World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Protecting the Grid: Cybersecurity strategies for renewable energy integration

Kehinde Adedapo Ogunmoye [1,*], Chijioke Paul Agupugo [2], Emmanuella Ejichukwu [3], Pedro Barros [4] and Mario David Hayden [4]

[1] *Department of Physics and Astronomy, Appalachian State University, Boone, NC, USA.*
[2] *Department of Sustainability Technology and Built Environment, Appalachian State University, Boone, North Carolina, USA.*
[3] *University of Michigan, Dearborn, USA.*
[4] *University of Hoston, Clear Lake, USA. 5Inti International University, Malaysia.*

World Journal of Advanced Research and Reviews, 2025, 26(03), 1302-1319

Publication history: Received on 26 April 2025; revised on 11 June 2025; accepted on 13 June 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.26.3.2234

Abstract

The global transition toward renewable energy sources, such as solar and wind, is reshaping modern power systems and introducing new vulnerabilities within the electrical grid. As distributed energy resources (DERs) and smart grid technologies become increasingly interconnected through digital communication networks, cybersecurity emerges as a critical component of resilient and sustainable energy infrastructure. This paper explores the unique cybersecurity challenges posed by renewable energy integration, including increased attack surfaces, insecure legacy systems, and vulnerabilities in supervisory control and data acquisition (SCADA) systems and Internet of Things (IoT)-enabled devices. The study analyzes recent incidents and threat vectors, such as malware attacks, data breaches, and supply chain compromises, that highlight the urgent need for robust security mechanisms across the energy value chain. Through a comprehensive review of current cybersecurity frameworks, this research proposes a multi-layered defense strategy that combines risk assessment, network segmentation, intrusion detection systems, blockchain for secure energy transactions, and artificial intelligence-driven threat intelligence. The role of regulatory compliance, workforce training, and stakeholder collaboration is emphasized as a prerequisite for ensuring grid integrity. Additionally, the study evaluates advanced cryptographic protocols and zero-trust architectures as proactive measures for safeguarding digital assets and operational technologies. Case studies from various global regions illustrate how countries are addressing cybersecurity in their renewable energy deployment plans, offering practical insights into scalable and adaptive defense models. The findings underscore the necessity of embedding cybersecurity in the planning, design, and operation phases of renewable energy projects. As power grids become more decentralized and dynamic, protecting them from cyber threats is no longer optional but essential for national security, economic stability, and public safety. The study concludes with strategic policy recommendations and a call for international cooperation to establish standardized cybersecurity benchmarks tailored to the evolving needs of renewable energy systems.

Keywords: Renewable Energy; Cybersecurity; Smart Grid; Distributed Energy Resources; SCADA; Internet of Things; Intrusion Detection; Zero Trust; Blockchain; Grid Resilience; Critical Infrastructure Protection

1. Introduction

The global energy landscape is currently experiencing a significant transformation aimed at reducing carbon emissions and combating climate change. This transformation is characterized by the accelerated integration of renewable energy sources including solar, wind, and hydro into both national and regional power grids. Such a shift necessitates substantial technical and operational adjustments to existing electricity infrastructures. The growing reliance on

* Corresponding author: Kehinde Adedapo Ogunmoye

renewable energy introduces considerable variability into electricity generation, which traditional power grids were not designed to handle efficiently (Krause et al., 2021; Baimel et al., 2016).

The move towards renewable energy systems is accompanied by a shift towards decentralized energy generation, which requires the adoption of advanced digital technologies. These technologies include smart meters, Internet of Things (IoT) devices, and Supervisory Control and Data Acquisition (SCADA) systems that allow for better management and optimization of electricity flow (Saleem et al., 2019; Attia, 2019; Sakhnini et al., 2021). The digitalization of energy systems enhances grid efficiency but also expands the attack surface for potential cyber threats (Kim et al., 2019; Mohammed et al., 2024). Vulnerabilities in these interconnected systems can be exploited by malicious actors, leading to disruptions in energy delivery, data manipulation, and severe economic consequences (Ahmed et al., 2019; Jahromi et al., 2020).

With the emerging reliance on digital platforms, the threats to the stability and reliability of critical energy infrastructure have escalated. Research indicates that traditional cybersecurity measures may not suffice in safeguarding against the sophisticated and evolving nature of cyber threats aimed at modern energy systems (Alekseichuk et al., 2023; Adegbite et al., 2023; Wu et al., 2018) . The necessity for robust cybersecurity strategies becomes critical, focusing on the unique vulnerabilities introduced through the integration of renewable energy sources and the deployment of smart technologies in power grids. The identification of key vulnerabilities, along with an assessment of emerging threats, is crucial in developing a comprehensive framework for cybersecurity specific to energy sectors (Tanyıldız et al., 2024; Sani et al., 2024).

Furthermore, the pressing need for innovative defense strategies arises from the complexities of securing grids that are increasingly decentralized and digitally interconnected (Galinec, 2023; Suciu et al., 2019). The proposal of multi-layered defense mechanisms, which incorporate best practices and regulatory frameworks, is essential for enhancing grid resilience against cyberattacks (Abdulwahid and Ateeq, 2019; Ko et al., 2015). Stakeholders, including grid operators and technology developers, must focus on actionable recommendations that not only address current security weaknesses but also anticipate future challenges in the ever-evolving energy landscape.

In conclusion, as power grids transition towards a more sustainable energy model, the integration of renewable sources presents both opportunities and significant cybersecurity challenges. It is imperative for energy sector stakeholders to collaboratively craft strategies that will protect vital infrastructure while facilitating a smooth transition to a low-carbon economy.

2. Methodology

This study adopted a mixed-methods approach comprising a systematic literature review, qualitative analysis, and conceptual modeling to develop robust cybersecurity strategies for renewable energy integration. The research began by identifying core vulnerabilities associated with integrating renewable energy systems into smart grids. Key sources included peer-reviewed literature from 2020–2024, focusing on artificial intelligence, zero-trust architectures, Internet of Things (IoT), and blockchain-based solutions.

A systematic review methodology was utilized to collect and screen relevant studies from indexed databases. The inclusion criteria centered on publications that provided empirical, theoretical, or simulation-based insights into protecting smart grid infrastructure. Duplicate entries and articles lacking full-text access or methodological transparency were excluded.

Data extraction focused on identifying key cybersecurity challenges and mitigation techniques, such as threat modeling frameworks, machine learning approaches to intrusion detection, endpoint protection algorithms, and encryption practices. The extracted data were synthesized using a thematic coding approach to align technological strategies with grid resilience goals.

The core analytical step involved comparative analysis across different cybersecurity models particularly zero-trust frameworks, AI-driven anomaly detection, and blockchain-enhanced access controls highlighting strengths, trade-offs, and contextual applications. A conceptual model was developed to visualize how these technologies could be integrated into a unified cybersecurity strategy for renewable grids.

Scenario-based validation techniques were proposed to assess the resilience and feasibility of the model in protecting against cyber-physical attacks. Simulation data from grid systems and IoT-enabled infrastructures were recommended for future trials.

The research concluded with actionable recommendations for policymakers, grid operators, and cybersecurity engineers on best practices for securing next-generation power infrastructure. Emphasis was placed on developing context-sensitive protocols, strengthening regulatory compliance, and fostering international collaboration to future-proof renewable energy networks.

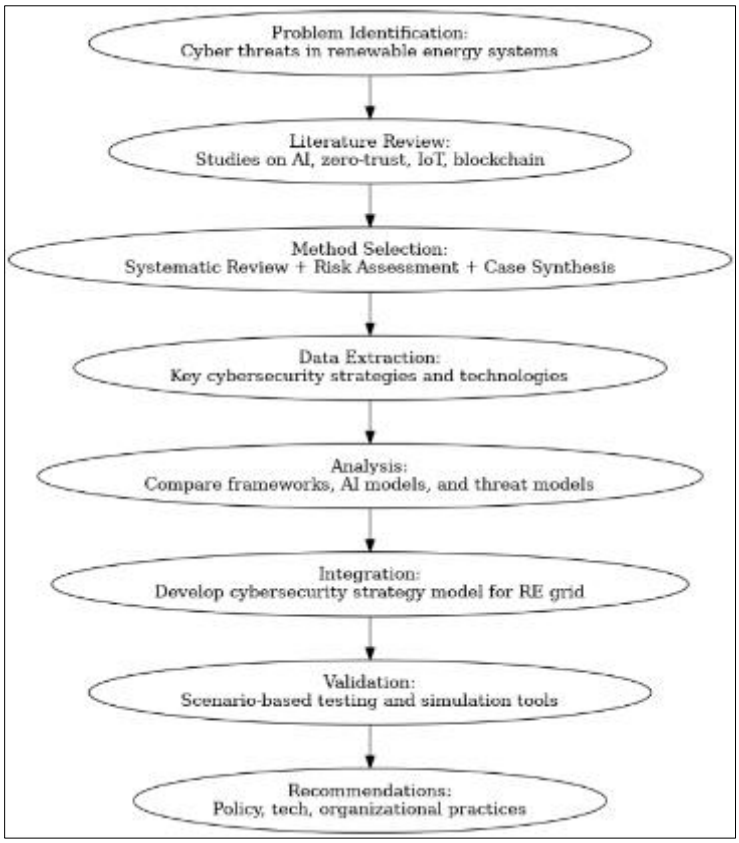

Figure 1 The flowchart for the Study Methodology

3. The Evolving Power Grid Landscape

The modernization of the power grid signifies a substantial transformation in electricity generation, transmission, and consumption. This shift is primarily driven by the increasing deployment of distributed energy resources (DERs), including rooftop solar panels, small-scale wind turbines, and residential battery storage systems. These DERs enable consumers to assume the dual role of "prosumers," actively engaging in both energy production and consumption. This decentralization creates a model of energy production that diverges from the traditional centralized framework characterized by large power plants (Sousa et al., 2019; Yang et al., 2022; Morstyn and McCulloch, 2019). Such a decentralized model not only enhances energy resilience and reduces transmission losses but also facilitates the better integration of renewable energy sources into the grid, promoting sustainability and overall efficiency (Tushar et al., 2020; Espe et al., 2018).

