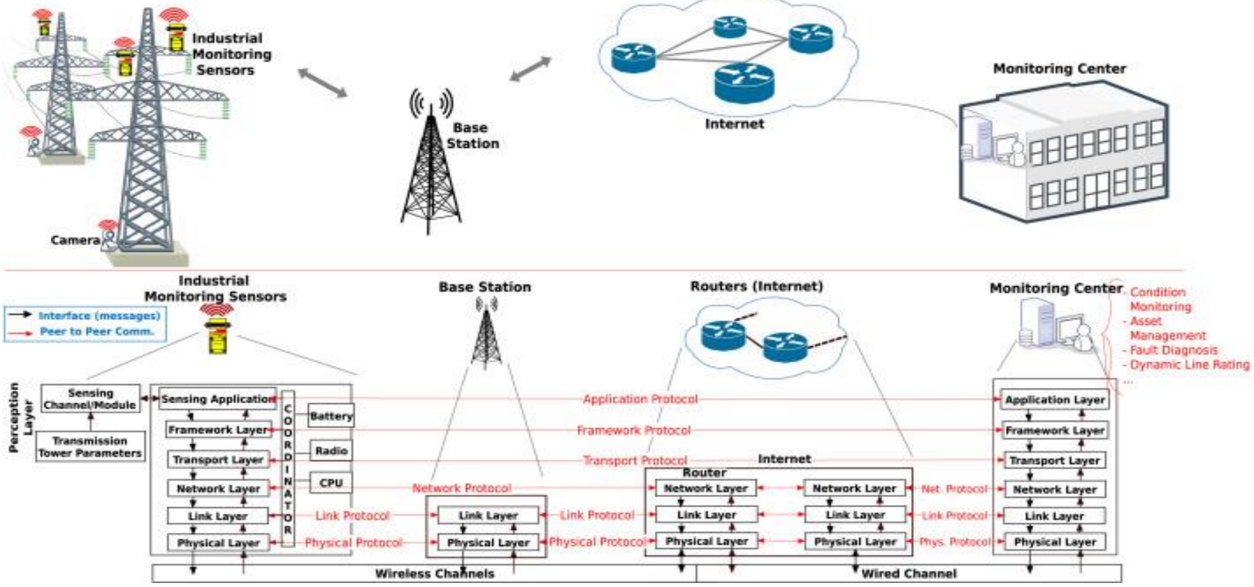

Figure 6: Cross-Layer Security Mechanisms in Smart Grids

Cross-layer security mechanisms transform the patchwork of communication technologies into a unified, trusted infrastructure. By embedding authentication, monitoring, access control, and secure updates across every level of the communication hierarchy, they mitigate the risks of cascading compromises and establish resilience against evolving cyber threats. Their effectiveness, however, depends not only on technical robustness but also on governance frameworks and consistent implementation across vendors and jurisdictions. As smart grids continue to expand, developing scalable and interoperable cross-layer security architectures will remain one of the defining challenges of the field.

3- Threat Landscape and Risk Taxonomy in Smart Grids:

The integration of pervasive digital communication technologies into power infrastructures has brought unparalleled capabilities to the smart grid, but it has also introduced an expanded set of vulnerabilities. Unlike traditional power systems that were relatively isolated, smart grids expose critical assets to adversaries through Internet connectivity, millions of end-devices, and globally distributed supply chains. As a result, the smart grid threat landscape is both broad and evolving, encompassing everything from household privacy risks to nation-state–level cyberattacks on wide-area control systems. Understanding this landscape requires a systematic taxonomy of threats that captures their nature, their technical mechanisms, and their potential consequences for confidentiality, integrity, availability, and privacy [28]. This section develops such a taxonomy by examining five major categories of threats confidentiality breaches, integrity attacks, availability disruptions, privacy violations, and supply-chain compromises each of which manifests uniquely across Home, Neighborhood/Field, and Wide Area Networks. Together, these categories illustrate how adversaries can exploit weaknesses in one layer of the communication hierarchy to launch cascading failures that undermine the resilience of the grid as a whole.

3.1- Confidentiality Threats:

Confidentiality in the smart grid refers to safeguarding sensitive data from unauthorized access, interception, or disclosure. Because smart grids rely on pervasive communication infrastructures that span from household devices to national transmission backbones, the confidentiality of exchanged information is constantly at risk. In practice, breaches of confidentiality often begin at the **weakest links** typically the Home Area Network (HAN) and Neighborhood/Field Area Networks (NAN/FAN) where millions of devices operate with inconsistent or weak cryptographic protections. In the HAN, smart meters and connected appliances continuously generate fine-grained energy consumption data, which is transmitted to utilities or aggregators through advanced metering infrastructure (AMI). If adversaries are able to eavesdrop on these channels, they can reconstruct usage profiles that disclose not only how much energy is consumed but also when and by which type of appliance [29]. For example, the operation of ovens, washing machines, or medical equipment leaves unique electrical signatures, allowing attackers to infer consumer routines, lifestyle choices, or even medical conditions. Beyond household privacy violations, intercepted billing data can provide a pathway to **identity theft** or targeted fraud. In the NAN, aggregation nodes transmit bulk data collected from hundreds or thousands of households. A single breach at this level can expose community-wide consumption patterns. The risks here are amplified by the use of heterogeneous and sometimes proprietary protocols. If security extensions are not consistently implemented, reverse engineering may reveal vulnerabilities, enabling adversaries to silently capture, modify, or replay sensitive information. The confidentiality of operational data in NAN/FAN networks is equally critical: intercepted feeder-level data may reveal distribution bottlenecks, asset loading conditions, or vulnerabilities in infrastructure that could be exploited in larger coordinated attacks [30]. At the WAN level, confidentiality risks extend to **market and operational transactions**. Leaked bidding information in electricity markets could be exploited for unfair competitive advantage, while intercepted SCADA or synchrophasor data could provide adversaries with deep insight into system operations. Although WAN infrastructures typically employ stronger encryption, they are not immune: misconfigurations, outdated key management systems, and insider threats can all compromise data confidentiality. Table 9 shows the representative confidentiality threats across smart grid layers.

Table 9: Representative Confidentiality Threats across Smart Grid Layers

Layer	Targeted Data	Representative Attack	Potential Impact
HAN	Smart meter readings, appliance data, billing info	Eavesdropping on ZigBee/Wi-Fi/PLC	Household profiling, identity theft
NAN/FAN	Aggregated meter data, feeder status	Interception at data concentrators	Exposure of community consumption, operational intelligence for adversaries
WAN	Market bids, SCADA/PMU traffic	Man-in-the-middle on utility backbones	Competitive market manipulation, grid situational awareness leakage

The consequences of confidentiality breaches extend well beyond privacy violations. When consumers perceive that their energy usage data is vulnerable, **trust in utilities and regulators erodes**, potentially slowing the adoption of smart grid technologies. From an economic perspective, the leakage of sensitive pricing or bidding data undermines the fairness of competitive energy markets. From a national security perspective, adversaries who gain access to detailed operational data may use it for reconnaissance, enabling future integrity or availability attacks on the grid. Real-world studies have highlighted these risks. For instance, researchers have demonstrated how **non-intrusive load monitoring (NILM)** algorithms can decompose aggregate meter readings into appliance-level usage without ever entering the household [31]. Similar work has shown that by correlating electricity use patterns with external information, it is possible to predict consumer behaviors such as working hours, meal times, or vacations. These insights make confidentiality not merely a consumer privacy concern but a vector for broader social and security challenges. To illustrate these risks, **Figure 7** presents a conceptual view of confidentiality threats across smart grid layers. At the household level, unencrypted smart meter traffic can be intercepted to reveal appliance behavior [32]. At the neighborhood level, bulk meter data flowing through concentrators can be captured to expose community-wide patterns. At the wide-area level, adversaries exploiting weak key management or misconfigured encryption may intercept market or SCADA traffic, gaining insights into system operations.

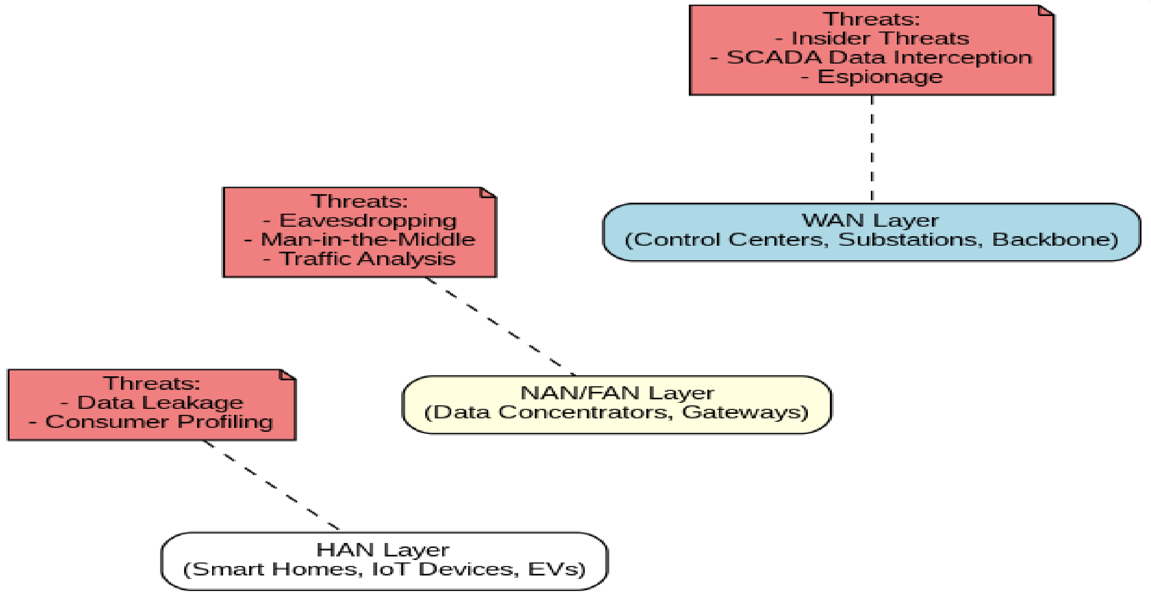

Figure 7: Confidentiality Threats across Smart Grid Communication Layers

Mitigating confidentiality threats requires a combination of **robust encryption, scalable key management,** and **context-aware data minimization**. For HAN devices, lightweight cryptographic protocols such as elliptic curve cryptography (ECC) or advanced lightweight block ciphers provide strong protection without overwhelming constrained resources. In NAN and WAN contexts, end-to-end encryption combined with frequent key rotation and secure certificate management ensures that data cannot be easily intercepted or decrypted. Beyond cryptography, privacy-preserving aggregation techniques and differential privacy methods can reduce the exposure of identifiable information while still enabling utilities to derive operational insights.

