Journal of Cybersecurity and Privacy

MDPI

Article

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

Ayat-Allah Bouramdane

Laboratory of Renewable Energies and Advanced Materials (LERMA), College of Engineering and Architecture, International University of Rabat (IUR), IUR Campus, Technopolis Park, Rocade Rabat-Salé, Sala Al Jadida 11103, Morocco; ayatallahbouramdane@gmail.com

Abstract: Smart grids have emerged as a transformative technology in the power sector, enabling efficient energy management. However, the increased reliance on digital technologies also exposes smart grids to various cybersecurity threats and attacks. This article provides a comprehensive exploration of cyberattacks and cybersecurity in smart grids, focusing on critical components and applications. It examines various cyberattack types and their implications on smart grids, backed by real-world case studies and quantitative models. To select optimal cybersecurity options, the study proposes a multi-criteria decision-making (MCDM) approach using the analytical hierarchy process (AHP). Additionally, the integration of artificial intelligence (AI) techniques in smart-grid security is examined, highlighting the potential benefits and challenges. Overall, the findings suggest that "security effectiveness" holds the highest importance, followed by "cost-effectiveness", "scalability", and "Integration and compatibility", while other criteria (i.e., "performance impact", "manageability and usability", "compliance and regulatory requirements", "resilience and redundancy", "vendor support and collaboration", and "future readiness") contribute to the evaluation but have relatively lower weights. Alternatives such as "access control and authentication" and "security information and event management" with high weighted sums are crucial for enhancing cybersecurity in smart grids, while alternatives such as "compliance and regulatory requirements" and "encryption" have lower weighted sums but still provide value in their respective criteria. We also find that "deep learning" emerges as the most effective AI technique for enhancing cybersecurity in smart grids, followed by "hybrid approaches", "Bayesian networks", "swarm intelligence", and "machine learning", while "fuzzy logic", "natural language processing", "expert systems", and "genetic algorithms" exhibit lower effectiveness in addressing smart-grid cybersecurity. The article discusses the benefits and drawbacks of MCDM-AHP, proposes enhancements for its use in smart-grid cybersecurity, and suggests exploring alternative MCDM techniques for evaluating security options in smart grids. The approach aids decision-makers in the smart-grid field to make informed cybersecurity choices and optimize resource allocation.

Keywords: analytical hierarchy process; artificial intelligence; cyberattacks; cybersecurity; multi-criteria decision-making; smart grids

Citation: Bouramdane, A.-A. 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. *J. Cybersecur. Priv.* **2023**, *3*, 662–705. https://doi.org/10.3390/jcp3040031

Academic Editor: Danda B. Rawat

Received: 24 July 2023
Revised: 22 August 2023
Accepted: 31 August 2023
Published: 27 September 2023

1. Introduction

1.1. Research Motivation

The ever-growing reliance on interconnected technologies in modern power systems has led to the emergence of smart grids, promising enhanced efficiency and sustainability [1,2] to combat the impacts of climate change [3,4] (SMRY [5]) [6–11] [Chapter 5] [12] (SMRY [13]). However, this increased complexity also exposes these critical infrastructures to a myriad of cyber threats [14,15]. In light of the escalating frequency and sophistication

of cyberattacks on smart grids, a comprehensive understanding of their components, vulnerabilities, and potential impacts becomes imperative. This research endeavor seeks to address this pressing concern by delving into multifaceted dimensions. It aims to unravel the intricate interplay between smart-grid components and cyber vulnerabilities, analyze the diverse spectrum of cyber threats and their short-term and long-term consequences, investigate cascading effects on grid components, draw insights from real-world case studies, and develop quantitative models to assess cyberattack impacts. By exploring the techno–economic–safety–social implications of cybersecurity measures and delving into the application of artificial intelligence (AI) techniques, this study aspires to contribute valuable insights to the field of smart-grid cybersecurity, ultimately fortifying the resilience of critical energy infrastructure.

1.2. Existing Research

There is extensive research on cyberattacks and cybersecurity in smart grids, with numerous studies focusing on understanding the threats, vulnerabilities, and countermeasures.

Researchers have developed various models and frameworks to assess the potential cyber threats and risks in smart grids [16,17]. These studies aim to identify the attack vectors, vulnerabilities, and potential consequences to guide the development of effective cybersecurity strategies.

Research has been conducted on developing advanced techniques for detecting and preventing cyberattacks in smart grids [18,19]. This includes anomaly detection algorithms [20,21], intrusion detection systems (IDS) [22,23], machine-learning-based approaches [24,25], and data analytics to detect and respond to suspicious activities in real time [26,27]. Securing communication channels and implementing robust authentication mechanisms are crucial for protecting smart-grid infrastructure [28]. The research has focused on encryption algorithms [29], secure protocols [30], access control mechanisms [31,32], and authentication schemes to ensure the confidentiality, integrity, and authenticity of the data transmitted in smart grids [33,34].

The researchers have explored resilient system architectures for smart grids to mitigate the impact of cyberattacks [35,36]. This includes decentralized architectures [37,38], redundancy [39,40], distributed control systems [41,42], and fault-tolerant designs to ensure continuous operation and quick recovery from cyber incidents [43].

The studies have analyzed the existing security standards and regulations applicable to smart grids and proposed improvements [44]. The researchers have also examined the gaps and challenges in standardization efforts [45], aiming to establish comprehensive security guidelines [46] and best practices specific to smart-grid deployments [47,48].

Understanding the role of insider threats [22,49] and human factors [50,51] in smart-grid cybersecurity is an emerging area of research. These studies investigate the impact of human behavior [52,53], social engineering [54,55], training and awareness programs [56,57], and policy frameworks to address the human element in cybersecurity [58,59]. Given the large amount of data generated by smart grids, the research has focused on secure data management, privacy-preserving techniques, and anonymization approaches to protect sensitive information while enabling data analysis for grid optimization and energy management [60,61]. The research has explored incident response and recovery strategies in smart grids [62,63]. This includes developing effective incident handling procedures, recovery mechanisms, backup systems, and disaster recovery plans to minimize the impact of cyber incidents and ensure the rapid restoration of services. The research has investigated the importance of threat intelligence and information sharing mechanisms to enhance cybersecurity in smart grids. This includes the development of collaborative platforms, information sharing networks, and sharing protocols to facilitate timely and effective responses to emerging cyber threats [64,65].

There is a growing body of research on the application of artificial intelligence (AI) in cybersecurity for smart grids [66]. AI techniques, such as machine learning (ML) [67] and deep learning [68,69], have shown promise in enhancing the security of smart-grid systems.

The researchers have explored the use of AI algorithms to detect and predict cyber threats in smart grids. ML models are trained on historical data to identify patterns and anomalies that indicate potential attacks or malicious activities [70,71]. AI-based anomaly detection techniques are being developed to identify unusual behavior or deviations from normal operations in smart grids. These methods leverage machine learning algorithms to establish baseline behavior and detect abnormal activities that may signify a cyberattack [72,73]. AI is being applied to enhance the intrusion detection systems in smart grids. Machine learning algorithms can analyze network traffic and system logs to identify and classify potential intrusions or suspicious activities [74,75]. AI techniques enable intelligent decision-making in real-time security operations [76,77]. This includes automated response mechanisms [78], adaptive access control [79,80], and dynamic security policies that adjust based on the evolving threats and system conditions [81]. AI is employed to ensure secure communication and protect data privacy in smart-grid networks [82,83]. AI algorithms can be used to encrypt sensitive data [84], authenticate communication channels [85], and identify potential vulnerabilities in the communication infrastructure [86]. The researchers are studying adversarial machine learning techniques to identify and mitigate attacks targeting AI-based cybersecurity systems in smart grids. Adversarial models simulate attack scenarios to test the robustness of AI algorithms and develop countermeasures [87].

1.3. Knowledge Gaps

The existing research has identified several knowledge gaps in the fields of cyberattacks and cybersecurity in smart grids.

First, there is a need for a comprehensive overview of smart-grid components and applications, including the identification of vulnerable components and potential types of cyberattacks. Furthermore, understanding the short-term and long-term techno–economic–safety–social impacts of cyberattacks on smart grids, including the cascading effects on interconnected components, is crucial. The real-world case studies of cyberattacks on operational smart grids and the development of quantitative models and metrics to assess the impacts of cyberattacks are necessary. Additionally, the implications of cybersecurity measures on operational smart grids and the development of quantitative models and metrics to assess the implications of cybersecurity on smart grids need further exploration.

Second, research on the use of the analytical hierarchy process (AHP) to solve multi-criteria decision-making (MCDM) problems in the context of cybersecurity in smart grids is relatively limited, as AHP is not commonly associated with cybersecurity specifically. However, AHP is a widely used decision-making tool that can be applied to various domains—such as renewable energy integration [88], the performance of residential energy management control algorithms [89], a day-ahead scheduling of electric vehicles and electrical storage systems in smart homes [90], optimization of the advanced metering infrastructure (AMI) customer ecosystem [91], including cybersecurity [92,93]. Therefore, the optimal cybersecurity options for smart grids, such as access control, authentication, encryption, intrusion detection systems (IDS), firewalls, security information and event management (SIEM), and others, need to be evaluated based on multiple criteria. These criteria include security effectiveness, scalability, integration, and compatibility; performance impact; cost-effectiveness; manageability and usability; compliance and regulatory requirements; resilience and redundancy; vendor support and collaboration; future readiness; network segmentation; patch management; threat intelligence; and vendor and supply chain security.

Third, understanding the potential and challenges of AI techniques, such as machine learning, deep learning, natural language processing (NLP), genetic algorithms (GA), fuzzy logic, expert systems, swarm intelligence, Bayesian networks, and hybrid approaches, is important. The use of MCDM-AHP to find the optimal cybersecurity option that in-

corporates AI techniques and methods needs to be explored. The criteria for evaluation may include security effectiveness, scalability, integration, and compatibility; performance impact; cost-effectiveness; manageability and usability; compliance and regulatory requirements; resilience and redundancy; vendor support and collaboration; future readiness; network segmentation; and explainability and transparency.

The advantages and drawbacks of employing AHP to assess cybersecurity options in smart grids need to be discussed. Furthermore, it is essential to propose enhancements for its application in smart-grid cybersecurity and to explore alternative MCDM techniques for evaluating security options in smart grids.

1.4. Research Questions

This study aims to address this existing knowledge gap (Section 1.3) and make a significant contribution by exploring the following research questions:

1. **(a)** What are the components and applications of smart grids, and how do they contribute to the vulnerability of cyberattacks? **(b)** What are the different types of cyberattacks that can target smart grids, and what are their short-term and long-term technological, economic, safety, and social impacts? **(c)** How do cyberattacks on smart grids result in cascading effects and interconnected impacts on various grid components? **(d)** What are the real-world case studies of cyberattacks on operational smart grids, and what can be learned from them? **(e)** How can quantitative models and metrics be developed to assess the impacts of cyberattacks on smart grids? **(f)** What are the short-term and long-term techno–economic–safety–social implications of cybersecurity in smart grids, emphasizing the importance of confidentiality, integrity, and availability? **(g)** How do cybersecurity measures implemented in operational smart grids affect their real-world implications? **(h)** How can quantitative models and metrics be used to assess the implications of cybersecurity in smart grids?
2. **(a)** What are the main criteria for evaluating cybersecurity options in smart grids? **(b)** What are the key cybersecurity options for protecting smart-grid infrastructure? **(c)** How can AHP be employed to assess and prioritize these cybersecurity options based on multiple criteria?
3. **(a)** What are the differences between artificial intelligence (AI) and machine learning (ML), and how do they apply to cybersecurity in smart grids? **(b)** What is the potential of AI techniques for enhancing smart-grid cybersecurity? **(c)** What are the challenges associated with implementing AI techniques in smart-grid cybersecurity, and how can they be addressed? **(d)** How can MCDM-AHP be used to find the optimal cybersecurity option that incorporates AI techniques and methods? **(e)** What are the key criteria for evaluating AI-based cybersecurity options in smart grids using MCDM-AHP?

We also discuss both the strengths and constraints of using AHP for MCDM in assessing cybersecurity options in smart grids. Additionally, we suggest improvements to its application in smart-grid cybersecurity and explore alternative MCDM methods for assessing security options in smart grids.