However, the transition toward a distributed energy model introduces complexities and vulnerabilities that need addressing. The emergence of the smart grid, which incorporates digital technologies and interconnected systems, represents a transformative evolution. The modern grid is not merely a network of physical infrastructure but functions as an intelligent system driven by digitalization. This enables real-time monitoring, automated control, and improved energy management (Marron et al., 2019; Szczepaniuk and Szczepaniuk, 2022). Innovations such as smart meters and advanced sensors support enhanced load management and reliability of the energy supply, demonstrating the dynamic nature of contemporary electricity networks (Castellini et al., 2021; Milanezi et al., 2020). While these advancements increase operational efficiency, they also elevate the grid's exposure to cyber threats and emphasize the necessity for robust cybersecurity measures (Bouramdane, 2023; Brambati et al., 2022). Figure 2 shows Schematic diagram for grid integration of HRES. PandC: Protection and Control presented by Eltamaly, et al., 2021.

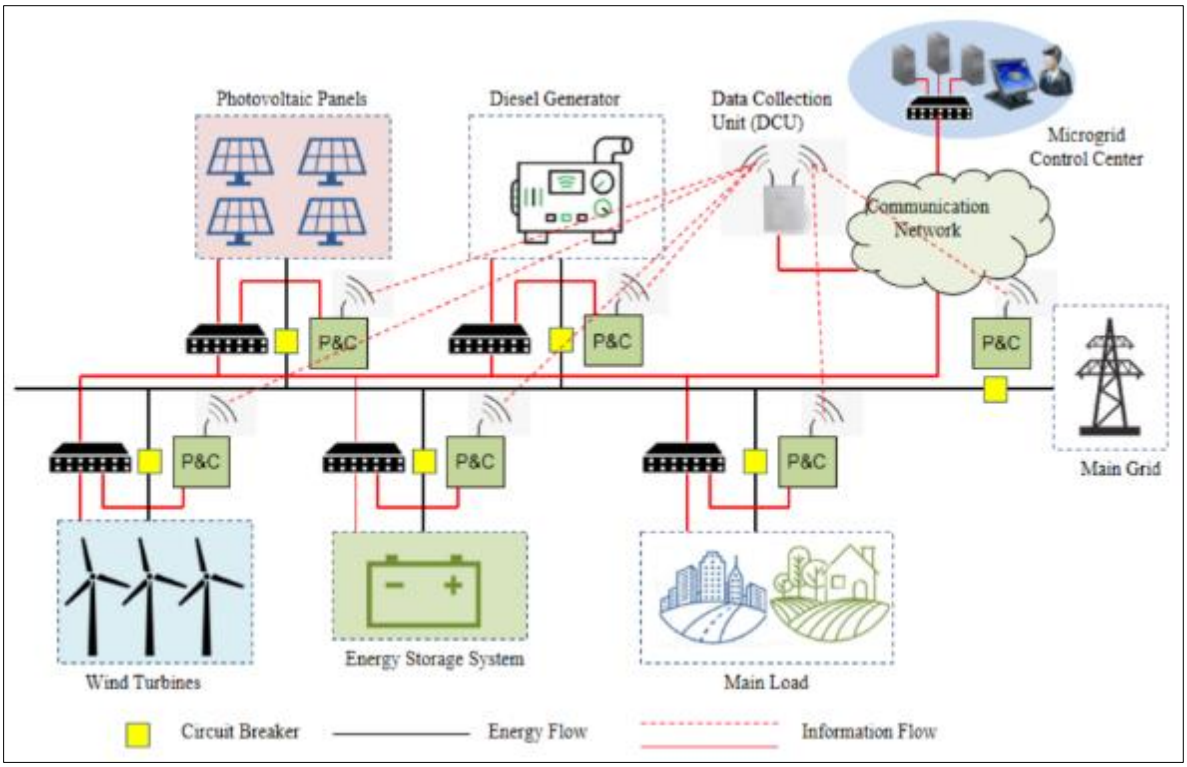

Figure 2 Schematic diagram for grid integration of HRES. PandC: Protection and Control (Eltamaly, et al., 2021)

Digitalization plays a pivotal role in accommodating the growing penetration of variable renewable energy sources. Technologies such as smart inverters and automated demand response systems enable utilities to balance supply and demand in an increasingly bidirectional energy flow context (Tushar et al., 2018; Taik, 2021). Data analytics and cloud computing support the processing of vast amounts of information generated by these distributed assets, aiding predictive maintenance and operational optimization. Nonetheless, this expanding digital footprint introduces significant cybersecurity concerns, as key grid components, particularly Supervisory Control and Data Acquisition (SCADA) systems, may lack robust security features necessary to withstand contemporary cyber threats (Le et al., 2020; Bouramdane, 2023).

Furthermore, the proliferation of Internet of Things (IoT) devices within the energy sector presents additional vulnerabilities. While these devices can enhance grid interconnectivity, they also create numerous entry points for cyber intrusions. Devices such as smart thermostats and connected appliances are often deployed with minimal security, potentially leading to larger-scale disruptions in energy management systems (Szczepaniuk and Szczepaniuk, 2022; Milanezi et al., 2020). The reliance on cloud computing for data storage and processing introduces further critical vulnerabilities, as misconfigured settings and insecure access controls can compromise sensitive data (AVCI, 2021; Annuk et al., 2021). Smart Grid Architecture: Components and Functions Across Energy Sectors presented by Zaman and Mazinani, 2023 is shown in figure 3.

As the power grid architecture becomes increasingly complex and diverse, establishing a comprehensive cybersecurity framework is essential. The integration of distributed resources and digital systems often outpaces the development of corresponding cybersecurity policies and standards. This highlights the need for adaptive security measures that encompass all endpoints, interfaces, and data streams (Adelana, et al., 2024; Bouramdane, 2023). Adopting zero-trust architectures, where every component within the network is treated as a potential target, necessitates stringent access controls and continuous monitoring to mitigate threats in real time (Bouramdane, 2023; Brambati et al., 2022).

The evolution of the power grid towards a digitalized, distributed system is vital for meeting future energy demands while enhancing sustainability and operational efficiency. However, these advancements must be paired with robust strategies to address cybersecurity risks, as failures in this area could result in significant disruptions, economic losses, and threats to public safety. Therefore, safeguarding the power grid is not just a technical challenge but a matter of national security, requiring coordinated efforts across public and private sectors (Bouramdane, 2023; Brambati et al., 2022).

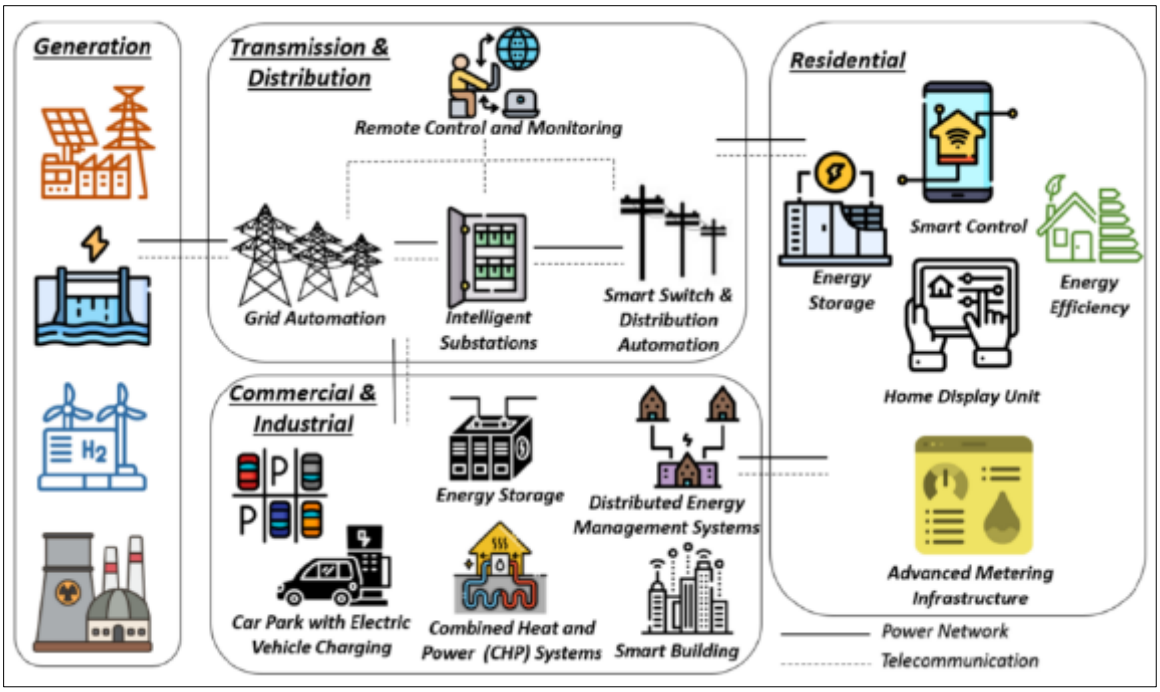

Figure 3 Smart Grid Architecture: Components and Functions Across Energy Sectors (Zaman and Mazinani, 2023)

4. Cybersecurity Challenges in Renewable Energy Systems

The transition toward integrating renewable energy sources into power grids has become imperative for enhancing environmental sustainability and achieving energy independence. However, this shift from centralized to decentralized energy systems, featuring distributed energy resources (DERs) such as wind farms and solar arrays, also introduces significant cybersecurity challenges. The proliferation of these interconnection points expands the potential attack surface for cyber threats dramatically compared to traditional power systems, which relied on a few high-capacity plants (Krause et al., 2021; Sen et al., 2022).