3.2- Integrity Threats:

Integrity in the smart grid context refers to the guarantee that data and control commands remain accurate, consistent, and unaltered from their origin to their destination. When this integrity is compromised, operators, automated control systems, and market mechanisms may act on falsified or misleading information, with consequences ranging from localized inefficiencies to cascading blackouts. Integrity threats differ fundamentally from confidentiality breaches because adversaries do not simply observe sensitive data; instead, they actively manipulate it in order to deceive monitoring systems, misguide operational responses, or exploit vulnerabilities for financial or strategic gain. Among the most critical forms of integrity compromise are false data injection (FDI) attacks, which have received significant attention in both research and practice. In these attacks, adversaries carefully modify measurement data to ensure that the alterations evade standard error detection mechanisms [33]. At the wide-area level, the primary targets are phasor measurement unit (PMU) streams and supervisory control and data acquisition (SCADA) traffic, which are indispensable for real-time state estimation and stability monitoring. A successful FDI attack on PMU data can lead operators to underestimate load imbalances, misallocate generation, or fail to detect oscillations, resulting in inappropriate dispatch and potentially destabilizing the transmission network. Similarly, corrupted

SCADA signals can alter breaker status reports or relay instructions, misleading human operators or automated systems into executing control actions that are harmful rather than protective. The severity of these threats has been confirmed in real-world incidents. The 2015 Ukraine power grid attack is perhaps the most widely cited case, not only because it caused widespread outages but also because it demonstrated how integrity attacks can be combined with availability disruptions. In that incident, adversaries manipulated operator screens at control centers to present false information, concealing the true status of substations while simultaneously injecting fraudulent control commands that disconnected feeders. This dual compromise illustrated the devastating potential of integrity violations, which, unlike mere denial of service, can create a false sense of operational security while the system is being actively sabotaged [34]. Integrity threats are not limited to wide-area infrastructures. In the Home Area Network (HAN), smart meters and local appliances are frequent targets for tampering, as compromised firmware or manipulated reporting functions can facilitate electricity theft and billing fraud. Such attacks, while individually small in scale, undermine the accuracy of demand forecasts and cause financial losses that accumulate across millions of consumers. In the intermediate Neighborhood and Field Area Networks (NAN/FAN), replaying demand-response signals or altering feeder automation commands can degrade operational efficiency or trigger localized blackouts. Because these signals are often transmitted in bulk, a single compromised concentrator or gateway can distort control actions across hundreds or thousands of households. The breadth of integrity risks across layers is summarized in **Table 10,** which categorizes the most prominent attack vectors, representative examples, and potential impacts. This comparative perspective emphasizes that while the forms of manipulation vary, the outcome is always the erosion of trust in the accuracy of data, which remains the cornerstone of reliable grid operation.

Table 10: Integrity Threats across Smart Grid Communication Layers

Layer	Attack Vector	Representative Example	Potential Consequences
HAN	Tampered smart meter firmware, falsified billing data	Manipulated consumption reports for electricity theft	Financial loss, inaccurate demand forecasting
NAN/FAN	Replay or modification of demand-response or feeder control signals	False feeder automation command	Operational inefficiencies, localized blackouts
WAN	False data injection in PMU or SCADA streams	Manipulated state estimation, altered SCADA commands	Incorrect dispatch, cascading failures, system instability

Detecting and mitigating integrity attacks is particularly challenging because many are designed to blend in with normal operational noise. False data injection vectors can be crafted using knowledge of system topology and redundancy, ensuring that corrupted values appear statistically consistent with legitimate measurements. Replay attacks in NAN/FAN domains exploit the validity of once-authentic signals, making them difficult to distinguish from current data. Addressing these challenges requires advanced countermeasures such as cross-validation of redundant sensors, machine learning–based anomaly detection, blockchain-enabled verification of SCADA transactions, and predictive risk management systems capable of identifying subtle patterns that indicate malicious manipulation [35]. However, these defenses must be implemented with caution, as they can introduce latency and computational burdens, particularly in wide-area environments where millisecond-level responsiveness is essential. The multi-layered nature of integrity threats is depicted in **Figure 8**, which illustrates how adversaries exploit different attack vectors at each stage of the smart grid communication hierarchy. At the household level, tampered meters introduce fraudulent readings; at the neighborhood level, compromised gateways replay or modify demand-response commands; and at the wide-area level, sophisticated FDI attacks distort PMU and SCADA streams, misleading operators and potentially triggering cascading failures. This layered view highlights not only the pervasiveness of integrity risks but also the possibility that attacks may escalate, beginning at the consumer edge and propagating upward toward critical infrastructures.

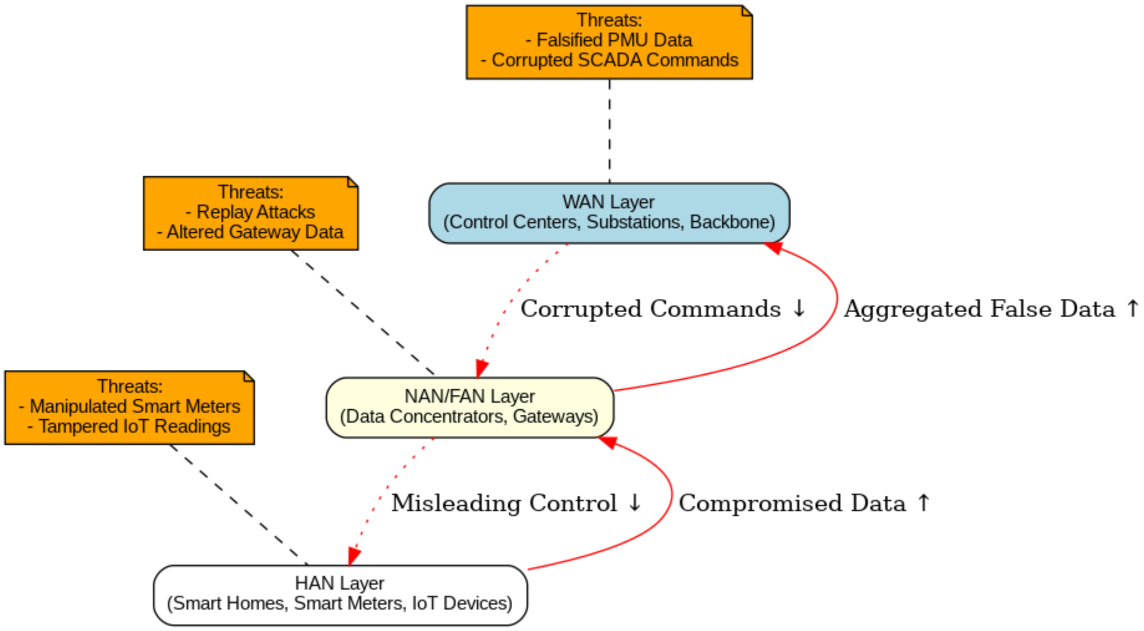

Figure 8: Integrity Threats across Smart Grid Layers

Integrity threats are among the most severe challenges facing smart grids because they directly compromise the accuracy and trustworthiness of the data on which all monitoring and control decisions rely. From billing fraud at the household level to large-scale manipulation of PMU data streams at the wide-area level, integrity violations undermine both the economic and operational foundations of the grid. They are uniquely insidious because they can remain hidden until their consequences are already unfolding, and because they often exploit the very trust relationships and redundancies designed to ensure resilience. Strengthening defenses against integrity attacks requires not only cryptographic reinforcement and anomaly detection but also a cultural shift toward continuous verification, redundancy, and resilience in all layers of smart grid communication.

3.3- Availability Threats:

Availability in the context of smart grids refers to the assurance that data, control signals, and communication services are accessible and functional when required. Because modern grids depend on the continuous exchange of real-time information, any disruption in availability whether momentary or prolonged can severely affect situational awareness, decision-making, and control operations. Availability threats are particularly critical because they can arise from both malicious adversaries and accidental failures, yet the impacts are often indistinguishable at first, creating uncertainty for operators and delaying corrective action. Denial-of-Service (DoS) and Distributed Denial-of-Service (DdoS) attacks are among the most widely recognized availability threats. By overwhelming communication channels, head-end servers, or SCADA gateways with illegitimate requests, adversaries can prevent legitimate traffic from being processed [36]. In Advanced Metering Infrastructure (AMI), DoS attacks targeting NAN or FAN concentrators may delay the delivery of consumption data or disrupt demand-response signals, leading to operational inefficiencies. In Wide Area Networks (WANs), volumetric DdoS attacks on IP-based gateways or control centers can paralyze grid monitoring functions, with consequences extending from delayed fault isolation to widespread blackouts. Wireless environments face additional risks from jamming attacks, where adversaries transmit interference signals that prevent legitimate communication over ZigBee, Wi-Fi, or LTE channels. Because jamming requires minimal technical sophistication or resources, it represents a low-cost yet high-impact threat, especially at the HAN and NAN levels. The consequences of availability disruptions extend well beyond mere communication delays. At the household level, intermittent failures may prevent participation in demand-response programs or stall EV charging coordination. At the neighborhood level, DoS attacks on concentrators can disconnect entire communities from utility monitoring, leading to inaccurate load balancing or missed outage detection. At the wide-area level, availability threats to PMU or SCADA streams may deny operators the visibility needed to detect oscillations, voltage collapse, or cyber–physical intrusions. In extreme cases, unavailability of critical data can force operators to rely on outdated or incomplete information, increasing the risk of cascading system failures. Historical incidents have highlighted the destructive potential of availability compromises. While not always directly targeting power grids, attacks such as the **2016 Mirai botnet DdoS campaign**, which overwhelmed global DNS infrastructure, demonstrated the scale at which adversaries can disrupt services by harnessing insecure IoT devices [37]. Extrapolated to the smart grid, a similar attack leveraging compromised meters or IoT-enabled DERs could deny availability of communication services at unprecedented scales. Similarly, field experiments have shown that simple **radio-frequency jamming** can blind substation wireless links, highlighting the vulnerability of operational technology systems to inexpensive attack methods. A comparative overview of availability threats across smart grid layers is presented in **Table 11**, which summarizes typical attack vectors, representative examples, and their potential impacts.

Table 11: Availability Threats across Smart Grid Communication Layers

Layer	Attack Vector	Representative Example	Potential Impact
HAN	Wireless jamming of ZigBee or Wi-Fi devices	Disrupted appliance coordination or EV	Inability to participate in demand-response; consumer

		charging	dissatisfaction
NAN/FAN	DoS on AMI concentrators; targeted jamming of LTE/PLC links	Overloaded data concentrator servers	Loss of aggregated meter data; inaccurate feeder monitoring
WAN	DdoS on SCADA gateways or IP backbones	Flooding attack on control center infrastructure	Loss of situational awareness; delayed fault detection; cascading failures

Availability threats are uniquely challenging to mitigate because of their dual nature: they can stem from deliberate adversarial action or from unintentional causes such as hardware failures, natural disasters, or misconfigurations. Moreover, the distributed nature of smart grids means that availability failures in one domain can propagate upward or downward, amplifying their effects. For example, a DoS attack on NAN concentrators may not only cut off household-level data but also obscure feeder-level anomalies, preventing WAN operators from recognizing early warning signs of instability. Similarly, flooding a SCADA server at the WAN level can sever command delivery to field devices, directly compromising the availability of protection mechanisms designed to isolate faults [38]. To illustrate the layered nature of these risks, **Figure 9** conceptually depicts availability threats across the HAN, NAN/FAN, and WAN. At the HAN, jamming disrupts wireless connectivity between meters and appliances; at the NAN/FAN, DoS attacks paralyze data concentrators; and at the WAN, large-scale DdoS floods SCADA gateways, impairing operator visibility. The diagram underscores how availability threats propagate across layers, highlighting their potential to escalate from local disruptions into wide-area operational crises.