1.5. Methodology

The methodology employed in this study encompasses four main areas related to cybersecurity in smart grids. First, it involves conducting a comprehensive analysis of smart-grid components and applications, examining the various types of cyberattacks that target these systems, and assessing their short-term and long-term impacts on the technological, economic, safety, and social aspects of smart grids. Real-world case studies are investigated to provide practical insights into the effects of cyberattacks on operational smart grids (Section 3.1). Second, the study uses the analytical hierarchy process (AHP) as a multi-criteria decision making (MCDM) technique to determine the optimal cybersecurity option. A set of cybersecurity measures, such as access control, authentication, encryption, IDPS, firewalls, SIEM, vulnerability assessment, and others, are evaluated based on mul-

tiple criteria, including security effectiveness, scalability, integration, and compatibility; performance impact; cost-effectiveness; manageability and usability; compliance and regulatory requirements; resilience and redundancy; vendor support and collaboration; future readiness; network segmentation; patch management; threat intelligence; and vendor and supply chain security (Section 3.2). Third, the research explores the difference between artificial intelligence (AI) and machine learning (ML), addressing their potential and challenges. AHP-MCDM is applied to find the optimal cybersecurity option that incorporates AI techniques and methods, such as machine learning, deep learning, natural language processing (NLP), genetic algorithms (GA), fuzzy logic, expert systems, swarm intelligence, Bayesian networks, and hybrid approaches. The criteria considered in this evaluation include security effectiveness, scalability, integration, and compatibility; performance impact; cost-effectiveness; manageability and usability; compliance and regulatory requirements; resilience and redundancy; vendor support and collaboration; future readiness; network segmentation; explainability; and transparency (Section 3.3). Finally, the study discusses the advantages (Section 4.1) and limitations of AHP-MCDM (Section 4.2), suggests improvements to its application in smart-grid cybersecurity (Section 4.3), and explores other MCDM techniques (Section 4.4) that can be implemented to assess cybersecurity options in smart grids.

1.6. Practical Implications

This study provides insights for researchers, policymakers, and practitioners in the field of smart-grid cybersecurity, guiding them in understanding the challenges, making informed decisions, and implementing effective cybersecurity measures.

1.7. Outline

This article follows a structured outline, starting with an introduction (Section 1) that establishes the research motivation (Section 1.1), existing studies (Section 1.2), knowledge gaps (Section 1.3), research questions (Section 1.4), methodology overview (Section 1.5), and practical implications (Section 1.6). In the methodology section (Section 2), the research approach and the methodology employed are described in detail. The application of the analytical hierarchy process (AHP) as a decision-making framework (Section 2.2) for evaluating cybersecurity options in smart grids is explained, emphasizing its ability to consider multiple criteria and prioritize options. The results section (Section 3) presents the key findings obtained through the application of the methodology described earlier. The discussion section (Section 4) delves deeper into the implications and significance of the research findings. It examines the advantages and limitations of the methodology employed, addressing potential challenges and areas for improvement. The conclusion section (Section 5) summarizes the key findings, insights, and implications discussed throughout the article.

2. Methodology

The methodology employed in this study combines the principles of multi-criteria decision-making (MCDM) with artificial intelligence (AI) techniques to address the challenges of cyberattacks in smart grids and facilitate the selection of effective cybersecurity options.

First, a comprehensive analysis of the cybersecurity landscape in smart grids is conducted to identify the key challenges and potential threats. This analysis includes an examination of the different types of cyberattacks, their potential impacts on smart-grid infrastructure, and the specific vulnerabilities that need to be addressed (Section 3.1).

Next, a set of relevant criteria is identified to evaluate the cybersecurity options available for smart grids. These criteria encompass factors such as security effectiveness, scalability, integration, and compatibility; performance impact; cost-effectiveness; manageability and usability; compliance with regulatory requirements; resilience and redundancy; vendor support and regulation; and future readiness. The analytical hierarchy process

(AHP) (Section 2.2) is then used as the core methodology for the MCDM process. AHP allows for the systematic comparison and prioritization of the cybersecurity options based on their performance against each criterion (Section 3.2).

To incorporate AI techniques, MCDM-AHP is applied to choose between different AI options. These options include machine learning, deep learning, swarm intelligence, Bayesian networks, etc. (Section 3.3).

Overall, the methodology employed in this study combines MCDM principles, and AI techniques to create a robust framework for evaluating and selecting cybersecurity options in smart grids, thereby mitigating the risks associated with cyberattacks and safeguarding the integrity and security of smart grid systems.

2.1. Motivation for Employing MCDM-AHP in Enhancing Cybersecurity Resilience for Smart Grids

The use of multi-criteria decision making (MCDM) with the analytical hierarchy process (AHP) methodology in smart-grid cybersecurity is driven by its effectiveness in handling the complex and diverse security decisions within this critical field. Smart grids involve interconnected elements, numerous stakeholders, and a wide range of potential cybersecurity risks. MCDM-AHP provides a structured way to assess and prioritize cybersecurity choices by considering multiple criteria, encompassing both technical and non-technical factors.

For smart-grid cybersecurity, MCDM-AHP enables a systematic evaluation of various security measures, considering aspects such as effectiveness, feasibility, cost, and potential impacts. This approach integrates expert insights, quantifies qualitative criteria, and accounts for the interdependencies between different security options. By utilizing MCDM-AHP, the intricate landscape of smart-grid cybersecurity can be navigated, ensuring a well-informed decision-making process that aligns with the ever-changing nature of cyber threats and grid operations.

To sum up, the motivation for using MCDM-AHP in smart-grid cybersecurity stems from its capacity to offer a robust, comprehensive, and adaptable framework for assessing and selecting optimal cybersecurity strategies. This methodology aids in addressing the complex challenges presented by cybersecurity threats in smart grids, ultimately contributing to improved grid resilience, reliability, and security.

2.2. Theoretical Framework of Multi-Criteria Decision-Making (MCDM) Using the Analytical Hierarchy Process (AHP)

Multi-criteria decision-making (MCDM) is a decision-making approach that addresses complex problems involving multiple criteria and options. In traditional decision-making, a single criterion is often used to evaluate alternatives, but MCDM recognizes that real-world decisions are influenced by multiple factors. MCDM provides a systematic framework for evaluating and comparing alternatives based on multiple criteria simultaneously, taking into account their relative importance and interdependencies. It helps decision-makers incorporate diverse perspectives, consider trade-offs, and make informed decisions that align with their goals and preferences [94].

MCDM is applied across various fields due to its ability to handle complex decision problems with multiple criteria and alternatives. Some of the fields where MCDM has found extensive applications include business and management (i.e., project or supplier selection, investment decisions, facility location decisions and risk management, etc.) [95], industry [96,97], economics [98,99], environment [100], water treatment [101], transportation and logistics (i.e., route planning, network design, etc.) [102,103], renewable energy development [104,105] and planning [106,107]—such as suitable areas for photovoltaic and concentrated solar power [108], onshore wind [109], offshore wind [110], and offshore floating photovoltaic systems [111]—, healthcare and medicine (i.e., patient treatment or medical equipment selection, resource allocation in hospitals, etc.) [112,113], and education (i.e., performances, teachers' recruitment process, etc.) [114,115].

In the energy sector, particularly in the context of smart grids, various multi-criteria approaches are employed to address complex decision problems [116]. While the analytical hierarchy process (AHP) is recognized as a significant and widely used MCDM technique [117,118], its application specifically to cybersecurity in smart grids is relatively limited (Section 1.3).

AHP provides a structured and systematic approach to decision-making when multiple criteria or factors need to be considered. It allows decision-makers to evaluate and prioritize alternatives based on their relative importance and preferences [119,120]. Thomas Saaty was the one who initially proposed this technique [121,122], and it has been considerably improved since then. In AHP, the problem is constructed as a hierarchy and broken down into elements. The overall goal is located at the top level, the criteria and sub-criteria are at the middle level, and the alternatives are at the bottom of the hierarchy [123,124].

The use of AHP typically involves five fundamental steps to facilitate a structured decision-making process. These steps are as follows [125,126]:

1. **Define the decision problem and establish the hierarchy**: The first step in using AHP is to decompose the decision-making problem into a hierarchy of elements, with the goal to be achieved at the highest level, criteria and sub-criteria at intermediate levels, and alternatives to be considered at the lowest level. This hierarchical structure (Figure 1) helps organize and decompose the problem into manageable components.

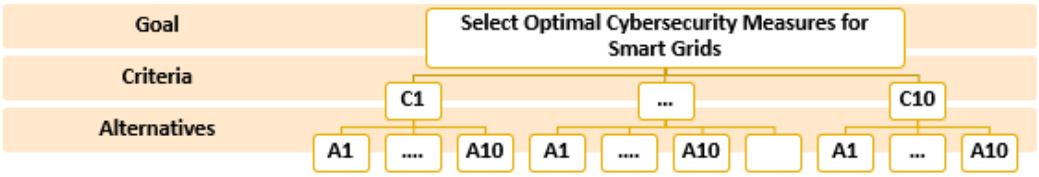

Figure 1. Hierarchical evaluation framework for cybersecurity measures in smart grids, which includes distinct levels: a top-level overarching goal, intermediate evaluation criteria, and a bottom level containing various cybersecurity measures. Source: The author's own elaboration.

2. **Perform Pairwise Comparisons**: Pairwise comparison matrices are performed between elements at the same level of the hierarchy. These matrices capture the relative importance or preference of one element compared to another at a specific level. Specifically, pairwise comparison matrices are performed:
   - **Between Criteria**: decision-makers compare the criteria to determine their relative importance in achieving the overall goal. Each criterion is compared to every other criterion to assess their relative weights or priorities. The resulting pairwise comparison matrix represents the importance of criteria relative to one another.
   - **Between Alternatives**: decision-makers compare the alternatives against each other based on specific criteria. Each alternative is compared to every other alternative to evaluate its relative performance or desirability. The pairwise comparison matrix represents the preference of alternatives relative to one another for each criterion.
   - **Between Criteria and Sub-Criteria**: In some cases, the AHP hierarchy may include sub-criteria within each criterion. Pairwise comparison matrices can also be performed between the criteria and their respective sub-criteria. This allows decision-makers to assess the relative importance or preference of each sub-criterion within its parent criterion.

   These matrices serve as the basis for deriving priority weights and aggregating preferences within the AHP process.

Let C be the pairwise comparison matrix with elements c_{ij} representing the importance of criterion i compared to criterion j (1).

$$C = [C_{ij}]_{nxn} = \begin{bmatrix} c_{11} & c_{12} & c_{13} & \dots & c_{1n} \\ c_{21} & c_{22} & c_{23} & \dots & c_{2n} \\ \vdots & \dots & \dots & \dots & \vdots \\ c_{n1} & c_{n2} & c_{n3} & \dots & c_{nn} \end{bmatrix} \quad (1)$$

C_{ij} is the pairwise comparison rating for the ith and the jth criteria. n is the number of criteria.

The matrix C is reciprocal, meaning that the elements satisfy the property of reciprocity: $C_{ij} = 1/C_{ij}$ for all i and j. Reciprocity ensures that the judgments made in the pairwise comparisons are consistent. It implies that if element A is considered, for example, twice as important as element B, then B is considered half as important as A.

Additionally, the diagonal elements of the pairwise comparison matrix are in unity ($C_{ij} = 1$ for $i = j$). This indicates that an element is perfectly equal to itself, which is a logical requirement.

The entries in the pairwise comparison matrix C are typically taken from a ratio-scale based on the values 1/9 to 9 [121]. In fact, in the AHP, decision-makers assign numerical values to represent the relative importance or preference between elements in the pairwise comparisons. The scale is as follows: 1 (equally important), 3 (moderately more important), 5 (strongly more important), 7 (very strongly more important), 9 (absolutely more important). The reciprocals of these values are used for the reverse comparisons: 1/3, 1/5, 1/7, and 1/9. Table 1 shows Saaty's comparison scale, also known as the AHP scale of relative importance. It includes the rating scale, its definition, and an explanation of each rating.

Table 1. Saaty's comparison scale [121]. Decision-makers use these ratings to express the relative importance or preference between elements in pairwise comparisons (1).

