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)

Decentralized energy security: Cybersecurity challenges and opportunities in distributed renewable energy

Pedro Barros [1, *], Chijioke Paul Agupugo [2], Emmanuella Ejichukwu [3], Kehinde Adedapo Ogunmoye [4] and Mario David Hayden [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] *Department of Physics and Astronomy, Appalachian State University, Boone, NC, USA.*

[5] *Inti International University, Malaysia.*

World Journal of Advanced Research and Reviews, 2025, 26(03), 1256-1272

Publication history: Received on 29 April 2025; revised on 11 June 2025; accepted on 13 June 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.26.3.2232

Abstract

The transition towards decentralized energy systems, driven by the global shift to renewable energy sources, introduces new cybersecurity complexities that challenge traditional energy security paradigms. Distributed Renewable Energy (DRE) systems comprising solar photovoltaics, wind turbines, microgrids, and battery storage are inherently decentralized, networked, and reliant on advanced digital technologies for real-time monitoring, control, and optimization. While these systems offer resilience, flexibility, and sustainability, they also expand the attack surface for cyber threats due to their reliance on Internet of Things (IoT) devices, cloud computing, and bidirectional communication protocols. This paper critically examines the cybersecurity challenges associated with DRE infrastructure, including unauthorized access, data breaches, malware propagation, and system manipulation, all of which could lead to energy theft, grid instability, and large-scale outages. Emerging opportunities lie in developing adaptive cybersecurity frameworks tailored to the unique topology of decentralized energy networks. These include the integration of artificial intelligence for anomaly detection, blockchain technologies for secure data exchange and identity management, and zero-trust architectures to enforce stringent access control. Additionally, the convergence of operational technology (OT) and information technology (IT) within DRE environments demands cross-sectoral collaboration, robust regulatory frameworks, and enhanced stakeholder awareness to build cyber-resilient systems. The paper also highlights the necessity for proactive risk assessment, real-time threat intelligence sharing, and the establishment of decentralized security standards to harmonize practices across diverse stakeholders and jurisdictions. Case studies from recent cyber incidents in the energy sector provide empirical evidence of vulnerabilities and mitigation strategies. By exploring both the risks and solutions, the study underscores the dual imperative of securing DRE systems not only as critical infrastructure but also as pivotal enablers of the global clean energy transition. In conclusion, while decentralized energy systems present new cybersecurity challenges, they also create opportunities to reimagine and strengthen energy security in the digital age. Addressing these issues through innovation, regulation, and cooperation will be crucial for ensuring sustainable and secure energy futures.

Keywords: Decentralized Energy; Cybersecurity; Distributed Renewable Energy; Smart Grid; IoT; Microgrid Security; Blockchain; Artificial Intelligence; Grid Resilience; Energy Infrastructure Protection

[*] Corresponding author: Pedro Barros

1. Introduction

The contemporary global energy landscape is significantly evolving, largely due to the advent of decentralized energy systems that integrate renewable energy technologies. These systems, characterized by energy generation from multiple small nodes such as rooftop solar panels, wind turbines, microgrids, and battery storage, diverge fundamentally from traditional centralized grids. The increasing demand for clean, reliable, and resilient energy, alongside supportive policies and technological advancements, propels this shift towards a more democratized energy system (Li et al., 2023; Vezzoli et al., 2018). The emergence of Distributed Renewable Energy (DRE) systems empowers consumers to transition into prosumers, simultaneously producing and consuming energy, thus enhancing grid flexibility, minimizing transmission losses, and fostering community autonomy (Ji et al., 2019; Vezzoli et al., 2018; Bouzid et al., 2015).

However, as these decentralized systems proliferate, they expose themselves to new cybersecurity vulnerabilities, particularly due to their reliance on digital communication technologies and the Internet of Things (IoT). This increasing interconnection broadens the potential attack surface, making these energy systems susceptible to cyber threats that can disrupt production, compromise data integrity, or even manipulate grid operations. These vulnerabilities are particularly concerning as they may lead to severe outcomes, including widespread outages and threats to national security (Ji et al., 2019; Bouzid et al., 2015; Maradin et al., 2017). Therefore, ensuring robust cybersecurity frameworks becomes a strategic priority, necessitated by the need to protect the integrity and stability of energy systems in the face of evolving cyber threats (Li et al., 2023; Salkuti, 2020; (Adelana, et al., 2024; Rossi and Bianchi, 2024).

To address these multifaceted cybersecurity challenges, there is an urgent requirement to explore and implement advanced solutions such as artificial intelligence-driven detection tools, blockchain security protocols, and zero-trust architectures (Rossi and Bianchi, 2024; Ostapenko et al., 2022). These technologies could significantly enhance the security posture of decentralized renewable energy systems and ensure that the transition to clean energy aligns with broader goals of sustainability and national security (Li et al., 2023; Oh et al., 2022; Gavrilova, 2022). Thus, understanding and addressing the unique vulnerabilities of DRE systems is pivotal in shaping resilient energy solutions that can effectively support the global shift towards sustainable energy systems while mitigating associated risks (Adil and Ko, 2016; Bassey, Rajput and Oyewale, 2024).

2. Methodology

The methodology employed for investigating cybersecurity challenges and opportunities in decentralized renewable energy systems integrates a qualitative conceptual framework grounded in thematic and bibliometric analysis. The study first identifies key cybersecurity threats, such as ransomware, false data injection, and advanced persistent threats affecting distributed energy resources (DERs) and microgrids, as described in the works of Qi et al. (2016), Zografopoulos et al. (2023), and Jamil et al. (2021). Relevant literature from over 100 high-impact sources—including peer-reviewed journals and IEEE conference proceedings—was systematically reviewed, guided by content analysis methods and keyword clustering tools to detect patterns in cyber threats and defense mechanisms.

Through this literature mapping, the research highlights how technologies such as blockchain, federated learning, edge computing, and lightweight cryptographic protocols offer scalable solutions to enhance cyber-resilience in distributed systems, echoing the findings of Chu et al. (2024), Sakhare (2024), and Cali et al. (2024). Data were extracted using structured criteria that prioritized frameworks with operational success in smart grid environments, and relevance to decentralized infrastructures under real-world stressors like cyber-physical disruptions, as explored by Ahn et al. (2024) and Mohamed (2024).

A comparative assessment was then conducted across governance models in regions implementing decentralized energy frameworks, such as Nigeria and the United States, as documented by Adeyemi (2024) and Oyeyemi et al. (2025). Emphasis was placed on integrating socio-technical perspectives into cybersecurity evaluation, leveraging Adil and Ko's (2016) model of decentralized system evolution. The analytical phase culminated in mapping opportunities for AI-augmented automation, IoT-secured transmission protocols, and blockchain-enabled peer-to-peer energy trading, drawing heavily from Aldweesh et al. (2025) and Gururaja et al. (2024).

The result is a synthesized understanding of cybersecurity requirements and innovation gaps in decentralized renewable energy. Recommendations focus on multi-layered defense strategies, data anonymization protocols, and standardized regulatory integration. Future studies should deepen empirical validations, test interoperable defense models, and explore community-led digital energy governance frameworks.