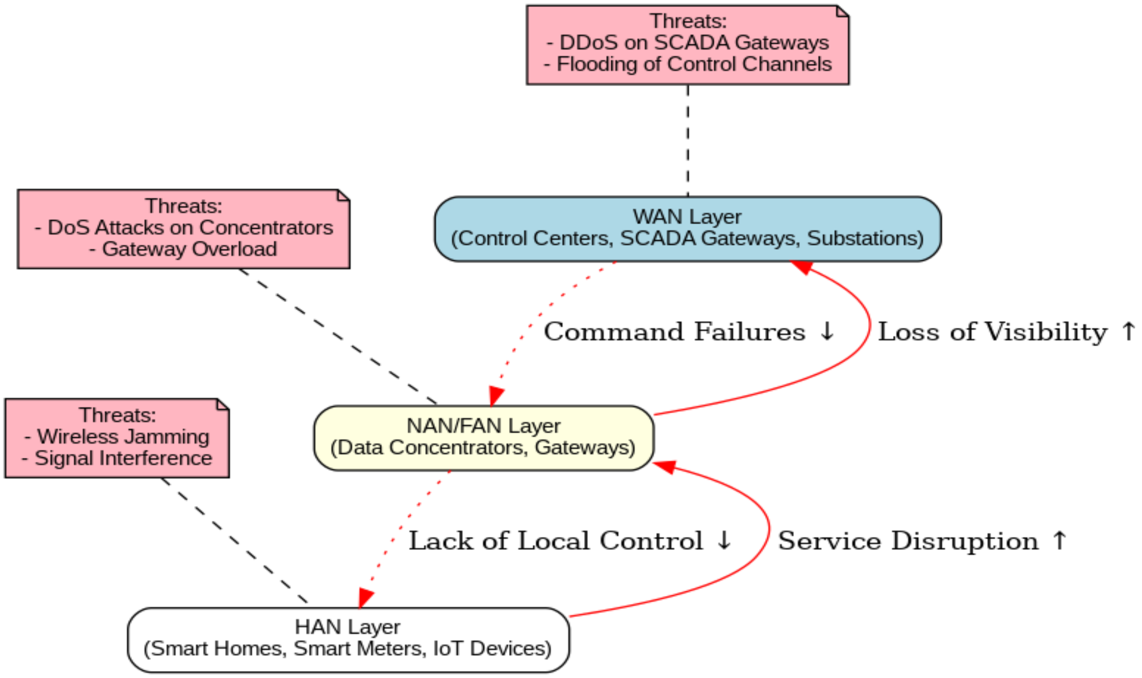

Figure 9: Availability Threats across Smart Grid Communication Layers

Availability threats in smart grids represent one of the most immediate risks to reliability because they do not necessarily require sophisticated adversaries or long-term preparation. From low-cost jamming attacks in households to large-scale DDoS campaigns against control centers, these threats can degrade visibility, delay fault isolation, and erode consumer trust in grid services. Their disruptive potential lies not only in denying communication but in doing so at moments of critical operational importance. As the smart grid continues to integrate millions of IoT devices, distributed resources, and IP-based backbones, availability will remain a contested domain that requires resilient architectures, redundant pathways, and proactive defense mechanisms.

3.4- Privacy Threats

Privacy threats in smart grids represent one of the most sensitive and socially significant dimensions of cybersecurity, because they directly affect consumer trust, acceptance, and regulatory compliance. Unlike confidentiality breaches, which involve unauthorized access to data, privacy threats stem from the **misuse, over-collection, or inappropriate secondary use of legitimately acquired information**. As smart grids evolve into highly data-driven infrastructures, the fine-grained and continuous nature of energy data introduces unique privacy vulnerabilities that extend well beyond traditional notions of data exposure. The cornerstone of these concerns lies in the **advanced metering infrastructure (AMI).** Modern smart meters are designed to capture consumption data at intervals as short as every 15 seconds, providing utilities with detailed visibility of load patterns. While this granularity enhances demand forecasting and enables sophisticated demand-response programs, it also makes consumers vulnerable to profiling. By applying **non-intrusive load monitoring (NILM)** algorithms, adversaries or even third parties with authorized access can disaggregate aggregate consumption data into appliance-specific signatures. Such analysis can reveal occupancy status, daily routines, appliance usage, and even sensitive lifestyle or health information. For example, the regular use of medical devices, the absence of activity during holidays, or the timing of household routines can all be inferred from electricity traces. Privacy risks are not confined to individual households [39]. At the **Neighborhood and Field Area Network (NAN/FAN)** level, aggregated data from hundreds or thousands of consumers may reveal community-wide trends. Such patterns can inadvertently expose the operational status of critical facilities such as hospitals, military installations, or industrial plants, as well as highlight vulnerable populations during extreme weather events. This raises not only privacy risks but also **national security implications**, since adversaries could use aggregated consumption data for reconnaissance. The integration of renewable energy sources and electric vehicles further complicates the privacy landscape. Data from rooftop solar inverters may inadvertently disclose information about the ownership of high-value assets, while logs from EV charging stations can reveal mobility patterns, travel routines, or even workplace locations. As distributed energy resources proliferate, the surface area for privacy compromise expands, intertwining household-level data with broader energy system intelligence. Compounding these technical risks are **regulatory and governance challenges**. In many jurisdictions, utilities and third-party service providers must comply with frameworks such as the **General Data Protection Regulation (GDPR)** in Europe, the **California Consumer Privacy Act (CCPA)** in the United States, and sector-specific energy data protection guidelines. Non-compliance not only leads to financial penalties but also undermines consumer trust in the smart grid transition. However, even with regulatory protections, the balance between enabling operational efficiency and preserving individual privacy remains precarious. Overly restrictive data-sharing policies may hinder innovation and optimization, while insufficient safeguards can erode consumer confidence. A comparative view of privacy threats across communication layers is presented in **Table 12**, which highlights the nature of data involved, representative risks, and potential consequences.

Table 12: Privacy Threats across Smart Grid Communication Layers

Layer	Type of Data Collected	Representative Privacy Risks	Potential Consequences
HAN	Fine-grained consumption from smart meters; appliance signatures	Household profiling through NILM; inference of routines and medical device usage	Loss of consumer trust; exposure of sensitive personal information
NAN/FAN	Aggregated meter data; feeder-level monitoring	Identification of critical sites; community-level consumption trends	Security risks; potential targeting of vulnerable populations
WAN	Market data; DER/EV integration logs	Disclosure of asset ownership, mobility patterns, or market behavior	Competitive manipulation; exposure of consumer or utility operations

Privacy threats have been extensively demonstrated in academic and industrial studies. One well-known class of research has shown that smart meter readings can be analyzed to distinguish between televisions, refrigerators, or washing machines, allowing detailed reconstruction of household activity. Other studies have highlighted the use of aggregated feeder-level data to monitor the operational behavior of large industrial consumers. These examples emphasize that privacy is not merely a theoretical concern but an empirical reality with demonstrated techniques for exploitation. The layered nature of these risks is conceptually depicted in **Figure 10**, which illustrates privacy threats across HAN, NAN/FAN, and WAN domains. The figure shows how individual household data can be disaggregated to reveal personal behavior, how aggregated neighborhood data can expose community-level patterns, and how wide-area renewable and EV integration logs can reveal consumer assets and mobility information.

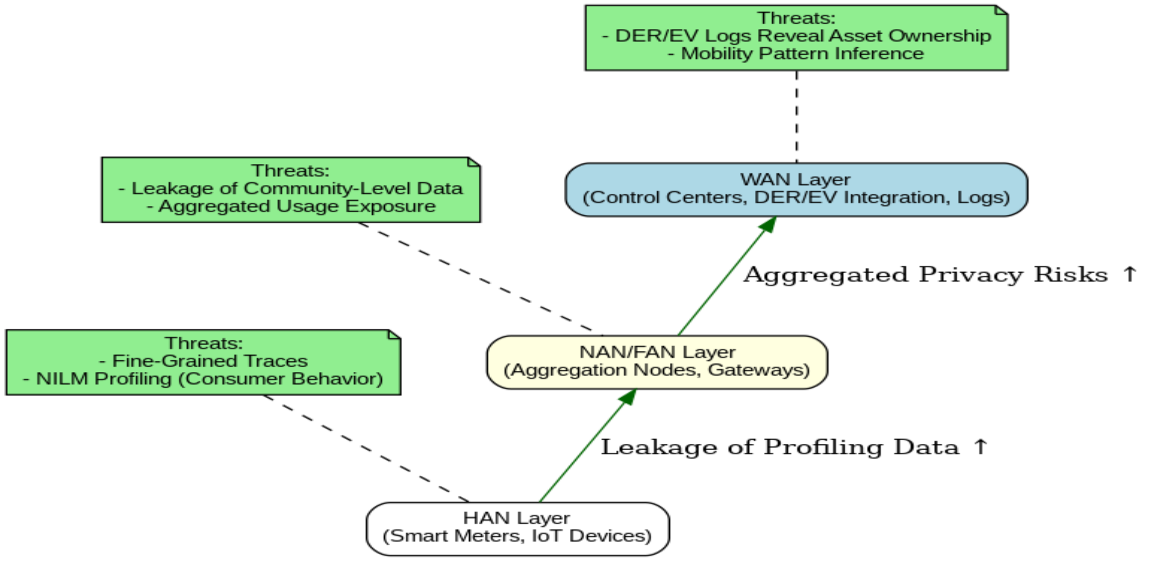
Threats:
- DER/EV Logs Reveal Asset Ownership
- Mobility Pattern Inference
Threats:
- Leakage of Community-Level Data
- Aggregated Usage Exposure
WAN Layer
(Control Centers, DER/EV Integration, Logs)
Aggregated Privacy Risks ↑
Threats:
- Fine-Grained Traces
- NILM Profiling (Consumer Behavior)
NAN/FAN Layer
(Aggregation Nodes, Gateways)
Leakage of Profiling Data ↑
HAN Layer
(Smart Meters, IoT Devices)

Figure 10: Privacy Threats across Smart Grid Communication Layers

Privacy threats in smart grids illustrate how data that is valuable for operational efficiency can also become a liability if misused or inadequately protected. They extend from the most intimate level of household behavior to the strategic intelligence of community and market operations, highlighting the dual role of data as both an enabler and a risk. Addressing these challenges requires not only technical measures such as privacy-preserving aggregation and differential privacy but also robust regulatory frameworks and consumer engagement strategies. Ultimately, the preservation of privacy will be central to ensuring public trust in the widespread adoption of smart grid technologies.

3.5- Supply Chain Threats:

One of the most insidious categories of risks facing smart grids arises from vulnerabilities in the hardware and software supply chain. Unlike traditional cyberattacks that target systems during operation, supply chain threats compromise the integrity of components before they are even deployed, embedding weaknesses that may persist undetected for years. Because smart grids rely on millions of interconnected devices ranging from consumer-level smart meters to substations and control center servers manufactured by diverse global vendors, they are particularly susceptible to malicious tampering during design, production, distribution, or maintenance processes. Supply chain attacks can take many forms. Malicious code may be inserted into firmware during development, counterfeit components may be introduced into hardware assemblies, or legitimate update mechanisms may be hijacked to deliver compromised software patches. Unlike availability or confidentiality threats, supply chain compromises undermine the very trustworthiness of devices, giving adversaries persistent footholds that are difficult to identify and almost impossible to eradicate once widely deployed. The danger is compounded by the fact that many grid components are procured from complex international supply chains, making it challenging for utilities and regulators to ensure end-to-end transparency and security assurance. The scope of these risks cuts across all layers of the smart grid. At the Home Area Network (HAN) level, a malicious firmware update to smart meters or IoT-enabled appliances could enable electricity theft, fraudulent reporting, or large-scale data exfiltration. Because smart meters often share common hardware and software platforms, a single vulnerability can be replicated across millions of households, creating opportunities for adversaries to orchestrate widespread attacks. At the Neighborhood and Field Area Network (NAN/FAN) level, compromised concentrators, gateways, or relay nodes can serve as powerful pivots for lateral movement, enabling adversaries to manipulate aggregated data, disrupt feeder automation, or coordinate community-scale denial-of-service attacks. At the Wide Area Network (WAN) level, tampered substation devices, programmable logic controllers (PLCs), or control center software could provide adversaries with direct access to the operational backbone of the grid. Because these systems support SCADA and synchrophasor applications, a successful compromise could lead to cascading operational failures and national-level energy insecurity. Recent events in other sectors highlight the plausibility of such threats. The **SolarWinds supply chain attack in 2020**, which compromised software updates for a widely used IT management platform, demonstrated how adversaries could infiltrate trusted distribution channels to gain access to sensitive networks worldwide [40]. Similarly, reports of counterfeit or backdoored hardware components in defense and telecom sectors underscore the risks of relying on opaque supply chains. In the smart grid context, where reliability and trust are paramount, such compromises could be catastrophic. A comparative overview of supply chain threats across grid layers is presented in **Table 13,** highlighting the attack vectors, representative risks, and potential consequences.