Rating Scale	Definition	Explanation
1	Equally preferred	Both elements are considered to have equal importance or preference. There is no significant difference between them.
3	Moderately preferred	One element is moderately preferred or has a moderate advantage over another. The difference in importance or preference is noticeable but not substantial.
5	Strongly preferred	One element is strongly preferred or has a significant advantage over another. The difference in importance or preference is substantial and clearly noticeable.
7	Very strongly preferred	One element is very strongly preferred or has a substantial advantage over another. The difference in importance or preference is considerably large and easily distinguishable.
9	Absolutely preferred	One element is absolutely preferred or has an overwhelming advantage over another. The difference in importance or preference is extremely significant and essentially indisputable.
2, 4, 6, 8	Intermediate values between the two adjacent judgment	When compromise is needed

Pairwise comparisons can be performed using different methods, such as direct judgment, expert opinions, surveys, or historical data. The key is to elicit and capture the decision-makers' subjective judgments regarding the relative importance or preference of the elements being compared.

3. **Calculate Priority Weights**: Calculate the priority weights for each element in the hierarchy based on the pairwise comparison judgments. Several methods can be used,

including the geometric mean and the eigenvector method. The priority weights reflect the relative importance of each element within its level and enable quantitative comparison and analysis.
Let g_i be the geometric mean of the ith row in the pairwise comparison matrix C. It can be calculated as (2).

$$g_i = (c_{i1} * c_{i2} * \ldots * c_{in})^{1/n} \tag{2}$$

Let N be the normalized pairwise comparison matrix obtained by dividing each element of C by its corresponding geometric mean. The normalized element is given by (3).

$$n_{ij} = \frac{c_{ij}}{g_i} \tag{3}$$

Let A be the average column vector obtained by calculating the average of each column in the normalized pairwise comparison matrix N. The average of the jth column is given by (4).

$$a_j = (1/n) * (n_{1j} + n_{2j} + \ldots + n_{nj}) \tag{4}$$

The average column vector A represents the relative weights of each criterion. The weights w_i can be obtained by normalizing the average column vector (5).

$$w_i = a_i/(a_1 + a_2 + \ldots + a_n) \tag{5}$$

Let O be the matrix representing the options evaluated. Each row o_k corresponds to the values of the options for each criterion. The weighted sum for the kth option is calculated as (6).

$$s_k = (w_1 * o_{k1}) + (w_2 * o_{k2}) + \ldots + (w_n * o_{kn}) \tag{6}$$

Calculate the eigenvalue (λ_{max}) and the corresponding eigenvector (V) of the pairwise comparison matrix C. The eigenvalue equation is given by (7).

$$(C - \lambda_{max} * I) * V = 0 \tag{7}$$

λ_{max} represents the eigenvalue that we want to solve for; I is the identity matrix of size nxn; V is the eigenvector associated with the eigenvalue (λ_{max}). To solve for the eigenvalue (λ_{max}), we need to find the values of λ) that satisfy the above Equation (7). This can be carried out using numerical methods or software tools that can compute eigenvalues.

4. **Check for Consistency**: Assess the consistency of the pairwise comparison judgments. Inconsistencies occur when the assigned values do not meet certain mathematical properties. Calculate the consistency ratio (CR) using a consistency index (CI) and a random index (RI). If the CR exceeds a predefined threshold (e.g., 0.10), further examination or adjustments to the pairwise comparisons are needed. The consistency index (CI) is calculated using the formula (8):

$$CI = \frac{\lambda_{max} - n}{(n-1)} \tag{8}$$

where λ_{max} is the maximum eigenvalue and n is the number of criteria.
The random index (RI) is a reference value based on the size of the matrix (Table 2). It helps determine whether the consistency of the pairwise comparison matrix is acceptable or not.

Table 2. Random Consistency Index (RI).

n	1	2	3	4	5	6	7	8	9	10	11
RI	0	0	0.58	0.90	1.12	1.24	1.32	1.41	1.45	1.49	1.51

The consistency ratio (CR) is the ratio of the CI to the RI. It is calculated as (9):

$$CR = \frac{CI}{RI} \tag{9}$$

If the CR is less than or equal to 0.1, the consistency of the matrix is considered acceptable. If the CR exceeds 0.1, the consistency should be re-evaluated (Figure 2).

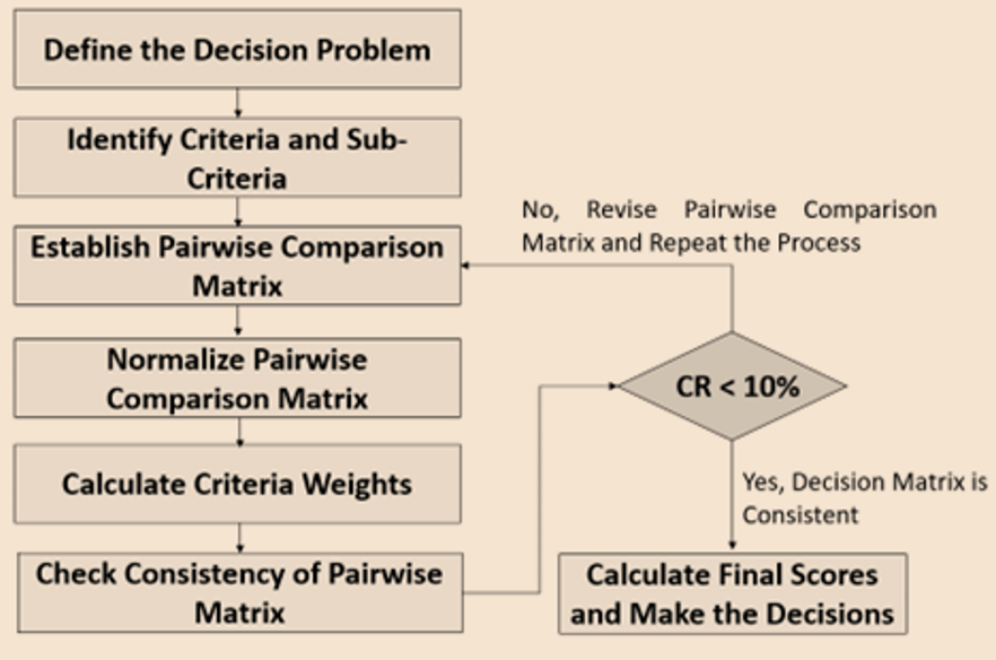

Figure 2. Analytical hierarchy process (AHP) algorithm: A methodical approach for assessing and ranking cybersecurity measures in smart grids. Source: the author's own elaboration.

5. **Interpretation and Decision-Making**: By examining the priority weights, it becomes apparent which criteria are more influential in achieving the overall goal. Moreover, the alternatives with higher weighted scores indicate better overall performance or desirability.

3. Results

In this section, we delve into a comprehensive examination of the various aspects related to cybersecurity in smart grids. First, we provide an overview of smart grids, including their components and applications (Section 3.1.1). We explore the different types of cyberattacks (Section 3.1.2) and their potential short-term and long-term impacts on smart grids, considering their techno–economic–safety–social dimensions (Section 3.1.3). This examination encompasses the identification of vulnerable components, the cascading effects of cyberattacks on smart-grid elements (Section 3.1.4), and real-world case studies of operational smart grids that have been targeted (Section 3.1.5). Additionally, we discuss the quantitative models and metrics that enable the assessment of cyberattack impacts (Section 3.1.5) and the associated implications for smart-grid cybersecurity (Sections 3.1.7–3.1.10).

Moving forward, we address the second point by investigating the utilization of the analytical hierarchy process (AHP) in solving the multi-criteria decision making (MCDM)

problem for selecting the optimal cybersecurity option. We explore a range of cybersecurity measures such as access control, encryption, intrusion detection and prevention systems, firewalls, security incident responses, and more. These measures are evaluated based on multiple criteria, including security effectiveness, scalability, performance impact, cost-effectiveness, compliance with regulatory requirements, resilience, and vendor support (Section 3.2).

Furthermore, we explore the differences between artificial intelligence (AI) and machine learning (ML) and their potential contributions to cybersecurity in smart grids (Section 3.3.1). By integrating AI techniques and methods such as machine learning, deep learning, genetic algorithms, and Bayesian networks, we aim to identify the optimal cybersecurity option. The application of the MCDM-AHP approach enables us to assess the performance of different AI-based techniques against multiple criteria such as security effectiveness, scalability, explainability, and transparency (Section 3.3.2).

Through this exploration, we aim to provide insights into the selection of the most suitable cybersecurity option that effectively addresses the challenges faced in securing smart grids.

3.1. Cyberattacks in Smart Grids: Challenges and Implications of Cybersecurity

3.1.1. Overview of Power Generation, Transmission, and Distribution in Smart Grids

A smart grid is an advanced electrical power system that integrates cutting-edge technologies, sensors, and communication networks to optimize the efficiency, reliability, and sustainability of electricity generation, transmission, distribution, and consumption (Figure 3). Its objective is to revolutionize the conventional grid into a dynamic, automated, and adaptable network for enhanced performance [127,128].

Smart grids operate in two distinct modes: stand-alone and grid-tied [129,130]. In stand-alone mode, the smart grid functions independently, generating and managing electricity locally, often in remote areas, using sources such as solar and wind, along with energy storage [131]. In grid-tied mode, the smart grid is interconnected with the main power grid, enabling bidirectional electricity flow and supporting stability through imports and exports of power. The choice between these modes depends on factors such as location, infrastructure, energy goals, and regulations [132].

Power generation within smart grids encompasses a diverse mix of sources, including traditional fossil fuel plants and renewables such as solar, wind, hydro, and biomass. The concept of distributed generation is central to smart grids, fostering smaller-scale facilities close to consumption points such as rooftop solar panels and micro-hydro setups. This approach bolsters grid resilience, reduces transmission losses, and encourages private investment, diversifying ownership and financing beyond utilities [133,134]. Energy storage systems, including batteries and pumped hydro, play a pivotal role by storing the excess electricity for peak demand, thus, enhancing grid stability and enabling the integration of renewables [12,135]. Smart grids employ demand–response programs to actively manage electricity consumption, allowing users to voluntarily adjust usage during peak demand or grid stress, promoting grid stability and energy efficiency. Home energy management systems enable the remote control of smart appliances via user-friendly interfaces, optimizing energy consumption based on preferences and occupancy patterns [136,137]. Time-of-use pricing models incentivize off-peak consumption [138], while smart grids also facilitate electric vehicle charging infrastructure and vehicle-to-grid technology, enabling EVs to contribute back to the grid [139]. Employing technologies such as supervisory control and data acquisition (SCADA) [140] and the Internet of Things (IoT) [141], smart grids optimize power generation through real-time data collection, analytics, and predictive algorithms, enhancing grid management and decision-making for load forecasting, demand management, and maintenance scheduling.

Smart grids optimize long-distance electricity transportation by employing high-voltage transmission lines, thereby minimizing losses [142]. These grids integrate sensors along these lines to gather real-time data on parameters such as power flow and voltage, which is transmitted to control centers for proactive analysis. Wide-area monitoring systems (WAMS) employing phasor measurement units (PMUs) enable comprehensive grid behavior monitoring, aiding with a swift response to disturbances [143,144]. The advanced control systems within smart grids optimize power flow and voltage, leveraging real-time data and mathematical algorithms. These systems adjust power flows, reduce losses, and maintain grid stability. Flexible AC transmission systems (FACTS) devices, such as static VAR compensators (SVC) and unified power flow controllers (UPFC), enhance voltage stability and power flow control [145,146]. The seamless coordination among power generation, transmission, and distribution is enabled by robust communication networks and information communication technologies (ICTs) [81,147].

Smart grids encompass substations that receive high-voltage electricity, stepping it down for distribution through networks involving overhead lines, underground cables, and transformers [148]. Utilizing distribution automation (DA) systems, smart grids monitor and control distribution networks in real time, leveraging data such as voltage and current to optimize operations, detect faults, and ensure prompt responses [149]. Fault detection mechanisms integrated into smart grids swiftly identify issues, enabling self-healing capabilities to isolate faults and reconfigure the network for uninterrupted power supply, enhancing distribution reliability and reducing outages [150,151]. The deployment of advanced metering infrastructure (AMI), featuring smart meters and communication infrastructure, is pivotal for power distribution. Smart meters facilitate two-way communication between utilities and consumers, offering real-time insights into consumption, load profiles, and power quality. These data empower utilities to optimize distribution, implement demand response programs, and enhance customer services [152,153].