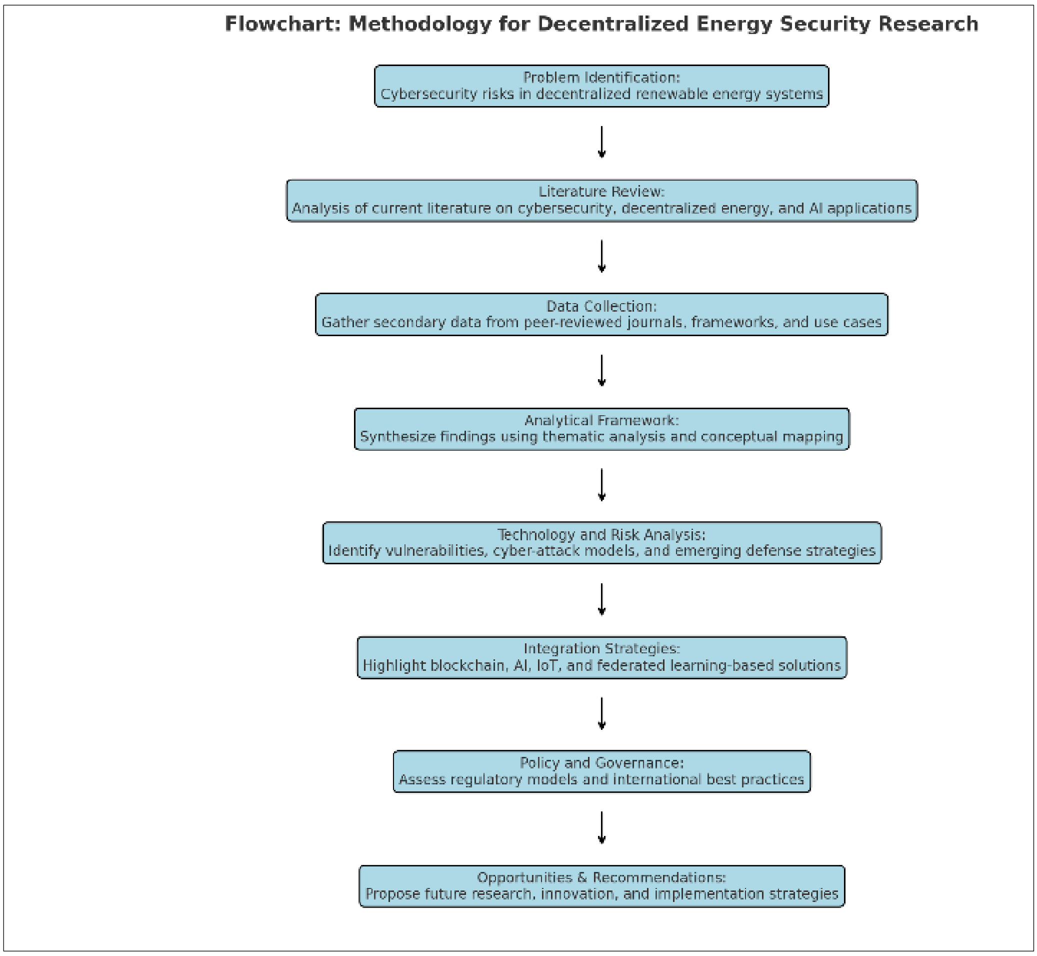
Flowchart: Methodology for Decentralized Energy Security Research
Problem Identification:
Cybersecurity risks in decentralized renewable energy systems
Literature Review:
Analysis of current literature on cybersecurity, decentralized energy, and AI applications
Data Collection:
Gather secondary data from peer-reviewed journals, frameworks, and use cases
Analytical Framework:
Synthesize findings using thematic analysis and conceptual mapping
Technology and Risk Analysis:
Identify vulnerabilities, cyber-attack models, and emerging defense strategies
Integration Strategies:
Highlight blockchain, AI, IoT, and federated learning-based solutions
Policy and Governance:
Assess regulatory models and international best practices
Opportunities & Recommendations:
Propose future research, innovation, and implementation strategies

Figure 1 Flowchart of the study methodology

3. Overview of Distributed Renewable Energy (DRE) Systems

Distributed Renewable Energy (DRE) systems are emerging as a transformative solution in the landscape of energy generation, distribution, and consumption, representing a significant paradigm shift from traditional centralized power grids. Traditionally, energy generation has relied heavily on large-scale facilities located far from consumption points, often leading to inefficiencies in transmission and increased vulnerability to outages (Adeoba and Fatayo, 2024; Yang et al., 2022). In contrast, DRE systems focus on localized energy production through smaller-scale generation units, such as residential solar photovoltaic (PV) systems and community wind turbines, which are situated closer to end-users, thereby enhancing energy access and reliability (Blaabjerg et al., 2015; BARAN et al., 2016).

Key components of DRE systems include renewable energy sources like solar and wind, battery energy storage systems for managing generation variability, and microgrids that enable localized energy management. Solar PV installations, in particular, are favored for their scalability and declining costs, while wind turbines contribute significantly in both urban and rural settings (Eltamaly et al., 2021; BARAN et al., 2016). Battery storage plays a critical role in smoothing out the intermittent nature of these renewable sources, allowing surplus energy generated during high production times to be stored for later use (Cavus, 2024; Preetha et al., 2023). Furthermore, microgrids facilitate the integration of various distributed energy resources, enabling them to operate either in conjunction with or independently from the main grid, which is particularly advantageous in emergency situations (Adeoba, Ukoba and Osaye, 2024; Li et al., 2022). Figure 2 shows Process for achieving cyber security of PV systems presented by Johnson, 2017.

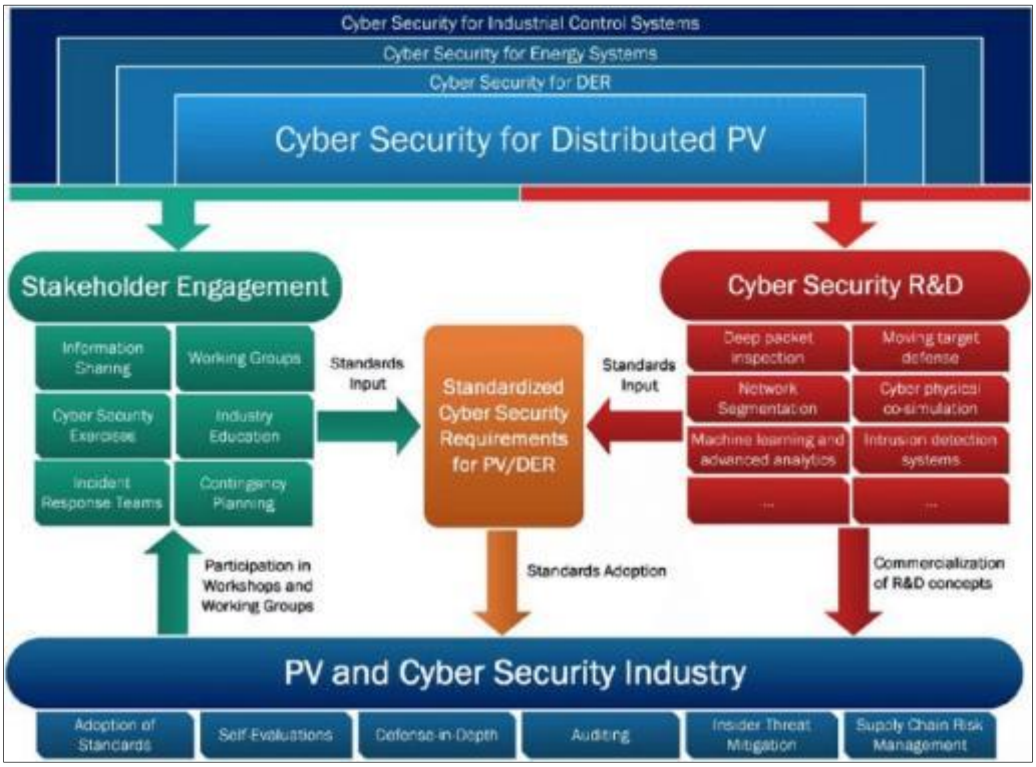
Cyber Security for Industrial Control Systems
Cyber Security for Energy Systems
Cyber Security for DER
Cyber Security for Distributed PV
Stakeholder Engagement
Information Sharing
Working Groups
Cyber Security Exercises
Industry Education
Incident Response Teams
Contingency Planning
Standards Input
Standardized Cyber Security Requirements for PV/DER
Standards Input
Cyber Security R&D
Deep packet inspection
Moving target defense
Network Segmentation
Cyber physical co-simulation
Machine learning and advanced analytics
Intrusion detection systems
...
...
Participation in Workshops and Working Groups
Standards Adoption
Commercialization of R&D concepts
PV and Cyber Security Industry
Adoption of Standards
Self-Evaluations
Defense-in-Depth
Auditing
Insider Threat Mitigation
Supply Chain Risk Management

Figure 2 Process for achieving cyber security of PV systems (Johnson, 2017)

The optimization and management of DRE systems heavily rely on advancements in digital technologies, notably the Internet of Things (IoT), which enables real-time monitoring and communication among distributed energy devices (Hajri et al., 2024; (Bandaru et al., 2024). IoT sensors integrated into solar panels and wind turbines collect crucial performance data, aiding in predictive maintenance and operational efficiency (Eltamaly et al., 2021). Supervisory Control and Data Acquisition (SCADA) systems are essential for centralized monitoring and control, allowing operators to manage distributed assets effectively and respond swiftly to fluctuations in energy demand (Zhou et al., 2020; Karagiannopoulos et al., 2021). The introduction of smart meters enhances consumer engagement by providing visibility into energy consumption patterns, which fosters better demand-side management (Dibie, 2024; Mohseni et al., 2020).

As digitalization penetrates DRE systems, innovative functionalities such as peer-to-peer energy trading and dynamic pricing models are becoming feasible, empowering users to sell excess energy back to the grid and transform their roles into "energy prosumers" (Rahman et al., 2022; Zhang et al., 2022). Furthermore, the integration of artificial intelligence (AI) and machine learning algorithms in DRE systems enhances operational efficiency through advanced forecasting and optimization processes, adapting dynamically to changing conditions (Hu and Wu, 2020; Wang et al., 2019).