The decentralized nature of modern power grids, while offering benefits like increased flexibility and resilience, comes with intricate cybersecurity issues. Each DER can act as a vulnerability point for malicious actors, particularly as many of these assets ranging from commercial solar installations to residential battery systems require internet connectivity for their operations. This inherent connectivity can expose them to unauthorized access, facilitating cybercriminal activities like data tampering or manipulation of energy flows (Adeoba and Fatayo, 2024; Krause et al., 2021). Specific evidence points to instances where inadequately secured solar inverters have been accessible via unsecured internet interfaces, exemplifying the extent to which these vulnerabilities can threaten grid stability (Rekeraho et al., 2024; Jahromi et al., 2020).

Legacy infrastructure compounds these complications. Many existing Supervisory Control and Data Acquisition (SCADA) systems and other grid management technologies were developed without contemporary cybersecurity considerations. They often lack essential features like encryption and proper authentication, which makes them susceptible when connected to modern networks. This lack of backward compatibility further complicates cybersecurity retrofitting efforts (Krause et al., 2021; Jahromi et al., 2020). Moreover, the fragmented landscape of proprietary communication protocols among DER manufacturers leads to inconsistent security measures, complicating the establishment of a uniform response strategy across the renewable energy sector (Adeoba, et al., 2024; Sen et al., 2022).

Additionally, the rise of Internet of Things (IoT) technologies marks another frontier for cybersecurity vulnerabilities. IoT devices, widely deployed across energy systems for monitoring and control, often possess limited processing power to implement robust security features. Many are shipped with default credentials and outdated firmware, making them easy targets for attackers who could leverage these devices for broader assaults on the network (Rekeraho et al., 2024). Alongside, the trend of deploying edge computing technologies essential for autonomy and efficiency in energy management also raises risks. Compromised edge devices can disrupt local operations or corrupt data sent upstream, thereby amplifying threats to overall system reliability (Sen et al., 2022; Boyaci et al., 2021).

Remote monitoring and control systems essential for maintaining renewable energy assets also present critical security concerns. Technicians commonly access these systems through VPNs and web portals, which can serve as entry points for attackers if not secured with adequate measures like multi-factor authentication Jahromi et al., 2020). Historical incidents, such as the 2015 cyberattack on Ukraine's power grid, underscore the physical ramifications of digital breaches, wherein attackers were able to manipulate operational technology to cause real-world disruptions Jahromi et al., 2020). Cavus, 2024 presented Data and power flow in SG infrastructure with renewable energy integration as shown in figure 4.

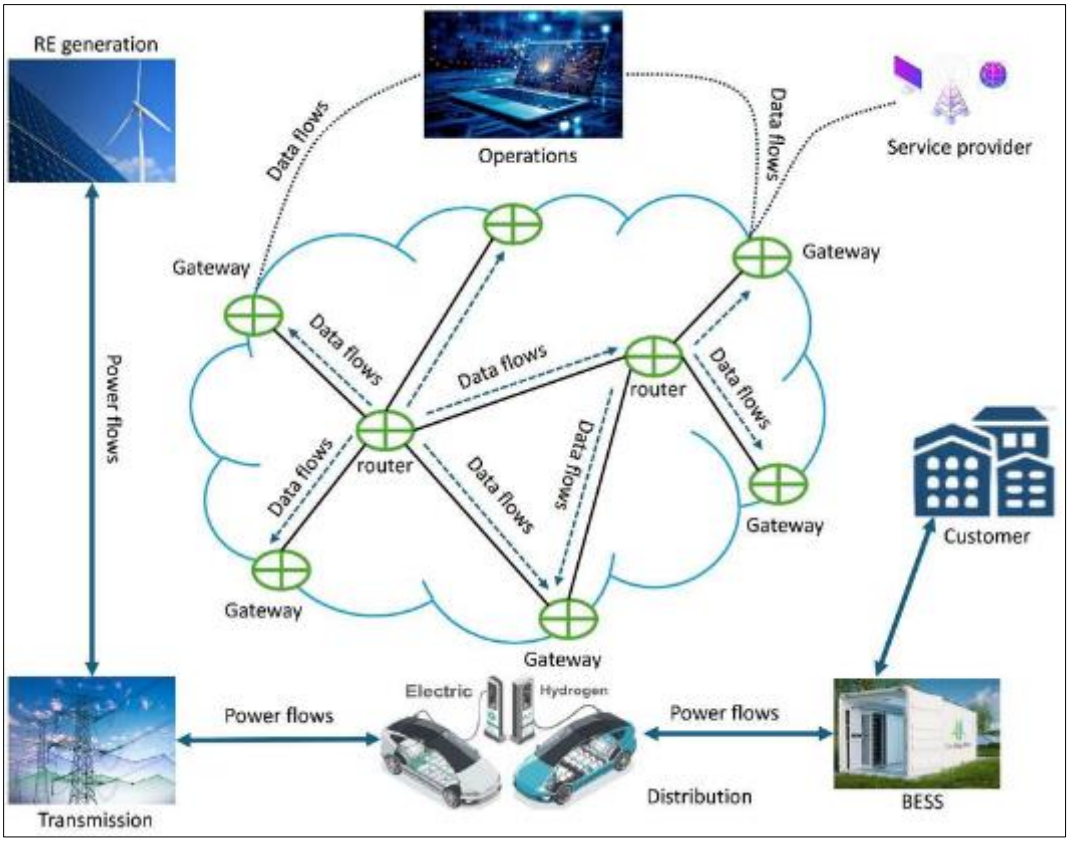

Figure 4 Data and power flow in SG infrastructure with renewable energy integration (Cavus, 2024)

To confront these cybersecurity challenges, a comprehensive approach is essential for the renewable energy sector. Stakeholders need to prioritize the modernization of aging systems and enforce stringent cybersecurity standards for new technologies. Furthermore, collaboration among energy providers, governmental agencies, and cybersecurity experts is vital to develop resilient architectures capable of withstanding potential threats (Krause et al., 2021; Jahromi et al., 2020). By understanding these multifaceted vulnerabilities, society can ensure that the transition to renewable energy does not compromise the security and reliability of critical infrastructure.

5. Threat Vectors and Risk Assessment

The integration of renewable energy technologies into modern power grids is reshaping the landscape of energy generation and distribution. While these advancements offer significant sustainability and efficiency benefits, they introduce considerable cybersecurity challenges that are critical to address. Ekechukwu and Simpa highlight that the intersection of renewable energy systems with cybersecurity reveals a pressing need for robust frameworks to secure these essential infrastructures against a variety of evolving threats (Ekechukwu and Simpa, 2024). They identify a range of cyber threats, such as malware and ransomware, that pose substantial risks to the operational integrity and reliability of energy systems.

Malware has become a pervasive threat within the energy sector, infiltrating grid systems through vectors including infected devices and software updates, potentially leading to severe operational disruptions. Ransomware, particularly virulent malware, encrypts critical operational data and can lock out energy operators from essential systems, jeopardizing grid stability (Rahim et al., 2023). Such attacks could have cascading effects, impacting not just isolated

systems but also the broader grid, potentially causing widespread outages and public safety threats. This is echoed in the findings of Mohamed et al., who outline the increasing sophistication of cyber threats targeting renewable energy systems (Adeoba, et al., 2025; Mohamed et al., 2023).

Phishing attacks represent another significant vector of cyber threat, primarily targeting individuals with access to sensitive operational information. Attackers often create deceptive communications to extract credentials or deploy malware. Ekechukwu and Simpa describe this tactic as particularly nefarious in the energy sector, where employees holding administrative controls are prime targets for infiltration attempts that can escalate into deeper network attacks (Ekechukwu and Simpa, 2024). The human element in cybersecurity remains a critical vulnerability, emphasizing the need for robust training and awareness initiatives to fortify defenses against such social engineering tactics.

Insider threats further complicate the cybersecurity landscape in renewable energy. Insiders, whether disgruntled employees or negligent contractors, possess unique access that can be exploited maliciously or unintentionally. Rahim et al. present organized frameworks for threat modeling and risk assessment that can highlight the nuances of insider threats, fostering the development of more effective mitigation strategies (Rahim et al., 2023). The complexity of security challenges is heightened by third-party access, which can amplify the risk of exploitation if security protocols are not meticulously established and managed.

Moreover, the emergence of sophisticated adversaries including state-sponsored actors and hacktivists introduces additional challenges. The targeted nature of these threats can lead to prolonged undetected breaches that might destabilize essential infrastructure (Ekechukwu and Simpa, 2024). The NIST Cybersecurity Framework serves as a critical tool for navigating these threats, guiding organizations in identifying vulnerabilities, managing risks, and establishing comprehensive defensive measures (Rahim et al., 2023). Ekechukwu and Simpa argue that tailoring such frameworks for renewable energy systems is essential for effectively responding to the sector-specific vulnerabilities (Ekechukwu and Simpa, 2024).

With the pressing need for robust cybersecurity measures, energy sector organizations must prioritize threat modeling and risk assessment processes. Such frameworks are invaluable in identifying potential attack vectors and evaluating the implications of various threat scenarios on system integrity. Al-Sada et al. emphasize utilizing resources like the MITRE ATTandCK framework, allowing energy operators to systematically analyze adversarial tactics and improve their defensive strategies (Al-Sada et al., 2024). The focus on continuous risk assessment and improvement aligns well with the evolving nature of threats in the domain, requiring ongoing vigilance and adaptation of security measures to safeguard the integrity of renewable energy systems.

In summary, while the shift toward renewable energy technologies heralds numerous benefits, it is crucial that cybersecurity is not sidelined. The multiplicity of cyber threats from malware and phishing to insider risks and organized crime mandates a comprehensive approach to secure renewable energy infrastructures. By leveraging advanced threat modeling frameworks and the collective knowledge of the cybersecurity community, organizations can build resilient defenses capable of protecting our increasingly digital and interdependent energy systems.

