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)

Smart grid security: Safeguarding sustainable energy systems from cyber threats

Pedro Barros [1, *], Chijioke Paul Agupugo [2], Emmanuella Ejichukwu [3], Mario David Hayden [4] and Kehinde Adedapo Ogunmoye [5]

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

World Journal of Advanced Research and Reviews, 2025, 26(03), 1284-1301

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.2025.26.3.2233

Abstract

The rapid advancement and integration of smart grid technologies have revolutionized energy systems by enabling real-time monitoring, enhanced efficiency, decentralized energy generation, and renewable energy integration. However, this increased digitization and connectivity have simultaneously exposed critical infrastructures to a growing array of sophisticated cyber threats. As smart grids evolve into complex, data-driven ecosystems, ensuring their cybersecurity becomes paramount to achieving sustainable and resilient energy systems. This paper explores the intersection of cybersecurity and smart grid sustainability, identifying vulnerabilities in advanced metering infrastructure (AMI), supervisory control and data acquisition (SCADA) systems, distributed energy resources (DERs), and communication protocols. It discusses real-world incidents and simulated attack scenarios to highlight the potential consequences of cyber intrusions on grid stability, data integrity, and energy availability. A comprehensive framework for smart grid security is proposed, focusing on proactive risk management, threat detection through artificial intelligence (AI) and machine learning (ML), blockchain-enabled data validation, and zero-trust architecture models. The framework emphasizes the importance of stakeholder collaboration, regulatory compliance, and continuous system auditing to reinforce cybersecurity postures. Additionally, this study investigates the role of digital twins in simulating cyber-physical interactions and enabling predictive threat modeling for proactive resilience. Furthermore, the paper examines policy gaps, standardization issues, and workforce capacity constraints that hinder effective implementation of cybersecurity measures across diverse energy infrastructures. Strategies for integrating cybersecurity into the lifecycle of smart grid components from design to deployment are also discussed. By aligning technological innovation with robust cybersecurity governance, the paper aims to support the development of secure, adaptive, and sustainable smart energy systems capable of withstanding emerging cyber threats. The insights provided are intended to guide policymakers, grid operators, technology developers, and researchers in fortifying energy systems against cyber vulnerabilities while ensuring the continued advancement of clean and intelligent energy solutions. Ultimately, safeguarding smart grids is not merely a technical imperative but a foundational element for achieving long-term energy sustainability and national security in the digital era.

Keywords: Smart Grid Security; Cybersecurity; Sustainable Energy; Cyber Threats; Artificial Intelligence; Blockchain; Zero-Trust Architecture; Digital Twins; Renewable Energy Integration; Advanced Metering Infrastructure

[*] Corresponding author: Pedro Barros

1. Introduction

Smart grids symbolize a pivotal transformation in energy infrastructure by transitioning traditional electrical grids into intelligent, interconnected systems that facilitate real-time communication, automation, and adaptive energy distribution. These advanced systems integrate various technologies including Advanced Metering Infrastructure (AMI), which enables two-way communication between utilities and consumers for enhanced energy management and operational efficiency (Tweneboah-Koduah et al., 2017; Ghosal and Conti, 2019). The implementation of smart grids is designed to improve energy efficiency, lower carbon emissions, and aid in the widespread adoption of renewable energy sources. This adaptation is crucial as the growing involvement of distributed generation and storage resources necessitates sophisticated metering systems capable of effectively managing energy flows (Adelana, et al., 2024; Uribe-Pérez et al., 2016). Consequently, smart grids enable dynamic interactions among consumers, producers, and utility providers, thus playing an essential role in advancing sustainability within energy sectors (Amini et al., 2023), Nik et al., 2020).

However, the digitalization that underlies smart grid operations introduces critical vulnerabilities. The reliance on interconnected devices and communication networks amplifies the potential for cyber threats, exposing these infrastructures to malicious attacks that can disrupt energy supply, compromise sensitive consumer data, and lead to economic and societal consequences (Ye et al., 2013). Key components such as supervisory control and data acquisition (SCADA) systems, AMI, and distributed energy resources are particularly susceptible to cyberattacks, posing significant risks to grid stability and national security (Govea et al., 2024). Consequently, cybersecurity must be viewed not merely as an auxiliary consideration but as a foundational element for ensuring the resilience and sustainability of smart grids (Amini et al., 2023).

This convergence of cybersecurity and smart grid sustainability necessitates a detailed examination of vulnerabilities, analysis of emerging threats, and exploration of protective strategies. Emerging technologies such as artificial intelligence for threat detection, blockchain for securing data transactions, and zero-trust security architectures are being evaluated for their applicability in bolstering smart grid defenses (Adeoba and Fatayo, 2024; Govea et al., 2024). Furthermore, a comprehensive approach that includes addressing policy gaps, regulatory challenges, and organizational barriers is essential for the effective implementation of cybersecurity measures in energy systems (Sarma and Zabaniotou, 2021). By providing a holistic perspective that encompasses technical, policy, and operational aspects of smart grid security, ongoing research contributes significantly to developing secure and adaptive energy infrastructures capable of withstanding evolving cyber threats.

2. Methodology

The methodology employed integrates a combination of systematic literature review, analytical modeling, and conceptual synthesis. By leveraging recent peer-reviewed studies on cybersecurity in smart grids, a multi-layered approach is adopted to evaluate, model, and enhance the security resilience of smart energy systems. Data were gathered from sources discussing the intersection of artificial intelligence, blockchain technology, digital twins, machine learning algorithms, and intrusion detection systems (IDS), particularly within cyber-physical environments. Drawing from studies such as those by Ahn et al. (2024) on cyber-resilient smart inverters, Alam et al. (2024) on machine learning-based cyber-attack mitigation, and Alkhiari et al. (2022) on blockchain-enhanced smart grid networks, the methodology focused on establishing a robust end-to-end framework.

The process commenced with the identification of common vulnerabilities in smart grid communication and control systems. From there, AI-based detection mechanisms were modeled based on data from both historical threat signatures and predictive anomaly detection algorithms. Next, blockchain technologies were incorporated to ensure secure, decentralized authentication and data transmission across the grid. This model was further enhanced with edge computing capabilities to reduce latency in threat response and digital twins to simulate attack scenarios and refine defensive protocols.

Expert-guided threat simulations and policy alignment were used to identify gaps between system readiness and existing international standards such as NIST and IEC. Feedback mechanisms were incorporated using reinforcement learning to continuously update system defenses in response to newly emerging threats. The result is a cyclical, adaptive security architecture that protects smart grid assets while enabling operational continuity and regulatory compliance.

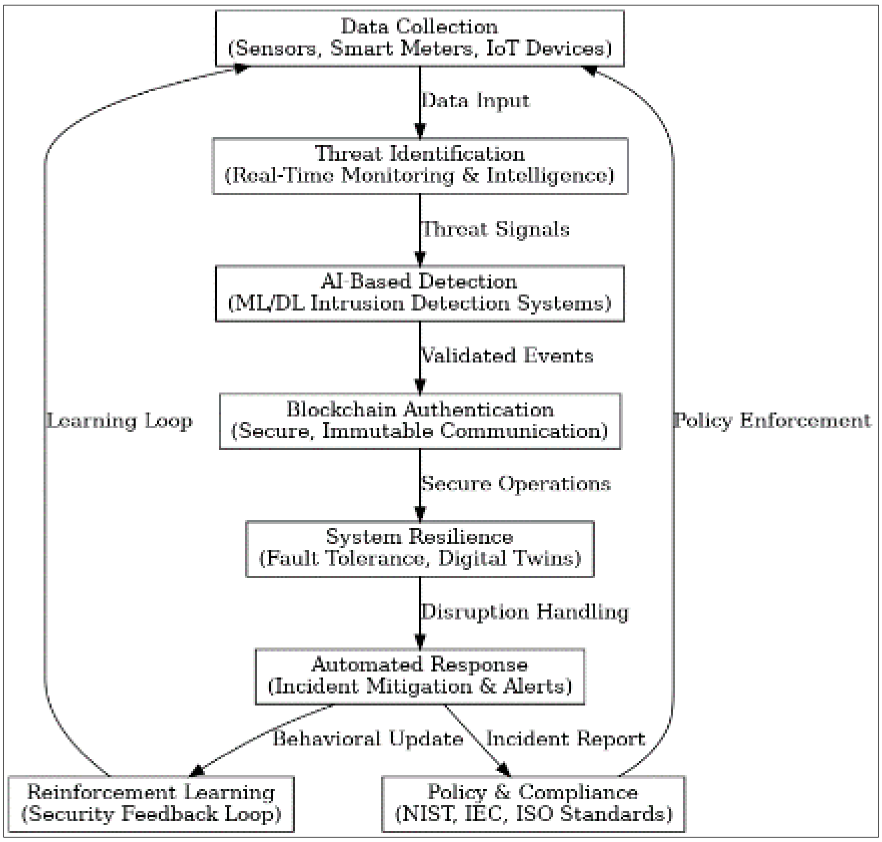

Figure 1 The flowchart for the Study Methodology

3. Smart Grid Architecture and Components

Smart grid systems represent a transformative evolution in energy infrastructure, crucial to advancing sustainable, efficient, and resilient energy solutions. These technologically advanced electric power systems leverage digital communication technologies, automation, and real-time data analytics, fundamentally enhancing how electricity is generated, distributed, and consumed. Unlike traditional grids, which are predominantly centralized and one-directional, smart grids support a bidirectional flow of electricity and data, allowing both utilities and consumers to respond adaptively to real-time conditions (Adeoba, et al., 2025; Kumar et al., 2019). This structural shift not only boosts operational efficiency and grid reliability but also facilitates the integration of renewable energy sources, contributing significantly to greenhouse gas emission reduction and the achievement of energy sustainability goals (Luo et al., 2022; Qureshi et al., 2021).