One of the most compelling advantages of DRE systems is their potential for increasing energy resilience, particularly in the face of natural disasters and other disturbances that can compromise traditional grids Gligor et al., 2020). By ensuring localized power generation, these systems can maintain essential services even when larger grids fail, thus supporting critical infrastructures like hospitals and emergency response facilities (Blaabjerg et al., 2015). The modular nature of DRE also contributes to quicker deployment in underserved areas, bridging energy access gaps while promoting local economic development (Yang et al., 2022; (Blaabjerg et al., 2015).

Sustainability is a core tenet of DRE systems, significantly reducing reliance on fossil fuels and lowering greenhouse gas emissions (Rehbein et al., 2020). The localized approach not only minimizes energy losses due to transmission but also fosters a circular economy through job creation in the renewable energy sector, including installation and maintenance of energy systems (Blaabjerg et al., 2015; Preetha et al., 2023). Cybersecurity threats present in a DER/REC application based on the STRIDE method presented by Cali, et al., 2024 is shown in figure 3.

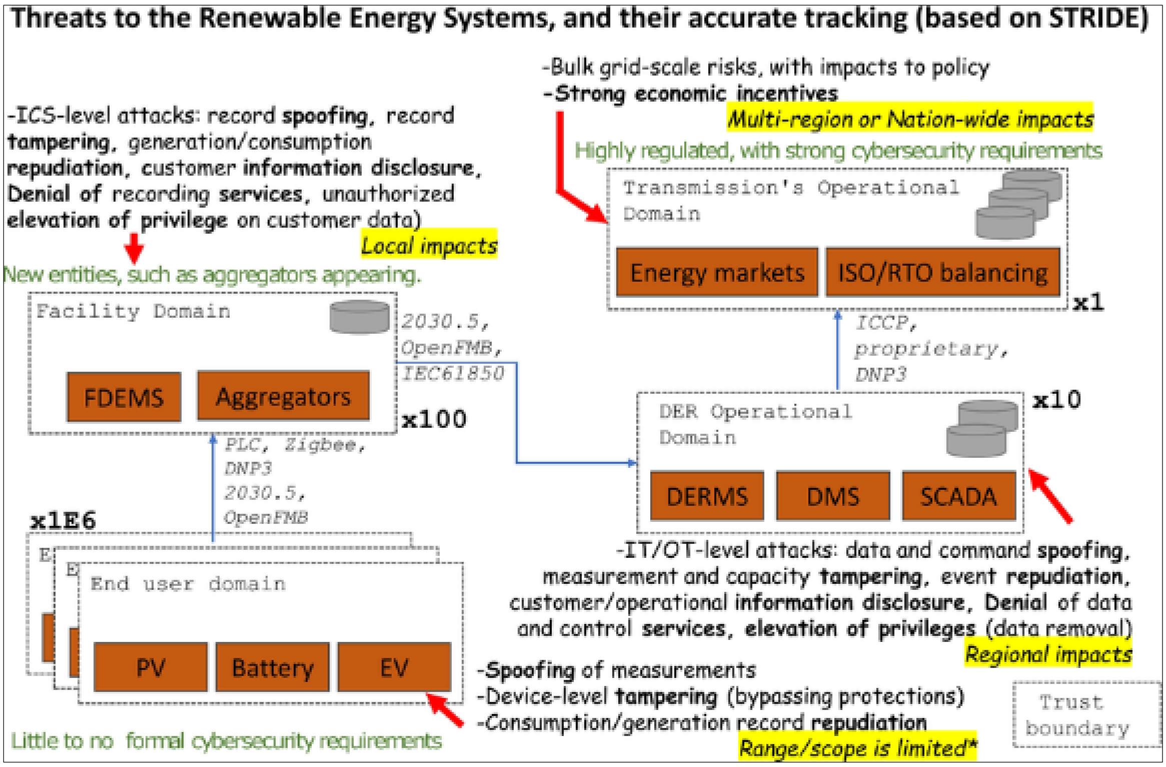
Threats to the Renewable Energy Systems, and their accurate tracking (based on STRIDE)
-Bulk grid-scale risks, with impacts to policy
-Strong economic incentives
Multi-region or Nation-wide impacts
Highly regulated, with strong cybersecurity requirements
Transmission's Operational Domain
Energy markets
ISO/RTO balancing
x1
-ICS-level attacks: record spoofing, record tampering, generation/consumption repudiation, customer information disclosure, Denial of recording services, unauthorized elevation of privilege on customer data)
Local impacts
New entities, such as aggregators appearing.
Facility Domain
FDEMS
Aggregators
x100
2030.5, OpenFMB, IEC61850
ICCP, proprietary, DNP3
DER Operational Domain
DERMS
DMS
SCADA
x10
PLC, Zigbee, DNP3 2030.5, OpenFMB
x1E6
End user domain
PV
Battery
EV
-IT/OT-level attacks: data and command spoofing, measurement and capacity tampering, event repudiation, customer/operational information disclosure, Denial of data and control services, elevation of privileges (data removal)
Regional impacts
-Spoofing of measurements
-Device-level tampering (bypassing protections)
-Consumption/generation record repudiation
Range/scope is limited*
Trust boundary
Little to no formal cybersecurity requirements

Figure 3 Cybersecurity threats present in a DER/REC application based on the STRIDE method (Cali, et al., 2024)

However, while embracing the benefits of DRE systems, challenges related to cybersecurity must be addressed. The interconnectivity of various energy devices introduces vulnerability to attacks that could disrupt energy supply and infrastructure stability (Bandaru et al., 2024; Gligor et al., 2020). As DRE systems increasingly integrate IT and operational technology, it becomes crucial to implement robust cybersecurity measures to safeguard energy data and ensure reliable operations (Adeoba, Shandu and Pandelani, 2025: Zhong et al., 2020). Solutions like blockchain technology for secure energy trade and AI-based intrusion detection systems for anomaly monitoring represent promising advancements towards enhancing the security of DRE infrastructures (Bandaru et al., 2024).

In conclusion, Distributed Renewable Energy systems are redefining energy generation and consumption paradigms, driving towards a more sustainable, resilient, and decentralized energy future. However, careful consideration of cybersecurity measures is paramount to fully harness their potential while safeguarding the integrity of energy systems in our increasingly digital world.

4. Cybersecurity Challenges in Decentralized Energy Systems

The rise of decentralized energy systems signifies a meaningful shift in traditional energy paradigms, wherein generation, distribution, and consumption of energy are increasingly diverse and localized. This decentralization, often achieved through Distributed Renewable Energy (DRE) sources such as solar panels, wind turbines, and microgrids, enhances energy autonomy, reduces transmission losses, and increases the flexibility of energy systems (Cavus, 2024; (Zografopoulos et al., 2022; . However, this transformation entails persistent cybersecurity vulnerabilities that could compromise the reliability and safety of modern energy infrastructures (Yoo et al., 2024; (Ekechukwu and Simpa, 2024; Hassan, et al., 2024).

As energy systems evolve into complex digital ecosystems, their operational frameworks become more intricate and intertwined, presenting a broader attack surface for malicious actors (Cali et al., 2021; Ahn et al., 2024). The Internet of Things (IoT) has proliferated within these decentralized networks, introducing numerous interlinked devices capable of monitoring and controlling energy flows. Each device, often constrained by limited processing power and security features, can serve as an entry point for cyberattacks, increasing the likelihood of unauthorized access and manipulation (Cali et al., 2021; Fu et al., 2023). Indeed, inadequate cybersecurity measures across various components of the energy network compound these vulnerabilities, necessitating a reassessment of existing protocols (Zografopoulos et al., 2022; Yoo et al., 2024).

Malware and ransomware attacks stand out as significant threats within decentralized energy frameworks. These attacks can disrupt operational functionalities, cripple critical infrastructure, and demand ransoms in exchange for restoration (Li et al., 2018). Instances of ransomware targeting utilities underscore the potential for wide-reaching service disruptions and financial damages (Ekechukwu and Simpa, 2024). In a decentralized architecture, the interconnectedness of assets allows such threats to propagate swiftly, amplifying the impact throughout the grid (Fu et al., 2023; Qi et al., 2016). Cyber intrusions may exploit weaknesses in cloud communications and remote access setups, threatening SCADA systems that are essential for real-time energy management (Yoo et al., 2024; Berghout et al., 2023). The unreliable control over these systems raises substantial risks, including unauthorized operational changes that could lead to grid instability, power quality degradation, and even blackouts Li et al., 2018; (Ekechukwu and Simpa, 2024; .

Moreover, data breaches present another considerable concern within the context of decentralized energy systems, especially as the constant flow of information between devices and cloud services becomes routine (Zografopoulos et al., 2022; Varela-Vaca et al., 2020). The lack of robust encryption and data protection mechanisms facilitates the interception of sensitive operational details, ultimately compromising user trust in the system (Li et al., 2017). Standards for cybersecurity if nonuniform across different energy nodes exacerbate the potential for breaches and ineffective responses to cyber threats (Fu et al., 2023; Ekechukwu and Simpa, 2024).