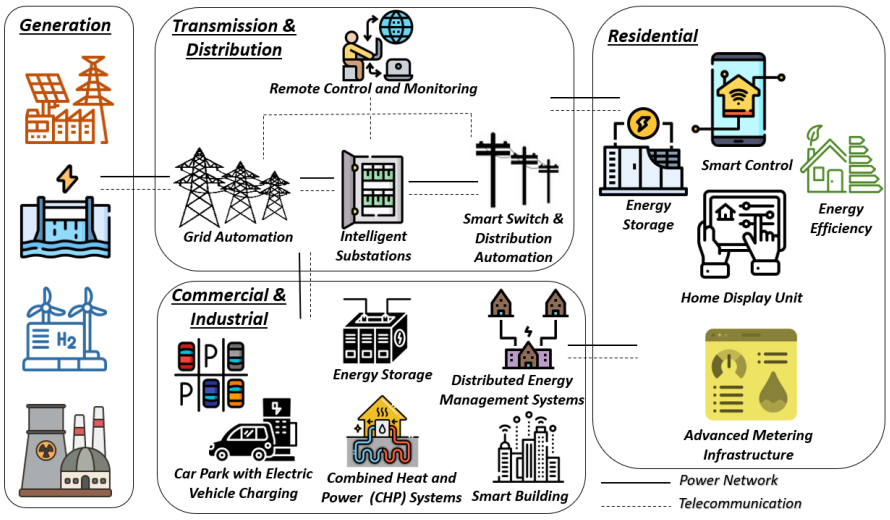

Figure 3. A schematic representation of the smart grid. Source: Own Elaboration.

3.1.2. Exploring the Landscape of Cyberattacks in Smart Grids

Smart grids are susceptible to various types of cyberattacks (Figure 4) that target their interconnected systems and infrastructure [154]. Here are some common types of cyberattacks in smart grids [155,156]:

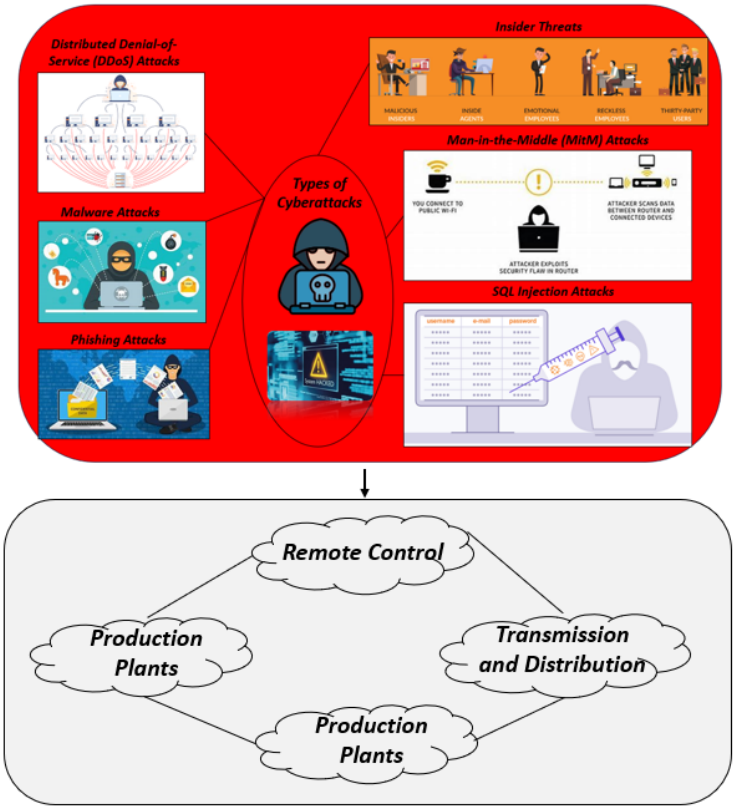

Figure 4. A visual representation depicting the interconnected relationship between production plants, transmission and distribution lines, consumption, and the integration of information, control, and communication technologies. Source: Own Elaboration.

- **Denial-of-Service (DoS) Attacks**: These attacks aim to temporarily make the targeted system inaccessible to legitimate users by overwhelming the smart grid's resources, such as communication networks or control systems, with an excessive volume of requests and flooding them with a high volume of traffic, launched from a single device. This disrupts the grid's operations and may result in service outages [157].
- **Distributed Denial-of-Service (DDoS) Attacks**: Similar to DoS attacks, DDoS attacks involve multiple compromised devices, located worldwide, forming a botnet that collectively overwhelms the grid's resources. DDoS attacks are more challenging to mitigate due to their distributed nature [158,159].
- **Malware Attacks**: Malware attacks in the context of smart grids refer to the infiltration of malicious software into the grid's systems, devices, or networks. Malware infects the smart grid's control systems, or human machine interfaces (HMIs), disrupts operations, compromises data integrity, and potentially gains unauthorized control over critical infrastructure. Here are some common types of malware attacks in smart grids [160,161]:
  - **Viruses**: viruses are self-replicating programs that attach themselves to legitimate files or programs and spread across the grid's systems. Once activated, viruses can cause system malfunctions, data corruption, or unauthorized access.
  - **Worms**: worms are standalone programs that replicate and spread across computer networks without requiring a host file. Worms can rapidly infect multiple devices within the smart grid, causing network congestion, system crashes, or unauthorized activities [162,163].
  - **Ransomware**: ransomware is a type of malware that encrypts files or locks users out of their systems, demanding a ransom payment in exchange for restoring access. Ransomware attacks can disrupt smart-grid operations, leading to service interruptions or financial losses [164,165]. Ransomware attacks have been on

the rise in recent years. According to a report by SonicWall [166], there were 304.7 million ransomware attacks globally in 2020, representing a 62% increase compared to the previous year. The financial impact of ransomware attacks is substantial. Cybersecurity Ventures [167] estimated that ransomware costs will reach 20 billion dollars in 2021, with a ransomware attack occurring every 11 s.

- **Trojan Horses**: Trojans disguise themselves as legitimate software or files and trick users into executing them. Once activated, Trojans can perform various malicious activities, such as data theft, system control, or backdoor creation for remote access [168,169].
- **Botnets**: botnets are networks of compromised devices that are controlled by a central command and control (C&C) server. Smart-grid devices infected with botnet malware can be used for coordinated attacks, such as DDoS attacks or spreading other forms of malware [170,171].
- **Keyloggers**: keyloggers capture keystrokes on infected devices, including passwords, login credentials, or other sensitive information. These data can be used to gain unauthorized access to smart-grid systems or compromise user accounts.
- **Spyware**: spyware is designed to collect information about a user's activities without their knowledge or consent. In the context of smart grids, spyware can monitor system operations, gather sensitive data, or capture user behavior, potentially compromising grid security.

The number of unique malware variants continues to grow rapidly. According to AV-TEST [172], an independent antivirus testing organization, more than 1 billion new malware variants were detected in 2020 alone.

- **Phishing Attacks**: phishing attacks involve the use of deceptive techniques to trick individuals or organizations into revealing sensitive information, such as login credentials, financial details, or personal data, or performing malicious actions. These attacks often come in the form of fraudulent emails, text messages, or websites that mimic trusted entities or institutions [173]. Phishing attacks continue to be a prevalent threat. In the 2021 Verizon Data Breach Investigations Report [174], phishing attacks accounted for 36% of all data breaches analyzed.
- **Insider Threats**: insider threats refer to attacks perpetrated by individuals who have authorized access to the smart grid's systems and misuse their privileges. These insiders may intentionally or inadvertently compromise the grid's security, privacy, or operational integrity [175,176]. Insider threats pose a significant risk to smart grids. The U.S. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) [177] reported that insider threats accounted for approximately 20% of the cybersecurity incidents in the energy sector.
- **Man-in-the-Middle (MitM) Attacks**: in MitM attacks, attackers can exploit insecure or unencrypted Wi-Fi networks to position themselves between the sender and the recipient, allowing them to eavesdrop on the communication, manipulate the data exchanged, or even impersonate one or both parties without their knowledge [178,179].
- **Advanced Persistent Threats (APTs)**: APTs are sophisticated, long-term cyberattacks aimed at gaining stealthy and persistent unauthorized access to the smart grid's systems (i.e., login credentials, financial details, or other confidential data being transmitted). APTs involve multiple stages and often target specific entities or organizations with the goal of gathering valuable information or sabotaging critical operations [179,180].
- **Data Manipulation Attacks**: these attacks involve the unauthorized modification or manipulation of data within the smart grid. Attackers may alter meter readings, billing information, or control signals, leading to inaccurate billing, load balancing, or compromised grid stability [181].
- **Supply Chain Attacks**: supply chain attacks exploit vulnerabilities in the software or hardware components used in smart-grid infrastructure. The attackers compromise

these components during the manufacturing or distribution process, allowing them to introduce backdoors or malicious functionalities into the grid's systems [182].

- **Physical Attacks with Cyber Components**, also known as cyber-physical attacks, refer to instances where physical systems or infrastructures are targeted through cyber means. These attacks exploit vulnerabilities in both the physical and cyber domains to cause disruptions, damage, or safety risks [183,184].
- **SQL Injection Attacks**: while smart grids primarily focus on power generation, transmission, and distribution, there are web-based applications and databases that support various functions and services within the grid. SQL injection attacks are a type of cyberattack that targets a vulnerability in a web application's database layer. It occurs when an attacker is able to manipulate or inject malicious SQL statements into the application's input fields that are later executed by the database. The objective of an SQL injection attack is to exploit poorly sanitized input data and gain unauthorized access to the database or perform malicious actions [185].
- **Zero-Day Exploits**: zero-day exploits are cyberattacks that target previously unknown vulnerabilities in software or systems, exploiting them before the vendor has a chance to develop and release a patch or fix. In the context of smart grids, zero-day exploits can have severe consequences due to the critical nature of the infrastructure [186].

It is important to note that the landscape of cyberattacks is continuously evolving, and new attack vectors may emerge over time. To mitigate these risks, robust cybersecurity measures are essential for smart-grid operators and stakeholders.

3.1.3. Short-Term and Long-Term Techno–Economic–Safety–Social Consequences of Cyberattacks on Smart Grids

Cyberattacks on smart grids have both immediate and lasting consequences across technological, economic, safety, and societal dimensions [187,188]. In the short term, attacks can cause power outages, disrupt operations, and compromise data integrity, undermining trust and reliability. This leads to financial losses, operational inefficiencies, and a hindrance to real-time grid monitoring. Economically,the attacks burden utility providers with recovery costs, potentially deterring sustainable energy investments. Safety-wise, the manipulation of grid components poses hazards to personnel and the public, impeding safety mechanisms. Attacks erode public trust, impacting technology adoption and critical services such as healthcare. In the long term, the cumulative effects hinder technological advancements, diverting resources from innovation. Cyberattacks, thus, challenge grid stability, functionality, and social acceptance, necessitating robust cybersecurity measures and comprehensive strategies for sustained resilience and progress.

3.1.4. Vulnerable Components and Cascading Consequences of Cyberattacks in the Smart Grid

A smart grid's susceptibility to cyberattacks spans multiple components [189], including control systems such as supervisory control and data acquisition (SCADA) systems and energy management systems (EMS), communication networks, smart meters, customer systems, distributed energy resources (DER) (e.g., solar panels, energy storage), and data systems. Interconnected and reliant on information technology, these areas are vulnerable, potentially causing operational disruptions, data issues, privacy breaches, and physical harm. Cyberattacks can also trigger cascading effects, disrupting control systems, communication networks, device operations, data integrity, and DER stability, possibly leading to a chain of attacks [190,191]. These cascades underscore the need for comprehensive cybersecurity measures that address interdependencies to ensure the overall resilience and security of the smart grid system.