Table 13: Supply Chain Threats across Smart Grid Layers

Layer	Attack Vector	Representative Example	Potential Consequences
HAN	Malicious firmware in smart meters or IoT appliances	Compromised over-the-air update delivering backdoor	Electricity theft, mass data exfiltration
NAN/FAN	Compromised concentrators, gateways, or relay nodes	Tampered hardware at aggregation points	Manipulation of aggregated data, feeder disruption
WAN	Backdoored substation devices or control center software	Altered PLC firmware or compromised SCADA vendor patch	Direct adversarial access to grid backbone; cascading failures

The systemic nature of supply chain threats makes them particularly challenging to defend against. Traditional perimeter-based security measures such as firewalls, intrusion detection systems, or encrypted communication are ineffective once the compromised device is already inside the trusted environment. Instead, mitigating these risks requires **supply chain governance frameworks** that enforce secure design practices, rigorous vendor auditing, trusted hardware certification, and cryptographically signed software updates. Emerging technologies such as blockchain-based provenance tracking and remote attestation mechanisms using trusted execution environments (TEEs) are also being explored as methods to verify device authenticity and integrity throughout the lifecycle. The layered nature of these risks is conceptually illustrated in **Figure 11**, which shows how malicious implants introduced at the supply chain level can propagate across HAN, NAN/FAN, and WAN infrastructures. The figure emphasizes that unlike other threat categories, supply chain compromises do not originate within operational networks but enter through devices themselves, silently embedding vulnerabilities at every layer of the grid.

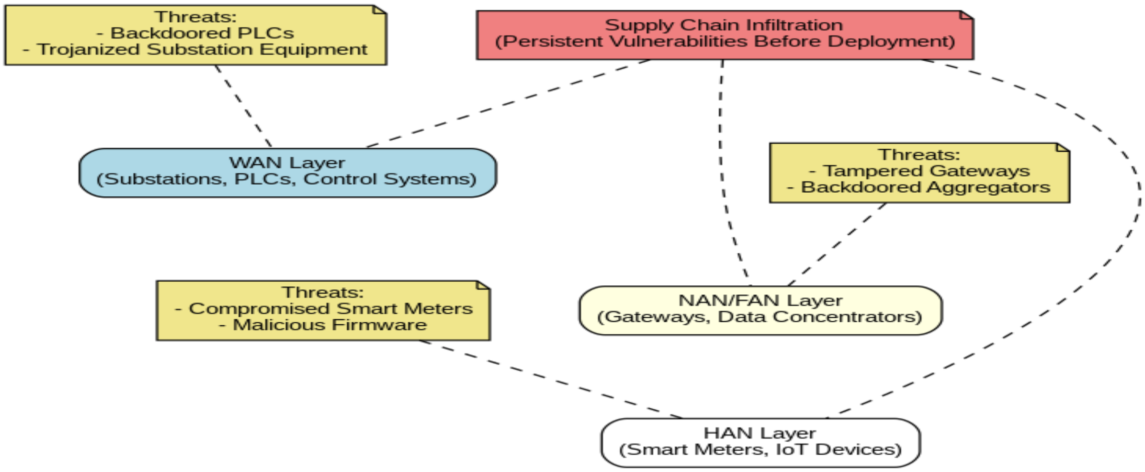
Threats:
- Backdoored PLCs
- Trojanized Substation Equipment
Supply Chain Infiltration
(Persistent Vulnerabilities Before Deployment)
WAN Layer
(Substations, PLCs, Control Systems)
Threats:
- Tampered Gateways
- Backdoored Aggregators
Threats:
- Compromised Smart Meters
- Malicious Firmware
NAN/FAN Layer
(Gateways, Data Concentrators)
HAN Layer
(Smart Meters, IoT Devices)

Figure 11: Supply Chain Threats across Smart Grid Layers

Supply chain threats represent one of the most dangerous and underappreciated risks to smart grid security. By targeting devices and software before they are deployed, adversaries can bypass traditional defenses and establish long-lasting backdoors across the communication hierarchy. These compromises undermine not only technical operations but also consumer confidence, regulatory compliance, and national energy security. Addressing supply chain risks therefore requires a holistic approach that extends beyond cybersecurity into procurement practices, vendor governance, and international cooperation. Without such measures, the very foundations of secure and privacy-preserving smart grids remain at risk.

4- Cybersecurity Innovations for Smart Grids:

The rapid digitization of power systems has heightened the urgency of developing innovative cybersecurity solutions that can match the complexity and adaptability of modern threats. Traditional methods, such as static firewalls, rigid encryption, or perimeter-based defenses, are increasingly insufficient in the context of smart grids, where adversaries exploit diverse entry points and employ sophisticated, multi-layered attack strategies. The emphasis of research and practice has therefore shifted from static prevention toward adaptive, intelligent, and resilience-oriented mechanisms. These innovations draw on advances in cryptography, distributed trust, artificial intelligence, privacy-preserving analytics, and systemic resilience to build security frameworks that are deeply embedded within the communication and operational fabric of the smart grid. One of the most pressing challenges lies in securing the vast number of devices deployed at the consumer and distribution levels, where computational and energy resources are highly constrained. Conventional cryptographic algorithms, while secure, often impose prohibitive computational burdens on smart meters and IoT-enabled appliances [41]. This limitation has motivated the adoption of lightweight cryptographic protocols, such as elliptic curve cryptography and optimized block ciphers, which deliver equivalent levels of security with significantly reduced overhead. These advances enable devices at the edge of the grid to authenticate, encrypt, and verify communications without compromising their functional efficiency. Complementing lightweight algorithms are scalable key management systems, which provide large-scale provisioning, renewal, and revocation of cryptographic credentials, ensuring that device identities and communications remain trustworthy across the entire system lifecycle. While cryptography strengthens the confidentiality and integrity of data flows, it does not by itself resolve the problem of trust in distributed environments. This gap has spurred growing interest in blockchain and distributed ledger technologies, which provide tamper-resistant records of transactions and decentralized mechanisms of verification. By recording metering data, billing information, or peer-to-peer energy trades on immutable ledgers, blockchain frameworks eliminate the reliance on centralized intermediaries that may become single points of compromise. Microgrid pilots have already shown how blockchain can secure local renewable energy exchanges while ensuring transparency and accountability among participants. Despite current challenges related to scalability, consensus latency, and resource efficiency, blockchain remains a promising innovation for embedding decentralized trust directly into the communication layers of the smart grid.

In parallel, the use of artificial intelligence and machine learning has transformed the way anomalies and intrusions are detected. Unlike traditional rule-based detection, which depends on predefined signatures of known attacks, machine learning models are capable of learning complex patterns of normal operation and identifying subtle deviations that may indicate malicious activity. Trained on historical synchrophasor and SCADA traffic, these models can provide real-time detection of false data injection or denial-of-service attacks in wide-area networks [42]. At the household or neighborhood level, lightweight anomaly detection algorithms deployed at gateways can flag suspicious consumption behaviors or identify compromised devices. To address privacy concerns associated with training centralized models, federated learning is being explored as a means to distribute the learning process itself, allowing models to be trained locally at devices while only sharing aggregated updates, thereby keeping sensitive consumer data within its original domain. This approach simultaneously advances security and privacy by ensuring that individual load profiles or appliance signatures are never centralized or exposed. Beyond detection and prevention, modern cybersecurity innovation also emphasizes consumer privacy, which has become a cornerstone of trust in the digital energy era. Fine-grained consumption data collected by smart meters is indispensable for accurate forecasting and demand-response optimization, but its sensitivity requires advanced safeguards. Techniques such as differential privacy ensure that while aggregated data remains analytically useful, individual contributions are statistically obfuscated, preventing the reconstruction of household routines. Privacy-preserving aggregation protocols further reduce the risk of consumer profiling by ensuring that utilities access only aggregated consumption levels rather than identifiable household data. At a more advanced level, homomorphic encryption and secure multiparty computation allow computations to be performed directly on encrypted datasets, enabling energy operators to run analytics without ever accessing raw, sensitive data. Although computationally demanding, these techniques illustrate the convergence of privacy and functionality as parallel design imperatives for smart grid communications [43]. Perhaps the most important shift in cybersecurity strategy is the recognition that absolute prevention of attacks is impossible in systems of this scale and complexity. Instead, resilience has become the guiding principle for smart grid defense. This resilience perspective acknowledges that attacks will occur and focuses on ensuring that the grid can continue to operate under duress, degrade gracefully, and recover quickly. Innovations such as moving target defense, which continuously changes system configurations, addresses, or cryptographic parameters, make it significantly harder for adversaries to exploit vulnerabilities that are constantly shifting. Similarly, zero trust architectures abandon the assumption that any part of the network is inherently secure. By requiring continuous verification of every device, user, and communication, and by enforcing least-privilege access policies, zero trust frameworks embed skepticism into the core of system interactions, significantly reducing the opportunities for lateral movement by adversaries once an initial compromise is achieved. These approaches, when combined with redundancy in communication pathways, fault-tolerant routing, and self-healing networks, provide the structural resilience needed to withstand the unpredictable and persistent nature of modern cyber threats. The breadth of these cybersecurity innovations is summarized in **Table 14,** which organizes them by their domain of application and their contribution to securing or preserving privacy within the smart grid.

Table 14: Emerging Cybersecurity Innovations for Smart Grids

Innovation	Domain of Application	Contribution to Security/Privacy
Lightweight Cryptography (ECC, block ciphers)	HAN, NAN/FAN	Secures communication in constrained devices without excessive overhead
Blockchain and Distributed Ledgers	NAN/FAN, WAN	Provides tamper-proof transactions, decentralized trust, and integrity assurance
AI/ML-based Anomaly Detection	All layers	Identifies stealthy intrusions, predicts cascading failures
Federated Learning	HAN, NAN	Enables collaborative learning without centralizing sensitive data
Differential Privacy & Aggregation	HAN, NAN	Protects consumer patterns while preserving analytical utility
Homomorphic Encryption & MPC	NAN/FAN, WAN	Allows secure computation on encrypted data
Moving Target Defense (MTD)	WAN, substations	Increases attacker uncertainty, enhances resilience
Zero Trust Architecture (ZTA)	All layers	Enforces continuous verification and least-privilege access

The conceptual integration of these innovations is illustrated in **Figure 12**, which depicts how different mechanisms operate across the communication hierarchy. At the household edge, lightweight cryptography and federated learning secure consumer devices and protect privacy. At the neighborhood and field levels, blockchain ensures integrity and transparency of aggregated data, while differential privacy techniques safeguard community load information. At the wide-area backbone, artificial intelligence enables real-time anomaly detection, while resilience mechanisms such as moving target defense and zero trust architectures overlay the entire system, providing adaptive, cross-layer security.