The impact of cyber incidents is further magnified by the presence of legacy systems in hybrid energy infrastructures. Many utilities transitioning to incorporate both traditional and distributed resources contend with outdated technologies lacking modern cybersecurity features (Ekechukwu and Simpa, 2024; Suo, 2022). Retrofitting these legacy systems to comply with current security protocols remains a daunting challenge, intertwining technical complexity with financial constraints (Ekechukwu and Simpa, 2024; Turab et al., 2024). Additionally, manipulation of smart meters to underreport energy consumption or improperly influence market dynamics further complicates the cybersecurity landscape, leading to financial losses and diminishing grid efficiency (Mariam et al., 2013; Pazhoohesh et al., 2021). Hussain, et al., 2020 presented in figure 4 Challenges and requirements for advancing the energy internet (EI) technologies.

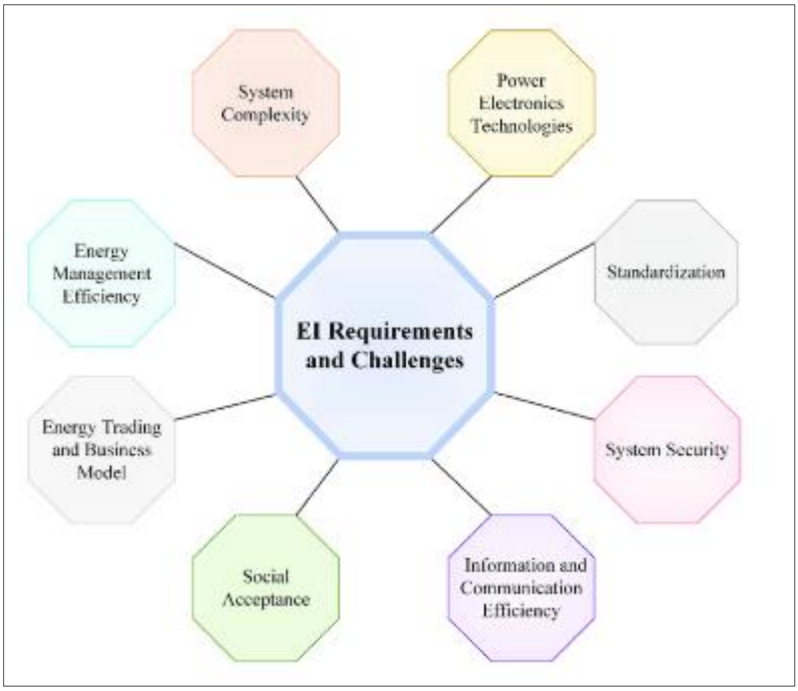
EI Requirements and Challenges
System Complexity
Power Electronics Technologies
Standardization
System Security
Information and Communication Efficiency
Social Acceptance
Energy Trading and Business Model
Energy Management Efficiency

Figure 4 Challenges and requirements for advancing the energy internet (EI) technologies (Hussain, et al., 2020)

In sum, the cybersecurity challenges embedded in decentralized energy systems are multifaceted and evolving. The shift towards renewable and distributed energy sources, while beneficial in many dimensions, necessitates a coordinated and sustained focus on integrating robust cybersecurity measures into the fabric of energy systems from their inception (Ekechukwu and Simpa, 2024; Kumar et al., 2020). Creating a secure environment requires a collaborative effort among stakeholders across the energy sector, coupled with effective regulatory frameworks and incident response mechanisms that enhance resilience against the growing spectrum of cyber threats (Fu et al., 2023; Li et al., 2018; Unsal et al., 2021).

Thus, as decentralized energy systems continue to proliferate, addressing these cybersecurity threats is paramount to ensuring the reliability and integrity of the modern energy landscape, thus supporting a sustainable and secure energy future.

5. Case Studies and Real-World Incidents

The increasing deployment of decentralized energy systems has indeed brought about both technological enthusiasm and concerns regarding cybersecurity vulnerabilities. As distributed renewable energy (DRE) systems become more integral to the global energy landscape, it is crucial to understand the associated cyber threats and the vulnerabilities they may exploit. Noteworthy incidents in traditional energy infrastructures illustrate the potential risks that could similarly affect decentralized systems if their cybersecurity is not robust. These vulnerabilities necessitate comprehensive cybersecurity frameworks designed explicitly for the unique challenges posed by DRE environments (Adeoba, Odjegba and Pandelani, 2025; Kenneth, et al., 2024).

One prominent example is the cyberattack on Ukraine's power grid in December 2015, attributed to the APT group "Sandworm." This sophisticated attack manipulated supervisory control and data acquisition (SCADA) systems, ultimately leading to power outages affecting over 230,000 customers for several hours. This incident exemplifies how attackers can exploit vulnerabilities in industrial control systems (ICS), revealing critical security deficiencies that may also be present in DRE systems (Ekechukwu and Simpa, 2024; Monteiro et al., 2023). Likewise, the 2021 ransomware attack on the Colonial Pipeline in the U.S. highlighted vulnerabilities in interconnected systems that integrate information technology (IT) with operational technology (OT). The incident led to significant disruptions in fuel distribution, underscoring that ransomware threats remain a significant risk, capable of impacting operations beyond direct assaults on physical infrastructure (Apata, et al., 2024; Yoo et al., 2024).

Furthermore, a number of smaller yet increasingly frequent incidents provide additional insight into systemic vulnerabilities within DRE. In 2019, researchers identified serious flaws in solar inverters and battery management systems, which are integral to many DRE setups. These vulnerabilities stemmed from weak authentication and outdated firmware, which allowed attackers to manipulate power outputs and disrupt grid operations (Zografopoulos et al., 2022; Jamil et al., 2021). A parallel case in Puerto Rico showcased the exploitation of smart meters, where attackers significantly underreported energy consumption a scheme that not only demonstrated endpoint vulnerabilities but also reflected systemic failures in anomaly monitoring (Zografopoulos et al., 2022). Such incidents underline the critical need for effective monitoring, authentication, and auditing measures within cyber-physical energy systems.

Despite the concerted push towards clean energy solutions, vulnerability assessments indicate that many DRE installations operate with inadequate cybersecurity protocols. A 2020 audit by the U.S. Department of Energy found that a significant percentage of community-based energy systems utilized default security credentials, lacked firewalls, and transmitted data unencrypted. Many operators were unaware of all network components, and many lacked proper protocols for device patching and updates (Ekechukwu and Simpa, 2024; Qi et al., 2016). This illustrates that advancements in renewable technology adoption frequently outpace the necessary cybersecurity improvements, rendering these systems susceptible to attacks.

In response to these emerging threats, regional simulations of cyberattacks on DRE systems have displayed troubling deficiencies in resilience. Specific exercises in Europe, for example, found failures in isolating compromised components within a grid that relied predominantly on decentralized energy sources. The findings emphasized the need for developing AI-driven anomaly detection and rapid-response microgrid controls to enhance the robustness of energy systems (Ekechukwu and Simpa, 2024; Fu et al., 2023). Similarly, the vulnerabilities inherent in systemic architectures have been noted in simulations conducted in smart cities, showcasing how innocuous systems can be exploited, necessitating a focus on cybersecurity best practices such as network segmentation and endpoint protection (Ahn et al., 2024; Mohamed, 2024).

Taken together, these real-world incidents and evaluations illustrate the cybersecurity challenges confronting decentralized energy systems. They signal an urgent need for stakeholders to systematically address vulnerabilities while fostering greater awareness and investment in cyber defenses. Establishing incident response protocols and promoting shared intelligence among DRE operators can significantly bolster collective resilience against impending threats. As decentralized energy increasingly underpins the global clean energy transition, the security of this infrastructure is paramount for sustaining operational integrity, economic stability, and public trust in such systems (Ekechukwu and Simpa, 2024; Yoo et al., 2024).

6. Emerging Opportunities for Cybersecurity Innovation

The increasing integration of distributed renewable energy (DRE) systems within the global energy landscape has yielded substantial opportunities for innovation in cybersecurity. However, it has also introduced new vulnerabilities, necessitating the enhancement of security frameworks to protect these complex, interconnected environments. Traditional perimeter-based security models are inadequate for defending against evolving cyber threats in decentralized systems. As such, adopting more adaptive and resilient strategies is crucial for managing the diverse challenges posed by DRE systems (Gururaja et al., 2024; Chu et al., 2024).