6. Cybersecurity Strategies for Grid Protection

As the global energy sector increasingly adopts renewable energy sources, the integration of these technologies into the energy grid necessitates advanced cybersecurity measures. The transition towards decentralized and digitalized grid systems has revealed vulnerabilities that traditional security models primarily perimeter-based defenses fail to address adequately (Park et al., 2023; Shaikh, 2024). This inadequacy presents dire consequences for critical energy infrastructures, demanding a shift toward comprehensive cybersecurity strategies that incorporate multi-layered defenses, dynamic architectures, and continuous monitoring to safeguard against cyberattacks (Bassfar et al., 2023; Shaikh, 2024).

Central to a resilient grid security model is a layered defense architecture based on the principle of defense-in-depth. This approach integrates a variety of security measures designed to mitigate risks even when some layers are breached, particularly in the context of renewable energy systems. Essential components include robust endpoint security for devices like solar inverters and wind turbine controllers, as well as fortified communication pathways between distributed assets and central control systems (Sharma et al., 2024; Paul and Rao, 2022). The application of technical measures such as firewalls, antivirus software, encrypted communications, and physical security significantly lowers the attack surface, which is crucial in enhancing detection chances and response times during potential cyber incidents (Adeoba, et al., 2025; Chamoli, 2020).

Moreover, network segmentation and strict access control are fundamental to this layered defense strategy. By isolating operational technology (OT) systems from less critical information technology (IT) environments, organizations reduce the potential for lateral movement by attackers. Techniques such as role-based access, multi-factor authentication, and the principle of least privilege minimize the risk of both insider threats and accidental exposures related to system vulnerabilities (Wylde, 2021; Sultana et al., 2020). These measures create a fortified framework essential in scenarios where intrusion attempts can originate from various sources, thus demanding thorough validation of all network interactions (Greenwood, 2021).

The incorporation of Artificial Intelligence (AI) and Machine Learning (ML) into cybersecurity processes is transforming threat detection and incident response capabilities. Traditional methods of monitoring systems are becoming insufficient given the sheer volume of data produced by smart grid components and IoT devices. AI-driven analytics can identify deviations from expected behavior, allowing for the detection of cyber threats such as unusual data transmissions or unauthorized access attempts (Bradatsch et al., 2023; Alevizos et al., 2021). Machine Learning models adapt over time, continually improving their accuracy and efficacy against evolving threats, thereby enabling faster and more effective responses to potential cyber incidents (Lv et al., 2022).

Blockchain technology also emerges as a revolutionary layer of security in decentralized energy networks, particularly in ensuring data integrity and transparent transactional operations. By creating immutable records validated by consensus mechanisms, blockchain facilitates secure interactions among numerous independent energy producers and consumers (prosumers) (Kang et al., 2023; Pop et al., 2018). Smart contracts can enhance the security of energy trading and operational agreements, mitigating reliance on centralized entities and bolstering trust among participants in peer-to-peer energy markets (Adeoba, Ukoba and Osaye, 2024; Hireche et al., 2022).

In light of these advancements, the implementation of zero-trust architectures is critical in modern grid cybersecurity. Unlike traditional systems that presume internal networks are secure, a zero-trust model mandates continuous verification of all users, devices, and applications (Braghin et al., 2002; Chen et al., 2021). This strategy is instrumental in preventing insider threats and unauthorized access, reinforcing a culture of skepticism toward implicit trust within network systems (Chen et al., 2022). Adopting components such as real-time behavioral analysis, micro-segmentation, and identity management systems can significantly streamline the security processes across utility organizations (Sallam et al., 2019).

To effectively combat cyber threats within renewable energy systems, organizations must employ intrusion detection and response systems (IDRS) as front-line defenses. These systems, utilizing both signature-based and anomaly-based methodologies, are crucial for real-time monitoring and responding to suspicious activities (Alagappan et al., 2022). With operational continuity paramount in energy systems, deploying IDRS at various levels including edge devices and centralized control units provides essential visibility and rapid response capabilities needed to neutralize threats before they escalate (Adeoba, Shandu and Pandelani, 2025: Han, 2023).

The success of these strategies is contingent upon seamless integration, active monitoring of threats, and adaptive management of cybersecurity measures. Continuous security assessments, investment in security orchestration platforms, and collaborative training exercises for IT and OT personnel cultivate an environment capable of dynamically responding to evolving cyber threats (Munsing et al., 2017; Bartakke and Kashyap, 2024). Furthermore, fostering security awareness and adherence to regulatory standards, such as the NIST Cybersecurity Framework and ISO/IEC 27001, ensures a comprehensive foundation for maintaining rigorous cybersecurity controls across the energy sector (Yang et al., 2018).

In conclusion, as the energy sector evolves toward more intelligent and decentralized infrastructures, cybersecurity must keep pace with innovation and emerging threats. The fusion of technologies like AI, blockchain, and zero-trust architecture, combined with proactive strategies for threat detection, offers a robust defense against a range of cyber risks. However, technology alone cannot secure the grid; a holistic approach intertwining technical defenses, human vigilance, and regulatory compliance is paramount for achieving a resilient and secure energy landscape (Sultana et al., 2020).

7. Regulatory and Policy Frameworks

The integration of renewable energy sources (RES) into modern power grids has become increasingly prevalent, contributing to the transformation of energy systems globally. However, this rise has simultaneously introduced significant cybersecurity concerns due to the digitization and interconnectivity of energy infrastructures. These vulnerabilities threaten the reliability and functionality of power systems and pose risks to national security and public

safety (Ekechukwu and Simpa, 2024; (Ekechukwu and Simpa, 2024). As a result, robust regulatory and policy frameworks have emerged as crucial tools to address these challenges and enhance the resilience of the energy sector (Mikac, 2023; Ekechukwu and Simpa, 2024).

Governments worldwide have initiated the development and enforcement of various cybersecurity regulations aimed at safeguarding energy infrastructures. For instance, the European Union has implemented the Network and Information Security (NIS) Directive, which mandates enhancing national cybersecurity capabilities and obligates operators of essential services, including energy providers, to adopt stringent security measures (Adeoba, Odjegba and Pandelani, 2025). The evolution of this directive into NIS2 has expanded its reach, integrating stricter enforcement mechanisms to bolster the cybersecurity frameworks across member states (Mikac, 2023). Additionally, the International Telecommunication Union (ITU) provides global standards and guidelines for critical infrastructure protection, while the International Electrotechnical Commission (IEC) offers specific standards like IEC 62443 that address cybersecurity in industrial automation and control systems, which are integral to energy systems (Bhusal et al., 2020; (Ekechukwu and Simpa, 2024; .

In the United States, one prominent framework is the North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC CIP) standards. These enforce mandatory cybersecurity protocols for entities managing the bulk electric system, encompassing risk management and incident response strategies aimed at shielding the electric grid from both cyber and physical threats (Tuyen et al., 2022; Ekechukwu and Simpa, 2024). The standards undergo strict oversight by the Federal Energy Regulatory Commission (FERC), with non-compliance potentially leading to penalties, indicating the vital importance of these frameworks (Sheikh et al., 2020; Mikac, 2023). Complementing NERC CIP, broader cybersecurity models such as the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) facilitate organizations in assessing and enhancing their security posture (Ekechukwu and Simpa, 2024; Tuyen et al., 2022). Furthermore, internationally recognized standards like ISO/IEC 27001 provide a systematic approach to managing sensitive information, thereby establishing a baseline for cybersecurity maturity in the energy domain (Manowska et al., 2024; Mikac, 2023).

Despite these frameworks, energy providers encounter significant hurdles in achieving compliance amid rapid technological advancements and evolving cyber threats. The decentralized nature of renewable energy systems, characterized by dispersed assets such as solar panels and wind turbines, complicates the implementation of comprehensive security measures (Lee et al., 2023; Rekeraho et al., 2023). Additionally, the dynamic nature of cyber threats can outpace regulatory frameworks, leading to a reactive compliance orientation where organizations may prioritize meeting regulatory requirements over proactive security enhancements (Tuyen et al., 2022; Mikac, 2023). The inconsistency of regulatory environments across jurisdictions further complicates compliance for transnational energy operators, resulting in fragmented efforts that are difficult to synchronize (Ekechukwu and Simpa, 2024; Mikac, 2023).

A critical factor in safeguarding the energy sector against cybersecurity threats is the existing shortage of skilled cybersecurity professionals. This shortage adds pressure on current teams and could create compliance gaps, emphasizing the necessity for continuous investment in workforce development (Ekechukwu and Simpa, 2024; Tuyen et al., 2022). In this context, public-private partnerships (PPPs) can be instrumental. Collaboration between government entities and private sector stakeholders fosters the sharing of threat intelligence and resources, enhancing the overall cybersecurity posture of energy systems (Sheikh et al., 2020; Tuyen et al., 2022). Moreover, initiatives such as the Electricity Information Sharing and Analysis Center (E-ISAC) exemplify how these partnerships can facilitate timely responses to cyber threats within the energy domain (Lee et al., 2023; Sheikh et al., 2020).

To address the existing compliance challenges, many frameworks are shifting towards emphasizing maturity models and risk-based approaches, thereby promoting flexibility and innovation in security practices. This evolving mindset reflects the understanding that cybersecurity is an ongoing process, requiring continuous adaptation and improvement (Ekechukwu and Simpa, 2024; Sheikh et al., 2020). A more sophisticated approach towards compliance can enable energy organizations to better navigate the complexities associated with the cybersecurity landscape.

In conclusion, while regulatory and policy frameworks play a pivotal role in securing the infrastructure supporting renewable energy integration, challenges related to complexity, regulatory inconsistency, workforce shortages, and rapid technological evolution persist. A comprehensive approach encompassing regulatory imperatives, collaborative strategies, and flexibility in compliance initiatives will be essential for effectively safeguarding the energy sector against emerging cyber threats and ensuring a secure transition to sustainable energy systems.