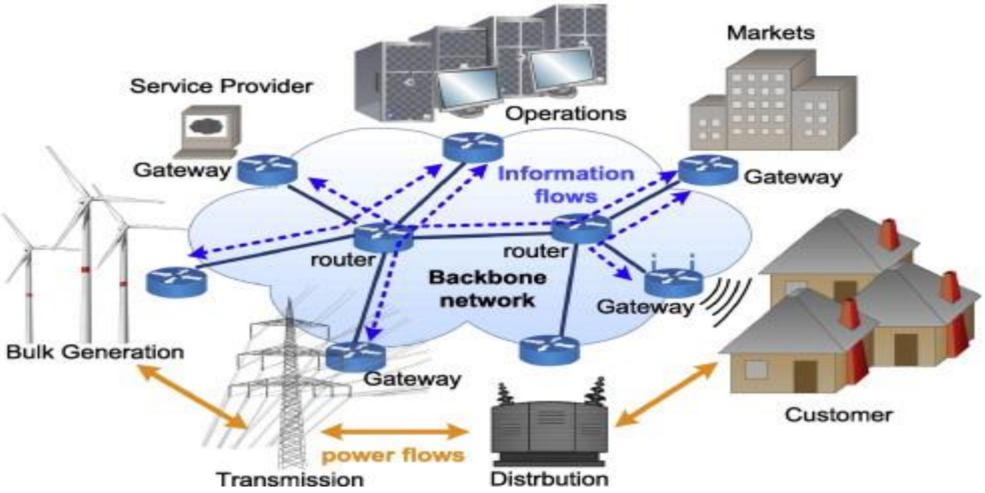

Figure 12: Cybersecurity Innovations across Smart Grid Layers

The cybersecurity innovations emerging in smart grids represent a fundamental transition from isolated, static defenses toward **adaptive, distributed, and resilience-oriented security ecosystems.** They reflect a new philosophy in which protection, detection, privacy, and resilience are integrated into the very design of communication infrastructures. By combining cryptographic efficiency, decentralized trust, machine intelligence, privacy-preserving analytics, and system-level resilience, the smart grid is being equipped to withstand the evolving threat landscape outlined in the previous section. Yet, for these innovations to be widely effective, they must be supported by coherent standards, interoperability frameworks, and policy-driven governance. This interconnection between technological advances and regulatory ecosystems forms the focus of the next section, which addresses **policy frameworks for secure and privacy-preserving smart grids.**

5- Methodology:

The methodological approach underpinning this study was designed to provide a comprehensive, structured, and interdisciplinary analysis of security and privacy challenges in smart grids, as well as to evaluate emerging innovations capable of addressing them. Because the research intersects communication engineering, information security, and regulatory governance, the methodology deliberately integrates both technical and conceptual perspectives. The process was organized into several iterative stages: a systematic review of literature and standards, thematic analysis and coding of findings, construction of a taxonomy of threats and defenses, validation through case studies and empirical reports, comparative synthesis of innovations, and incorporation of governance frameworks. Each of these stages built on the preceding one to ensure both breadth and depth, resulting in a holistic framework for secure and privacy-preserving smart grids. The first stage consisted of a **systematic literature review**. To capture a broad spectrum of perspectives, multiple databases were consulted, including IEEE Xplore, Elsevier ScienceDirect, SpringerLink, ACM Digital Library, and Google Scholar. The initial search used combinations of keywords such as *"smart grid communication security," "HAN/NAN/WAN cybersecurity," "false data injection," "privacy-preserving energy systems,"* *"blockchain in smart grids," and "policy frameworks for cyber-physical infrastructures."* This search yielded approximately 300 primary sources. To refine this corpus, inclusion criteria were applied: (i) the publication had to be directly relevant to smart grids or cyber-physical energy systems; (ii) it had to present either empirical evidence, technical proposals, or policy analysis; and (iii) it needed to meet minimum scholarly standards of peer review, recognized technical body (e.g., IEEE, IEC, NIST), or equivalent institutional authority. Exclusion criteria filtered out redundant, outdated, or purely speculative sources without technical grounding. After this process, roughly 150 high-quality sources formed the evidence base of the study, supplemented by regulatory documents such as GDPR guidelines, NERC CIP standards, and IEC protocols. The second stage involved **thematic coding and analysis**. Findings from the literature were categorized into three overarching domains: communication infrastructures, threat landscape, and defensive innovations. Within these domains, recurring subthemes were identified. For communication, these included the layered structures of HAN, NAN/FAN, and WAN. For threats, the analysis revealed five recurrent categories aligning with the CIA triad—confidentiality, integrity, and availability—augmented by privacy and supply chain risks, which emerged repeatedly as distinct and under-explored vulnerabilities. For defenses, five clusters were identified: cryptographic advances, blockchain-based trust frameworks, AI and machine learning, privacy-preserving methods, and resilience-oriented architectures. The iterative coding ensured that the study could logically progress from describing infrastructures, to identifying vulnerabilities, and finally to evaluating solutions. The third stage focused on **taxonomy construction**. Threats were mapped systematically against communication layers and classified by type. The fourth stage was the integration of **case studies and empirical validation**. Real-world incidents were selected to ground the theoretical analysis in observable evidence. The 2015 Ukraine power grid attack was included as a landmark event demonstrating integrity and availability compromises at the WAN level. The 2021 Colonial Pipeline ransomware incident was analyzed for its implications on availability and supply chain vulnerabilities. Academic demonstrations of non-intrusive load monitoring (NILM) attacks on smart meter data were used to validate privacy risks. These cases were chosen not only for their prominence but also for their alignment with the categories identified in the taxonomy, providing practical validation of the conceptual framework. By drawing on both cyber-physical incidents and experimental studies, the methodology ensured that risks were not assessed in abstraction but within the lived reality of critical infrastructures. The fifth stage entailed **comparative synthesis of emerging innovations**. Defensive technologies identified in the literature were systematically compared against the threat categories developed in the taxonomy. For instance, blockchain solutions were evaluated for their ability to prevent integrity breaches in decentralized transactions, while federated learning was assessed for its capacity to preserve privacy in smart meter data. Machine learning models were considered both as anomaly detectors and as predictive risk management tools, while resilience mechanisms such as moving target defense and zero trust were positioned as systemic strategies capable of addressing multi-vector attacks [44]. This comparative analysis ensured that the study not only catalogued innovations but also contextualized their relevance, feasibility, and potential trade-offs. The final stage incorporated **policy and governance analysis**. Recognizing that technological advances must operate within legal and institutional frameworks, this study

reviewed regulatory standards and governance models relevant to smart grid security. International standards such as IEC 61850 and CIM were assessed for their role in interoperability. Data protection regulations such as GDPR and CCPA were analyzed for their implications on privacy-preserving communication. Sector-specific frameworks, including the NERC CIP standards, were integrated to demonstrate how governance overlays shape the deployment of technical innovations. This policy analysis was not treated as a separate layer but embedded throughout, reflecting the interdisciplinary nature of secure smart grids where technical and regulatory measures must evolve in tandem. To summarize the methodology, **Table 15** provides a structured overview of the research design, from literature review to policy analysis.

Table 15: Methodological Framework of the Study

Stage	Activity	Purpose	Outcome
Literature Review	Systematic search of scholarly databases and standards	Establish comprehensive evidence base	Corpus of 150 high-quality sources
Thematic Analysis	Coding into infrastructures, threats, and defenses	Organize findings for logical progression	Identification of key themes and categories
Taxonomy Construction	Mapping threats and countermeasures across layers	Structure vulnerabilities and defenses systematically	Tables and conceptual diagrams
Case Study Validation	Ukraine 2015, Colonial Pipeline, NILM studies	Empirically ground theoretical risks	Practical confirmation of taxonomy
Comparative Synthesis	Evaluation of innovations (cryptography, blockchain, AI, etc.)	Connect defenses to identified risks	Structured countermeasure framework
Policy Integration	Review of GDPR, NERC CIP, IEC standards	Align technical with governance contexts	Holistic framework for secure adoption

The methodological process is conceptually represented in **Figure 13**, which depicts the research flow as an iterative cycle. Beginning with literature collection, the process moves through thematic analysis, taxonomy development, and case study validation, before synthesizing innovations and integrating governance perspectives. Feedback loops between these stages reflect the iterative refinement of findings as insights from one stage informed subsequent stages.

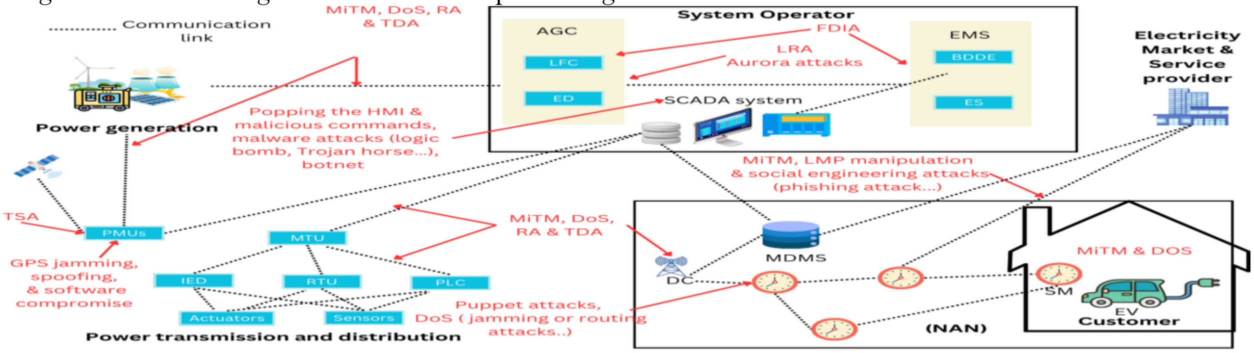
Communication link
MiTM, DoS, RA & TDA
Power generation
Popping the HMI & malicious commands, malware attacks (logic bomb, Trojan horse...), botnet
TSA
PMUs
GPS jamming, spoofing, & software compromise
MTU
IED
RTU
PLC
Actuators
Sensors
MiTM, DoS, RA & TDA
Puppet attacks, DoS (jamming or routing attacks..)
Power transmission and distribution
System Operator
AGC
LFC
ED
FDIA
LRA
Aurora attacks
SCADA system
EMS
BDDE
ES
Electricity Market & Service provider
MiTM, LMP manipulation & social engineering attacks (phishing attack...)
MDMS
DC
MiTM & DOS
SM
EV
Customer
(NAN)

Figure 13: Conceptual Flow of Methodology

The methodology of this study combined systematic review, thematic analysis, taxonomy building, empirical validation, comparative synthesis, and policy integration into a unified research framework. By blending technical, empirical, and regulatory perspectives, the methodology ensured that findings were not only theoretically sound but also practically relevant to the secure and privacy-preserving deployment of smart grids. This rigorous process provides a foundation for the analysis presented in the subsequent sections, ensuring that the conclusions drawn are both comprehensive and robust.