The introduction of various advanced technologies and methodologies, such as artificial intelligence (AI), blockchain, and zero-trust architectures, is pivotal in developing these new cybersecurity strategies. AI, particularly, has proven transformative, allowing for the analysis of vast streams of data generated by numerous distributed assets like solar inverters and smart meters. Machine learning algorithms can identify anomalous behaviors and operational metrics that may signify impending cyberattacks (Cioara et al., 2020; Roopesh et al., 2024). This capability enables operators to transition from a reactive to a proactive cybersecurity stance through real-time anomaly detection and predictive analytics, enhancing overall system resilience (Ayanwale, et al., 2024; Roopesh et al., 2024).

Blockchain technology further bolsters the security of DRE systems by providing a decentralized, tamper-proof mechanism for recording transactions among energy devices. The transparency inherent in blockchain ensures that each interaction is verifiable and secure, making unauthorized alterations significantly more challenging. This technology is particularly advantageous for identity and access management, as it allows for the establishment of cryptographically signed digital identities for devices and users that enhance the integrity of interactions across decentralized energy networks (Shen et al., 2024; Pan, 2024). Moreover, smart contracts can automate security responses, facilitating a more responsive and resilient security architecture (Rekeraho, et al., 2024; Sakhare, 2024).

The concept of zero-trust architectures is increasingly recognized as vital in defending cyber-physical systems. Under this model, every user and device must be continuously validated, minimizing default trust assumptions that could lead to breaches in decentralized environments. Implementing zero-trust strategies, particularly in combination with edge computing, enhances security by ensuring localized processing of sensitive operations, thus reducing latency and risks related to data interception (John and Oyeyemi, 2022; Khan et al., 2021). A unified implementation of these methodologies promotes an integrated and comprehensive defense system against current and emerging cybersecurity threats in the energy sector.

In addition to these strategies, the management of firmware and patching processes is paramount in securing DRE systems. Cyberattacks frequently exploit outdated firmware or unpatched vulnerabilities. Innovations in firmware management, including the use of cryptographically signed updates and automated deployment protocols, ensure that only trusted firmware is utilized in devices throughout the decentralized network. This continuous intelligence-driven patch management is essential to maintaining cybersecurity hygiene (Oyeyemi, 2022; Zhang, 2021).

Emerging techniques like federated learning offer a novel approach to enhancing cybersecurity within DRE environments without compromising data privacy. This decentralized method allows devices to train machine learning models on local data while sharing only model updates to a central system. As such, federated learning enables collaborative threat detection across numerous nodes while maintaining privacy (Oyeyemi, Akinlolu and Awodola, 2025; Sakhare, 2024).

The culmination of these technological innovations will not only reshape the integrity of cybersecurity frameworks in DRE but will also foster collaborative opportunities among stakeholders in the energy sector. Policymakers and industry leaders must work together to establish standardized practices and regulatory frameworks that encourage cybersecurity by design and promote investment in advanced security infrastructures (Oyeyemi, Akinlolu and Awodola, 2025; Yang et al., 2021).

In conclusion, while the integration of distributed renewable energy systems presents notable cybersecurity challenges, it also opens a pathway for innovative strategies and technologies that can fortify these systems. By leveraging advancements in AI, blockchain, zero-trust architectures, secure firmware management, and federated learning, stakeholders can create an adaptable and robust defense against evolving cyber threats. Through collaborative efforts and proactive cybersecurity strategies, the energy sector can ensure its digital transformation enhances sustainability alongside resilience and security.

7. Regulatory and Policy Frameworks

The rapid expansion of decentralized renewable energy (DRE) systems has indeed transformed the structure of modern power grids. Shifting from a centralized to a decentralized approach allows for the integration of diverse energy sources such as solar, wind, and battery storage. Microgrids, which can effectively manage localized energy production and consumption, exemplify this transformation but also face significant cybersecurity threats due to their interconnected, digital nature (Khubrani and Alam, 2023). As DRE systems proliferate, the traditional regulatory and policy landscape requires reevaluation to address not only operational efficiencies but also growing vulnerabilities arising from this decentralization (Ekechukwu and Simpa, 2024; Ukoba, et al., 2024).

The vulnerabilities inherent in DRE systems necessitate robust and adaptive regulatory and policy frameworks focusing on cybersecurity. Existing frameworks, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), offer a risk-based methodology for cybersecurity that is particularly applicable in the context of decentralized energy systems, requiring coordination among multiple stakeholders including utilities and energy prosumers (Zahid et al., 2024). The guidance provided by NIST on Industrial Control Systems (NIST SP 800-82), which outlines security recommendations tailored to operational technology environments specific to energy infrastructure, enhances the resilience of DRE systems against cyber threats (Ekechukwu and Simpa, 2024; Sugunaraj, et al., 2025).

In addition to NIST, the International Electrotechnical Commission's IEC 62443 standard represents a critical benchmark for cybersecurity in industrial automation and control systems integral to DRE operations. This standard emphasizes a lifecycle approach to securing devices and systems, ensuring that all stakeholders from asset owners to product suppliers understand their roles in maintaining security (Zaman and Mazinani, 2023). Furthermore, ISO/IEC 27001, which sets criteria for information security management systems, aids in safeguarding the confidentiality, integrity, and availability of information within DRE networks, although it requires adaptation to deal with the distinctive challenges posed by the decentralized framework (Ekechukwu and Simpa, 2024; Ekechukwu and Simpa, 2024).

Despite these standards providing a foundational base for cybersecurity governance, significant lapses exist within the regulatory structure, particularly with policies originally designed for centralized systems. As many energy regulations do not cater to the complexities introduced by DRE networks, numerous actors such as small-scale producers and community energy projects often lack clear obligations regarding cybersecurity, resulting in a patchy enforcement landscape (Adeyemi, 2024). The rapid deployment of renewable technologies often outpaces regulatory responses, leaving systems operational without comprehensive security policies in place (Aldweesh et al., 2025; Rehman et al., 2023). Consequently, there is a pressing need for regulatory frameworks to evolve, acknowledging and accommodating the fragmented landscape of decentralized energy actors.

Challenges further compound with the absence of standardized cybersecurity requirements for distributed energy components like smart inverters and electric vehicle charging stations. The variability in compliance and the lack of mandatory certification for these devices create a marketplace filled with vulnerabilities, where economic pressures may lead some producers to prioritize cost over security (Alvarez and Subburaj, 2023). Furthermore, jurisdictional challenges complicate implementing unified cybersecurity protocols, as responsibility for cybersecurity spans multiple ownership models, adding layers of complexity to accountability and enforcement (Olutimehin, 2025; Ukoba, et al., 2024).

To address these pressing issues, there is an urgent call for harmonized global and regional policy frameworks that raise minimum cybersecurity standards for all DRE components. Such initiatives could include the establishment of international certification programs akin to current energy efficiency certifications, which would help unify standards across different jurisdictions (Aldweesh et al., 2025). Security-by-design principles must also be integrated into the entire lifecycle of DRE systems, from conception to deployment, ensuring that security measures are embedded within the design and operational phases rather than retrofitted post-implementation (Onukwulu et al., 2023; Zografopoulos, Hatziargyriou and Konstantinou, 2023).

In conclusion, while existing regulatory standards like NIST CSF, IEC 62443, and ISO/IEC 27001 support the cybersecurity governance of decentralized energy systems, they must be adapted and extended to ensure their efficacy in this rapidly evolving context. By addressing gaps in existing regulations and fostering collaborative efforts among various stakeholders, a more resilient, secure, and equitable decentralized energy future can be envisioned. The shared goal must be to build a decentralized energy landscape that not only meets current demands but also withstands the threats of tomorrow.

8. Strategic Recommendations

Securing decentralized renewable energy (DRE) systems in the face of increasing cyber threats necessitates a multidimensional strategy that extends beyond solely technological solutions. As the global energy ecosystem increasingly shifts towards decentralized models powered by renewable sources such as solar, wind, microgrids, and energy storage systems, cybersecurity measures must evolve correspondingly to address the complexities introduced by this transformation (Ekechukwu and Simpa, 2024), (Alvarez and Subburaj, 2023; . The inherent vulnerabilities associated with the integration of digital technologies and data-driven insights into DRE systems are significant. While these technologies present benefits such as improved sustainability, resilience, and accessibility, they simultaneously expose the systems to a variety of cyber threats (Cali et al., 2021; , (Khubrani and Alam, 2023).

In addressing these challenges, cross-sectoral collaboration emerges as a critical enabler of cybersecurity resilience in decentralized energy systems (Ekechukwu and Simpa, 2024). The interconnectedness of DRE infrastructure implies that no single entity can tackle all security challenges independently; effective cybersecurity requires coordinated efforts from governments, private companies, academia, and civil society (Cavus, 2024). These collaborative frameworks can facilitate the real-time exchange of information regarding threats, vulnerabilities, and effective mitigation strategies (Alvarez and Subburaj, 2023; , Provatas et al., 2023). Establishing regional or national cybersecurity centers can enhance this information-sharing capability, enabling stakeholders from various sectors, including energy, IT, and emergency services, to join forces in addressing cybersecurity concerns effectively (Cavus, 2024).