3.1.5. Examining the Real-World Impacts: Case Studies of Cyberattacks on Operational Smart Grids

Real-world case studies examine the actual effects of cyberattacks on operational smart grids:

- **Ukraine Power Grid Cyberattack (2015)**: analyzes a sophisticated attack on Ukraine's power grid, leading to widespread outages. The lessons learned encompass the methods used, impacts, and incident response [192].
- **BlackEnergy and CrashOverride Attacks (2016)**: focuses on malware-driven attacks in Ukraine causing power grid disruptions. Explores technical aspects, implications, and mitigation strategies [193,194].
- **NotPetya Ransomware Attack (2017)**: explores how the NotPetya attack impacted smart grids globally, disrupting grid management, communication, and billing systems [195].
- **Dragonfly/Energetic Bear Attacks (2011–2014)**: investigates a series of cyberattacks on energy companies, emphasizing tactics, motives, and consequences for smart grids [196].
- **Israel Electric Corporation Cyberattacks (2016–2018)**: studies cyberattacks on Israel Electric Corporation's grid infrastructure, highlighting disruptions and cybersecurity measures [197].

These case studies showcase the tangible impacts of cyberattacks on operational smart grids, emphasizing the significance of cybersecurity measures, incident response planning, and collaboration among utilities to safeguard critical infrastructure.

3.1.6. Quantitative Models and Metrics for Assessing the Impacts of Cyberattacks

Various quantitative models and metrics are available to assess the impacts of cyberattacks on smart grids [198]. Some examples include:

- **Economic Impact Model**: evaluates financial consequences by quantifying direct and indirect costs, considering lost revenue, recovery expenses, legal liabilities, and reputation damage.
- **Availability and Reliability Metrics**: measure cyberattack effects on critical systems' availability and reliability, including downtime, failure rates, mean time between failures (MTBF), and mean time to repair (MTTR).
- **Risk Assessment Models**: assess attack probability and severity using vulnerability, threat, and consequence considerations, employing risk matrices, attack trees, and threat modeling.
- **Operational Impact Metrics**: gauge cyberattack impact on operational efficiency, encompassing performance degradation, response delays, data integrity issues, and workflow disruptions.
- **Customer Satisfaction Metrics**: measure customer trust and satisfaction impact, using customer complaints, service level agreement (SLAs) violations, churn rates, and surveys to assess perception.
- **Resilience and Recovery Metrics**: evaluate recovery effectiveness against cyberattacks by tracking system recovery time, backup capabilities, redundancy levels, and incident response success.

Importantly , the specific models and metrics may vary based on assessment goals and context. Organizations can adapt existing frameworks or create customized models to align with their needs.

3.1.7. Securing Information Assets: The Importance of Confidentiality, Integrity, and Availability in Cybersecurity

The CIA triad, encompassing confidentiality, integrity, and availability, is a foundational concept in information security across various domains, including smart grids [199,200].

- **Confidentiality** ensures authorized access by safeguarding data from unauthorized exposure using encryption, access controls, and secure communication protocols.
- **Integrity** maintains data accuracy by preventing unauthorized alterations through data validation, checksums, digital signatures, and audit trails.
- **Availability** guarantees system and data access, preventing disruptions with redundancy, backup systems, disaster recovery, and network resilience techniques.

The CIA triad offers a comprehensive framework for security strategies, safeguarding against cyber threats, breaches, and unauthorized access. It extends beyond information security, guiding physical, personnel, and operational security. By integrating these principles into systems and processes, organizations mitigate risks and ensure valuable assets' confidentiality, integrity, and availability.

3.1.8. Short-Term and Long-Term Techno–Economic–Safety–Social Implications of Cybersecurity Measures on Smart Grids

The implementation of cybersecurity measures in smart grids has multi-faceted implications across various timeframes and aspects [201,202].

In the short term, robust cybersecurity measures ensure immediate safety and security by mitigating cyber risks and preserving the integrity, availability, and confidentiality of critical grid components. These measures yield techno–economic benefits by reducing disruptions and financial losses and maintaining efficient grid operations.

In the long term, cybersecurity measures extend beyond the technical and economic realms. They enhance smart-grid resilience, reliability, and sustainability by countering evolving cyber threats. This protection safeguards power supply stability, lessens infrastructure vulnerability, and builds public trust. Moreover, it has safety implications, preventing accidents and harm to personnel.

Socially, robust cybersecurity cultivates consumer trust and privacy. It shields personal information, maintains energy data confidentiality, and upholds privacy rights. By ensuring smooth smart-grid operations, cybersecurity enhances the well-being and quality of life of individuals and communities.

In conclusion, cybersecurity measures' short-term and long-term implications in smart grids are interconnected, offering immediate safety, operational efficiency, and long-term benefits of resilience, sustainability, public trust, and privacy protection. Prioritizing cybersecurity enables smart grids to effectively address cyber threats and establish a secure, reliable, and sustainable energy future.

3.1.9. Quantitative Models and Metrics for Assessing the Implications of Cybersecurity in Smart Grids

Various models and metrics offer a quantitative approach to measuring the implications of cybersecurity in smart grids [203]:

- **Risk Assessment Models**: frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework or ISO/IEC 27005 quantify risks and impacts by evaluating threats and vulnerabilities. They estimate the overall risk exposure, aiding in risk prioritization and mitigation.
- **Economic Impact Models**: these assess the financial consequences of cybersecurity incidents, factoring in downtime, disruptions, data breaches, recovery costs, penalties, and reputation damage. These models guide investment decisions and assess the return on investment (ROI) of security measures.
- **Availability and Reliability Metrics**: metrics such as mean time between failures (MTBF), mean time to repair (MTTR), system uptime, and service-level agreements (SLAs) gauge system availability amidst cybersecurity threats. They help evaluate the impact on performance and customer service.
- **Incident Response Metrics**: mean time to detect (MTTD), mean time to respond (MTTR), and mean time to recover (MTTR) assess the response efficiency to incidents, guiding improvements in incident management capabilities.

- **User Awareness and Training Metrics**: these measure the effectiveness of cybersecurity education programs through completion rates, campaign frequency, and policy adherence.
- **Compliance Metrics**: these assess adherence to the cybersecurity standards, regulations, and best practices. These metrics cover security controls, patch management, vulnerability assessments, and audits.
- **Resilience Metrics**: these evaluate the system's ability to withstand and recover from incidents, including redundancy, backup, recovery capabilities, and service restoration time.

The customization of these models and metrics for specific smart-grid implementations is crucial. The regular monitoring, analysis, and refinement enable the continuous improvement of the cybersecurity posture and ensure smart-grid resilience.

3.1.10. Analyzing the Real-World Implications of Cybersecurity Measures on Operational Smart Grids: Case Studies and Insights

Two case studies offer insights into cybersecurity implementation in operational smart grids:

- **Fortinet's Security Fabric Solution**: this study analyzes the implementation of Fortinet's Security Fabric in a smart grid. It assesses the cybersecurity implications, including protecting critical assets, detecting and responding to threats, and enhancing system resilience. The study evaluates how these measures mitigate risks and ensure secure grid operation [204].
- **National Institute of Standards and Technology (NIST) Cybersecurity Framework Adoption**: another case study focuses on a smart-grid utility adopting the NIST Cybersecurity Framework. It explores aligning cybersecurity practices with NIST, covering risk assessment, incident response, and continuous monitoring. The study examines how these measures impact operational efficiency, grid resilience, and cyber threat protection [205].

3.2. Cybersecurity Options in Smart Grids: Solving Multi-Criteria Decision-Making (MCDM) Using the Analytical Hierarchy Process (AHP)

Smart grids, being highly interconnected and reliant on digital technologies, face significant cybersecurity challenges that require careful consideration and decision-making.

The multi-criteria decision-making (MCDM) approach provides a systematic framework to assess and compare different cybersecurity options based on multiple criteria. These criteria may include effectiveness, cost, feasibility, comparability with existing systems, regulatory compliance, and impact on grid performance. By employing MCDM techniques, decision-makers can quantitatively evaluate the trade-offs between different cybersecurity options and make informed decisions.

We first identify the cybersecurity options available for smart grids, which may include encryption mechanisms, access controls, intrusion detection systems, incident response plans, and others. Next, we define the criteria that are used to evaluate these options, considering both technical and non-technical aspects (Section 3.2.1).

Once the criteria are established, we conduct pairwise comparisons to determine the relative importance or weight of each criterion. This can be performed through expert judgment, surveys, or data analysis. The analytical hierarchy process (AHP) technique is used in this study to structure these comparisons and derive the priority scales. With the criteria weights determined, we then assess the performance of each cybersecurity option against the identified criteria. The results are then used to rank the cybersecurity options and identify the most suitable ones for implementation in the smart-grid environment (Section 3.2.2).

By applying the MCDM-AHP approach, decision-makers can make well-informed decisions regarding cybersecurity options in smart grids. The methodology helps in considering multiple factors, addressing the complexity and uncertainties associated with

cybersecurity, and selecting the most effective and appropriate measures to protect the smart-grid infrastructure from cyber threats.

3.2.1. Alternatives and Criteria

There are several different cybersecurity options that can be implemented in smart grids to enhance their security and protect against cyber threats [206]. Here are some key cybersecurity options:

1. **"A1" Access Control and Authentication**: implementing strong authentication mechanisms, authorization controls, and user access restrictions to ensure only authorized individuals can access critical systems and data.
2. **"A2" Encryption**: utilizing encryption techniques to secure data transmission and storage, ensuring that sensitive information remains confidential and protected from unauthorized access.
3. **"A3" Intrusion Detection and Prevention Systems (IDPS)**: deploying IDPS solutions that monitor network traffic, detect suspicious activities or intrusion attempts, and take preventive actions to mitigate potential threats.
4. **"A4" Firewalls**: deploying firewalls to establish network security boundaries and control incoming and outgoing traffic based on predefined security policies.
5. **"A5" Security Information and Event Management (SIEM)**: implementing SIEM solutions to collect, analyze, and correlate security events and log data, enabling early detection and response to potential cyber threats.
6. **"A6" Vulnerability Assessment and Penetration Testing**: conducting regular vulnerability assessments and penetration testing, implementing timely patching and updates to identify potential vulnerabilities and weaknesses in the smart-grid infrastructure, software, and hardware components and proactively addressing them.
7. **"A7" Security Incident Response**: establishing a comprehensive incident response plan to effectively respond to and manage cybersecurity incidents, minimizing the impact of attacks and facilitating recovery.
8. **"A8" Security Monitoring and Logging**: implementing monitoring and logging mechanisms to track and record activities within the smart-grid infrastructure, enabling the detection and investigation of potential security breaches.
9. **"A9" Security Awareness and Training**: conducting regular cybersecurity awareness programs and training sessions for employees and stakeholders to educate them about potential threats, best practices, and their role in maintaining a secure smart-grid environment.
10. **"A10" Data Backup and Recovery**: implementing robust data backup and recovery mechanisms to ensure that critical data can be restored in the event of a cyberattack or system failure.
11. **"A11" Secure Software Development Lifecycle (SSDL)**: following secure SDLC practices to develop and maintain secure software solutions, including secure coding practices, code reviews, and vulnerability testing.
12. **"A12" Incident Response Coordination**: establishing effective coordination and collaboration with relevant stakeholders, including government agencies, law enforcement, and industry partners, to address and mitigate cybersecurity incidents effectively.
13. **"A13" Compliance and Regulatory Requirements**: ensuring compliance with the relevant cybersecurity standards, regulations, and industry best practices specific to the smart-grid sector.

It is important to note that the specific implementation of these cybersecurity options may vary depending on the smart grid's architecture, size, complexity, and risk profile. However, it is important to note that cybersecurity is a complex and evolving field, and there may be additional measures and technologies that can be employed based on specific smart-grid requirements and risk assessments.