A critical component of the smart grid architecture is the Advanced Metering Infrastructure (AMI), which serves as the essential interface between utility companies and consumers. AMI systems encompass smart meters, communication networks, and data management platforms that facilitate real-time monitoring and analysis of energy usage. These smart meters provide detailed consumption data, enhancing billing accuracy, enabling demand response initiatives, and improving fault detection capabilities (Barbierato et al., 2019; Kuang et al., 2024). However, this enhanced connectivity brings the challenge of increased vulnerability to cyber threats, particularly when these systems lack adequate encryption or secure communication protocols, potentially leading to energy theft, privacy breaches, and even manipulation of grid operations (Qureshi et al., 2021; Xu et al., 2023). Figure 2 shows The architecture of the smart grid presented by Diaba, Shafie-khah and Elmusrati, 2024.

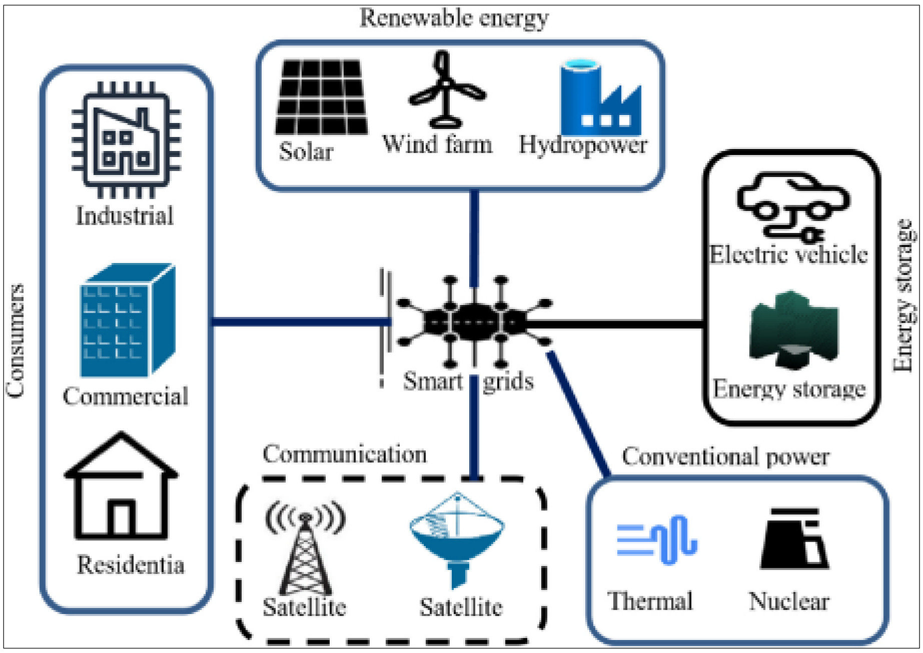

Figure 2 The architecture of the smart grid (Diaba, Shafie-khah and Elmusrati, 2024)

Additionally, the Supervisory Control and Data Acquisition (SCADA) system acts as the operational nerve center within smart grids, allowing comprehensive monitoring and control of grid assets such as substations and transformers. SCADA systems collect critical data via remote sensors and issue commands to field devices across vast geographical areas. Yet, as these systems evolve to integrate more extensively with IT infrastructures and internet-based communication, their susceptibility to cyberattacks also increases. A successful intrusion can result in significant service disruptions, equipment damage, or widespread blackouts, underscoring the urgency of enhancing SCADA cybersecurity measures (Suman et al., 2020; Vakulenko et al., 2021).

The integration of Distributed Energy Resources (DERs), including solar panels, wind turbines, and electric vehicles, adds complexity to smart grid systems due to the decentralized nature of these resources. While DERs contribute to grid resilience and allow for flexible energy consumption patterns, they also present unique cybersecurity challenges. Each access point to the grid can be a potential vulnerability, with attacks on DERs capable of leading to destabilization of the grid if not adequately secured (Hou et al., 2024; Luo et al., 2022; Lyulyov et al., 2021).

Effective communication networks and protocols are foundational to the functionality of smart grids, fostering seamless interactions between devices, control systems, and end users. These networks must handle substantial data flows across various grid layers and can utilize numerous types of communication technologies, including fiber optics, power line communications, and cellular networks. However, many of the communication protocols utilized, such as DNP3 and IEC 61850, were not originally designed with cybersecurity in mind. This oversight exposes the system to risks such as protocol spoofing, unauthorized command injection, and data interception (DEVI, 2022; Sani et al., 2024). Ensuring secure communication is crucial for maintaining the integrity and confidentiality of smart grid operations ("December 2019", 2019). General conceptual model of the smart grid presented by Kim, Hakak and Ghorbani, 2023 is shown in figure 3.

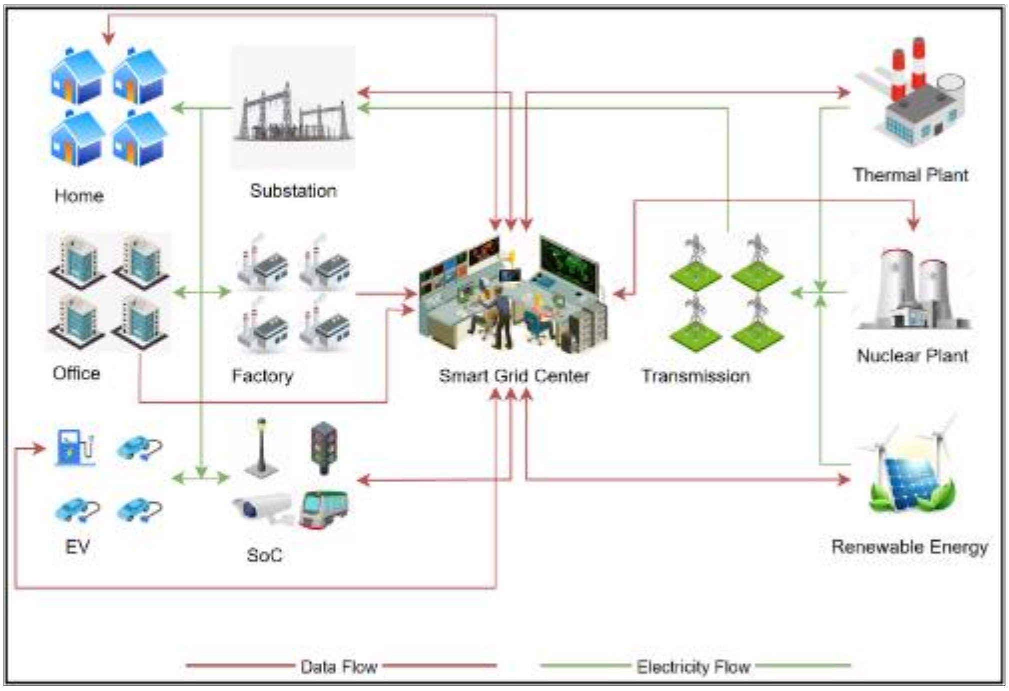

Figure 3 General conceptual model of the smart grid (Kim, Hakak and Ghorbani, 2023)

The dense interconnectivity of smart grid components means that a breach in one element can lead to widespread systemic failures. For instance, a compromised smart meter could serve as a gateway for larger breaches, affecting both SCADA operations and DER controls. Consequently, a comprehensive cybersecurity strategy is essential to protect the entire smart grid ecosystem covering everything from edge devices through to central management systems (Li et al., 2023; Alkhiari et al., 2022). This requires robust identity management, advanced intrusion detection systems, and continuous real-time monitoring to avert potential security threats (Borgaonkar et al., 2021; Zou et al., 2020).