Moreover, the unification of cybersecurity standards across diverse DRE actors is crucial for achieving a consistent and effective security posture (Ekechukwu and Simpa, 2024). Many small-scale DRE providers lack the resources to implement comprehensive security protocols, often leading to fragmented practices that can create exploitable vulnerabilities (Khubrani and Alam, 2023). Standardizing cybersecurity benchmarks through inclusive dialogue and considering the constraints of various stakeholders, particularly in resource-constrained markets, can help ensure that all actors adhere to effective cybersecurity measures (Cavus, 2024).

Capacity building and workforce development play vital roles in sustaining long-term cybersecurity resilience in decentralized energy systems. There is a recognized shortage of skilled cybersecurity professionals in the energy sector, raising concerns about the field's overall ability to defend against cyber threats (Saravanan et al., 2024). Educational institutions need to integrate cybersecurity training into engineering and IT curricula while offering specialized training programs for existing professionals (Ajayi and Masunda, 2025). Meanwhile, incentivizing careers in energy cybersecurity through scholarships and public recognition can stimulate interest in this critical area (Cali et al., 2021; .

Integrating cybersecurity from the earliest design stages of DRE systems is another strategic imperative. Employing security-by-design principles ensures that security features are embedded in the architecture of the systems themselves, rather than being retrofitted later (Saravanan et al., 2024). This approach not only helps to minimize vulnerabilities but also supports cost-effective operations over the entire lifecycle of a DRE installation (Khubrani and Alam, 2023). Regular threat modeling and risk assessments during planning stages are essential to identify potential vulnerabilities and inform mitigation strategies that account for the full operational lifespan of the systems (Opirskyy and Petriv, 2024).

Furthermore, public-private partnerships (PPPs) and stakeholder engagement are crucial to a robust cybersecurity strategy for DRE systems. Governments can engage private sector innovations to leverage technological advancements while also providing regulatory frameworks and incentives that facilitate enhanced security measures (Cali et al., 2021; , Sakhare, 2024). Effective PPPs rely on mutual trust, clear objectives, and transparency to effectively manage cybersecurity risks (Ajayi and Masunda, 2025).

Finally, community engagement is critical, particularly in local energy initiatives that may cater to underserved populations. Empowering community stakeholders with knowledge and tools to manage cybersecurity risks fosters a shared responsibility for security practices (Švažas and Navickas, 2024). Educational outreach and local participation in policy consultations can demystify cybersecurity, enabling local actors to understand their roles in fortifying these systems against cyber threats (Waheed et al., 2025).

In conclusion, addressing the cybersecurity challenges of decentralized renewable energy systems requires a comprehensive strategy rooted in collaboration, education, foresight, and inclusivity. A concerted focus on cross-sectoral cooperation, capacity development, integral cybersecurity design, and robust stakeholder engagement will enhance the resilience and security of DRE systems as they become increasingly central to the clean energy transition.

9. Conclusion

Decentralized energy systems, powered by the increasing adoption of renewable energy sources and supported by digital technologies, represent a pivotal shift in the global energy landscape. While these systems offer significant advantages in terms of sustainability, resilience, and access, they also introduce complex cybersecurity challenges that must be addressed with urgency and foresight. The proliferation of interconnected devices, reliance on real-time data exchange, and integration of both operational and information technologies have expanded the potential attack surface across distributed renewable energy networks. From malware and ransomware attacks to unauthorized remote access, data breaches, and vulnerabilities in SCADA systems, the threat landscape is diverse and evolving. Furthermore, the integration of legacy infrastructure into hybrid energy systems, along with fragmented responsibilities and regulatory gaps, exacerbates these vulnerabilities, increasing the risk of energy theft, system manipulation, and grid instability.

In response to these challenges, a range of innovative solutions and strategic recommendations have emerged. Artificial intelligence and machine learning enhance anomaly detection and enable predictive analytics to anticipate potential breaches. Blockchain technologies offer tamper-proof mechanisms for secure data exchange and identity management. Zero-trust architectures and edge computing introduce layered defenses, while secure firmware update protocols and federated learning models ensure distributed and privacy-preserving threat detection. Beyond technological solutions, regulatory frameworks like NIST, IEC 62443, and ISO 27001 provide foundational guidance, though these must be adapted to the specific needs of decentralized systems. Equally important are strategic imperatives such as cross-sectoral collaboration, capacity building, integration of cybersecurity from the earliest design stages, and the fostering of public-private partnerships that align diverse stakeholders toward common security goals.

As decentralized energy systems become more integral to national and global energy strategies, proactive and adaptive cybersecurity measures will be crucial to ensuring their resilience and reliability. Cyber threats cannot be entirely eliminated, but through coordinated action, continuous innovation, and a shared commitment to securing energy infrastructure, the risks can be mitigated effectively. Governments, industry players, researchers, and communities must work together to embed cybersecurity into the very fabric of energy transition efforts. Only through such collective vigilance and preparedness can the promise of decentralized renewable energy be fully realized in a secure, stable, and sustainable manner.

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] Adeyemi, A. (2024). Promoting renewable energy through a decentralised electricity regulatory framework – an analysis of nigeria's electricity act 2023. Journal of Sustainable Development Law and Policy (The), 15(3), 399-421. https://doi.org/10.4314/jsdlp.v15i3.15

[10] Adil, A. M., and Ko, Y. (2016). Socio-technical evolution of Decentralized Energy Systems: A critical review and implications for urban planning and policy. Renewable and Sustainable Energy Reviews, 57, 1025-1037.

[11] 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

[12] Ajayi, R. and Masunda, M. (2025). Integrating edge computing, data science and advanced cyber defense for autonomous threat mitigation. International Journal of Science and Research Archive, 15(2), 063-080. https://doi.org/10.30574/ijsra.2025.15.2.1292

[13] Aldweesh, A. Y., Alauthman, M., Alateef, S., and Al-Qerem, A. (2025). Decentralized Energy Markets Transforming Energy Distribution and Trading With Blockchain Technology. In Blockchain Applications for the Energy and Utilities Industry (pp. 265-284). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-2439-5.ch012

[14] Alvarez, M. and Subburaj, V. (2023). Smart resilient cyber secure micro-grids: a study on cyber-attacks and resilience.. https://doi.org/10.36227/techrxiv.23995506.v1

[15] 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.

[16] 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.

[17] Bandaru, V., Kaligotla, V., Varma, U., Prasadaraju, K., and Sugumaran, S. (2024). A enhancing data security solutions for smart energy systems in iot-enabled cloud computing environments through lightweight cryptographic techniques. Iop Conference Series Earth and Environmental Science, 1375(1), 012003. https://doi.org/10.1088/1755-1315/1375/1/012003

[18] BARAN, B., Mamiş, M., and Alagöz, B. (2016). Utilization of energy from waste plants for microgrids., 1-5. https://doi.org/10.1109/sgcf.2016.7492431

[19] Bassey, K. E., Rajput, S. A., and Oyewale, K. (2024). Peer-to-peer energy trading: Innovations, regulatory challenges, and the future of decentralized energy systems. World Journal of Advanced Research and Reviews, 24, 172-186.

[20] Berghout, T., Benbouzid, M., and Amirat, Y. (2023). Towards resilient and secure smart grids against pmu adversarial attacks: a deep learning-based robust data engineering approach. Electronics, 12(12), 2554. https://doi.org/10.3390/electronics12122554

[21] Blaabjerg, F., Yang, Y., Ma, K., and Wang, X. (2015). Power electronics - the key technology for renewable energy system integration., 1618-1626. https://doi.org/10.1109/icrera.2015.7418680

[22] Bouzid, A., Guerrero, J., Chériti, A., Bouhamida, M., Sicard, P., and Benghanem, M. (2015). A survey on control of electric power distributed generation systems for microgrid applications. Renewable and Sustainable Energy Reviews, 44, 751-766. https://doi.org/10.1016/j.rser.2015.01.016

[23] Cali, U., Kuzlu, M., Sebastian-Cardenas, D. J., Elma, O., Pipattanasomporn, M., and Reddi, R. (2024). Cybersecure and scalable, token-based renewable energy certificate framework using blockchain-enabled trading platform. Electrical Engineering, 106(2), 1841-1852.

[24] 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

[25] Cavus, M. (2024). Integration smart grids, distributed generation, and cybersecurity: strategies for securing and optimizing future energy systems.. https://doi.org/10.20944/preprints202410.1225.v1

[26] Chu, Y., Kim, S., Song, Y., Yoon, Y., and Jin, Y. (2024). Blockchain-based rec system for improving the aspects of procedural complexity and cyber security. Ieee Access, 12, 40657-40667. https://doi.org/10.1109/access.2024.3370687

[27] Cioara, T., Pop, C., Zanc, R., Anghel, I., Antal, M., and Salomie, I. (2020). Smart grid management using blockchain: future scenarios and challenges., 1-5. https://doi.org/10.1109/roedunet51892.2020.9324874

[28] Dibie, E. U. (2024). Enhancing Cybersecurity for Renewable Energy with Quantum Algorithms and Cloud-Based AI. Journal of Advances in Mathematics and Computer Science, 39(11), 10-9734.