When evaluating cybersecurity options for smart grids, several relevant criteria need to be considered. These criteria help assess the effectiveness, feasibility, and suitability of different cybersecurity measures [207]. Here are some important criteria to consider:

1. **"C1": Security Effectiveness**: the ability of the cybersecurity solution to detect and prevent cybersecurity threats accurately and effectively.
2. **"C2" Scalability**: the capability of the solution to scale and accommodate the growing complexity and size of the smart-grid systems, including the ability to handle increased data volumes, growing infrastructure requirements, and network traffic.
3. **"C3" Integration and Compatibility**: the ease with which the cybersecurity solution can integrate with the existing smart-grid infrastructure, technologies, and tools, ensuring compatibility and minimal disruption to operations.
4. **"C4" Performance Impact**: the impact of cybersecurity solutions on the performance and efficiency of smart-grid systems, including factors such as latency, response time, and system availability.
5. **"C5" Cost-Effectiveness**: the overall cost–benefit ratio of implementing the cybersecurity solution, considering both upfront costs and ongoing maintenance expenses, and evaluating the value it brings in terms of risk mitigation.
6. **"C6" Manageability and Usability**: the ease of managing and administering the cybersecurity solution, including the user interface, configuration options, and the ability to monitor and analyze security events effectively.
7. **"C7" Compliance and Regulatory Requirements**: the extent to which the cybersecurity solution aligns with the relevant industry standards, regulations, and compliance requirements specific to smart grids, ensuring adherence to legal and operational obligations.
8. **"C8" Resilience and Redundancy**: the ability of the cybersecurity solution to provide resilience and redundancy measures, such as backup systems and failover capabilities, to ensure continuous operations even in the event of a security breach or system failure.
9. **"C9" Vendor Support and Collaboration**: the level of support and collaboration provided by the cybersecurity solution vendor, including the availability of updates, patches, and technical assistance, as well as the commitment to the ongoing research and development.
10. **"C10" Future Readiness**: the solution's ability to adapt and evolve with emerging technologies, threat landscapes, and evolving cybersecurity best practices, ensuring long-term viability and protection.
11. **"C11" Network Segmentation**: the ability to segment the smart-grid network into separate zones or segments to minimize the impact of a security breach and limit the lateral movement of attackers.
12. **"C12" Patch Management**: the capability to efficiently manage and apply software patches and updates to address vulnerabilities and ensure the system is up to date with the latest security measures.
13. **"C13" Threat Intelligence**: the use of advanced techniques and tools and access to timely and accurate threat intelligence information, including real-time threat detection, analysis, and sharing of indicators of compromise, to enhance the proactive cybersecurity measures.
14. **"C14" Vendor and Supply Chain Security**: assessing the security practices and controls of the vendors and suppliers involved in the smart-grid ecosystem to mitigate risks associated with third-party access and potential supply chain vulnerabilities.

Considering these criteria will help in making informed decisions when selecting and implementing cybersecurity options in smart grids, ensuring a comprehensive and robust cybersecurity framework, taking into account various aspects such as the effectiveness of the security measures, the ability to scale and adapt to evolving threats, integration with existing systems, performance impact on grid operations, cost-effectiveness, ease of management and usability, compliance with regulations, resilience and redundancy

to withstand attacks or failures, vendor support and adherence to regulations, future readiness, network segmentation, patch management, threat intelligence, and vendor and supply chain security.

3.2.2. Pairwise Comparison Matrix, Relative Weights of Criteria, and Weighted Sum of Alternatives

In this section, we explore the evaluation of cybersecurity options by comparing them against a set of described criteria (Section 3.2.1). We construct a pairwise comparison matrix (Table 3), which allows us to assess the relative importance of each criterion compared to the others (Table 4). Using these relative weights, we compute the weighted sum for each cybersecurity option (Table 5), providing an overall score that considers the importance of each criterion.

Each element of the matrix (Table 3) represents the relative importance or preference of one criterion over another. The values in the matrix are the pairwise comparison judgments based on a scale of 1 to 9, where 1 represents equal importance or preference and 9 represents extreme importance or preference. For instance, the value of 7 in the cells C1–C2 indicates that the criterion "Security Effectiveness (C1)" is considered to be seven times more important than the criterion "Scalability (C2)". Similarly, the value of 5 in the cells C4–C10 suggests that the criterion "Performance impact (C4)" is considered to be five times more important than the criterion "Future Readiness (C10)".

Table 3. The pairwise comparison matrix between criteria. We assume a scale from 1 to 9, where 1 represents equal importance and 9 represents significantly more importance (Section 2.2). This is a subjective assessment, and individual opinions may vary based on their perspectives and priorities.

Criteria	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14
C1	1	7	6	5	8	8	7	9	8	7	6	7	7	6
C2	$\frac{1}{7}$	1	3	4	6	5	6	4	7	4	5	4	6	5
C3	$\frac{1}{6}$	$\frac{1}{3}$	1	3	5	5	5	6	7	5	6	5	6	5
C4	$\frac{1}{5}$	$\frac{1}{4}$	$\frac{1}{3}$	1	5	4	4	6	6	5	5	4	5	5
C5	$\frac{1}{8}$	$\frac{1}{6}$	$\frac{1}{5}$	$\frac{1}{5}$	1	3	4	6	6	4	5	4	4	4
C6	$\frac{1}{8}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{4}$	$\frac{1}{3}$	1	4	6	7	4	5	4	5	4
C7	$\frac{1}{7}$	$\frac{1}{6}$	$\frac{1}{5}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	1	5	6	3	4	4	4	4
C8	$\frac{1}{9}$	$\frac{1}{4}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{5}$	1	5	2	4	4	3	4
C9	$\frac{1}{8}$	$\frac{1}{7}$	$\frac{1}{7}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{7}$	$\frac{1}{6}$	$\frac{1}{5}$	1	3	5	4	4	4
C10	$\frac{1}{7}$	$\frac{1}{4}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{3}$	$\frac{1}{2}$	$\frac{1}{3}$	1	4	3	4	4
C11	$\frac{1}{6}$	$\frac{1}{5}$	$\frac{1}{6}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{5}$	$\frac{1}{4}$	1	3	4	4
C12	$\frac{1}{7}$	$\frac{1}{6}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{3}$	$\frac{1}{3}$	1	4	4
C13	$\frac{1}{7}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{5}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{3}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	1	4
C14	$\frac{1}{6}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	1

The values in Table 4 indicate the relative contribution of each criterion in the decision-making process. Higher weights indicate greater importance, while lower weights indicate lesser importance.

From Table 4, we can categorize the criteria as follows:

- **The criteria with high relative weights (above 10%)**: "Security effectiveness (C1)" has the highest relative weight (25%), indicating its significant importance in cybersecurity options for smart grids. Emphasizing security effectiveness ensures that the chosen options can accurately and effectively detect and prevent cybersecurity threats.
- **The criteria with medium relative weights (between 7% and 10%)** suggest that they are moderately important in the evaluation process. They should be considered alongside other factors to ensure the overall suitability and performance of the cybersecurity options.
  - "Cost-effectiveness (C5)" (10.18%) holds significant importance in evaluating cybersecurity options. It indicates the need to consider the overall cost–benefit

ratio, ensuring that the chosen options provide effective security enhancements while being cost-effective".
  - "Scalability (C2)" (7.89%): this criterion highlights the importance of considering the ability of the options to scale and accommodate the growing complexity and size of the smart-grid systems.
  - "Integration and compatibility (C3)" (7.89%): this criterion emphasizes the need for seamless integration with the existing smart-grid infrastructure and technologies, minimizing disruptions and ensuring compatibility.
- **The criteria with low relative weights (below 7%)**:
  - "Performance impact (C4)" (6.93%): this criterion suggests that the performance impact of cybersecurity options is relatively less influential but still important to consider.
  - C6 to C14: these criteria, including manageability and usability "C6" (6.32%), compliance and regulatory requirements "C7" (5.93%), resilience and redundancy "C8" (4.97%), vendor support and collaboration "C9" (4.84%), and future readiness "C10" (1.76%), have relatively lower weights but still contribute to the overall evaluation. While their impact is slightly smaller compared to higher-weighted criteria, they should be considered in conjunction with other factors.

Table 4. Relative Weights (RWs) of criteria (i.e., the importance or priority assigned to each criterion in the evaluation of the cybersecurity options). These weights indicate the relative significance of each criterion in determining the overall effectiveness of the options.

Criteria	Relative Weights (RWs)
C1 "Security Effectiveness"	25%
C2 "Scalability"	7.89%
C3 "Integration and Compatibility"	7.89%
C4 "Performance Impact"	6.93%
C5 "Cost-Effectiveness"	10.18%
C6 "Manageability and Usability"	6.32%
C7 "Compliance and Regulatory Requirements"	5.93%
C8 "Resilience and Redundancy"	4.97%
C9 "Vendor Support and Collaboration"	4.84%
C10 "Future Readiness"	1.76%
C11 "Network Segmentation"	4.7%
C12 "Patch Management"	4.59%
C13 "Threat Intelligence"	4.59%
C14 "Vendor and Supply Chain Security"	4.47%

After performing the calculations, the consistency ratio (CR) for the obtained pairwise comparison matrix (Table 3) is approximately 0.063. The CR value indicates that the matrix is consistent since it is below the threshold of 0.1. Therefore, the pairwise comparison matrix satisfies the consistency requirements.

The weighted sums (Table 5) represent the overall scores or evaluations of each alternative based on the criteria and their corresponding relative weights. The alternatives with higher weighted sums are considered more suitable or preferable in terms of meeting the cybersecurity needs of smart grids, while the alternatives with lower weighted sums may have some limitations or may not perform as strongly in the evaluated criteria.

Based on the weighted sums (Table 5), we can categorize the alternatives as follows:

- **The alternatives with high weighted sums (above 5)**:
  - "Access Control and Authentication (A1)" (6.25) has the highest weighted sum, indicating its effectiveness and importance in enhancing cybersecurity in smart grids. Implementing strong authentication mechanisms and access controls is crucial for ensuring only authorized individuals can access critical systems and data.

  - "Security Information and Event Management (SIEM) (A5)" (5.762) has a relatively high weighted sum, suggesting its significance in smart-grid cybersecurity. Implementing SIEM solutions enables the collection, analysis, and correlation of security events and log data, enabling early detection and response to potential cyber threats.
- **The alternatives with medium-weighted sums (between 5 and 5.5)** suggest that they offer a solid performance in the evaluated criteria. They are important components for detecting and responding to security incidents.
  - "Intrusion Detection and Prevention Systems (IDPS) (A3)" (5.487): this alternative falls within the medium range, indicating its effectiveness in monitoring network traffic, detecting suspicious activities, and taking preventive actions against potential threats.
  - "Security Incident Response (A7)" (5.297): this alternative also falls within the medium range, highlighting the importance of establishing a comprehensive incident response plan to effectively respond to and manage cybersecurity incidents, minimizing their impact.
- **The alternatives with low weighted sums (below 4.5)** compared to others. While they still provide value in their respective criteria, they may not excel as strongly overall.
  - "Compliance and Regulatory Requirements (A13)" (4.349): this alternative has the lowest weighted sum among the alternatives, indicating that while compliance with cybersecurity standards and regulations is important, it may not have as high a priority as other options in the context of smart-grid cybersecurity.
  - "Encryption (A2)" (3.739): this alternative has a relatively low weighted sum, suggesting that while encryption is important for securing data transmission and storage, it may not have as significant an impact as other alternatives in the evaluated criteria.

Overall, the alternatives with high weighted sums (A1 and A5) are considered critical for enhancing smart-grid cybersecurity, while those with medium- and low-weighted sums still provide value but may have relatively less impact or priority in the evaluated criteria.

Table 5. Weighted sum for each option. Higher weighted sums indicate better overall performance.

Alternatives	Weighted Sum
A1 "Access Control and Authentication"	6.250
A2 "Encryption"	3.739
A3 "Intrusion Detection and Prevention Systems (IDPS)"	5.487
A4 "Firewalls"	4.838
A5 "Security Information and Event Management (SIEM)"	5.762
A6 "Vulnerability Assessment and Penetration Testing"	5.256
A7 "Security Incident Response"	5.297
A8 "Security Monitoring and Logging"	4.688
A9 "Security Awareness and Training"	4.706
A10 "Data Backup and Recovery"	4.690
A11 "Secure Software Development Lifecycle (SSDL)"	4.661
A12 "Incident Response Coordination"	4.730
A13 "Compliance and Regulatory Requirements"	4.349

3.3. Enhancing Cybersecurity of Smart Grids: Unveiling the Difference between AI and ML, Exploring their Potential and Addressing Challenges, and Leveraging MCDM-AHP for Optimal AI Selection

In this section, we analyze artificial intelligence (AI) techniques for cybersecurity options in smart grids to enhance the security and decision-making processes.