8. Workforce Development and Capacity Building

The advancement of smart grid technologies has indeed brought transformative benefits to modern energy systems, enhancing efficiency, flexibility, sustainability, and facilitating the integration of renewable energy sources (Uzondu and Lele, 2024). By employing advanced digital technologies and automation, smart grids have redefined energy management across various sectors, promoting a shift from traditional power systems to more reliable and responsive configurations that can accommodate variable energy production from renewables (Liu et al., 2012). However, such advancements also increase reliance on digital systems and real-time data exchange, which in turn raise significant cybersecurity concerns (Apata, et al., 2024; Bouramdane, 2023).

The substantial expansion of the attack surface in energy infrastructures necessitates a robust cybersecurity posture, underpinned by comprehensive regulatory and policy frameworks (Leszczyna, 2019). A critical element in this regard is the regulatory landscape that aims to secure the integrity and resilience of smart grids against escalating cyber threats. For instance, the North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC CIP) standards stand out as a fundamental framework for mandatory compliance among entities managing the bulk electric system (Marron et al., 2019). These standards encompass stringent requirements for identifying critical assets, implementing access control measures, and ensuring secure communications, thus establishing a consistent baseline for cybersecurity readiness across the sector (Ayanwale, et al., 2024; Marron et al., 2019).

Internationally, the International Electrotechnical Commission (IEC) has crafted the IEC 62443 series, which delineates frameworks for securing industrial automation and control systems including those pivotal to smart grids. This standard promotes a defense-in-depth strategy, emphasizing secure design principles, ongoing risk assessment, and continuous monitoring practices (Leszczyna, 2019). Such international regulatory efforts are vital for aligning security expectations across the supply chain, especially as the integration of renewable energy sources continues to evolve (Uzondu and Lele, 2024).

Nonetheless, the pursuit of a cohesive global cybersecurity framework faces significant hurdles, including policy gaps and variabilities in regulatory approaches across different jurisdictions (Ye et al., 2012). This lack of uniformity can result in fragmented compliance landscapes, complicating operations for multinational entities within the energy sector. Variations in cybersecurity regulations may lead to inconsistencies in risk exposure and responses, as companies may have different obligations in different regions (DEVI, 2022; John and Oyeyemi, 2022). Moreover, existing policies often struggle to keep pace with the rapid technological advancements and sophisticated cyber threats emerging in the digital landscape, signaling a crucial need for adaptable regulatory frameworks (Liu et al., 2012).

Furthermore, the integration of cybersecurity considerations within broader energy and environmental goals has become increasingly paramount. As nations set ambitious renewable energy and decarbonization targets, there is a pressing need to ensure that innovation does not compromise security (Iyer, 2011). Policymakers must embed cybersecurity into the very fabric of energy policy rather than treating it as an adjunct to safeguard the long-term sustainability of smart grids (Oyeyemi, 2022).

Lastly, effective cybersecurity governance relies on collaboration among government agencies, private sector stakeholders, and regulators. Public-private partnerships play a vital role in facilitating information sharing, threat intelligence exchange, and coordinated response efforts among different players in the energy ecosystem (Bouramdane, 2023; Ukoba, et al., 2024). Initiatives like the Electricity Information Sharing and Analysis Center (E-ISAC) exemplify the benefits of collaborative defense mechanisms in consolidating cyber threat information and bolstering the resilience of smart grid systems (Marron et al., 2019; Oyeyemi, Akinlolu and Awodola, 2025).

In conclusion, addressing the regulatory and policy dimensions of smart grid security is essential in creating an energy system that not only embraces modern technological advancements but also upholds the highest standards of cybersecurity. International standards like NERC CIP and IEC 62443 provide necessary guidance, yet harmonization efforts and collaborative governance frameworks must evolve to meet the unique and growing challenges posed by digital transformations in the energy landscape. By ensuring that cybersecurity remains integrated with broader energy policy objectives, we can cultivate a more secure, sustainable, and resilient energy future.

9. Global Case Studies and Best Practices

As renewable energy technologies continue to gain prominence in the global electricity landscape, the fortification of power grids against cybersecurity threats has emerged as a paramount concern for nations worldwide. With the

electrification of energy systems, cybersecurity must evolve to counter the growing risks associated with increased reliance on digital technologies. This necessity is highlighted in the review by Ekechukwu and Simpa, which emphasizes the need for strong cybersecurity frameworks tailored specifically for renewable energy infrastructures to address evolving cyber threats and vulnerabilities (Ekechukwu and Simpa, 2024).

Diverse approaches to grid cybersecurity have been adopted globally, shaped by regional regulatory frameworks, technological sophistication, geopolitical dynamics, and existing energy infrastructures. For example, in the United States, cybersecurity measures for the energy sector are governed by stringent federal regulations and collaborative public-private partnerships. The North American Electric Reliability Corporation (NERC) enforces Critical Infrastructure Protection (CIP) standards, ensuring that energy organizations adhere to rigorous access controls and incident response protocols Powell et al., 2020). The Department of Energy (DOE) spearheads initiatives like the Cybersecurity for Energy Delivery Systems (CEDS) program, which funds innovative solutions to enhance the security of energy delivery systems (Ekechukwu and Simpa, 2024; . The recent Colonial Pipeline ransomware attack underscored the urgency of these efforts, reinforcing the critical role of cybersecurity in protecting vital energy infrastructures (Mohamed et al., 2023).

In contrast, Europe has enacted comprehensive regulations, particularly through the Network and Information Security (NIS) Directive and its successor NIS2, which mandates risk management practices for operators of essential services, including energy providers (Salvaggio and González, 2022; Contreras, 2023). The European Union Agency for Cybersecurity (ENISA) plays a pivotal role in facilitating collaboration between member states, providing training, guidelines, and intelligence sharing to bolster cybersecurity resilience among energy operators (Cassotta and Sidortsov, 2019). Noteworthy examples include Germany's BSI, which has developed technical standards promoting secure smart grid operations, and Denmark's proactive approaches for conducting simulations to test for potential cyber threats (Mohamed et al., 2023).

Beyond the United States and Europe, countries in Asia, such as Japan, South Korea, China, and India, exhibit distinctive strategies toward cybersecurity, catering to their unique energy needs and infrastructure challenges. Japan's Cybersecurity Strategy for Critical Infrastructure emphasizes the integration of public-private information-sharing and advanced technological deployments for threat detection, particularly following the Fukushima incident (Hu et al., 2022)Abrahams et al., 2024). Meanwhile, South Korea's significant investment in cybersecurity aligns with its smart grid initiatives and involves community awareness campaigns (Hu et al., 2022). China's government enforces strict regulations addressing cybersecurity risks within its expansive energy sector, promoting standardization in security protocols amidst rapid growth in renewable energy sources (Abdullahi et al., 2022; Oyeyemi, Akinlolu and Awodola, 2025).

A common thread across these diverse case studies is the recognition of best practices critical to fostering resilient and secure energy systems. This includes proactive measures, termed "cyber-informed engineering," where security considerations are integral to system design rather than an afterthought (Ekechukwu and Simpa, 2024; Ukoba, et al., 2024). Concepts of layered defense, continuous monitoring, and real-time threat intelligence are emphasized to ensure the resilience of energy infrastructures against potential breaches (Ekechukwu and Simpa, 2024; Powell et al., 2020). The necessity for capacity building through education and cross-sector collaboration is also crucial, as nations strive to prepare their workforces and organizations to navigate the increasingly complex cyber landscape (Wallis et al., 2022; Powell et al., 2019).

In summary, integrating cybersecurity into renewable energy systems is an ongoing global endeavor, underscored by distinct national strategies and collaborative frameworks. As the digital transformation of energy systems accelerates worldwide, adapting insights from varying regional frameworks and best practices will become increasingly vital. The shared challenges in cybersecurity necessitate collective action among nations, energy providers, and cybersecurity experts to secure a stable and resilient energy future.

10. Conclusion, Recommendations and Future Outlook

Protecting the power grid in an era of rapid renewable energy integration demands a comprehensive, forward-thinking approach to cybersecurity. As the energy sector becomes more decentralized and digitized, the surface area for cyber threats grows significantly, exposing vulnerabilities in both legacy systems and new digital interfaces. This paper has explored the complex intersection of renewable energy and cybersecurity, highlighting the multifaceted challenges that arise from distributed energy resources, smart grid technologies, and the global shift toward clean energy systems. It has also examined threat vectors, risk assessment strategies, regulatory frameworks, workforce development, and global case studies to present a holistic understanding of the current landscape.

The integration of cybersecurity into renewable energy planning must be strategic, proactive, and deeply embedded at every stage from infrastructure design and technology deployment to operations and maintenance. Cybersecurity should no longer be viewed as a reactive layer added post-deployment but as a foundational design principle in the development of modern energy systems. This involves applying cyber-informed engineering, adopting layered defense strategies, and building cross-disciplinary teams that understand both operational and information technology systems. Key components such as SCADA systems, IoT devices, and cloud-based platforms must be designed and managed with security as a priority, with clearly defined protocols for access control, encryption, authentication, and data integrity.

Continuous monitoring and adaptive cybersecurity frameworks are vital in maintaining resilience as threats evolve. Static defenses are no longer sufficient against adversaries that deploy advanced, adaptive, and persistent tactics. Real-time analytics powered by artificial intelligence and machine learning offer valuable capabilities for threat detection, anomaly identification, and rapid response. These tools must be complemented by intrusion detection systems, regular vulnerability assessments, and automated incident response mechanisms. Importantly, adaptive cybersecurity frameworks should support learning from every breach attempt and integrate those insights into ongoing system improvements.