[29] 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

[30] 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

[31] Eltamaly, A., Alotaibi, M., Alolah, A., and Ahmed, M. (2021). Iot-based hybrid renewable energy system for smart campus. Sustainability, 13(15), 8555. https://doi.org/10.3390/su13158555

[32] Fu, R., Lichtenwalner, M., and Johnson, T. (2023). A review of cybersecurity in grid-connected power electronics converters: vulnerabilities, countermeasures, and testbeds. Ieee Access, 11, 113543-113559. https://doi.org/10.1109/access.2023.3324177

[33] Gavrilova, Z. (2022). Development of an algorithm for creating res-based facilities. Iop Conference Series Earth and Environmental Science, 979(1), 012184. https://doi.org/10.1088/1755-1315/979/1/012184

[34] Gligor, A., Cofta, P., Marciniak, T., and Dumitru, C. (2020). Challenges for the large-scale integration of distributed renewable energy resources in the next generation virtual power plants., 20. https://doi.org/10.3390/proceedings2020063020

[35] Gururaja, H., Hebbar, A., Poojary, A., Bharadwaj, A., and Rakshitha, B. (2024). Decentralized energy trading for grids using blockchain for sustainable smart cities. Int Res J Adv Engg Hub, 2(02), 134-141. https://doi.org/10.47392/irjaeh.2024.0025

[36] Hajri, N., Harthi, R., Pasam, G., and Natarajan, R. (2024). Iot and machine learning based green energy generation using hybrid renewable energy sources of solar, wind and hydrogen fuel cells. E3s Web of Conferences, 472, 01008. https://doi.org/10.1051/e3sconf/202447201008

[37] Hassan, Q., Viktor, P., Al-Musawi, T. J., Ali, B. M., Algburi, S., Alzoubi, H. M., ... and Jaszczur, M. (2024). The renewable energy role in the global energy Transformations. Renewable Energy Focus, 48, 100545.

[38] Hu, Y. and Wu, M. (2020). Kalman filtering based adaptive transfer in energy harvesting iot networks. Ieee Access, 1-1. https://doi.org/10.1109/access.2020.2995366

[39] Hussain, H. M., Narayanan, A., Nardelli, P. H., and Yang, Y. (2020). What is energy internet? Concepts, technologies, and future directions. IEEE access, 8, 183127-183145.

[40] Jamil, N., Qassim, Q., Bohani, F., Mansor, M., and Ramachandaramurthy, V. (2021). Cybersecurity of microgrid: state-of-the-art review and possible directions of future research. Applied Sciences, 11(21), 9812. https://doi.org/10.3390/app11219812

[41] Ji, T., Ye, X., Li, M., Wu, Q., and Yang, X. (2019). Operating mechanism for profit improvement of a smart microgrid based on dynamic demand response. Iet Smart Grid, 2(3), 364-370. https://doi.org/10.1049/iet-stg.2018.0082

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

[43] Johnson, J. T. (2017). Roadmap for photovoltaic cyber security (No. SAND2017-13262). Sandia National Lab.(SNL-NM), Albuquerque, NM (United States).

[44] Karagiannopoulos, S., Mylonas, C., Aristidou, P., and Hug, G. (2021). Active distribution grids providing voltage support: the swiss case. Ieee Transactions on Smart Grid, 12(1), 268-278. https://doi.org/10.1109/tsg.2020.3010884

[45] Kenneth, I. I., Peter, E. O., Onyinyechukwu, C., Aniekan, A. U., Bright, N., Valentine, I. I., and Adetomilola, V. F. (2024). Microgrid systems in US energy infrastructure: A comprehensive review: Exploring decentralized energy solutions, their benefits, and challenges in regional implementation.

[46] Khan, A., Shaikh, Z., Laghari, A., Bourouis, S., Wagan, A., and Ali, G. (2021). Blockchain-aware distributed dynamic monitoring: a smart contract for fog-based drone management in land surface changes. Atmosphere, 12(11), 1525. https://doi.org/10.3390/atmos12111525

[47] Khubrani, M. and Alam, S. (2023). Blockchain-based microgrid for safe and reliable power generation and distribution: a case study of saudi arabia. Energies, 16(16), 5963. https://doi.org/10.3390/en16165963

[48] Kumar, N., Chand, A., Malvoni, M., Prasad, K., Mamun, K., Islam, F., ... and Chopra, S. (2020). Distributed energy resources and the application of ai, iot, and blockchain in smart grids. Energies, 13(21), 5739. https://doi.org/10.3390/en13215739

[49] Li, B., Xu, Q., Lin, G., Lin, X., Zhao, R., Yu, L., ... and Pan, S. (2022). Research on plug-and-play technology of distributed renewable energy. Journal of Physics Conference Series, 2378(1), 012055. https://doi.org/10.1088/1742-6596/2378/1/012055

[50] Li, L., Zhou, P., and Wen, W. (2023). Distributed renewable energy investment: the effect of time-of-use pricing. The Energy Journal, 44(5), 251-276. https://doi.org/10.5547/01956574.44.5.luli

[51] Li, Z., Kang, J., Yu, R., Ye, D., Deng, Q., and Zhang, Y. (2017). Consortium blockchain for secure energy trading in industrial internet of things. Ieee Transactions on Industrial Informatics, 1-1. https://doi.org/10.1109/tii.2017.2786307

[52] Li, Z., Shahidehpour, M., and Liu, X. (2018). Cyber-secure decentralized energy management for iot-enabled active distribution networks. Journal of Modern Power Systems and Clean Energy, 6(5), 900-917. https://doi.org/10.1007/s40565-018-0425-1

[53] Maradin, D., Cerović, L., and Mjeda, T. (2017). Economic effects of renewable energy technologies. Naše Gospodarstvo/Our Economy, 63(2), 49-59. https://doi.org/10.1515/ngoe-2017-0012

[54] Mariam, L., Basu, M., and Conlon, M. (2013). A review of existing microgrid architectures. Journal of Engineering, 2013, 1-8. https://doi.org/10.1155/2013/937614

[55] Mohamed, N. (2024, June). Renewable Energy in the Age of AI: Cybersecurity Challenges and Opportunities. In 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE.

[56] Mohseni, M., Joorabian, M., and Ara, A. (2020). Distribution system reconfiguration in presence of internet of things. Iet Generation Transmission and Distribution, 15(8), 1290-1303. https://doi.org/10.1049/gtd2.12102

[57] Monteiro, L., Rodrigues, Y., and Souza, A. (2023). Cybersecurity in cyber–physical power systems. Energies, 16(12), 4556. https://doi.org/10.3390/en16124556

[58] Oh, M., Kim, B., Yun, C., Kim, C., Kim, J., Hwang, S., ... and Kim, H. (2022). Spatiotemporal analysis of hydrogen requirement to minimize seasonal variability in future solar and wind energy in south korea. Energies, 15(23), 9097. https://doi.org/10.3390/en15239097

[59] Olutimehin, A. (2025). Assessing the effectiveness of cybersecurity frameworks in mitigating cyberattacks in the banking sector and its applicability to decentralized finance (defi). Asian Journal of Research in Computer Science, 18(3), 130-151. https://doi.org/10.9734/ajrcos/2025/v18i3583

[60] Onukwulu, E., Agho, M., and Eyo-Udo, N. (2023). Decentralized energy supply chain networks using blockchain and iot. International Journal of Scholarly Research in Multidisciplinary Studies, 2(2), 066-085. https://doi.org/10.56781/ijsrms.2023.2.2.0055

[61] Ostapenko, O., Olczak, P., Koval, V., Hren, L., Matuszewska, D., and Postupna, O. (2022). Application of geoinformation systems for assessment of effective integration of renewable energy technologies in the energy sector of ukraine. Applied Sciences, 12(2), 592. https://doi.org/10.3390/app12020592

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

[63] 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.

[64] 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.