Moreover, the convergence of Information Technology (IT) and Operational Technology (OT) within smart grids has obscured historic security boundaries. IT emphasizes data integrity, while OT focuses on real-time operational performance. Bridging these priorities necessitates a unified security framework that accommodates both operational requirements and rigorous cybersecurity practices (Jin et al., 2018). The human element also plays a critical role; vulnerabilities can be introduced through inadequate password management, social engineering, or misconfigurations, underscoring the need for ongoing security awareness training and the implementation of a zero-trust security model (Adeoba, et al., 2025; Zhu, 2018).

In summary, the architecture of smart grids embodies complex interrelations of digital technologies, decentralized resources, and intricate communication systems that enhance efficiency but also broaden the landscape of cybersecurity threats. Core components such as AMI, SCADA, DERs, and advanced communication protocols are vital for grid performance yet are equally vulnerable if security measures are not diligently applied. Protecting these components and their interconnected data flows is essential for sustaining the reliability and security of future energy systems, necessitating an integrated focus on robust cybersecurity practices across the smart grid landscape.

4. Emerging Cyber Threat Landscape

The evolving nature of smart grids, characterized by the convergence of operational technologies (OT) and information technologies (IT), has significantly altered the energy landscape while also introducing complex cybersecurity challenges. The integration of digital systems enhances grid efficiency, flexibility, and sustainability, but this interconnected architecture also increases vulnerability to various cyber threats. Cybercriminals, nation-state actors, hacktivist groups, and insider threats exploit the extensive attack surface created by advanced metering infrastructure, supervisory control and data acquisition (SCADA) systems, distributed energy resources, and diverse communication protocols (Gopstein et al., 2021; (Ding et al., 2022). Thus, understanding the classification of these threats is essential for developing effective defenses against potential exploits.

Among the prevalent types of cyber threats encountered within smart grids, malware, including ransomware and phishing attacks, poses significant risks. Malware is typically introduced through vectors such as infected emails, compromised software updates, or unsecured devices connected to the network, aiming to disrupt operations or gain unauthorized access (Nejabatkhah et al., 2020)(Bouramdane, 2023). Ransomware can encrypt critical data and systems, jeopardizing operational integrity for utility companies and potentially leading to systemic instability affecting numerous consumers (Adeoba, et al., 2024; Ding et al., 2022). Phishing attacks often serve as entry points for these malicious software threats, exploiting human vulnerabilities due to inadequate cybersecurity awareness training among personnel (Adeoba, Ukoba and Osaye, 2024; Rahim et al., 2023).

Equally concerning are Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks, which flood systems with excessive traffic, effectively paralyzing communication networks essential for grid operations. Such attacks can delay data collection and disrupt controls between different components of the smart grid, potentially resulting in cascading failures (Ding et al., 2022). Man-in-the-Middle (MitM) attacks represent another covert and damaging cyber threat; by intercepting communications between devices, such attacks can manipulate data streams, generate false meter readings, or modify control signals (Nejabatkhah et al., 2020). The proliferation of unsecured communication protocols can exacerbate the impact of these attacks, necessitating robust encryption and authentication measures (Nejabatkhah et al., 2020; Bouramdane, 2023). Chinnasamy, et al., 2024 presented Smart grid-based CPS structure shown in figure 4.

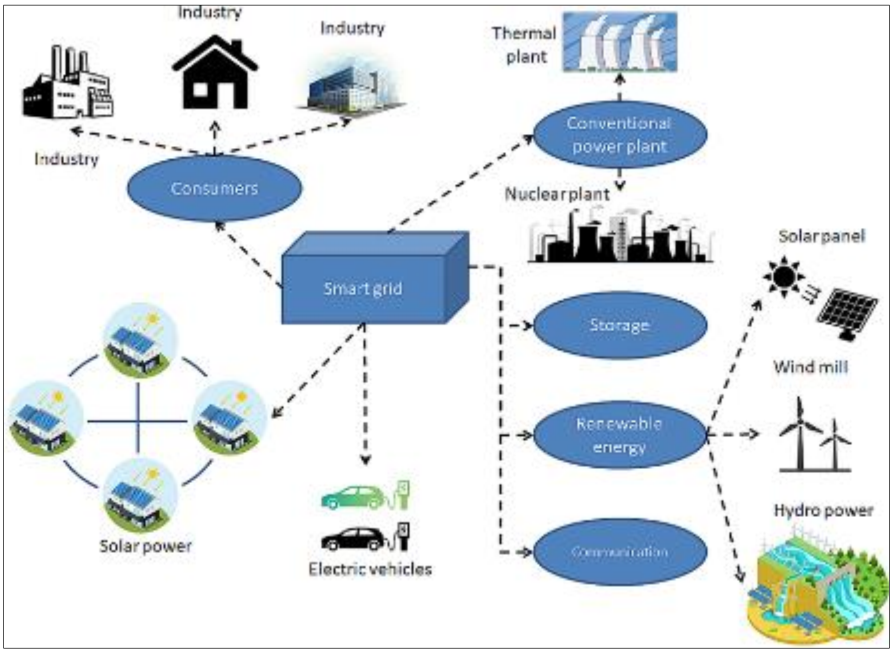

Figure 4 Smart grid-based CPS structure (Chinnasamy, et al., 2024)

Data breaches and insider threats are especially concerning within the context of smart grids due to the sensitive nature of the data involved. Unauthorized access to energy usage data, customer identities, and operational configurations presents significant risks, providing attackers with the intelligence needed to execute more severe attacks (Nejabatkhah et al., 2020). Insider threats, whether malicious or inadvertent, complicate the security landscape, as employees with legitimate access can exploit their privileges for nefarious purposes, which is challenging to monitor and mitigate using standard cybersecurity frameworks (Bouramdane, 2023).

Real-world incidents underscore the tangible risks associated with these cyber threats. The 2015 cyberattack in Ukraine, which disabled power for over 230,000 residents, serves as a stark example of cybercriminals employing phishing techniques alongside malware to infiltrate critical infrastructure (Saxena, 2024). Similarly, a 2020 attack against the U.S. Department of Energy demonstrated vulnerabilities in software supply chains a key concern for smart grid security as interconnected systems become more common (Bouramdane, 2023). Another case in the United States involved a cyber breach in 2019 that revealed vulnerabilities in substation automation communication protocols, raising alarms about the susceptibility of grid communications to peripheral threats (Adeoba, Shandu and Pandelani, 2025: Nejabatkhah et al., 2020).

As smart grids expand in complexity and scope, the potential for adverse impacts from cyberattacks increases. This necessitates a multi-layered approach to cybersecurity that involves technical solutions like intrusion detection systems, network segmentation, and robust encryption, coupled with organizational strategies, including rigorous training, heightened cybersecurity awareness, and strict access controls (Bouramdane, 2023). Furthermore, evolving regulatory frameworks to establish minimum cybersecurity standards while facilitating information sharing among stakeholders is crucial for safeguarding energy infrastructures (Nejabatkhah et al., 2020).

In conclusion, the convergence of operational and information technologies within smart grids has given rise to numerous cyber threats. Traditional malware, sophisticated DoS and DDoS attacks, and the intricacies of insider threats underscore the necessity for a comprehensive understanding and proactive defense against cyber threats that can have real-world implications on energy systems. As the cybersecurity landscape evolves in tandem with technological advancements in the energy sector, the development of adaptive strategies will be imperative to ensure the resilience and reliability of sustainable energy systems.

5. Vulnerability Assessment

Vulnerability assessment in the context of smart grid security is crucial, as it involves identifying, analyzing, and mitigating potential entry points that adversaries could exploit to compromise the integrity, availability, or confidentiality of energy systems. The rapid evolution of smart grid systems, which integrate traditional energy infrastructure with advanced digital technologies, has significantly expanded the landscape of potential vulnerabilities. This integration results in risks arising from various sources, including hardware and software components, network configurations, operational procedures, and human factors. To effectively safeguard these sustainable energy systems, understanding the full spectrum of attack surfaces and the limitations of legacy systems is vital (Rahim et al., 2023; Banik and Banik, 2024; Marron et al., 2019).