6- Results:

The methodological process employed in this research produced a comprehensive body of results that collectively reveal the contours of the cybersecurity landscape in smart grids, the nature of vulnerabilities across communication infrastructures, and the potential of emerging innovations to mitigate these risks within appropriate governance frameworks. Unlike narrowly focused studies that consider either technical vulnerabilities or policy measures in isolation, the results of this analysis integrate findings across disciplines and communication layers, producing a unified framework for understanding and addressing the challenges of building secure and privacy-preserving smart grids. The first major result of the study was the layered mapping of vulnerabilities across smart grid communication infrastructures, which demonstrated the asymmetry of risks across Home Area Networks (HAN), Neighborhood and Field Area Networks (NAN/FAN), and Wide Area Networks (WAN). In HANs, vulnerabilities clustered around confidentiality and privacy, primarily due to the weak or inconsistent deployment of encryption in smart meters and IoT-enabled devices, as well as the inherent sensitivity of fine-grained consumption data. In NAN/FAN environments, the concentration of aggregated data and control functions at gateways and concentrators created exposure to integrity compromises and availability threats, as attackers could manipulate or replay bulk data streams or launch denial-of-service attacks that paralyze feeder-level communication. The WAN, serving as the backbone of supervisory control and market coordination, emerged as the most critical and most heavily targeted layer, particularly vulnerable to false data injection (FDI) in phasor measurement unit streams and SCADA signals. This result highlighted a vertical gradient of threats, where consumer-level privacy breaches at HAN may appear localized, but their exploitation can provide a foothold for more disruptive attacks that escalate through NAN/FAN into WAN infrastructures. The second significant outcome was the construction of a taxonomy of threats and risks, which organized the complex array of attack vectors into five coherent categories: confidentiality, integrity, availability, privacy, and supply chain compromises. By applying this taxonomy across communication layers, the study revealed not only the diversity of threats but also their layered interdependencies. For example, confidentiality violations at the HAN level, such as eavesdropping on smart meter traffic, may evolve into privacy risks if data is misused for profiling, or escalate into integrity attacks if adversaries inject manipulated consumption data to alter billing and forecasting systems. Similarly, supply chain compromises cut horizontally across all layers, bypassing traditional perimeter defenses and embedding persistent vulnerabilities into hardware and software before deployment. The taxonomies presented in Table 10 and Table 11 provided a structured lens through which to view these relationships, demonstrating how traditional CIA principles must be expanded in the context of smart grids to include privacy and supply chain risks as equally critical dimensions.

A third result emerged from the comparative synthesis of cybersecurity innovations, which systematically mapped defensive mechanisms to the vulnerabilities identified in the taxonomy. The synthesis revealed that no single innovation can comprehensively address the wide spectrum of risks; instead, effective defense requires combinations of complementary measures. Lightweight cryptography directly mitigates confidentiality risks in HAN devices, while blockchain ensures the integrity and non-repudiation of energy transactions in NAN and WAN environments. Artificial intelligence and machine learning were found to operate as cross-cutting solutions, capable of detecting subtle anomalies in traffic streams at all layers, while federated learning provided a privacy-preserving model for training detection systems without centralizing consumer data. Differential privacy, aggregation protocols, and homomorphic encryption further addressed privacy-specific threats by limiting the exposure of identifiable data while preserving analytical utility. Finally, resilience-oriented architectures such as moving target defense (MTD) and zero trust architecture (ZTA) emerged as systemic solutions capable of addressing multi-vector threats, particularly those introduced by supply chain compromises. The mapping of these innovations in Table 17 illustrated how each mechanism aligns with specific categories of threats, while also highlighting areas of overlap that reinforce the argument for integrated, multilayered defense. The fourth major result of the study was the validation of theoretical risks through empirical case studies, which confirmed that the identified threats are not hypothetical but observable within operational infrastructures. The 2015 Ukraine power grid attack provided direct evidence of the potential for integrity compromises at the WAN level, where adversaries manipulated operator interfaces and injected fraudulent SCADA commands to disconnect substations. The Colonial Pipeline ransomware incident of 2021 demonstrated how availability threats, when directed against critical infrastructure, can lead to cascading societal impacts, even beyond the energy sector itself. Privacy risks were validated through academic demonstrations of non-intrusive load monitoring (NILM), where researchers reconstructed appliance-level behavior from aggregated smart meter data, illustrating how even "legitimately collected" data can be misused. Together, these case studies grounded the taxonomy in real-world evidence, underscoring the urgency of deploying advanced cybersecurity mechanisms in smart grids. A fifth key result was the integration of governance and regulatory frameworks into the analysis of technical innovations. The alignment of GDPR requirements with differential privacy, federated learning, and data minimization practices demonstrated that technical and legal frameworks can reinforce each other. Similarly, NERC CIP standards corresponded to the deployment of secure key management, continuous authentication, and segmentation practices in WAN environments. However, the results also revealed significant gaps: supply chain risks remain inadequately addressed by existing regulations, which often lack enforceable provisions for verifying the security of hardware and firmware in global manufacturing processes. This finding emphasizes that without stronger governance and international cooperation, even the most advanced technical solutions may fail to secure the foundations of the smart grid. A notable emergent result was the conceptual integration of vulnerabilities, defenses, and governance into a holistic framework, depicted in Figure 14. This framework illustrates HAN, NAN/FAN, and WAN layers as the structural base, overlaid with mapped threat categories, defensive innovations, and governance anchors. It shows visually how confidentiality and privacy protections operate most strongly at the HAN, how blockchain and AI reinforce the NAN/FAN, and how resilience architectures safeguard the WAN, with governance mechanisms cutting vertically across all layers. The integrated framework demonstrates that security in smart grids is not the responsibility of any single domain but arises from the interplay of technology, regulation, and system design.

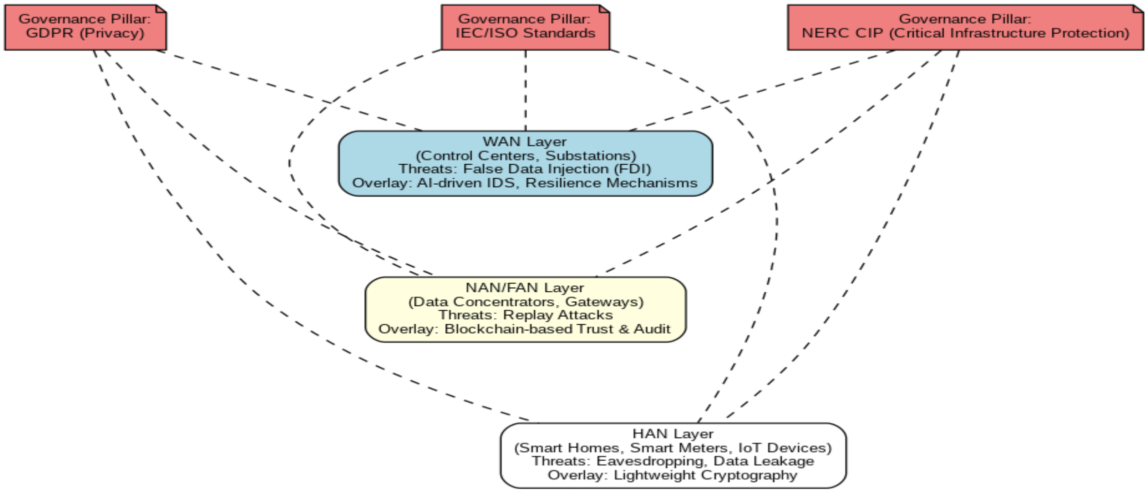
Governance Pillar:
GDPR (Privacy)
Governance Pillar:
IEC/ISO Standards
Governance Pillar:
NERC CIP (Critical Infrastructure Protection)
WAN Layer
(Control Centers, Substations)
Threats: False Data Injection (FDI)
Overlay: AI-driven IDS, Resilience Mechanisms
NAN/FAN Layer
(Data Concentrators, Gateways)
Threats: Replay Attacks
Overlay: Blockchain-based Trust & Audit
HAN Layer
(Smart Homes, Smart Meters, IoT Devices)
Threats: Eavesdropping, Data Leakage
Overlay: Lightweight Cryptography

Figure 14: Integrated Results Framework for Secure and Privacy-Preserving Smart Grids

In addition to these core findings, the results revealed several cross-cutting insights. First, threats often overlap categories, demonstrating that the boundaries between confidentiality, integrity, availability, privacy, and supply chain are porous rather than rigid. For instance, supply chain attacks often compromise integrity by introducing malicious firmware, while simultaneously threatening confidentiality through data exfiltration and availability by enabling denial-of-service backdoors. Second, defensive innovations show similar overlaps; blockchain addresses both integrity and non-repudiation, while federated learning simultaneously enhances privacy and improves detection accuracy. These overlaps suggest that security in smart grids must be conceptualized not as a collection of isolated measures but as an ecosystem of mutually reinforcing protections. Finally, the results highlight a fundamental tension between operational efficiency and security/privacy protections. Many defensive innovations, particularly homomorphic encryption, secure multiparty computation, and blockchain, introduce computational and latency costs that may be incompatible with the strict real-time requirements of WAN infrastructures. Conversely, lightweight solutions suitable for HAN may be insufficiently robust for high-value WAN transactions. This tension underscores the importance of tailoring defenses to specific layers, while ensuring interoperability and coordination across the system. The results of this study provide a multi-dimensional view of smart grid cybersecurity. They confirm that vulnerabilities exist across all communication layers, that these vulnerabilities can be systematically categorized into an expanded CIA framework, that emerging innovations provide promising but partial solutions that case studies validate the real-world nature of these risks, and that governance frameworks play a pivotal but still incomplete role in securing smart grids. The integrated results framework synthesizes these findings into a cohesive vision, demonstrating that the path toward secure and privacy-preserving smart grids lies in the convergence of technological innovation, systemic resilience, and regulatory governance.

7- Challenges and Limitations:

While the results of this study highlight the significant progress being made toward building secure and privacy-preserving smart grids, they also reveal persistent challenges and limitations that must be addressed before these innovations can be fully realized in practice. The challenges arise from the inherent complexity of smart grid infrastructures, the evolving sophistication of adversaries, and the gaps between technological innovation, regulatory frameworks, and practical implementation. The limitations reflect both the constraints of the current body of knowledge and the methodological boundaries of this research. One of the foremost challenges concerns the **heterogeneity and scale of smart grid devices**. Modern power systems incorporate millions of interconnected endpoints, from household smart meters and IoT appliances to substations and wide-area SCADA systems. Securing this ecosystem requires cryptographic and authentication schemes that are lightweight enough to function on resource-constrained devices yet robust enough to withstand advanced adversaries. Although lightweight cryptographic primitives have been proposed, their deployment at scale faces challenges of interoperability, backward compatibility, and secure key management [45]. In particular, updating or patching devices across millions of consumers remains logistically complex, creating opportunities for adversaries to exploit outdated or inconsistent implementations. Another persistent challenge lies in the **detection and attribution of sophisticated cyberattacks**. False data injection, supply chain infiltration, and insider threats are designed to blend into normal operations, making them extremely difficult to detect. While artificial intelligence and machine learning offer promising detection capabilities, their accuracy depends heavily on the quality and representativeness of training data. Smart grid environments are highly dynamic, and models trained on historical datasets may struggle to identify novel attack vectors. Moreover, adversaries are increasingly capable of conducting adversarial machine learning, in which detection systems themselves are manipulated or misled. This cat-and-mouse dynamic underscores the difficulty of achieving truly adaptive and reliable detection mechanisms. A further challenge arises from **balancing privacy with operational efficiency**. The granularity of data collected through advanced metering infrastructure enables precise demand forecasting and optimization, yet also threatens consumer privacy when misused. Techniques such as differential privacy and homomorphic encryption offer potential solutions but introduce additional computational and latency overheads. In latency-sensitive domains such as synchrophasor monitoring in WANs, even small delays can undermine system stability. This tension between data utility and data protection remains unresolved, making privacy preservation one of the most delicate challenges in smart grid cybersecurity.