A critical component of building a resilient energy cybersecurity posture is global collaboration and the development of standardized best practices. As energy markets and infrastructure become increasingly interconnected across borders, the vulnerabilities of one nation can quickly impact others. Cybersecurity must therefore be treated as a shared global responsibility. International standards, such as those developed by NIST, ISO/IEC, and ENISA, should be promoted and adapted to national contexts to ensure uniformity in protection measures. Forums for information exchange, public-private partnerships, and bilateral agreements should be strengthened to facilitate rapid threat sharing and collective response planning.

The findings of this paper underscore the pressing need to prioritize cybersecurity in every facet of renewable energy development. Key insights include the growing exposure created by distributed and interconnected systems, the inadequacy of legacy technologies, the benefits of multi-layered defense and AI-driven threat monitoring, the value of cross-sector collaboration, and the urgent need for skilled professionals to manage evolving risks. Global case studies demonstrate that success in protecting the grid depends not only on technological innovation but also on governance, capacity building, and a culture of security embedded within institutions.

The urgency of strengthening cybersecurity in renewable energy systems cannot be overstated. As societies become increasingly dependent on clean electricity, the consequences of cyberattacks on grid infrastructure extend beyond financial loss to threaten national security, public health, and social stability. A successful cyberattack on a major renewable energy provider could disrupt electricity supply, destabilize grid operations, and erode public confidence in sustainable energy transitions. Therefore, the resilience of the energy grid is not just a technical challenge it is a national and global imperative.

Policymakers, regulators, industry leaders, and technology developers must take decisive action. Investment in secure technologies, support for cybersecurity research, the enforcement of strong regulatory standards, and the promotion of workforce development should be top priorities. Policymakers should mandate cybersecurity impact assessments for all renewable energy projects, provide incentives for compliance with international standards, and support the creation of collaborative platforms for threat intelligence and incident response. Meanwhile, utilities and grid operators must embed cybersecurity into their governance structures, operational practices, and procurement processes.

Looking ahead, the future of renewable energy cybersecurity lies in integration, innovation, and international cooperation. As the energy ecosystem becomes more complex and intelligent, cybersecurity must keep pace through scalable, interoperable, and adaptive solutions. Smart grid technologies, blockchain-enabled energy trading, and AI-enhanced monitoring will redefine how energy is produced, distributed, and secured. These advancements must be guided by ethical considerations, privacy protections, and equitable access to ensure that digital energy transitions benefit all communities.

In conclusion, protecting the grid in the age of renewable energy integration requires more than technological fixes it requires a paradigm shift in how we design, operate, and govern our energy systems. Cybersecurity must be recognized as a core pillar of energy resilience, embedded in policy, practice, and education. The time to act is now. By prioritizing cybersecurity, embracing innovation, and fostering global solidarity, stakeholders can ensure that the energy systems of the future are not only sustainable and efficient but also secure and resilient.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L., … and Abdulkadir, S. (2022). Detecting cybersecurity attacks in internet of things using artificial intelligence methods: a systematic literature review. Electronics, 11(2), 198. https://doi.org/10.3390/electronics11020198

[2] Abdulwahid, A. and Ateeq, A. (2019). Innovative differential protection scheme for microgrids based on rc current sensor.. https://doi.org/10.5772/intechopen.85473

[3] Abrahams, T., Ewuga, S., Dawodu, S., Adegbite, A., and Hassan, A. (2024). A review of cybersecurity strategies in modern organizations: examining the evolution and effectiveness of cybersecurity measures for data protection. Computer Science and It Research Journal, 5(1), 1-25. https://doi.org/10.51594/csitrj.v5i1.699

[4] Adegbite, A., Akinwolemiwa, D., Uwaoma, P., Kaggwa, S., Akindote, O., and Dawodu, S. (2023). Review of cybersecurity strategies in protecting national infrastructure: perspectives from the usa. Computer Science and It Research Journal, 4(3), 200-219. https://doi.org/10.51594/csitrj.v4i3.658

[5] Adelana, O. P., Ayanwale, M. A., Adeoba, M. I., Oyeniran, D. O., Matsie, N., and Olugbade, D. (2024, November). Machine Learning Algorithm for Predicting Pre-Service Teachers' Readiness to Use Brain-Computer Interfaces in Inclusive Classrooms. In 2024 IEEE 5th International Conference on Electro-Computing Technologies for Humanity (NIGERCON) (pp. 1-10). IEEE.

[6] Adeoba, M. I., and Fatayo, O. C. (2024). A Review of Innovative Technologies for Sustaining Water Catchment Areas: Toward Sustainability Development. Sustainable Engineering: Concepts and Practices, 21-31.

[7] Adeoba, M. I., Pandelani, T., Ngwagwa, H., and Masebe, T. (2024). Generation of Renewable Energy by Blue Resources for a Clean Environment. In Marine Bioprospecting for Sustainable Blue-bioeconomy (pp. 337-353). Cham: Springer Nature Switzerland.

[8] Adeoba, M. I., Pandelani, T., Ngwangwa, H., and Masebe, T. (2025). The Role of Artificial Intelligence in Sustainable Ocean Waste Tracking and Management: A Bibliometric Analysis. Sustainability, 17(9), 3912.

[9] Adeoba, M. I., Ukoba, K., and Osaye, F. (2024). Blue Carbon: Roles in Climate Change and Energy Generation, and Effects on Coastal Communities. In Marine Bioprospecting for Sustainable Blue-bioeconomy (pp. 319-335). Cham: Springer Nature Switzerland.

[10] Adeoba, M., Pandelani, T., Ngwangwa, H., and Masebe, T. (2025, May). The Role of Artificial Intelligence Technology in the Fulfilment of Sustainable Development Goals in Biogas Production. In CONECT. International Scientific Conference of Environmental and Climate Technologies (pp. 72-73).

[11] Adeoba, M., Shandu, K. E., and Pandelani, T. (2025, May). Review of Biogas Production and Bio-Methane Potential of Fish Solid Waste and Fish Waste. In CONECT. International Scientific Conference of Environmental and Climate Technologies (pp. 74-75).

[12] Adeoba, M.I., Odjegba, E.E. and Pandelani, T., 2025. Nature-based solutions: Opportunities and challenges for water treatment. Smart Nanomaterials for Environmental Applications, pp.575-596.

[13] Ahmed, S., Lee, Y., Hyun, S., and Koo, I. (2019). Mitigating the impacts of covert cyber attacks in smart grids via reconstruction of measurement data utilizing deep denoising autoencoders. Energies, 12(16), 3091. https://doi.org/10.3390/en12163091

[14] Alagappan, A., Venkatachary, S., and Andrews, L. (2022). Augmenting zero trust network architecture to enhance security in virtual power plants. Energy Reports, 8, 1309-1320. https://doi.org/10.1016/j.egyr.2021.11.272

[15] Alekseichuk, L., Новиков, О., Yakobchuk, D., and Rodionov, A. (2023). Cyber security logical and probabilistic model of a critical infrastructure facility in the electric energy industry. Theoretical and Applied Cybersecurity, 5(1). https://doi.org/10.20535/tacs.2664-29132023.1.287365

[16] Alevizos, L., Ta, V., and Eiza, M. (2021). Augmenting zero trust architecture to endpoints using blockchain: a state-of-the-art review. Security and Privacy, 5(1). https://doi.org/10.1002/spy2.191

[17] Al-Sada, B., Sadighian, A., and Oligeri, G. (2024). Analysis and characterization of cyber threats leveraging the mitre attandck database. Ieee Access, 12, 1217-1234. https://doi.org/10.1109/access.2023.3344680

[18] Annuk, A., Yaïci, W., Lehtonen, M., Ilves, R., Kabanen, T., and Miidla, P. (2021). Simulation of energy exchange between single prosumer residential building and utility grid.. https://doi.org/10.37247/aderes2edn.3.2021.1

[19] Apata, S. B., Oyenuga, M. O., Adeoba, M. I., Ugom, M. K., and Abiodun, A. O. (2024). Internet of Things (IoT) Solutions for smart transportation infrastructure and fleet management. Tuijin Jishu/Journal of Propulsion Technology, 45(4), 1492-509.

[20] Attia, T. (2019). The challenges and risks facing ict in the management and operation of the smart grid. Renewable Energy and Sustainable Development, 5(1), 3. https://doi.org/10.21622/resd.2019.05.1.003

[21] AVCI, İ. (2021). Investigation of cyber-attack methods and measures in smart grids. Sakarya University Journal of Science, 25(4), 1049-1060. https://doi.org/10.16984/saufenbilder.955914

[22] Ayanwale, M.A., Adeoba, M.I., Adelana, O.P., Lawal, R.O., Makhetha, I.M. and Mochekele, M., 2024, November. Cybersecurity for Educational Excellence: Bibliometric Insights from Higher Education. In 2024 IEEE 5th International Conference on Electro-Computing Technologies for Humanity (NIGERCON) (pp. 1-8). IEEE.