The interconnected and distributed nature of smart grid components introduces numerous attack surfaces. Critical components such as Advanced Metering Infrastructure (AMI), Supervisory Control and Data Acquisition (SCADA) systems, and Distributed Energy Resources (DERs) are particularly at risk due to their reliance on interconnectivity. For instance, AMI systems, including smart meters, often reside at the network's edge and typically lack robust security features, making them susceptible to exploitation. Attackers may exploit weaknesses such as insufficient encryption or default credentials, potentially leading to data manipulation or broader network intrusions (Rashed et al., 2022; Leszczyna, 2019; (Alonso et al., 2021; . SCADA systems serve as the operational nerve centers for grid management and control, originally designed for isolated environments, leaving them vulnerable when exposed to less secure infrastructures. Common communication protocols used across these systems, like Modbus and DNP3, have security limitations in modern cyber environments, increasing their risk exposure (Sadi et al., 2015; Banik et al., 2023).

The advent of Distributed Energy Resources also introduces additional vulnerabilities, as these systems are typically monitored and managed through internet-connected controllers. If compromised, DERs can be manipulated to inject or withdraw power unsafely, thereby destabilizing the grid (Adeoba, Odjegba and Pandelani, 2025: Bouramdane, 2023). Furthermore, legacy systems still prevalent in many utilities pose significant challenges. These systems often lack modern security mechanisms and may not interface effectively with newer technologies, thus creating vulnerabilities during their integration into the smart grid. This coexistence can lead to oversight and misconfiguration, which attackers may exploit (Alonso et al., 2021; Ye et al., 2013).

To combat these vulnerabilities, systematic risk assessment methodologies and tools are essential. Frameworks such as the NIST Cybersecurity Framework and the NERC Critical Infrastructure Protection (CIP) standards provide structured approaches for evaluating and enhancing cybersecurity in the smart grid context. The NIST Risk Management Framework (RMF) is particularly valuable, guiding the categorization of information systems and the selection and implementation of appropriate security controls while ensuring continuous monitoring (Borenius et al., 2022; Mohammed et al., 2024). Additionally, methodologies like Failure Mode and Effects Analysis (FMEA) and attack tree analysis can be utilized to identify critical system components and visualize potential attack routes, thereby enhancing overall security posture (Banik et al., 2023).

Furthermore, advanced security tools, including vulnerability scanners and intrusion detection systems (IDS), are indispensable for maintaining the integrity of the smart grid. Regularly using these tools allows utilities to identify and address weaknesses proactively, mitigating risks before they can be exploited. The inclusion of machine learning and artificial intelligence into vulnerability assessment processes enhances threat detection capabilities by analyzing large amounts of data to identify unusual patterns that may signify an impending attack, facilitating a shift toward proactive security measures ("December 2019", 2019; Khan et al., 2020; Pan et al., 2017).

Finally, effective vulnerability assessment also hinges on fostering an organizational culture that prioritizes cybersecurity. Utilities must establish training, clear incident response policies, and collaborate with national cybersecurity entities and industry groups to build a robust threat intelligence framework. As the cyber threat landscape continues to evolve, continuous assessment and adaptation of security strategies are critical to ensuring that smart grids remain secure and resilient against emerging threats (Tanyıldız et al., 2024; He and Yan, 2016).

In conclusion, vulnerability assessment within the smart grid is an ongoing and multidimensional process that is vital for effective cybersecurity. The unique characteristics of smart grids, including their digital components and the integration of legacy and modern technologies, create a complex and dynamic environment susceptible to various cyber threats. Utilizing structured methodologies, advanced tools, and collaborative governance is essential in addressing these vulnerabilities to secure the reliability and integrity of modern energy infrastructures.

6. Cybersecurity Strategies and Technologies

The issue of cybersecurity in smart grid systems has become increasingly critical due to the complexities associated with their interconnectedness, automation, and reliance on real-time digital communication. As smart grids evolve, they face a landscape of potential cyber threats that could disrupt energy supplies, compromise sensitive data, and undermine public trust. Therefore, the implementation of comprehensive cybersecurity strategies and technologies is essential for ensuring reliability, safety, and sustainability in modern energy infrastructures.

A proactive approach to risk management and threat modeling is foundational for effective cybersecurity within smart grid environments. Such strategies underscore the importance of anticipating vulnerabilities and planning preventative measures rather than merely responding to incidents post facto. Identifying critical assets, such as SCADA systems, distributed energy resources (DERs), smart meters, and communication networks, is crucial in this regard. Proactive frameworks, such as the MITRE ATTandCK for Industrial Control Systems and the National Institute of Standards and Technology (NIST) Cybersecurity Framework, offer systematic methodologies for evaluating exposure to cyber risks and designing multi-layered defense mechanisms (Marron et al., 2019; Zheng et al., 2022).

In recent years, there has been a significant integration of Artificial Intelligence (AI) and Machine Learning (ML) technologies to bolster intrusion detection and cybersecurity monitoring within smart grids. These technologies leverage vast datasets to identify anomalies indicative of cyber-attacks, providing the ability to learn from past operational behaviors to establish baselines for normal activity. The adaptability of AI and ML systems allows them to detect emerging threat vectors, offering a substantial advancement over traditional rule-based detection methods, which typically lag behind the pace of evolving threats (Alam et al., 2024; Saxena, 2024; Ding et al., 2022). By utilizing historical data and real-time inputs, AI can alert operators to deviations that may signify malicious activity, making these technologies invaluable to smart grid security frameworks (Sadik et al., 2020; DEVI, 2022).

In addition to AI and ML, blockchain technology presents innovative opportunities for securing smart grid operations. Its decentralized ledger system guarantees data integrity and provides tamper-proof transaction capabilities, essential for maintaining trust among various stakeholders utilities, consumers, and DER operators engaged in energy exchanges. Blockchain specifically enhances the security of peer-to-peer energy trading platforms by authenticating transactions and implementing smart contracts that automate processes without intermediary involvement Coppolino et al., 2023; Bouramdane, 2023). Its utility in tracking the lifecycle of critical components also contributes to supply chain security, mitigating risks from compromised hardware (Apata, et al., 2024; Basharat and Huma, 2024).

The implementation of zero-trust architectures and micro-segmentation further fortifies smart grid defenses against cyber incursions. Zero-trust principles eliminate the presumption of trust within network perimeters, mandating continuous verification of user identities and device statuses prior to granting access. This approach dramatically limits lateral movement within the network, reducing the potential impact of insider threats or compromised credentials (Le et al., 2022). Micro-segmentation divides networks into isolated zones with individualized security controls, ensuring that breaches in one area such as a smart meter cluster do not automatically enable access to higher-level systems (Pirta-Dreimane et al., 2024; Kumari et al., 2023).

Furthermore, digital twins serve as a frontier in enhancing smart grid cybersecurity by providing real-time, virtual simulations of physical assets. They allow for predictive analyses and resilience planning, enabling operators to model potential attack scenarios and assess the implications of different threat vectors. This capability is vital for developing robust incident response strategies, akin to testing in a controlled environment before implementing changes in the actual infrastructure (Ding et al., 2022; Ghadi et al., 2024; Annor-Asante and Pranggono, 2018). By simulating potential cyberattacks on operational assets, utilities can optimize their defenses and recovery plans proactively, thereby reducing vulnerabilities (Mansour et al., 2023; Habib et al., 2023).

In summary, addressing the cybersecurity challenges of smart grids necessitates a sophisticated blend of advanced technologies and strategic foresight. The integration of proactive risk management, AI and ML-driven monitoring, blockchain for transaction integrity, zero-trust architectures, and digital twin simulations collectively contributes to a resilient cybersecurity posture. For these strategies to be effective, they should be part of a broader governance framework that promotes continuous improvement, collaboration across sectors, and workforce development (Zheng et al., 2022; Coppolino et al., 2023; Sadik et al., 2020). Studying and adapting to technological advancements and an evolving threat landscape remains paramount for the sustainability and security of energy infrastructures.

7. Regulatory and Policy Considerations

As the integration of renewable energy systems becomes increasingly digital and decentralized, the urgency for a proficient workforce that can safeguard the energy grid from cyber threats has intensified. The resilience and security of energy infrastructures rely on the preparedness of personnel responsible for designing, managing, operating, and securing these systems (Ekechukwu and Simpa, 2024; Peralta et al., 2021). Developing workforce capacity is an essential aspect of a comprehensive cybersecurity strategy aimed at grid protection (Ayanwale, et al., 2024; Kour and Karim, 2020). This involves substantial investments in training energy professionals, promoting cross-disciplinary collaboration, and enhancing both academic and industry initiatives to create a robust talent pool (Almoughem, 2023; Chidolue et al., 2024; Ekechukwu and Simpa, 2024).