Supply chain security presents another formidable obstacle. The globalization of manufacturing and software development has created opaque and complex supply chains, in which malicious modifications to hardware or firmware can be introduced long before devices are deployed. Existing governance mechanisms, such as standards for procurement and certification, remain insufficient to guarantee end-to-end security. Unlike traditional threats that can be countered with firewalls or encryption, supply chain compromises embed themselves invisibly within trusted environments, often remaining dormant until strategically activated. This makes them both difficult to detect and devastating in potential impact. The challenges are not solely technical but also **institutional and regulatory [46]**. The study revealed misalignments between technological capabilities and policy frameworks. While regulations such as GDPR and NERC CIP provide strong foundations, their implementation often lags behind the pace of technological innovation. Moreover, regulatory requirements are fragmented across jurisdictions, creating difficulties for international utilities and manufacturers who must navigate a patchwork of overlapping, and sometimes conflicting, standards. Without greater harmonization of global cybersecurity and privacy frameworks, achieving consistent protection across interconnected grids remains elusive. From the perspective of this research itself, several **limitations** must be acknowledged. The analysis was based primarily on secondary data in the form of published literature, case studies, and regulatory documents. While this ensured breadth and rigor, it did not include primary data collection through field experiments, simulations, or direct utility engagement. As such, some of the mappings and frameworks remain conceptual rather than empirically tested at scale. Similarly, the evaluation of innovations such as blockchain, federated learning, and homomorphic encryption was based on their demonstrated potential in pilot projects and academic studies, rather than on large-scale industrial deployment. The limitations of these technologies in real-world environments such as computational overhead, interoperability with legacy infrastructure, and consumer acceptance remain areas requiring further empirical research.

Another limitation arises from the **inevitable trade-off between generalization and specificity**. To create a holistic taxonomy, the study abstracted threats and defenses into broad categories, which facilitates conceptual clarity but may obscure contextual nuances. For example, the specific technical implementation of denial-of-service protection in a fiber-based WAN may differ significantly from that in a wireless HAN, yet both were generalized under "availability threats." While this abstraction was necessary for systematic mapping, it highlights the need for follow-up studies focusing on domain-specific implementations and performance evaluations. Finally, there is the limitation of **temporal relevance**. Cybersecurity is a rapidly evolving field, and what is considered state-of-the-art today may quickly become obsolete as adversaries adapt and new technologies emerge. Blockchain consensus mechanisms, AI-based intrusion detection, and lightweight cryptography are all subject to rapid advances as well as new forms of attack. Therefore, the frameworks and mappings developed in this study should be regarded as current best analyses rather than permanent solutions, with the expectation that continuous updating will be necessary.

8- Future Work:

The analysis presented in this study demonstrates that while substantial progress has been made toward the development of secure and privacy-preserving smart grids, many questions remain unanswered, and significant opportunities for further research and innovation persist. Future work must focus on deepening the technical robustness of defensive mechanisms, expanding empirical validation in real-world contexts, and advancing policy frameworks that align with the rapidly evolving technological landscape. One of the most pressing avenues for future research lies in the development of **lightweight yet scalable cryptographic frameworks**. Although elliptic curve cryptography and optimized block ciphers provide promising directions, there remains a need for algorithms that can operate seamlessly on the most constrained devices while still supporting millions of nodes in interconnected networks. Future work should explore adaptive cryptographic schemes capable of dynamically adjusting security parameters based on device capacity, network conditions, and operational priorities. Integrating post-quantum cryptographic primitives into smart grid environments also represents an emerging priority, given the anticipated rise of quantum computing and its potential to undermine current public key infrastructures [47]. Another critical research direction involves **advancing detection and response mechanisms through artificial intelligence and machine learning**. While anomaly detection models have shown great promise, their current dependence on historical datasets limits their effectiveness against novel and adversarially crafted attacks. Future efforts should emphasize the creation of self-learning and self-adaptive systems capable of continuously updating models in real time. The integration of federated learning with edge computing could further decentralize detection while maintaining privacy. At the same time, adversarial machine learning must be studied in greater depth, with future work directed at building resilient models that cannot be easily manipulated by adversaries. The **tension between privacy and operational efficiency** also demands continued exploration. Techniques such as differential privacy, homomorphic encryption, and secure multiparty computation remain computationally intensive, and their deployment in latency-sensitive environments such as synchrophasor monitoring or real-time load balancing is currently impractical. Future research should therefore investigate hybrid approaches that combine privacy-preserving mechanisms with edge intelligence, enabling selective protection of the most sensitive data without compromising real-time system stability. In parallel, large-scale pilot deployments are needed to evaluate consumer acceptance and trust in these techniques, ensuring that privacy-preserving innovations are not only technically feasible but also socially sustainable.

Addressing **supply chain security** remains another urgent priority for future work. Current research offers limited solutions to the problem of ensuring integrity across global manufacturing and distribution processes. Future directions include the exploration of blockchain-based provenance tracking for hardware components, trusted execution environments for firmware verification, and international certification schemes for vendors. Research should also investigate proactive monitoring strategies that treat supply chain risk not as a static problem but as an evolving threat vector requiring continuous validation throughout the device lifecycle. From a governance perspective, future work must expand on the integration of **technical innovation with regulatory frameworks**. While this study highlighted the alignment between GDPR and differential privacy or between NERC CIP and zero trust principles, many gaps remain, particularly in the harmonization of cross-border regulations. Future research should examine models for international coordination, potentially through bodies such as the International Energy Agency (IEA) or the International Telecommunication Union (ITU), to develop globally consistent cybersecurity and privacy standards for energy systems. Comparative policy analysis across regions could further reveal best practices and provide pathways toward harmonization. Another area of future exploration involves the **evaluation of resilience-oriented security architectures** in live operational environments [48]. Concepts such as moving target defense and zero trust architecture remain largely at the pilot or theoretical stage in the energy sector. Future research must test their scalability, latency implications, and interoperability with legacy infrastructure, particularly in WAN environments where millisecond-level decisions are required for grid stability. Similarly, the concept of self-healing networks and adaptive restoration following cyber incidents warrants deeper experimental validation, particularly through co-simulation platforms that integrate both power and communication domains. Finally, the **integration of emerging technologies** such as 5G/6G, edge intelligence, and quantum communication into the smart grid opens promising yet underexplored research opportunities. While these technologies offer higher bandwidth, ultra-low latency, and enhanced security capabilities, they also introduce new attack surfaces that must be proactively understood. Future research should therefore pursue dual investigations: leveraging the benefits of these technologies for enhanced grid performance while simultaneously anticipating and mitigating their unique cybersecurity risks.

Conclusion:

The modernization of power systems into smart grids represents both an unprecedented opportunity and a profound challenge. By integrating advanced communication infrastructures with distributed energy resources and intelligent control systems, smart grids promise greater efficiency, sustainability, and consumer empowerment. Yet, as this study has shown, the very features that enable these benefits pervasive connectivity, fine-grained data collection, and layered interoperability also create new avenues of vulnerability that threaten the confidentiality, integrity, availability, and privacy of critical energy infrastructures. Addressing these vulnerabilities requires not only technical innovation but also coherent policy frameworks and a commitment to systemic resilience. This paper has contributed to the understanding of secure and privacy-preserving smart grids in several important ways. It first examined the layered communication infrastructures Home Area Networks, Neighborhood and Field Area Networks, and Wide Area Networks that form the foundation of modern energy systems, identifying how each layer introduces unique exposures. It then developed a taxonomy of threats, expanding the traditional CIA triad to include privacy risks and supply chain compromises, and mapping these categories across communication layers to illustrate their interdependencies. The analysis demonstrated that vulnerabilities at the consumer edge can escalate into broader systemic risks, and that supply chain compromises cut across all layers, embedding persistent weaknesses that bypass traditional defenses. The study further synthesized emerging cybersecurity innovations, highlighting how lightweight cryptography, blockchain-based trust frameworks, artificial intelligence and machine learning, privacy-preserving analytics, and resilience-oriented architectures collectively provide a defensive ecosystem. These innovations were mapped against the identified threats to show their complementarities and limitations, emphasizing that no single technology is sufficient in isolation. The integration of case studies including the Ukraine power grid attack, the Colonial Pipeline incident, and demonstrations of non-intrusive load monitoring validated the practical relevance of these risks and underscored the urgency of deploying advanced defensive measures. Governance and regulatory frameworks were also analyzed, revealing both synergies with technical solutions and persistent gaps, particularly in addressing supply chain vulnerabilities and ensuring cross-border harmonization. Taken together, the results of this study underscore that smart grid cybersecurity is not a matter of incremental improvement but of systemic transformation. Effective security requires a holistic framework in which vulnerabilities are systematically categorized, defensive innovations are synergistically combined, and governance anchors provide oversight and accountability. The integrated results framework developed here provides such a vision, illustrating how technical and regulatory measures must converge to build trust, resilience, and long-term sustainability. Nevertheless, significant challenges remain. The heterogeneity of devices, the difficulty of detecting stealthy intrusions, the tension between privacy and operational efficiency, and the opacity of global supply chains all present unresolved obstacles. The limitations of this research, including its reliance on secondary data and the conceptual nature of its frameworks, highlight the need for empirical validation and domain-specific testing. As such, the study's findings should be understood as a foundation upon which future work spanning cryptographic innovation, adaptive machine learning, privacy-preserving computation, and international policy harmonization must continue to build.

REFERENCES

Ferrag, M. A., Maglaras, L. A., Janicke, H., & Jiang, J. (2016). A survey on privacy-preserving schemes for smart grid communications. *arXiv preprint arXiv:1611.07722*.

Parihar, V., Malik, A., Bhushan, B., Bhattacharya, P., & Shankar, A. (2023). Innovative smart grid solutions for fostering data security and effective privacy preservation. In *Data Analytics for Smart Grids Applications—A Key to Smart City Development* (pp. 351-380). Cham: Springer Nature Switzerland.

Naiho, H. N. N., Layode, O., Adeleke, G. S., Udeh, E. O., & Labake, T. T. (2024). Addressing cybersecurity challenges in smart grid technologies: Implications for

Dawood, B. A., Al-Turjman, F., Hussain, A. A., & Deebak, B. D. (2022). Data protection and privacy preservation sustainable energy infrastructure. *Engineering Science & Technology Journal*, *5*(6), 1995-2015.

Ali, M., Suchismita, M., Ali, S. S., & Choi, B. J. (2025). Privacy-Preserving Machine Learning for IoT-Integrated Smart Grids: Recent Advances, Opportunities, and Challenges. *Energies (19961073)*, *18*(10).

Abdel-Basset, M., Moustafa, N., & Hawash, H. (2022). Privacy-preserved generative network for trustworthy anomaly detection in smart grids: A federated semisupervised approach. *IEEE transactions on industrial informatics*, *19*(1), 995-1005.

Desai, S., Alhadad, R., Chilamkurti, N., & Mahmood, A. (2019). A survey of privacy preserving schemes in IoE enabled smart grid advanced metering infrastructure. *Cluster Computing*, *22*(1), 43-69.

Alshamasi, R. Z., & Ibrahim, D. M. (2025). Federated intelligence for smart grids: a comprehensive review of security and privacy strategies. *Journal of Electrical Systems and Information Technology*, *12*(1), 43.