3.3.1. Understanding the Difference between AI and ML: Benefits and Challenges for Cybersecurity in Smart Grids

Indeed, AI and ML are two related concepts that play significant roles in cybersecurity but have distinct differences [208]. Key differences:

- **Scope**: AI is a broader field of computer science that encompasses various techniques to develop intelligent machines or systems capable of performing tasks that typically require human intelligence and cognitive functions—such as reasoning, problem solving, decision-making, perception, and natural language processing—while ML is a specific approach within AI that focuses on learning from data.
- **Programming vs. Learning**: AI often involves explicitly programming intelligent behavior or rules, whereas ML is a sunset or application of AI that focuses on training models to learn patterns and make predictions based on data without being explicitly programmed.
- **Data Dependency**: ML heavily relies on large datasets for training models and improving performance. The quality and quantity of data play a crucial role in ML algorithms' effectiveness. AI, on the other hand, can utilize various data sources but may not be solely dependent on them.
- **Human Intervention**: AI may involve human intervention in designing and specifying rules or heuristics for intelligent systems. ML, however, aims to automate the learning process and reduce human intervention by allowing models to learn from data independently.
- **Flexibility**: ML algorithms are flexible and can adapt to new data and patterns, enabling them to handle complex and dynamic tasks. AI, as a broader field, encompasses both rule-based systems and learning-based systems, providing a wider range of approaches for different types of problems.

Artificial intelligence (AI) can significantly enhance cybersecurity in smart grids by providing advanced capabilities for threat detection, prevention, and response. They can analyze large volumes of data from various sources, such as network traffic, system logs, and sensor data, to detect anomalies, identify potential cyber threats in real-time, and automate incident response processes. AI techniques power intrusion detection and prevention systems (IDPS), predict equipment failures, and optimize maintenance schedules. They can also analyze threat intelligence data, use behavioral analysis, and employ user and entity behavior analytics (UEBA) to identify emerging threats, detect unauthorized access, and mitigate risks. Overall, AI enables smarter threat management, reduces response times, and enhances the resilience and security of the smart-grid infrastructure [209].

While artificial intelligence (AI) offers significant benefits in enhancing the cybersecurity of smart grids, there are also several challenges that need to be addressed [210]. Here are some potential challenges:

- **Data Quality and Availability**: AI algorithms heavily rely on high-quality and representative data for training and decision-making. In the context of smart grids, obtaining labeled and diverse cybersecurity data can be challenging. Collaborating with smart-grid operators, cybersecurity organizations, and researchers to collect and share cybersecurity data to ensure the availability, accuracy, completeness, and reliability of the data is crucial for the effective training of AI models. Establishing mechanisms for continuous acquisition and the labeling of training data to keep AI models updated with the latest threats and attack patterns is also important.
- **Adversarial Attacks**: AI models can be susceptible to adversarial attacks where malicious actors intentionally manipulate or deceive the models to bypass security defenses. Adversarial attacks in the context of the smart grid can have severe consequences, such as disrupting power distribution or causing physical damage. Developing robust defenses against adversarial attacks is an ongoing challenge.
- **Model Interpretability and Explainability**: AI models often operate as black boxes, making it difficult to understand their decision-making processes. In the context of smart grids, where the consequences of incorrect decisions can be significant,

the interpretability and explainability of AI models are crucial to gain trust and enable effective human oversight. Prioritizing the development of interpretable and explainable AI models for cybersecurity in smart grids enables human analysts to understand the reasoning behind model decisions and ensures transparency and accountability in the decision-making process.

- **Privacy Concerns**: smart-grid systems handle sensitive and personal data, including energy consumption patterns and user behavior. The application of AI may involve collecting and processing such data, raising privacy concerns. Ensuring proper data anonymization, encryption, and compliance with privacy regulations is essential to protect user privacy.
- **Scalability and Performance**: Smart grids generate massive amounts of data in real-time, requiring AI models to process and analyze the data efficiently. Ensuring the scalability and performance of AI algorithms to handle the volume and velocity of the data in smart-grid environments is a significant challenge.
- **Ethical and Bias Concerns**: AI models can inadvertently inherit biases present in the training data, leading to discriminatory or unfair outcomes. Biases in smart-grid systems can have societal implications, such as uneven energy distribution or unfair treatment of certain user groups. Addressing bias and ensuring ethical considerations in AI models are essential.
- **Human Expertise and Collaboration**: AI technologies augment human capabilities but do not replace the need for human expertise in cybersecurity. Collaboration between domain experts, cybersecurity professionals, and data scientists is crucial to effectively apply AI techniques to smart-grid cybersecurity. Developing hybrid systems that combine the strengths of AI algorithms with human expertise for better decision-making, threat hunting, and incident response is essential.
- **Regulatory Compliance**: Smart grids are subject to regulatory requirements and standards to ensure the security and privacy of energy systems. Integrating AI solutions in compliance with regulatory frameworks, such as data protection and cybersecurity regulations, presents a challenge that requires careful implementation and validation.
- **System Complexity and Integration**: smart grids consist of interconnected and heterogeneous systems, making the integration of AI solutions complex. Ensuring seamless integration with the existing infrastructure, legacy systems, and diverse components while maintaining interoperability and reliability is a challenge when deploying AI in smart- grid cybersecurity.

Addressing these challenges requires a multidisciplinary approach, involving cybersecurity experts, data scientists, policymakers, and industry stakeholders to develop robust and trustworthy AI solutions that effectively protect smart-grid systems from cyber threats while addressing privacy, fairness, and regulatory requirements.

3.3.2. Leveraging MCDM-AHP for Selecting the Optimal AI Option for Cybersecurity in Smart Grids

In this section, we delve into the evaluation of cybersecurity options using AI in the context of smart grids. We begin by establishing a set of criteria to assess the effectiveness of these options for ensuring robust cybersecurity. We then employ a pairwise comparison matrix (Table 6) to determine the relative importance of each criterion when compared to others (Table 7). These relative weights are used to calculate the weighted sum for each cybersecurity option (Table 8), yielding a comprehensive score that takes into account the significance of each criterion. Through this evaluation process, we gain valuable insights into the strengths and weaknesses of different cybersecurity options considering AI in addressing the specific needs of smart grids.

In the field of cybersecurity for smart grids, a variety of AI techniques and methods can be applied to enhance security measures [211]. Here are several types and methods of AI commonly used in cybersecurity for smart grids:

1. **"A1" Machine Learning (ML)**:

- **Supervised Learning**: ML models are trained on labeled data to make predictions or classifications based on known patterns.
- **Unsupervised Learning**: ML models analyze unlabeled data to identify patterns, anomalies, or clustering structures without prior knowledge.
- **Semi-Supervised Learning**: a combination of labeled and unlabeled data is used to train ML models, making use of both supervised and unsupervised techniques.
- **Reinforcement Learning**: ML models learn to make decisions by interacting with an environment and receiving feedback in the form of rewards or penalties.

2. **"A2" Deep Learning (DL)**:
   - **Convolutional Neural Networks (CNNs)**: DL models designed for processing structured grid-like data, such as image or time-series data.
   - **Recurrent Neural Networks (RNNs)**: DL models that handle sequential or time-series data by maintaining internal memory.
3. **"A3" Natural Language Processing (NLP)**:
   - **Sentiment Analysis**: NLP techniques are used to analyze text data and determine the sentiment or opinion expressed.
   - **Named Entity Recognition**: NLP models identify and classify named entities, such as person names, locations, or organizations, in text data.
   - **Text Classification**: NLP algorithms classify text documents into predefined categories based on their content.
4. **"A4" Genetic Algorithms (GA)**: GA methods can be employed to optimize complex problems, such as finding optimal security configurations or identifying optimal control parameters.
5. **"A5" Fuzzy Logic**: fuzzy logic models capture and reason with imprecise or uncertain data, enabling decision-making in scenarios with ambiguity or vagueness.
6. **"A6" Expert Systems**:
   - **Rule-Based Systems**: expert systems use predefined rules and knowledge bases to mimic the decision-making processes of human experts.
   - **Knowledge Representation**: techniques for capturing and representing domain-specific knowledge to support decision-making and inference.
7. **"A7" Swarm Intelligence**:
   - **Particle Swarm Optimization (PSO)**: swarm intelligence methods are used for optimization problems where a group of particles iteratively searches for the optimal solution.
   - **Ant Colony Optimization (ACO)**: swarm intelligence techniques inspired by the foraging behavior of ants to solve complex optimization problems.
8. **"A8" Bayesian Networks**: probabilistic models that represent uncertain relationships between variables using directed acyclic graphs are useful for modeling and reasoning under uncertainty.
9. **"A9" Hybrid Approaches**: combinations of different AI techniques, such as integrating ML algorithms with expert systems or using hybrid models that combine DL and traditional ML methods.

These are some of the prominent types and methods of AI used in cybersecurity for smart grids. The selection and application of specific techniques depend on the specific cybersecurity challenges, available data, and desired outcomes of the smart-grid security system.

When evaluating cybersecurity options for smart grids that incorporate artificial intelligence (AI) techniques and methods, several relevant criteria should be considered. These criteria help assess the effectiveness, feasibility, and suitability of cybersecurity options. Here are the key criteria considered in this study:

1. **"C1" Security Effectiveness**:

- **Detection Accuracy**: the ability of the AI system to accurately detect and identify security threats and attacks.
- **False Positive Rate**: the frequency of incorrectly flagging legitimate activities as security threats.
- **False Negative Rate**: the frequency of failing to detect actual security threats or attacks.

2. **"C2" Scalability**:
   - **Ability to Handle Large Volumes of Data**: the capacity of the AI system to process and analyze a high volume of data generated by smart-grid systems in real-time.
   - **Computational Efficiency**: the ability of the AI algorithms to perform complex computations within acceptable time frames.
3. **"C3" Integration and Compatibility**:
   - **Compatibility with Existing Infrastructure**: the extent to which the AI cybersecurity solution can integrate with the existing smart-grid infrastructure, including hardware, software, and communication protocols.
   - **Interoperability**: the ability of the AI system to work seamlessly with other cybersecurity tools and systems in the smart-grid environment.
4. **"C4" Performance Impact**:
   - **System Overhead**: the additional computational and resource requirements imposed by the AI cybersecurity solution on the smart-grid system.
   - **Latency**: the delay introduced by the AI system in detecting and responding to security threats.
5. **"C5" Cost-Effectiveness**:
   - **Implementation Costs**: the upfront costs associated with acquiring, deploying, and maintaining the AI cybersecurity solution.
   - **Operational Costs**: the ongoing expenses related to the operation, monitoring, and maintenance of the AI system.
6. **"C6" Manageability and Usability**:
   - **Ease of Deployment**: the simplicity and efficiency of deploying the AI solution within the smart-grid environment.
   - **User-Friendliness**: the intuitiveness and ease of use for the cybersecurity personnel responsible for managing and monitoring the AI system.
7. **"C7" Compliance and Regulatory Requirements**:
   - **Alignment with Industry Standards**: the extent to which the AI cybersecurity solution complies with the relevant industry standards and best practices.
   - **Adherence to Legal and Regulatory Requirements**: the ability of the AI system to meet the specific legal and regulatory obligations governing smart-grid cybersecurity.
8. **"C8" Resilience and Redundancy**:
   - **Robustness**: the AI system's ability to withstand and recover from security incidents or cyberattacks.
   - **Redundancy**: the availability of backup mechanisms or redundant AI components to ensure continuous operation and protection.
9. **"C9" Vendor Support and Collaboration**:
   - **Availability of Support**: the level of technical support and assistance provided by the AI solution vendor.
   - **Collaboration Opportunities**: the vendor's willingness to collaborate with smart-grid operators, cybersecurity experts, and researchers to enhance the AI system's capabilities.

10. **"C10" Future Readiness**:
    - **Adaptability and Flexibility**: the AI system's capability to adapt to evolving security threats, technologies, and regulatory changes in the smart-grid domain.
    - **Upgradability**: the ease with which the AI solution can be upgraded or enhanced with new features or improved algorithms.
11. **"C11" Network Segmentation**: the ability of the cybersecurity solution to effectively implement network segmentation and isolation to limit the spread of threats and contain potential breaches.
12. **"C12" Explainability and Transparency**: the ability of the AI system to provide explanations and justifications for its decisions and actions, ensuring transparency and accountability in the cybersecurity processes.