The unique challenges presented by the convergence of Information Technology (IT) and Operational Technology (OT) in today's energy systems necessitate targeted cybersecurity training for energy professionals (Keyser and Tegen, 2019; Almutairy et al., 2021). These professionals must cultivate both technical knowledge related to renewable technologies such as solar, wind, and battery storage and an understanding of digital tools that facilitate real-time system monitoring, automation, remote access, and analytics (Chidolue et al., 2024; Ekechukwu and Simpa, 2024). Traditional training methodologies often prioritize engineering and policy-focused curricula while frequently neglecting essential cybersecurity aspects (Tuyen et al., 2022; . Consequently, there is a growing need for energy practitioners to enhance their capabilities to identify cyber risks, respond to threats, and establish effective security controls within their operational frameworks (Dawson and Thomson, 2018). Therefore, it is crucial that ongoing cybersecurity education and training become a staple in the professional development landscape of the energy sector (Cali et al., 2021; John and Oyeyemi, 2022).

The development of cross-disciplinary teams is vital for building a robust cybersecurity capacity in renewable energy systems, especially where IT and OT intersect (Mohamed et al., 2023). Successful integration of security protocols in renewable energy systems requires collaboration among engineers, cybersecurity professionals, and IT experts to ensure that system functionalities are not only maintained but also strengthened against potential cyber threats (Mengidis et al., 2019; Peralta et al., 2021). Coordination among system architects, software developers, and network engineers is crucial to prevent vulnerabilities from being embedded in the systems designed for critical infrastructure management (Ahn et al., 2024; Ekechukwu and Simpa, 2024). Fostering a collaborative culture that bridges departmental divides necessitates effective communication and mutual respect for various roles within an organization, addressing cybersecurity protocols adequately Pollini et al., 2021).

Long-term workforce development can be achieved by strengthening the talent pipeline through initiatives led by academic institutions and industries. Universities must adapt their curricula to align with the realities of contemporary digital energy landscapes, incorporating courses focused on cybersecurity, data science, and system engineering related to renewable energy Perälä and Lehto, 2024)Boza and Evgeniou, 2021). Additionally, industry partnerships can provide students with invaluable experiences through internships and apprenticeships, enabling them to navigate real-world challenges associated with grid operations and cybersecurity (Chidolue et al., 2024; Perälä and Lehto, 2024). Furthermore, establishing mentorship programs will connect budding professionals with seasoned experts to discuss career trajectories and emerging trends in cybersecurity (Constant et al., 2021; Oyeyemi, 2022).

Industry-led initiatives are pivotal in enhancing continuous workforce development and upskilling existing professionals (Almoughem, 2023). Government initiatives, professional associations, and nonprofit organizations are championing programs emphasizing robust cybersecurity education focused on critical infrastructure protection (Chidolue et al., 2024; Peralta et al., 2021). The U.S. Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) provides substantial support for such training initiatives, targeting essential workforce improvements (Parrish et al., 2018; Kour and Karim, 2020). Additionally, vendor-led training programs and online education platforms offer flexible learning opportunities, empowering a broader demographic to acquire essential cybersecurity competencies at their own pace (Dawson and Thomson, 2018; Pollini et al., 2021). Promoting diversity and inclusion within the cybersecurity workforce is critical, addressing the shortage of qualified professionals while introducing varied perspectives that can enhance problem-solving capabilities (Tuyen et al., 2022; (Almoughem, 2023). Scholarship programs and inclusive hiring practices are essential for ensuring access to cybersecurity careers for underrepresented groups (Almoughem, 2023; Oyeyemi, Akinlolu and Awodola, 2025).

In summary, addressing the cybersecurity demands of renewable energy systems necessitates a comprehensive workforce development and capacity-building approach. Energy professionals must be equipped with the skills to navigate emerging cyber threats actively. Collaboration across disciplines should be fostered to secure all facets of energy system operations. Ongoing academic and industry efforts should aim to develop a diverse, skilled, and forward-looking talent pool. Ultimately, investing in human resources which encompass education, training, collaboration, and inclusiveness represents a strategic imperative for energy organizations aiming to ensure a resilient, secure, and sustainable energy future.

8. Implementation Challenges

Implementing robust cybersecurity for smart grids is crucial as these infrastructures evolve into interconnected, data-driven networks essential for sustainable energy systems. The transition from traditional centralized grids to smart grids introduces a multitude of complex challenges associated with cybersecurity, requiring both technical and strategic solutions. The multi-dimensional nature of these challenges encompasses issues related to interoperability, scalability, latency, organizational dynamics, and economic constraints.

From a technical standpoint, one of the core challenges faced during smart grid security implementation is achieving interoperability across diverse components and systems. Smart grids consist of numerous devices from legacy infrastructure to advanced metering systems each produced by different manufacturers and often utilizing varying communication protocols. This diversity complicates the establishment of consistent and robust security measures, as misconfigurations and incompatible standards may lead to significant security vulnerabilities (Fang et al., 2012; , (Rawat and Bajracharya, 2015; . Critically, many existing communication protocols, such as Modbus and DNP3, were not originally designed with cybersecurity in mind, necessitating complex retrofitting efforts to integrate security features effectively (Rawat and Bajracharya, 2015; Rohokale and Prasad, 2016; . This underscores the need for a harmonized approach to develop interoperable security protocols that address the unique risks posed by smart grid environments.

In addition to interoperability concerns, scalability remains a pressing technical obstacle. As smart grids encompass an increasing number of interconnected devices, the demand for security solutions capable of managing vast volumes of data while ensuring real-time performance intensifies. Approaches to cybersecurity must efficiently scale to cover intrusion detection systems, identity management, and encryption mechanisms, as existing solutions may falter under heightened demands (Wu et al., 2018; Khan et al., 2020). The challenge is particularly critical in contexts where latency cannot be compromised, such as in SCADA systems, where delays could directly impact grid performance (Lei et al., 2016; Oyeyemi, Akinlolu and Awodola, 2025).

Organizational challenges further exacerbate the difficulty of implementing effective cybersecurity measures within smart grids. A notable barrier is the shortage of personnel proficient in both cybersecurity and power systems, resulting in under-resourced security teams that struggle with incident response and system maintenance (Sajjadi and Niknia, 2013). Moreover, there exists a prevalent deficiency in cybersecurity awareness among stakeholders at various levels of the organization, which often leads to the perception of cybersecurity as a secondary concern rather than a strategic priority. This cultural challenge can result in inadequate training, underinvestment, and delays in crucial upgrades or maintenance (Wang et al., 2019). Resistance to change is a common phenomenon in organizations reliant on legacy systems, which may prevent the timely adoption of modern cybersecurity practices. Such inertia is often fueled by regulatory uncertainties and fears of operational disruption Ukoba, et al., 2024; Ye et al., 2012).

Economic realities play a significant role in shaping the implementation strategies for smart grid cybersecurity. The need for justifiable investments in cybersecurity is complicated by the fact that the benefits are primarily preventative and often not immediately apparent. Utilities face challenges in aligning cybersecurity expenses with their budget constraints and often must weigh the costs of potential cyber incidents against the necessary investments for preventive measures (Lu et al., 2012; Liang et al., 2013). Additionally, the lack of comprehensive actuarial data related to cyber risk in energy infrastructures may lead organizations to underestimate actual vulnerabilities, further compounding the hesitance to invest in robust cybersecurity frameworks (Rohokale and Prasad, 2016; Jin et al., 2018).

Ultimately, while the challenges surrounding the implementation of robust cybersecurity for smart grids are multi-faceted and complex, it is essential to recognize that the costs associated with inaction can significantly outweigh the investment required for proactive security measures. Cyberattacks on smart grids risk not only service disruptions but also potential harm to public safety and national security (Koch et al., 2011; Vasilomanolakis et al., 2013). Thus, cybersecurity must be perceived as a foundational element that undergirds the reliability and sustainability of future energy infrastructures.

In conclusion, addressing the multifaceted challenges of cybersecurity in smart grids necessitates a comprehensive approach that harmonizes technical solutions with organizational and economic considerations. Stakeholders must prioritize the development of interoperable, scalable systems and invest in workforce training and cultural shifts within organizations. By recognizing cybersecurity as a strategic asset rather than an expense, stakeholders can harness the full potential of secure smart grid systems to adapt to the evolving cyber threat landscape.

9. Future Directions and Research Opportunities

The transformation of modern energy systems into smart grids has instigated a significant evolution in electricity distribution and consumption, aligned with digital transformation and decentralization. The enhanced functionalities of smart grids not only improve operational efficiency but also expose these systems to sophisticated cybersecurity threats. As identified by Borgaonkar et al., the integration of IoT and edge computing in smart grids presents critical security challenges that necessitate a re-examination of current cyber defense mechanisms to effectively adapt to these advancements (Borgaonkar et al., 2021). The priority for securing smart grids involves continuous enhancements in risk management strategies to address the rapidly evolving threat landscape (Suman et al., 2017; Ukoba, et al., 2024).