[23] Baimel, D., Tapuchi, S., and Baimel, N. (2016). Smart grid communication technologies. Journal of Power and Energy Engineering, 04(08), 1-8. https://doi.org/10.4236/jpee.2016.48001

[24] Bartakke, J. and Kashyap, R. (2024). The usage of clouds in zero-trust security strategy. Journal of Information and Organizational Sciences, 48(1), 149-165. https://doi.org/10.31341/jios.48.1.8

[25] Bassfar, Z., Sayeed, A., Bala, P., Alshehri, A., Alanazi, A., and Zubair, S. (2023). Toward secure and resilient networks: a zero-trust security framework with quantum fingerprinting for devices accessing network. Mathematics, 11(12), 2653. https://doi.org/10.3390/math11122653

[26] Bhusal, N., Gautam, M., and Benidris, M. (2020). Cybersecurity of electric vehicle smart charging management systems.. https://doi.org/10.48550/arxiv.2008.07511

[27] Bouramdane, 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. https://doi.org/10.3390/jcp3040031

[28] Boyaci, O., Narimani, M., Davis, K., and Serpedin, E. (2021). Cyberattack detection in large-scale smart grids using chebyshev graph convolutional networks.. https://doi.org/10.48550/arxiv.2112.13166 Jahromi, M., Jahromi, A., Sanner, S., Kundur, D., and Kassouf, M. (2020). Cybersecurity enhancement of transformer differential protection using machine learning., 1-5. https://doi.org/10.1109/pesgm41954.2020.9282161

[29] Bradatsch, L., Miroshkin, O., and Kargl, F. (2023). Ztsfc: a service function chaining-enabled zero trust architecture. Ieee Access, 11, 125307-125327. https://doi.org/10.1109/access.2023.3330706

[30] Braghin, C., Cortesi, A., and Focardi, R. (2002). Security boundaries in mobile ambients. Computer Languages Systems and Structures, 28(1), 101-127. https://doi.org/10.1016/s0096-0551(02)00009-7 Chamoli, S. (2020). Blockchain-based iot systems: techniques, applications, and challenges. Turkish Journal of Computer and Mathematics Education (Turcomat), 11(3), 2108-2118. https://doi.org/10.17762/turcomat.v11i3.13608

[31] Brambati, F., Ruscio, D., Biassoni, F., Hueting, R., and Tedeschi, A. (2022). Predicting acceptance and adoption of renewable energy community solutions: the prosumer psychology. Open Research Europe, 2, 115. https://doi.org/10.12688/openreseurope.14950.1

[32] Cassotta, S. and Sidortsov, R. (2019). Sustainable cybersecurity? rethinking approaches to protecting energy infrastructure in the european high north. Energy Research and Social Science, 51, 129-133. https://doi.org/10.1016/j.erss.2019.01.003

[33] Castellini, M., Menoncin, F., Moretto, M., and Vergalli, S. (2021). Photovoltaic smart grids in the prosumers investment decisions: a real option model. Journal of Economic Dynamics and Control, 126, 103988. https://doi.org/10.1016/j.jedc.2020.103988

[34] Cavus, M. (2024). Integration Smart Grids, Distributed Generation, and Cybersecurity: Strategies for Securing and Optimizing Future Energy Systems.

[35] Chen, B., Qiao, S., Zhao, J., Liu, D., Shi, X., Lyu, M., … and Zhai, Y. (2021). A security awareness and protection system for 5g smart healthcare based on zero-trust architecture. Ieee Internet of Things Journal, 8(13), 10248-10263. https://doi.org/10.1109/jiot.2020.3041042

[36] Chen, X., Feng, W., Ge, N., and Zhang, Y. (2022). Zero trust architecture for 6g security.. https://doi.org/10.48550/arxiv.2203.07716

[37] Contreras, P. (2023). The transnational dimension of cybersecurity: the nis directive and its jurisdictional challenges., 327-341. https://doi.org/10.1007/978-981-19-6414-5_18

[38] DEVI, M. (2022). Relevance of cybersecurity in smart grid. Interantional Journal of Scientific Research in Engineering and Management, 06(04). https://doi.org/10.55041/ijsrem12216

[39] Ekechukwu, D. and Simpa, P. (2024). The future of cybersecurity in renewable energy systems: a review, identifying challenges and proposing strategic solutions. Computer Science and It Research Journal, 5(6), 1265-1299. https://doi.org/10.51594/csitrj.v5i6.1197

[40] Ekechukwu, D. and Simpa, P. (2024). The importance of cybersecurity in protecting renewable energy investment: a strategic analysis of threats and solutions. Engineering Science and Technology Journal, 5(6), 1845-1883. https://doi.org/10.51594/estj.v5i6.1186

[41] Eltamaly, A. M., Alotaibi, M. A., Alolah, A. I., and Ahmed, M. A. (2021). IoT-based hybrid renewable energy system for smart campus. Sustainability, 13(15), 8555.

[42] Espe, E., Potdar, V., and Chang, E. (2018). Prosumer communities and relationships in smart grids: a literature review, evolution and future directions. Energies, 11(10), 2528. https://doi.org/10.3390/en11102528

[43] Galinec, D. (2023). Cyber security and cyber defense: challenges and building of cyber resilience conceptual model. International Journal of Applied Sciences and Development, 1, 83-88. https://doi.org/10.37394/232029.2022.1.10

[44] Greenwood, D. (2021). Applying the principles of zero-trust architecture to protect sensitive and critical data. Network Security, 2021(6), 7-9. https://doi.org/10.1016/s1353-4858(21)00063-5

[45] Han, J. (2023). Data access security monitoring system based on zero trust mechanism., 88. https://doi.org/10.1117/12.2685667

[46] Hireche, O., Benzaïd, C., and Taleb, T. (2022). Deep data plane programming and ai for zero-trust self-driven networking in beyond 5g. Computer Networks, 203, 108668. https://doi.org/10.1016/j.comnet.2021.108668

[47] Hu, J., Chen, Y., and Yang, Y. (2022). The development and issues of energy-ict: a review of literature with economic and managerial viewpoints. Energies, 15(2), 594. https://doi.org/10.3390/en15020594

[48] Iyer, S. (2011). Cyber security for smart grid, cryptography, and privacy. International Journal of Digital Multimedia Broadcasting, 2011, 1-8. https://doi.org/10.1155/2011/372020

[49] Jahromi, A., Kemmeugne, A., Kundur, D., and Haddadi, A. (2020). Cyber-physical attacks targeting communication-assisted protection schemes. Ieee Transactions on Power Systems, 35(1), 440-450. https://doi.org/10.1109/tpwrs.2019.2924441

[50] John, A. O., and Oyeyemi, B. B. (2022). The Role of AI in Oil and Gas Supply Chain Optimization.

[51] Kang, H., Liu, G., Wang, Q., Lei, M., and Liu, J. (2023). Theory and application of zero trust security: a brief survey. Entropy, 25(12), 1595. https://doi.org/10.3390/e25121595

[52] Kim, S., Lee, T., Kim, S., Park, L., and Park, S. (2019). Security issues on smart grid and blockchain-based secure smart energy management system. Matec Web of Conferences, 260, 01001. https://doi.org/10.1051/matecconf/201926001001

[53] Ko, J., Lee, S., and Shon, T. (2015). Towards a novel quantification approach based on smart grid network vulnerability score. International Journal of Energy Research, 40(3), 298-312. https://doi.org/10.1002/er.3356

[54] Krause, T., Ernst, R., Klaer, B., Hacker, I., and Henze, M. (2021). Cybersecurity in power grids: challenges and opportunities. Sensors, 21(18), 6225. https://doi.org/10.3390/s21186225

[55] Le, T., Anwar, A., Loke, S., Beuran, R., and Tan, Y. (2020). Gridattacksim: a cyber attack simulation framework for smart grids. Electronics, 9(8), 1218. https://doi.org/10.3390/electronics9081218

[56] Lee, J., Shin, J., and Seo, J. (2023). Solar power plant network packet-based anomaly detection system for cybersecurity. Computers Materials and Continua, 77(1), 757-779. https://doi.org/10.32604/cmc.2023.039461

[57] Leszczyna, R. (2019). Standards with cybersecurity controls for smart grid a systematic analysis. International Journal of Communication Systems, 32(6). https://doi.org/10.1002/dac.3910

[58] Liu, J., Xiao, Y., Li, S., Liang, W., and Chen, C. (2012). Cyber security and privacy issues in smart grids. Ieee Communications Surveys and Tutorials, 14(4), 981-997. https://doi.org/10.1109/surv.2011.122111.00145

[59] Lv, P., Sun, X., Huang, H., Qian, J., Sun, C., and Dai, H. (2022). Dynamic trust continuous evaluation-based zero-trust access control for power grid cloud service. Journal of Physics Conference Series, 2402(1), 012008. https://doi.org/10.1088/1742-6596/2402/1/012008

[60] Manowska, A., Boroš, M., Hassan, M., Bluszcz, A., and Tobór–Osadnik, K. (2024). A modern approach to securing critical infrastructure in energy transmission networks: integration of cryptographic mechanisms and biometric data. Electronics, 13(14), 2849. https://doi.org/10.3390/electronics13142849

[61] Marron, J., Gopstein, A., Bartol, N., and Feldman, V. (2019). Cybersecurity framework smart grid profile.. https://doi.org/10.6028/nist.tn.2051

[62] Mikac, R. (2023). Protection of the eu's critical infrastructures: results and challenges. Applied Cybersecurity and Internet Governance, 2(1), 1-5. https://doi.org/10.60097/acig/162868

[63] Milanezi, J., Costa, J., Garcez, C., Albuquerque, R., Arancibia, A., Weichenberger, L., … and Sousa, R. (2020). Data security and trading framework for smart grids in neighborhood area networks. Sensors, 20(5), 1337. https://doi.org/10.3390/s20051337

[64] Mohamed, N., El-Guindy, M., Oubelaid, A., and Almazrouei, S. (2023). Smart energy meets smart security: a comprehensive review of ai applications in cybersecurity for renewable energy systems. International Journal of Electrical and Electronics Research, 11(3), 728-732. https://doi.org/10.37391/ijeer.110313

[65] Mohammed, S., Al-Jumaily, A., Singh, M., Jiménez, V., Jaber, A., Hussein, Y., … and Al-Jumeily, D. (2024). A review on the evaluation of feature selection using machine learning for cyber-attack detection in smart grid. Ieee Access, 12, 44023-44042. https://doi.org/10.1109/access.2024.3370911

[66] Morstyn, T. and McCulloch, M. (2019). Multiclass energy management for peer-to-peer energy trading driven by prosumer preferences. Ieee Transactions on Power Systems, 34(5), 4005-4014. https://doi.org/10.1109/tpwrs.2018.2834472

[67] Munsing, E., Mather, J., and Moura, S. (2017). Blockchains for decentralized optimization of energy resources in microgrid networks., 2164-2171. https://doi.org/10.1109/ccta.2017.8062773

[68] Oyeyemi, B. B. (2022). Artificial Intelligence in Agricultural Supply Chains: Lessons from the US for Nigeria.