[65] Pan, B. (2024). Integrating blockchain as a service (baas) for bioenernet in the internet of things (iot) landscape. Applied and Computational Engineering, 70(1), 139-149. https://doi.org/10.54254/2755-2721/70/20240983

[66] Pazhoohesh, M., Allahham, A., Das, R., and Walker, S. (2021). Investigating the impact of missing data imputation techniques on battery energy management system. Iet Smart Grid, 4(2), 162-175. https://doi.org/10.1049/stg2.12011

[67] Preetha, R., S., R., Srisainath, R., and Divya, P. (2023). Integrating renewable energy sources with micro grid using iot and machine learning. E3s Web of Conferences, 387, 02004. https://doi.org/10.1051/e3sconf/202338702004

[68] Provatas, K., Tzannetos, I., and Vescoukis, V. (2023). Standards-based cyber threat intelligence sharing using private blockchains.. https://doi.org/10.15439/2023f6880

[69] Qi, J., Hahn, A., Lu, X., Wang, J., and Liu, C. (2016). Cybersecurity for distributed energy resources and smart inverters. Iet Cyber-Physical Systems Theory and Applications, 1(1), 28-39. https://doi.org/10.1049/iet-cps.2016.0018

[70] Rahman, M., Mukta, M., Asyhari, A., Moustafa, N., Patwary, M., Yousuf, A., ... and Gupta, B. (2022). Renewable energy re-distribution via multiscale iot for 6g-oriented green highway management. Ieee Transactions on Intelligent Transportation Systems, 23(12), 23771-23780. https://doi.org/10.1109/tits.2022.3203208

[71] Rehbein, J., Watson, J., Lane, J., Sonter, L., Venter, O., Atkinson, S., ... and Allan, J. (2020). Renewable energy development threatens many globally important biodiversity areas. Global Change Biology, 26(5), 3040-3051. https://doi.org/10.1111/gcb.15067

[72] Rehman, N., Ahmad, R., Waqar, A., and Mehmood, S. (2023). Analyzing the viability of decentralized renewable energy solutions for rural electrification in marginalized communities of pakistan. Proceedings of International Exchange and Innovation Conference on Engineering and Sciences (Ieices), 9, 267-271. https://doi.org/10.5109/7157983

[73] Rekeraho, A., Cotfas, D. T., Cotfas, P. A., Bălan, T. C., Tuyishime, E., and Acheampong, R. (2024). Cybersecurity challenges in IoT-based smart renewable energy. International Journal of Information Security, 23(1), 101-117.

[74] Roopesh, M., Nishat, N., Arif, I., and Bajwa, A. (2024). A comprehensive review of machine learning and deep learning applications in cybersecurity: an interdisciplinary approach. AJSTEME, 4(04), 37-53. https://doi.org/10.69593/ajsteme.v4i04.118

[75] Rossi, L. and Bianchi, G. (2024). Sustainable solutions: integrating renewable energy and electric vehicles for cleaner operations. Journal of Energy Research and Reviews, 16(3), 52-63. https://doi.org/10.9734/jenrr/2024/v16i3342

[76] Sakhare, E. (2024). A decentralized approach to threat intelligence using federated learning in privacy-preserving cyber security. jes, 19(3), 106-125. https://doi.org/10.52783/jes.658

[77] Salkuti, S. (2020). Comparative analysis of electrochemical energy storage technologies for smart grid. Telkomnika (Telecommunication Computing Electronics and Control), 18(4), 2118. https://doi.org/10.12928/telkomnika.v18i4.14039

[78] Saravanan, S., Kumar, N., Reddy, P., Sri, R., Ramesh, M., and Boopathi, S. (2024). Adaptive intelligence in microgrid systems., 158-180. https://doi.org/10.4018/979-8-3693-3735-6.ch010

[79] Shen, G., Xia, C., Li, Y., Shen, H., Meng, W., and Zhang, M. (2024). Traceable and privacy-preserving authentication scheme for energy trading in v2g networks. Ieee Internet of Things Journal, 11(4), 6664-6676. https://doi.org/10.1109/jiot.2023.3311800

[80] Sugunaraj, N., Balaji, S. R. A., Chandar, B. S., Rajagopalan, P., Kose, U., Loper, D. C., ... and Ranganathan, P. (2025). Distributed Energy Resource Management System (DERMS) Cybersecurity Scenarios, Trends, and Potential Technologies: A Review. IEEE Communications Surveys and Tutorials.

[81] Suo, D. (2022). Research on primary frequency modulation control strategy of wind power based on energy storage. Journal of Physics Conference Series, 2237(1), 012021. https://doi.org/10.1088/1742-6596/2237/1/012021

[82] Švažas, M. and Navickas, V. (2024). Energy transformation development strategies: evaluation of asset conversion in the regions. Energies, 17(7), 1612. https://doi.org/10.3390/en17071612

[83] Turab, N., Owida, H., and Al-Nabulsi, J. (2024). Harnessing the power of blockchain to strengthen cybersecurity measures: a review. Indonesian Journal of Electrical Engineering and Computer Science, 35(1), 593. https://doi.org/10.11591/ijeecs.v35.i1.pp593-600

[84] 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.

[85] 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.

[86] Unsal, D., Ustun, T., Hussain, S., and Önen, A. (2021). Enhancing cybersecurity in smart grids: false data injection and its mitigation. Energies, 14(9), 2657. https://doi.org/10.3390/en14092657

[87] Varela-Vaca, Á., Gasca, R., Carmona-Fombella, J., and Gómez-López, M. (2020). Amadeus., 1-12. https://doi.org/10.1145/3382025.3414952

[88] Vezzoli, C., Ceschin, F., Osanjo, L., M'Rithaa, M., Moalosi, R., Nakazibwe, V., ... and Diehl, J. (2018). Distributed/decentralised renewable energy systems., 23-39. https://doi.org/10.1007/978-3-319-70223-0_2

[89] Waheed, U., Khan, M., Masud, M., Jamshed, H., Jumani, T., and Malik, N. (2025). Blockchain-based, dynamic attribute-based access control for smart home energy systems. Energies, 18(8), 1973. https://doi.org/10.3390/en18081973

[90] Wang, S., Liu, Q., Yüksel, S., and Dınçer, H. (2019). Hesitant linguistic term sets-based hybrid analysis for renewable energy investments. Ieee Access, 7, 114223-114235. https://doi.org/10.1109/access.2019.2935427

[91] Yang, Q., Li, Z., Chen, Y., Zhu, Y., and Dou, Q. (2022). An investment efficiency evaluation model for distribution network with distributed renewable energy resources. Frontiers in Energy Research, 10. https://doi.org/10.3389/fenrg.2022.931486

[92] Yang, Q., Wang, H., Wang, T., Zhang, S., Wu, X., and Wang, H. (2021). Blockchain-based decentralized energy management platform for residential distributed energy resources in a virtual power plant. Applied Energy, 294, 117026. https://doi.org/10.1016/j.apenergy.2021.117026

[93] Yoo, D., Lee, S., Yang, S., Jeong, J., Lee, Y., and Shin, D. (2024). Enhancing cybersecurity in energy it infrastructure through a layered defense approach to major malware threats. Applied Sciences, 14(22), 10342. https://doi.org/10.3390/app142210342

[94] Zahid, H., Zulfiqar, A., Khan, M., Iqbal, S., and Mohamed, S. (2024). A review on socio-technical transition pathway to european super smart grid: trends, challenges and way forward via enabling technologies.. https://doi.org/10.31224/4068

[95] Zaman, D. and Mazinani, M. (2023). Cybersecurity in smart grids: protecting critical infrastructure from cyber attacks. SHIFRA, 2023, 86-94. https://doi.org/10.70470/shifra/2023/010.

[96] Zhang, T. (2021). Federated learning for internet of things: a federated learning framework for on-device anomaly data detection.. https://doi.org/10.48550/arxiv.2106.07976

[97] Zhang, W., Li, Z., Zhang, X., Tang, H., and Mei, S. (2022). Peer-to-peer transactive network with shared energy storage in distribution network.. https://doi.org/10.1145/3529299.3531482

[98] Zhong, J., Hu, X., Yüksel, S., Dınçer, H., and Ubay, G. (2020). Analyzing the investments strategies for renewable energies based on multi-criteria decision model. Ieee Access, 8, 118818-118840. https://doi.org/10.1109/access.2020.3005064

[99] Zhou, T., Shen, J., Ji, S., Ren, Y., and Yan, L. (2020). Secure and intelligent energy data management scheme for smart iot devices. Wireless Communications and Mobile Computing, 2020, 1-11. https://doi.org/10.1155/2020/8842885

[100] Zografopoulos, I., Hatziargyriou, N. D., and Konstantinou, C. (2023). Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations. IEEE Systems Journal, 17(4), 6695-6709.

[101] Zografopoulos, I., Hatziargyriou, N., and Konstantinou, C. (2022). Distributed energy resources cybersecurity outlook: vulnerabilities, attacks, impacts, and mitigations. https://doi.org/10.48550/arxiv.2205.11171

[102] Opirskyy, I. and Petriv, P. (2024). Effectiveness of blockchain logging and sso in cyber security mechanisms. Cybersecurity Education Science Technique, 4(24), 50-68. https://doi.org/10.28925/2663-4023.2024.24.5068