The future of smart grid security emphasizes the significance of predictive threat intelligence. Traditional cybersecurity models predominantly operate on reactive frameworks, which may not suffice given the critical nature of energy infrastructure (Wu et al., 2018). According to Wu et al., leveraging big data analytics and machine learning can significantly enhance the ability to predict and respond to emergent threats (Wu et al., 2018). Machine learning algorithms can analyze patterns in network traffic and operational behaviors, thereby facilitating early detection of potential intrusions before they escalate into severe incidents (Al-Shaer and Rahman, 2016). Consequently, predictive modeling can further enhance the development of digital twins simulated environments that enable rigorous testing of security protocols without compromising operational systems (Vempati, 2024).

Furthermore, creating systems that integrate threat intelligence from a variety of sources is paramount for building a comprehensive defense framework. By amalgamating insights from international cybersecurity databases, national CERTs, and industrial platforms, the effective aggregation of threat data supports a proactive security posture. This comprehensive view allows stakeholders within the energy ecosystem to unearth shared vulnerabilities and correlations of attack vectors (DEVI, 2022). This highlights the need for interdisciplinary cooperation among academia, industry, and governmental bodies (Radoglou-Grammatikis and Sarigiannidis, 2019).

The pressing demands for robust smart grid cybersecurity also necessitate an early-stage integration of security measures during the design and development phases. As argued by Devi, treating cybersecurity as an integral aspect rather than an afterthought reduces the risks of deploying insecure infrastructures (DEVI, 2022). Implementing "security-by-design" practices positions each layer of the smart grid with security considerations from the inception of the architecture. This proactive model has been identified as a fundamental shift necessary to ensure long-term security and resiliency in smart grid operations (Ekechukwu and Simpa, 2024).

Investment in education and collaboration across various sectors is equally essential in shaping the future of smart grid cybersecurity. Developing specialized training programs that encompass technical, operational, and regulatory knowledge is critical in forming a competent workforce equipped to handle contemporary challenges (Mohamed et al., 2023). The incorporation of multidisciplinary research involving energy systems, cybersecurity, behavioral science, and regulatory law is expected to yield comprehensive strategies that effectively transcend technical limitations, aligning with contemporary smart grid innovation and resilience (Ekechukwu and Simpa, 2024).

In conclusion, the evolving landscape of smart grids presents both significant challenges and opportunities in cybersecurity. A focused approach on predictive capabilities, interdisciplinary cooperation, and early integration of security measures will pave the way for resilient energy systems. To build smarter and more secure infrastructure, stakeholders must engage in continuous research, knowledge sharing, and strategic foresight to foster security measures that are not only reactive but also predictive and preventive in nature

10. Conclusion

Smart grid security stands at the intersection of technological innovation and critical infrastructure protection, playing a pivotal role in ensuring the sustainability, reliability, and resilience of modern energy systems. This exploration into smart grid security has highlighted several key findings that underscore the urgency and complexity of securing these digital energy ecosystems. The integration of advanced metering infrastructure, SCADA systems, distributed energy resources, and real-time communication networks has introduced significant efficiencies and flexibility into grid operations. However, these same components have also expanded the attack surface, exposing energy infrastructures to a diverse array of cyber threats including malware, denial-of-service attacks, man-in-the-middle intrusions, and insider exploits. Vulnerability assessments reveal that legacy systems, interoperability issues, and insufficiently secured interfaces often leave critical gaps, while challenges related to workforce expertise, financial constraints, and organizational inertia further complicate implementation efforts.

In response to these risks, a layered and proactive cybersecurity approach is essential. Advanced technologies such as artificial intelligence, machine learning, blockchain, zero-trust architectures, and digital twins offer promising solutions to detect, prevent, and mitigate cyber threats. Regulatory frameworks and international standards like NERC CIP and IEC 62443 provide guidance, yet inconsistencies and policy gaps still need to be addressed through harmonized governance and collaborative enforcement. Future directions emphasize the importance of predictive threat intelligence, cross-sector collaboration, and embedding cybersecurity from the earliest design stages of smart grid systems. Together, these strategies form a holistic defense model capable of adapting to the dynamic threat landscape.

Cybersecurity is not a peripheral concern but a foundational pillar for the future of smart energy systems. Without robust protections, the promise of digitalized, decentralized, and sustainable energy cannot be fully realized. Ensuring the security of smart grids is therefore imperative not just for the technical functioning of energy networks, but for national security, economic stability, and public trust.

This reality calls for coordinated action from all stakeholders. Governments, utilities, technology developers, academic researchers, and consumers must work collectively to prioritize cybersecurity as an integral component of smart grid deployment and operation. Investments in innovation, education, policy reform, and cross-industry collaboration must be accelerated to build energy systems that are not only smart but also secure.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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).

[7] 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).

[8] 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.

[9] Ahn, B., Kim, T., Ahmad, S., Mazumder, S., Johnson, J., Mantooth, H., … and Farnell, C. (2024). An overview of cyber-resilient smart inverters based on practical attack models. Ieee Transactions on Power Electronics, 39(4), 4657-4673. https://doi.org/10.1109/tpel.2023.3342842

[10] Alam, K., Imran, M., Mahmud, U., and Fathah, A. (2024). Cyber attacks detection and mitigation using machine learning in smart grid systems. NHJ, 1(01), 83-99. https://doi.org/10.70008/jeser.v1i01.43

[11] Alkhiari, A., Mishra, S., and Alshehri, M. (2022). Blockchain-based sqkd and ids in edge enabled smart grid network. Computers Materials and Continua, 70(2), 2149-2169. https://doi.org/10.32604/cmc.2022.019562

[12] Almoughem, K. (2023). The future of cybersecurity workforce development. Academic Journal of Research and Scientific Publishing, 4(45), 37-48. https://doi.org/10.52132/ajrsp.en.2023.45.3

[13] Almutairy, F., Šćekić, L., Elmoudi, R., and Wshah, S. (2021). Accurate detection of false data injection attacks in renewable power systems using deep learning. Ieee Access, 9, 135774-135789. https://doi.org/10.1109/access.2021.3117230

[14] Alonso, M., Turanzas, J., Amarís, H., and Ledo, A. (2021). Cyber-physical vulnerability assessment in smart grids based on multilayer complex networks. Sensors, 21(17), 5826. https://doi.org/10.3390/s21175826

[15] Al-Shaer, E. and Rahman, M. (2016). Analytics for smart grid security and resiliency., 15-26. https://doi.org/10.1007/978-3-319-32871-3_2

[16] Amini, F., Zadeh, S., Rostami, N., and Tabar, V. (2023). Electrical energy systems resilience: a comprehensive review on definitions, challenges, enhancements and future proceedings. Iet Renewable Power Generation, 17(7), 1835-1858. https://doi.org/10.1049/rpg2.12705

[17] Annor-Asante, M. and Pranggono, B. (2018). Development of smart grid testbed with low-cost hardware and software for cybersecurity research and education. Wireless Personal Communications, 101(3), 1357-1377. https://doi.org/10.1007/s11277-018-5766-6

[18] 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.

[19] 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.

[20] Banik, S. and Banik, T. (2024). Survey on simulation and vulnerability testing in smart grid.. https://doi.org/10.20944/preprints202402.0047.v2

[21] Banik, S., Banik, T., and Banik, S. (2023). Using virtual environment to analyze cyber-attacks on smart grid protocol.. https://doi.org/10.20944/preprints202309.0984.v1

[22] Barbierato, L., Estebsari, A., Pons, E., Pau, M., Salassa, F., Ghirardi, M., … and Patti, E. (2019). A distributed iot infrastructure to test and deploy real-time demand response in smart grids. Ieee Internet of Things Journal, 6(1), 1136-1146. https://doi.org/10.1109/jiot.2018.2867511

[23] Basharat, A. and Huma, Z. (2024). Enhancing resilience: smart grid cybersecurity and fault diagnosis strategies. Asian Journal of Research in Computer Science, 17(6), 1-12. https://doi.org/10.9734/ajrcos/2024/v17i6453

[24] Borenius, S., Gopalakrishnan, P., Tjernberg, L., and Kantola, R. (2022). Expert-guided security risk assessment of evolving power grids. Energies, 15(9), 3237. https://doi.org/10.3390/en15093237

[25] Borgaonkar, R., Tøndel, I., Degefa, M., and Jaatun, M. (2021). Improving smart grid security through 5g enabled iot and edge computing. Concurrency and Computation Practice and Experience, 33(18). https://doi.org/10.1002/cpe.6466

[26] 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

[27] Boza, P. and Evgeniou, T. (2021). Artificial intelligence to support the integration of variable renewable energy sources to the power system. Applied Energy, 290, 116754. https://doi.org/10.1016/j.apenergy.2021.116754

[28] Cali, Ü., Kuzlu, M., Sharma, V., Pipattanasomporn, M., and Çatak, F. (2021). Internet of predictable things (iopt) framework to increase cyber-physical system resiliency.. https://doi.org/10.48550/arxiv.2101.07816

[29] Chidolue, O., Daudu, C., Illojianya, V., Fafure, A., Ibekwe, K., and Ngozichukwu, B. (2024). Control systems in renewable energy: a review of applications in canada, usa, and africa. World Journal of Advanced Engineering Technology and Sciences, 11(1), 029-036. https://doi.org/10.30574/wjaets.2024.11.1.0011

[30] Chinnasamy, P., Samrin, R., Sujitha, B. B., Augasthega, R., Rajagopal, M., and Nageswaran, A. (2024). Integrating Intelligent breach detection system into 6 g enabled smart grid-based cyber physical systems. Wireless Personal Communications, 1-16.