[69] Oyeyemi, B. B., Akinlolu, M., and Awodola, M. I. (2025). Ethical challenges in AI-powered supply chains: A U.S.-Nigeria policy perspective. International Journal of Applied Research in Social Sciences, 7(5), 367–388.

[70] Oyeyemi, B. B., John, A. O., and Awodola, M. I. (2025, May 13). Infrastructure and regulatory barriers to AI supply chain systems in Nigeria vs. the U.S. Engineering Science and Technology, 6(4), 155–172.

[71] Park, U., Hong, J., Kim, A., and Son, K. (2023). Endpoint device risk-scoring algorithm proposal for zero trust. Electronics, 12(8), 1906. https://doi.org/10.3390/electronics12081906

[72] Paul, B. and Rao, M. (2022). Zero-trust model for smart manufacturing industry. Applied Sciences, 13(1), 221. https://doi.org/10.3390/app13010221

[73] Pop, C., Cioara, T., Antal, C., Anghel, I., Salomie, I., and Bertoncini, M. (2018). Blockchain based decentralized management of demand response programs in smart energy grids. Sensors, 18(1), 162. https://doi.org/10.3390/s18010162

[74] Powell, C., Hauck, K., Sanghvi, A., and Reynolds, T. (2020). Distributed energy resource cybersecurity framework best practices.. https://doi.org/10.2172/1598143

[75] Powell, C., Hauck, K., Sanghvi, A., Hasandka, A., Natta, J., and Reynolds, T. (2019). Guide to the distributed energy resources cybersecurity framework.. https://doi.org/10.2172/1581499

[76] Rahim, F., Ahmad, N., Magalingam, P., Jamil, N., Cob, Z., and Salahudin, L. (2023). Cybersecurity vulnerabilities in smart grids with solar photovoltaic: a threat modelling and risk assessment approach. International Journal of Sustainable Construction Engineering Technology, 14(3). https://doi.org/10.30880/ijscet.2023.14.03.018

[77] Rekeraho, A., Cotfas, D., Cotfas, P., Bălan, T., Tuyishime, E., and Acheampong, R. (2023). Cybersecurity challenges in iot-based smart renewable energy.. https://doi.org/10.21203/rs.3.rs-2840528/v1

[78] Rekeraho, A., Cotfas, D., Cotfas, P., Tuyishime, E., Bălan, T., and Acheampong, R. (2024). Enhancing security for iot-based smart renewable energy remote monitoring systems. Electronics, 13(4), 756. https://doi.org/10.3390/electronics13040756

[79] Sakhnini, J., Karimipour, H., Dehghantanha, A., Parizi, R., and Srivastava, G. (2021). Security aspects of internet of things aided smart grids: a bibliometric survey. Internet of Things, 14, 100111. https://doi.org/10.1016/j.iot.2019.100111

[80] Saleem, Y., Crespi, N., Rehmani, M., and Copeland, R. (2019). Internet of things-aided smart grid: technologies, architectures, applications, prototypes, and future research directions. Ieee Access, 7, 62962-63003. https://doi.org/10.1109/access.2019.2913984

[81] Sallam, A., Refaey, A., and Shami, A. (2019). On the security of sdn: a completed secure and scalable framework using the software-defined perimeter. Ieee Access, 7, 146577-146587. https://doi.org/10.1109/access.2019.2939780

[82] Salvaggio, S. and González, N. (2022). The european framework for cybersecurity: strong assets, intricate history. International Cybersecurity Law Review, 4(1), 137-146. https://doi.org/10.1365/s43439-022-00072-9

[83] Sani, A., Yuan, D., Lawal, Y., Loukas, G., and Dong, Z. (2024). A sustainable dispositional and situational security awareness model for smart grids., 135-140.

[84] Sen, Ö., Schmidtke, F., Carere, F., Santori, F., Ulbig, A., and Monti, A. (2022). Investigating the cybersecurity of smart grids based on cyber-physical twin approach.. https://doi.org/10.1109/smartgridcomm52983.2022.9961061

[85] Shaikh, A. (2024). Zero trust security paradigm: a comprehensive survey and research analysis. jes, 19(2), 28-37. https://doi.org/10.52783/jes.688

[86] Sharma, S., Sharma, T., Tiwari, A., and Gupta, S. (2024). Streamlining iot-driven data using blockchain. Int Res J Adv Engg Mgt, 2(05), 1509-1514. https://doi.org/10.47392/irjaem.2024.0204

[87] Sheikh, A., Kamuni, V., Urooj, A., Wagh, S., Singh, N., and Patel, D. (2020). Secured energy trading using byzantine-based blockchain consensus. Ieee Access, 8, 8554-8571. https://doi.org/10.1109/access.2019.2963325

[88] Sousa, T., Soares, T., Pinson, P., Moret, F., Baroche, T., and Sorin, E. (2019). Peer-to-peer and community-based markets: a comprehensive review. Renewable and Sustainable Energy Reviews, 104, 367-378. https://doi.org/10.1016/j.rser.2019.01.036

[89] Suciu, G., Istrate, C., Vulpe, A., Sachian, M., Vochin, M., Farao, A., … and Xenakis, C. (2019). Attribute-based access control for secure and resilient smart grids.. https://doi.org/10.14236/ewic/icscsr19.9

[90] Sultana, M., Hossain, A., Laila, F., Taher, K., and Islam, M. (2020). Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology. BMC Medical Informatics and Decision Making, 20(1). https://doi.org/10.1186/s12911-020-01275-y

[91] Sultana, T., Almogren, A., Akbar, M., Zuair, M., Ullah, I., and Javaid, N. (2020). Data sharing system integrating access control mechanism using blockchain-based smart contracts for iot devices. Applied Sciences, 10(2), 488. https://doi.org/10.3390/app10020488

[92] Szczepaniuk, H. and Szczepaniuk, E. (2022). Applications of artificial intelligence algorithms in the energy sector. Energies, 16(1), 347. https://doi.org/10.3390/en16010347

[93] Taik, A. (2021). Empowering prosumer communities in smart grid with wireless communications and federated edge learning.. https://doi.org/10.48550/arxiv.2104.03169

[94] Tanyıldız, H., Şahin, C., and DİNLER, Ö. (2024). Enhancing cybersecurity through gan-augmented and hybrid feature selection machine learning models: a case study on evse data. Naturengs Mtu Journal of Engineering and Natural Sciences Malatya Turgut Ozal University. https://doi.org/10.46572/naturengs.1495489

[95] Tushar, W., Saha, T., Yuen, C., Azim, M., Morstyn, T., Poor, H., … and Bean, R. (2020). A coalition formation game framework for peer-to-peer energy trading. Applied Energy, 261, 114436. https://doi.org/10.1016/j.apenergy.2019.114436

[96] Tushar, W., Yuen, C., Mohsenian-Rad, H., Saha, T., Poor, H., and Wood, K. (2018). Transforming energy networks via peer-to-peer energy trading: the potential of game-theoretic approaches. Ieee Signal Processing Magazine, 35(4), 90-111. https://doi.org/10.1109/msp.2018.2818327

[97] Tuyen, N., Quan, N., Linh, V., Vu, T., and Fujita, G. (2022). A comprehensive review of cybersecurity in inverter-based smart power system amid the boom of renewable energy. Ieee Access, 10, 35846-35875. https://doi.org/10.1109/access.2022.3163551

[98] Ukoba, K., Adeoba, M. I., Fatoba, S., and Jen, T. C. (2024). Blue Biomass Production for Renewable Energy. In Marine Bioprospecting for Sustainable Blue-bioeconomy (pp. 277-295). Cham: Springer Nature Switzerland.

[99] Ukoba, K., Adeoba, M., Fatoba, O. S., and Jen, T.-C. (2024). Marine bioprospecting for sustainable blue-bioeconomy: Blue biomass production for renewable energy. In Marine Bioprospecting for Sustainable Blue-bioeconomy (pp. 277–296). Springer.

[100] Uzondu, N. and Lele, D. (2024). Comprehensive analysis of integrating smart grids with renewable energy sources: technological advancements, economic impacts, and policy frameworks. Engineering Science and Technology Journal, 5(7), 2334-2363. https://doi.org/10.51594/estj.v5i7.1347

[101] Wallis, T., Paul, G., and Irvine, J. (2022). Organisational contexts of energy cybersecurity., 384-402. https://doi.org/10.1007/978-3-030-95484-0_22

[102] Wu, J., Ota, K., Dong, M., Li, J., and Wang, H. (2018). Big data analysis-based security situational awareness for smart grid. Ieee Transactions on Big Data, 4(3), 408-417. https://doi.org/10.1109/tbdata.2016.2616146

[103] Wylde, A. (2021). Zero trust: never trust, always verify., 1-4. https://doi.org/10.1109/cybersa52016.2021.9478244

[104] Yang, S., Hu, X., Wang, H., Li, H., Meng, L., Zhou, W., … and Zhou, H. (2022). A prosumer-based energy sharing mechanism of active distribution network considering household energy storage. Ieee Access, 10, 113839-113849. https://doi.org/10.1109/access.2022.3217540

[105] Yang, T., Zhu, L., and Peng, R. (2018). Fine-grained big data security method based on zero trust model., 1040-1045. https://doi.org/10.1109/padsw.2018.8644614

[106] Ye, Y., Qian, Y., Sharif, H., and Tipper, D. (2012). A survey on cyber security for smart grid communications. Ieee Communications Surveys and Tutorials, 14(4), 998-1010. https://doi.org/10.1109/surv.2012.010912.00035

[107] Zaman, D., and Mazinani, M. (2023). Cybersecurity in smart grids: protecting critical infrastructure from cyber attacks. SHIFRA, 2023, 86-94.