EL-Husseini, F., Noura, H. N., & Vernier, F. (2025). Security and privacy-preserving for machine learning models: attacks, countermeasures, and future directions. *Annals of Telecommunications*, 1-22.

Mirzaee, P. H., Shojafar, M., Cruickshank, H., & Tafazolli, R. (2022). Smart grid security and privacy: From conventional to machine learning issues (threats and countermeasures). *IEEE access*, *10*, 52922-52954.

mechanisms for applications of IoT in smart grids using AI. In *Sustainable Networks in Smart Grid* (pp. 207-231). Academic Press.

Kalejaiye, A. N. (2025). Federated learning in cybersecurity: privacy-preserving collaborative models for threat intelligence across geopolitically sensitive organizational boundaries. *Int J Adv Res Publ Rev*, 2(07), 227-50.

Aurangzeb, M., Wang, Y., Iqbal, S., Naveed, A., Ahmed, Z., Alenezi, M., & Shouran, M. (2024). Enhancing cybersecurity in smart grids: Deep black box adversarial attacks and quantum voting ensemble models for blockchain privacy-preserving storage. *Energy Reports*, *11*, 2493-2515.

Rele, M., Julian, A., Patil, D., Mary, G. I., Ramyadevi, R., & Udaya Krishnan, M. (2024, August). Secure Data Analytics in Smart Grids: Preserving Privacy and Enabling Advanced Monitoring. In *International Conference on Sustainable Energy and Environmental Technology for Circular Economy* (pp. 127-137). Singapore: Springer Nature Singapore.

Abdi, N., Albaseer, A., & Abdallah, M. (2024). The role of deep learning in advancing proactive cybersecurity measures for smart grid networks: A survey. *IEEE Internet of Things Journal*, *11*(9), 16398-16421.

Yogi, M. K., & Chakravarthy, A. S. N. (2025). Privacy-Preserving Deep Reinforcement Learning for Secure Resource Orchestration in Cyber-Physical Systems. *International Journal of Scientific Research in Network Security and Communication*, *13*(2), 12-21.

Keshk, M., Turnbull, B., Sitnikova, E., Vatsalan, D., & Moustafa, N. (2021). Privacy-preserving schemes for safeguarding heterogeneous data sources in cyber-physical systems. *IEEe Access*, *9*, 55077-55097.

Liu, H., Ning, H., Zhang, Y., & Yang, L. T. (2012). Aggregated-proofs based privacy-preserving authentication for V2G networks in the smart grid. *IEEE Transactions on Smart Grid*, *3*(4), 1722-1733.

Hu, C., Liu, Z., Li, R., Hu, P., Xiang, T., & Han, M. (2023). Smart contract assisted privacy-preserving data aggregation and management scheme for smart grid. *IEEE Transactions on Dependable and Secure Computing*, *21*(4), 2145-2161.

Alamatsaz, N. R. (2014). *Towards an Analytical Framework for Privacy-preserving Aggregation in Smart Grid* (Doctoral dissertation, Wichita State University).

Chim, T. W., Yiu, S. M., Li, V. O., Hui, L. C., & Zhong, J. (2014). PRGA: Privacy-preserving recording & gateway-assisted authentication of power usage information for smart grid. *IEEE Transactions on Dependable and Secure Computing*, *12*(1), 85-97.

Farao, A., Veroni, E., Ntantogian, C., & Xenakis, C. (2021). P4G2Go: a privacy-preserving scheme for roaming energy consumers of the smart grid-to-go. *Sensors*, *21*(8), 2686.

Elshazly, A. A., Elgarhy, I., Mahmoud, M., Ibrahem, M. I., & Alsabaan, M. (2025). A Privacy-Preserving RL-Based Secure Charging Coordinator Using Efficient FL for Smart Grid Home Batteries. *Energies (19961073)*, *18*(4).

Jeyakumar, S. R., Rahman, M. Z. U., Sinha, D. K., Kumar, P. R., Vimal, V., Singh, K. U., ... & Balajee, J. (2024). An Innovative Secure and Privacy-Preserving Federated Learning-Based Hybrid Deep Learning Model for Intrusion Detection in Internet-Enabled Wireless Sensor Networks. *IEEE Transactions on Consumer Electronics*, *71*(1), 273-280.

Chen, Y. W., & Sutanto, L. (2020, May). The privacy preserving framework with virtual ring and identity-based cryptography for smart grid. In *17th International Conference on Information Technology–New Generations (ITNG 2020)* (pp. 271-276). Cham: Springer International Publishing.

Akgün, M., Soykan, E. U., & Soykan, G. (2023). A privacy-preserving scheme for smart grid using trusted execution environment. *IEEE Access*, *11*, 9182-9196.

Larbi, K. K. B. (2020). Achieving continuous privacy-preserving histogram query in smart grid communications.

Rahmati, M., & Pagano, A. (2025, July). Federated Learning-Driven Cybersecurity Framework for IoT Networks with Privacy Preserving and Real-Time Threat Detection Capabilities. In *Informatics* (Vol. 12, No. 3, p. 62). MDPI.

Fan, K., Ren, Y., Bai, Y., Wei, G., Zhang, K., Li, H., & Yang, Y. (2023). Fault-tolerant and collusion-resistant lattice-based multidimensional privacy-preserving data aggregation in edge-based smart grid. *IEEE Internet of Things Journal*, *11*(6), 9487-9504.

Chen, W., & Liu, G. P. (2024). Privacy-preserving consensus-based distributed economic dispatch of smart grids via state decomposition. *IEEE/CAA Journal of Automatica Sinica*, *11*(5), 1250-1261.

Moulahi, T., Jabbar, R., Alabdulatif, A., Abbas, S., El Khediri, S., Zidi, S., & Rizwan, M. (2023). Privacy-preserving federated learning cyber-threat detection for intelligent transport systems with blockchain-based security. *Expert Systems*, *40*(5), e13103.

Tran, Q. N., Turnbull, B. P., Wu, H. T., De Silva, A. J. S., Kormusheva, K., & Hu, J. (2021). A survey on privacy-preserving blockchain systems (PPBS) and a novel PPBS-based framework for smart agriculture. *IEEE Open Journal of the Computer Society*, *2*, 72-84.

Shen, J., Zhou, T., Wei, F., Sun, X., & Xiang, Y. (2017). Privacy-preserving and lightweight key agreement protocol for V2G in the social Internet of Things. *IEEE Internet of things Journal*, *5*(4), 2526-2536.

Zhan, S., Huang, L., Luo, G., Zheng, S., Gao, Z., & Chao, H. C. (2025). A Review on Federated Learning Architectures for Privacy-Preserving AI: Lightweight and Secure Cloud–Edge–End Collaboration. *Electronics*, *14*(13), 2512.

Liu, Y., Yang, X., Wen, W., & Xia, M. (2021). Smarter grid in the 5G Era: A framework integrating power internet of things with a cyber physical system. *Frontiers in Communications and Networks*, *2*, 689590.

Kumar, K. S. S. (2025). Distributed Intelligence for smart grid management: Architectures, applications, and future. *World Journal of Advanced Engineering Technology and Sciences*, *15*(2), 2868-2883.

Afzal, Z., Gaggero, G., & Asplund, M. (2025). Towards Privacy-Preserving Anomaly-Based Intrusion Detection in Energy Communities. *arXiv preprint arXiv:2502.19154*.

Jørgensen, B. N., Gunasekaran, S. S., & Ma, Z. G. (2025). Impact of EU Laws on AI Adoption in Smart Grids: A Review of Regulatory Barriers, Technological Challenges, and Stakeholder Benefits. *Energies*, *18*(12), 3002.

Fuxen, P., Hachani, M., Hackenberg, R., & Ross, M. (2024). MANTRA: Towards a Conceptual Framework for Elevating Cybersecurity Applications Through Privacy-Preserving Cyber Threat Intelligence Sharing. *Cloud Comput*, *2024*, 43.

Yin, X. C., Liu, Z. G., Nkenyereye, L., & Ndibanje, B. (2019). Toward an applied cyber security solution in IoT-based smart grids: An intrusion detection system approach. *Sensors*, *19*(22), 4952.

Sundarraj, S. (2024). Privacy Preserving Data Aggregation Algorithm for IoT-Enabled Advanced Metering Infrastructure Network in Smart Grid. In *5G and Fiber Optics Security Technologies for Smart Grid Cyber Defense* (pp. 289-305). IGI Global.

Bouramdane, A. A. (2023). Cyberattacks in smart grids: challenges and solving the multi-criteria decision-making for cybersecurity options, including ones that incorporate artificial intelligence, using an analytical hierarchy process. *Journal of Cybersecurity and Privacy*, *3*(4), 662-705.

Madhuranthakam, R. S., Vadlakonda, G., Simuni, G., & Sinha, M. (2025). Securing the Smart Grid: Integrating Blockchain Technology for Cyber-Physical Systems in Energy Management. *Available at SSRN 5239959*.

Waseem, M., Adnan Khan, M., Goudarzi, A., Fahad, S., Sajjad, I. A., & Siano, P. (2023). Incorporation of blockchain technology for different smart grid applications: Architecture, prospects, and challenges. *Energies*, *16*(2), 820.

Aramide, O. O. (2025). Federated Learning for Distributed Network Security and Threat Intelligence: A Privacy-Preserving Paradigm for Scalable Cyber Defense. *Journal of Data Analysis and Critical Management*, *1*(02).

Liu, L., Li, J., Lv, J., Wang, J., Zhao, S., & Lu, Q. (2024). Privacy-preserving and secure industrial big data analytics: A survey and the research framework. *IEEE Internet of Things Journal*, *11*(11), 18976-18999.

Jithish, J., Mahalingam, N., Wang, B., & Yeo, K. S. (2025). Towards enhancing security for upcoming 6G-ready smart grids through federated learning and cloud solutions. *Cybersecurity*, *8*(1), 61.

pratap Singh, V., Kumar, A., Dubey, A., & Batra, H. (2025, May). Privacy-Preserving Data Aggregation in Smart Cities: Secure and Efficient Techniques for Urban Data Management. In *2025 International Conference on Networks and Cryptology (NETCRYPT)* (pp. 1-5). IEEE.

Jithish, J., Mahalingam, N., & Seng, Y. K. (2024). Empowering smart grid security: Towards federated learning in 6G-enabled smart grids using cloud.

Butt, O. M., Zulqarnain, M., & Butt, T. M. (2021). Recent advancement in smart grid technology: Future prospects in the electrical power network. *Ain Shams Engineering Journal*, *12*(1), 687-695.

Wang, Z., Yu, P., & Zhang, H. (2022). Privacy-preserving regulation capacity evaluation for hvac systems in heterogeneous buildings based on federated learning and transfer learning. *IEEE Transactions on Smart Grid*, *14*(5), 3535-3549.

Amer, D., Shukur, M. A. N., Mohammed, H. A., & Almulla, A. RSA-DLT for Secure and Privacy-Preserving 6G Communications. *Available at SSRN 4924247*.

Garg, S., Kaur, K., Kaddoum, G., Ahmed, S. H., & Jayakody, D. N. K. (2019). SDN-based secure and privacy-preserving scheme for vehicular networks: A 5G perspective. *IEEE Transactions on Vehicular Technology*, *68*(9), 8421-8434.

Hasan, M. K., Alkhalifah, A., Islam, S., Babiker, N. B., Habib, A. A., Aman, A. H. M., & Hossain, M. A. (2022). Blockchain technology on smart grid, energy trading, and big data: security issues, challenges, and recommendations. *Wireless Communications and Mobile Computing*, *2022*(1), 9065768.