[31] Constant, C., Kotarbinski, M., Stefek, J., Green, R., DeGeorge, E., and Baring-Gould, I. (2021). Accelerating ocean-based renewable energy educational opportunities to achieve a clean energy future. Progress in Energy, 3(4), 042002. https://doi.org/10.1088/2516-1083/ac1509

[32] Coppolino, L., Nardone, R., Petruolo, A., and Romano, L. (2023). Building cyber-resilient smart grids with digital twins and data spaces. Applied Sciences, 13(24), 13060. https://doi.org/10.3390/app132413060

[33] Dawson, J. and Thomson, R. (2018). The future cybersecurity workforce: going beyond technical skills for successful cyber performance. Frontiers in Psychology, 9. https://doi.org/10.3389/fpsyg.2018.00744

[34] 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

[35] Diaba, S. Y., Shafie-khah, M., and Elmusrati, M. (2024). Cyber-physical attack and the future energy systems: A review. Energy Reports, 12, 2914-2932.

[36] Ding, J., Qammar, A., Zhang, Z., Karim, A., and Ning, H. (2022). Cyber threats to smart grids: review, taxonomy, potential solutions, and future directions. Energies, 15(18), 6799. https://doi.org/10.3390/en15186799

[37] 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

[38] 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

[39] Fang, X., Misra, S., Xue, G., and Yang, D. (2012). Smart grid the new and improved power grid: a survey. Ieee Communications Surveys and Tutorials, 14(4), 944-980. https://doi.org/10.1109/surv.2011.101911.00087

[40] Ghadi, Y., Mazhar, T., Aurangzeb, K., Haq, I., Shahzad, T., Laghari, A., ... and Anwar, M. (2024). Security risk models against attacks in smart grid using big data and artificial intelligence. Peerj Computer Science, 10, e1840. https://doi.org/10.7717/peerj-cs.1840

[41] Ghosal, A. and Conti, M. (2019). Key management systems for smart grid advanced metering infrastructure: a survey. Ieee Communications Surveys and Tutorials, 21(3), 2831-2848. https://doi.org/10.1109/comst.2019.2907650

[42] Gopstein, A., Hastings, N., Feldman, L., Agarwal, R., and Bartol, N. (2021). Distributed energy resource security :.. https://doi.org/10.6028/nist.tn.2182

[43] Govea, J., Gaibor-Naranjo, W., and Villegas-Ch, W. (2024). Transforming cybersecurity into critical energy infrastructure: a study on the effectiveness of artificial intelligence. Systems, 12(5), 165. https://doi.org/10.3390/systems12050165

[44] Habib, M., Shoukat, M., Irfan, M., Zubair, M., Ahmed, S., Raza, M., ... and Sarwar, A. (2023). Smart meter development using digital twin technology for green energy distribution optimization. European Journal of Theoretical and Applied Sciences, 1(3), 181-190. https://doi.org/10.59324/ejtas.2023.1(3).20

[45] He, H. and Yan, J. (2016). Cyber-physical attacks and defences in the smart grid: a survey. Iet Cyber-Physical Systems Theory and Applications, 1(1), 13-27. https://doi.org/10.1049/iet-cps.2016.0019

[46] Hou, B., Zhe-feng, L., Zuo, X., Guo, Y., and Zhou, J. (2024). Application of intelligent cloud computing technology in optical communication network security of smart grid. Journal of Cyber Security and Mobility, 605-632. https://doi.org/10.13052/jcsm2245-1439.1342

[47] Jin, C., Chen, G., Yu, C., Shan, J., Zhao, J., and Jin, Y. (2018). An efficient heterogeneous signcryption for smart grid. Plos One, 13(12), e0208311. https://doi.org/10.1371/journal.pone.0208311

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

[49] Keyser, D. and Tegen, S. (2019). The wind energy workforce in the united states: training, hiring, and future needs.. https://doi.org/10.2172/1547263

[50] Khan, S., Kifayat, K., Bashir, A., Gurtov, A., and Hassan, M. (2020). Intelligent intrusion detection system in smart grid using computational intelligence and machine learning. Transactions on Emerging Telecommunications Technologies, 32(6). https://doi.org/10.1002/ett.4062

[51] Kim, Y., Hakak, S., and Ghorbani, A. (2023). Smart grid security: Attacks and defence techniques. IET Smart Grid, 6(2), 103-123.

[52] Koch, S., Galus, M., Chatzivasileiadis, S., and Andersson, G. (2011). Emergency control concepts for future power systems. Ifac Proceedings Volumes, 44(1), 6121-6129. https://doi.org/10.3182/20110828-6-it-1002.02389

[53] Kour, R. and Karim, R. (2020). Cybersecurity workforce in railway: its maturity and awareness. Journal of Quality in Maintenance Engineering, 27(3), 453-464. https://doi.org/10.1108/jqme-07-2020-0059

[54] Kuang, L., Shi, W., and Zhang, J. (2024). Hierarchical privacy protection model in advanced metering infrastructure based on cloud and fog assistance. Computers Materials and Continua, 80(2), 3193-3219. https://doi.org/10.32604/cmc.2024.054377

[55] Kumar, A., Vishnoi, P., and Letha, S. (2019). Smart grid security with cryptographic chip integration. Eai Endorsed Transactions on Energy Web, 6(23), 157037. https://doi.org/10.4108/eai.13-7-2018.157037

[56] Kumari, N., Sharma, A., Tran, B., Chilamkurti, N., and Alahakoon, D. (2023). A comprehensive review of digital twin technology for grid-connected microgrid systems: state of the art, potential and challenges faced. Energies, 16(14), 5525. https://doi.org/10.3390/en16145525

[57] Le, T., Ge, M., Anwar, A., Loke, S., Beuran, R., Doss, R., ... and Tan, Y. (2022). Gridattackanalyzer: a cyber attack analysis framework for smart grids. Sensors, 22(13), 4795. https://doi.org/10.3390/s22134795

[58] Lei, J., Zhu, Z., Yang, Y., and Zhang, S. (2016). Research of marketing big data security storage in smart grid based on spark.. https://doi.org/10.2991/icimm-16.2016.139

[59] 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

[60] Li, Y., Di, Z., Wang, Z., and Liu, G. (2023). A blockchain-based cooperative authentication mechanism for smart grid. Applied Sciences, 13(11), 6831. https://doi.org/10.3390/app13116831

[61] Liang, X., Gao, K., Zheng, X., and Zhao, T. (2013). A study on cyber security of smart grid on public networks., 301-308. https://doi.org/10.1109/greentech.2013.53

[62] Lu, R., Liang, X., Li, X., Lin, X., and Shen, X. (2012). Eppa: an efficient and privacy-preserving aggregation scheme for secure smart grid communications. Ieee Transactions on Parallel and Distributed Systems, 23(9), 1621-1631. https://doi.org/10.1109/tpds.2012.86

[63] Luo, B., Xu, G., Xie, J., and Wang, Y. (2022). A blockchain-based security framework for secure and resilient smart grid. Journal of Physics Conference Series, 2218(1), 012033. https://doi.org/10.1088/1742-6596/2218/1/012033

[64] Lyulyov, O., Vakulenko, I., Pimonenko, T., Kwiliński, A., Dźwigoł, H., and Dźwigoł–Barosz, M. (2021). Comprehensive assessment of smart grids: is there a universal approach?. Energies, 14(12), 3497. https://doi.org/10.3390/en14123497

[65] Mansour, D., Numair, M., Zalhaf, A., Ramadan, R., Darwish, M., Huang, Q., … and Abdel-Rahim, O. (2023). Applications of iot and digital twin in electrical power systems: a comprehensive survey. Iet Generation Transmission and Distribution, 17(20), 4457-4479. https://doi.org/10.1049/gtd2.12940

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

[67] Mengidis, N., Tsikrika, T., Vrochidis, S., and Kompatsiaris, I. (2019). Blockchain and ai for the next generation energy grids: cybersecurity challenges and opportunities. Information and Security an International Journal, 43(1), 21-33. https://doi.org/10.11610/isij.4302

[68] 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

[69] 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

[70] Nejabatkhah, F., Li, Y., Liang, H., and Ahrabi, R. (2020). Cyber-security of smart microgrids: a survey. Energies, 14(1), 27. https://doi.org/10.3390/en14010027

[71] Nik, V., Perera, A., and Chen, D. (2020). Towards climate resilient urban energy systems: a review. National Science Review, 8(3). https://doi.org/10.1093/nsr/nwaa134

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

[73] 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.

[74] 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.

[75] Pan, T., Mishra, S., Nguyen, L., Lee, G., Kang, J., Seo, J., … and Thai, M. (2017). Threat from being social: vulnerability analysis of social network coupled smart grid. Ieee Access, 5, 16774-16783. https://doi.org/10.1109/access.2017.2738565

[76] Parrish, A., Impagliazzo, J., Raj, R., Santos, H., Asghar, M., Jøsang, A., … and Stavrou, E. (2018). Global perspectives on cybersecurity education for 2030: a case for a meta-discipline., 36-54. https://doi.org/10.1145/3293881.3295778

[77] Perälä, P. and Lehto, M. (2024). Educating cybersecurity experts: analysis of cybersecurity education in finnish universities. European Conference on Cyber Warfare and Security, 23(1), 371-378. https://doi.org/10.34190/eccws.23.1.2256

[78] Peralta, F., Watson, M., Bays, R., Boles, J., and Powers, F. (2021). Cybersecurity resiliency of marine renewable energy systems part 2: cybersecurity best practices and risk management. Marine Technology Society Journal, 55(2), 104-116. https://doi.org/10.4031/mtsj.55.2.4

[79] Pirta-Dreimane, R., Romānovs, A., Bikovska, J., Pekša, J., Vartiainen, T., Valliou, M., … and Eltahawy, B. (2024). Enhancing smart grid resilience: an educational approach to smart grid cybersecurity skill gap mitigation. Energies, 17(8), 1876. https://doi.org/10.3390/en17081876

[80] Pollini, A., Callari, T., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., … and Guerri, D. (2021). Leveraging human factors in cybersecurity: an integrated methodological approach. Cognition Technology and Work, 24(2), 371-390. https://doi.org/10.1007/s10111-021-00683-y

[81] Qureshi, K., Najam-ul-Islam, M., and Jeon, G. (2021). A trust evaluation model for secure data aggregation in smart grids infrastructures for smart cities. Journal of Ambient Intelligence and Smart Environments, 13(3), 235-252. https://doi.org/10.3233/ais-210602

[82] Radoglou-Grammatikis, P. and Sarigiannidis, P. (2019). Securing the smart grid: a comprehensive compilation of intrusion detection and prevention systems. Ieee Access, 7, 46595-46620. https://doi.org/10.1109/access.2019.2909807

[83] 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

[84] Rashed, M., Kamruzzaman, J., Gondal, I., and Islam, S. (2022). Vulnerability assessment framework for a smart grid., 449-454. https://doi.org/10.1109/gpecom55404.2022.9815621

[85] Rawat, D. and Bajracharya, C. (2015). Cyber security for smart grid systems: status, challenges and perspectives., 1-6. https://doi.org/10.1109/secon.2015.7132891

[86] Rohokale, V. and Prasad, R. (2016). Cyber security for smart grid – the backbone of social economy. Journal of Cyber Security and Mobility. https://doi.org/10.13052/2245-1439.514

[87] Sadi, M., Ali, M., Dasgupta, D., and Abercrombie, R. (2015). Opnet/simulink based testbed for disturbance detection in the smart grid.. https://doi.org/10.1145/2746266.2746283

[88] Sadik, S., Ahmed, M., Sikos, L., and Islam, A. (2020). Toward a sustainable cybersecurity ecosystem. Computers, 9(3), 74. https://doi.org/10.3390/computers9030074

[89] Sajjadi, M. and Niknia, B. (2013). Smart power grid security services: risk management approach considering both ot and it domains case study: shiraz power distribution company., 1155-1155. https://doi.org/10.1049/cp.2013.1099

[90] 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. https://doi.org/10.1109/gec61857.2024.10880948

[91] Sarma, G. and Zabaniotou, A. (2021). Understanding vulnerabilities of renewable energy systems for building their resilience to climate change hazards: key concepts and assessment approaches. Renewable Energy and Environmental Sustainability, 6, 35. https://doi.org/10.1051/rees/2021035

[92] Saxena, K. (2024). Enhancing cybersecurity in smart grids through machine learning-based intrusion detection systems. jes, 20(7s), 2524-2533. https://doi.org/10.52783/jes.4076

[93] Smys, S., Bashar, A., and Wang, H. (2019). Secure and sustainable smart grid framework using the cloud computing. *Journal of ISMAC*, *1*(03), 137-146. https://doi.org/10.36548/jismac.2019.3

[94] Suman, S., Aqib, M., and Singh, S. (2017). A security approach for smart grid on review. Aptikom Journal on Computer Science and Information Technologies, 2(1), 12-19. https://doi.org/10.11591/aptikom.j.csit.93

[95] Suman, S., Aqib, M., and Singh, S. (2020). A security approach for smart grid on review. Aptikom Journal on Computer Science and Information Technologies, 2(1), 12-19. https://doi.org/10.34306/csit.v2i1.63

[96] 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

[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] Tweneboah-Koduah, S., Tsetse, A., Azasoo, J., and Endicott-Popovsky, B. (2017). Evaluation of cybersecurity threats on smart metering system., 199-207. https://doi.org/10.1007/978-3-319-54978-1_28

[99] 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.

[100] 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.

[101] Uribe-Pérez, N., Hernández-Callejo, L., Vega, D., and Angulo, I. (2016). State of the art and trends review of smart metering in electricity grids. Applied Sciences, 6(3), 68. https://doi.org/10.3390/app6030068

[102] Vakulenko, I., Saher, L., Syhyda, L., Kolosok, S., and Yevdokymova, A. (2021). The first step in removing communication and organizational barriers to stakeholders' interaction in smart grids: a theoretical approach. E3s Web of Conferences, 234, 00020. https://doi.org/10.1051/e3sconf/202123400020

[103] Vasilomanolakis, E., Fischer, M., Mühlhäuser, M., Ebinger, P., Kikiras, P., and Schmerl, S. (2013). Collaborative intrusion detection in smart energy grids.. https://doi.org/10.14236/ewic/icscsr2013.11

[104] Vempati, S. (2024). Securing smart cities: a cybersecurity perspective on integrating iot, ai, and machine learning for digital twin creation. jes, 20(3), 1420-1429. https://doi.org/10.52783/jes.3548

[105] Wang, T., Wei, X., Huang, T., Wang, J., Valencia-Cabrera, L., Fan, Z., … and Pérez–Jiménez, M. (2019). Cascading failures analysis considering extreme virus propagation of cyber-physical systems in smart grids. Complexity, 2019(1). https://doi.org/10.1155/2019/7428458

[106] 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

[107] Xu, Z., S., A., and Rudolph, C. (2023). Blockchain-based malicious behaviour management scheme for smart grids. Smart Cities, 6(5), 3005-3031. https://doi.org/10.3390/smartcities6050135

[108] 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

[109] Ye, Y., Qian, Y., Sharif, H., and Tipper, D. (2013). A survey on smart grid communication infrastructures: motivations, requirements and challenges. Ieee Communications Surveys and Tutorials, 15(1), 5-20. https://doi.org/10.1109/surv.2012.021312.00034

[110] Zheng, T., Liu, M., Puthal, D., Yi, P., Wu, Y., and He, X. (2022). Smart grid: cyber attacks, critical defense approaches, and digital twin.. https://doi.org/10.48550/arxiv.2205.11783

[111] Zhu, Q. (2018). Multilayer cyber-physical security and resilience for smart grid., 225-239. https://doi.org/10.1007/978-3-319-98310-3_14

[112] Zou, T., Bretas, A., Ruben, C., Dhulipala, S., and Bretas, N. (2020). Smart grids cyber-physical security: parameter correction model against unbalanced false data injection attacks. Electric Power Systems Research, 187, 106490. https://doi.org/10.1016/j.epsr.2020.106490