These criteria provide a comprehensive framework for evaluating cybersecurity options that incorporate AI techniques and methods in the context of smart grids. By considering these criteria, decision-makers can assess and compare different options to make informed choices that align with the specific needs and requirements of their smart-grid cybersecurity initiatives.

The pairwise comparison matrix between criteria is presented in the Table 6.

Table 6. Pairwise comparison matrix between criteria.

Criteria	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12
C1	1	3	3	3	5	3	5	3	5	3	3	3
C2	$\frac{1}{3}$	1	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	
C3	$\frac{1}{3}$	3	1	1	3	3	3	3	5	3	3	3
C4	$\frac{1}{3}$	3	1	1	3	3	3	3	3	3	3	3
C5	$\frac{1}{5}$	3	$\frac{1}{3}$	$\frac{1}{3}$	1	$\frac{1}{3}$	3	3	5	3	3	3
C6	$\frac{1}{3}$	3	$\frac{1}{3}$	$\frac{1}{3}$	3	1	3	3	3	3	3	3
C7	$\frac{1}{5}$	3	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	1	3	3	3	1	1
C8	$\frac{1}{3}$	3	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	1	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$
C9	$\frac{1}{5}$	3	$\frac{1}{5}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	3	1	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$
C10	$\frac{1}{3}$	3	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	3	3	1	$\frac{1}{3}$	$\frac{1}{3}$
C11	$\frac{1}{3}$	3	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	1	3	3	3	1	1
C12	$\frac{1}{3}$	3	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	1	3	3	3	1	1

Based on the calculated relative weights of criteria (Table 7), we can categorize them into three groups:

- **High Relative Weights**: C1 "Security Effectiveness" (26.6%) has the highest relative weight, indicating its significant importance in evaluating cybersecurity options that incorporate artificial intelligence (AI) techniques. This criterion focuses on the accuracy of threat detection, false positive, and false negative rates, which are crucial for effective security measures in smart grids.
- **Medium Relative Weights**: C3 "Integration and Compatibility" (21.5%) and C4 "Performance Impact" (21.5%) have relatively high weights. These criteria emphasize the seamless integration of AI cybersecurity solutions with the existing infrastructure and the impact on system performance, both of which are important considerations in evaluating options.
- **Low Relative Weights**: criteria such as C6 "Manageability and Usability" (15.8%) (i.e., the ease of managing and using the cybersecurity options within the smart-grid environment, emphasizing user-friendliness and efficient management practices), C5 "Cost-Effectiveness" (8.5%) (i.e., considering the balance between cost and the value of security enhancements), C8 "Resilience and Redundancy" (8.3%) (i.e., the ability for the cybersecurity options to provide resilience and redundancy, ensuring the continuity and availability of smart-grid operations even in the face of cyber threats or failures), C10 "Future Readiness" (7.6%) (i.e., the preparedness of the cybersecurity options to

adapt and evolve in response to future cybersecurity challenges and advancements in smart-grid technologies), C7 "Compliance and Regulatory Requirements" (7.6%) (i.e., the adherence to relevant compliance and regulatory standards and requirements in the deployment of cybersecurity solutions for smart grids), C2 "Scalability" (7.5%) (i.e., ability of the cybersecurity options to handle increased demands and expanding smart-grid networks effectively), C9 "Vendor Support and Collaboration" (5.9%), C11 "Network Segmentation" (5.9%), and C12 "Explainability and Transparency" (5.9%) have lower relative weights. While these criteria are still important, they are relatively less influential compared to the higher-weighted criteria.

Overall , the results suggest that security effectiveness, integration and compatibility, and performance impact are key considerations when evaluating cybersecurity options in smart grids. However, it is important to consider all the criteria holistically to make informed decisions that align with the specific needs and requirements of the smart-grid cybersecurity initiatives.

Table 7. Relative weights of the criteria.

Criteria	Relative Weights (RWs) of Criteria
C1 "Security Effectiveness"	26.6%
C2 "Scalability"	7.5%
C3 "Integration and Compatibility"	21.5%
C4 "Performance Impact"	21.5%
C5 "Cost-Effectiveness"	8.5%
C6 "Manageability and Usability"	15.8%
C7 "Compliance and Regulatory Requirements"	7.6%
C8 "Resilience and Redundancy"	8.3%
C9 "Vendor Support and Collaboration"	5.9%
C10 "Future Readiness"	7.6%
C11 "Network Segmentation"	5.9%
C12 "Explainability and Transparency"	5.9%

We find that the consistency ratio (CR) is 0.857, which is less than the threshold value of 0.1. This indicates acceptable consistency in the pairwise comparison matrix.

Based on the calculated weighted sums (Table 8), which represent the overall evaluation of each AI technique or method in addressing the cybersecurity needs of smart grids, considering the given criteria and their relative weights, we can categorize the alternatives into three groups:

- **High Weighted Sum**: "Deep Learning (A2)" emerges as the alternative with the highest weighted sum (0.635), indicating its strong potential in enhancing cybersecurity in smart grids. It demonstrates favorable performance across multiple criteria and aligns well with the specific requirements of the evaluated criteria.
- **Medium Weighted Sum**:
  - "Hybrid approaches (A9)" show a relatively medium weighted sum (0.574), suggesting their effectiveness in addressing cybersecurity challenges in smart grids. These approaches combine multiple AI techniques and methods to leverage their respective strengths and overcome limitations.
  - "Bayesian Networks (A8)" (0.531) also fall into the medium-weighted sum category, indicating their relevance and potential in addressing cybersecurity needs. They use probabilistic modeling to capture dependencies and uncertainties in smart-grid systems.
  - "Swarm Intelligence" (A7): This alternative also falls within the medium range of weighted sums (0.405). Swarm intelligence techniques, such as particle swarm optimization and ant colony optimization, offer potential benefits for optimizing cybersecurity solutions in smart grids.

  - "Machine Learning (ML) (A1)": This alternative has a moderate weighted sum (0.453), indicating that machine learning techniques have some value but are not ranked as highly as deep learning or hybrid approaches.
- **Low Weighted Sum**:
  - "Fuzzy Logic (A5)": This alternative has a relatively lower weighted sum (0.324), suggesting that fuzzy logic methods may have limited applicability or effectiveness compared to other alternatives.
  - "Natural Language Processing (NLP) (A3)": this alternative also falls within the lower range of weighted sums (0.312). While NLP techniques can be useful for certain cybersecurity tasks, they may not be as prominent or effective as other alternatives in the context of smart-grid security.
  - "Expert Systems (A6)": this alternative has a lower weighted sum (0.247), indicating that expert systems may have limitations or are perceived to have less impact on smart-grid cybersecurity compared to other approaches.
  - "Genetic Algorithms (GA) (A4)": This alternative has the lowest weighted sum (0.148) among the options, suggesting that genetic algorithms may have limited applicability or effectiveness for addressing smart-grid cybersecurity challenges.

Table 8. Weighted sum of alternatives.

Alternatives	Weighted Sum of Alternatives
A1 "Machine Learning (ML)"	0.453
A2 "Deep Learning (DL)"	0.635
A3 "Natural Language Processing (NLP)"	0.312
A4 "Genetic Algorithms (GA)"	0.148
A5 "Fuzzy Logic"	0.324
A6 "Expert Systems"	0.247
A7 "Swarm Intelligence"	0.405
A8 "Bayesian Networks"	0.531
A9 "Hybrid Approaches"	0.574

4. Discussion: Advantages, Limitations, Enhancements of MCDM-AHP in Evaluating Cybersecurity Options in Smart Grids: Exploring Alternative MCDM Approaches

This study employs the multi-criteria decision-making analytical hierarchy process (MCDM-AHP) methodology to evaluate and determine the most effective cybersecurity options for smart grids. While the AHP approach offers various advantages (Section 4.1), it also presents several challenges (Section 4.2) and improvements (Section 4.3) that need to be addressed in the evaluation process [212].

4.1. Advantages of the Analytical Hierarchy Process (AHP)

The analytical hierarchy process (AHP) offers several advantages, such as:

- **Structured Decision-Making**: AHP provides a structured framework for decision-making by breaking down complex problems into a hierarchical structure of criteria, sub-criteria, and the alternatives. This helps decision-makers systematically evaluate and compare different options.
- **Pairwise Comparisons**: AHP allows decision-makers to make pairwise comparisons between the criteria and the alternatives based on their relative importance. This enables a more nuanced assessment of the criteria and facilitates the consideration of multiple factors in the decision-making process.
- **Consistency Checking**: AHP incorporates a consistency checking mechanism to ensure that decision-makers provide reliable and consistent judgments during the pairwise comparisons. This helps to enhance the credibility and validity of the decision-making process.

- **Flexibility and Adaptability**: AHP can accommodate changes in the decision problem by allowing decision-makers to revise their judgments and priorities. This flexibility enables the adjustment of criteria weights and the reassessment of alternatives as new information becomes available.
- **Transparency and Communication**: AHP provides a clear structure for decision-making and facilitates transparent communication among decision-makers. The hierarchical representation and pairwise comparisons enable stakeholders to understand the decision rationale and engage in meaningful discussions.

4.2. Limitations of the Analytical Hierarchy Process (AHP)

Despite its advantages, the analytical hierarchy process (AHP) also has several disadvantages, including:

- **Subjectivity**: AHP heavily relies on subjective judgments and pairwise comparisons made by decision-makers. The accuracy and consistency of these judgments can vary, introducing potential bias and uncertainty into the decision-making process.
- **Complexity**: AHP can become complex when dealing with a large number of criteria and alternatives. The hierarchical structure and pairwise comparisons require significant effort and time from decision-makers, making it challenging to handle highly complex decision problems.
- **Sensitivity to Input**: small changes in the pairwise comparison judgments can lead to significant variations in the final results. AHP's sensitivity to input can make the decision outcomes vulnerable to individual biases or inconsistencies in judgment.
- **Lack of Quantifiability**: AHP relies on qualitative judgments and does not provide a quantitative measurement of the decision criteria or alternatives. This can limit the ability to conduct precise numerical analysis or statistical inference in the decision-making process.
- **Limited Representation of Interactions**: AHP assumes independence between the criteria and does not explicitly capture interactions or dependencies among them. This can oversimplify the decision problem and overlook the complex relationships that exist between the criteria.

While AHP offers a structured and systematic approach to decision-making, it is important to consider these limitations and apply the method judiciously, taking into account the specific characteristics and requirements of the decision problem at hand.

4.3. Enhancing MCDM-AHP for Smart-Grid Cybersecurity: Exploring Strategies for Improvement

Improving the multi-criteria decision making with the analytical hierarchy process (MCDM-AHP) methodology for smart-grid cybersecurity involves enhancing its effectiveness, adaptability, and robustness in addressing the complex and evolving challenges posed by cyber threats. Below are several approaches to enhancing MCDM-AHP for smart-grid cybersecurity:

- **Incorporate More Comprehensive Criteria**: expand the list of evaluation criteria to encompass a broader range of factors relevant to smart-grid cybersecurity. Consider including technical, economic, social, environmental, and regulatory criteria to capture a holistic view of the cybersecurity landscape.
- **Quantify Qualitative Criteria**: develop methods to quantify qualitative criteria, such as expert opinions, using appropriate scales or weights. This allows for a more objective assessment and comparison of cybersecurity measures.
- **Dynamic Weight Adjustments**: implement dynamic weight adjustments to reflect the changing significance of criteria over time or in response to evolving cyber threats. This ensures that the decision-making process remains adaptable and aligned with the emerging challenges.
- **Consider Uncertainty and Risk**: integrate methods to handle uncertainty and risk, such as probabilistic modeling and sensitivity analysis. This enhances the robustness

of the decision-making by accounting for the inherent uncertainties in the cybersecurity scenarios.

- **Integrate Real-Time Data**: incorporate real-time data feeds and analytics into the MCDM-AHP framework to enable continuous monitoring and adjustment of the cybersecurity measures based on the current threat landscape.
- **Include Machine Learning**: integrate machine learning algorithms to enhance predictive capabilities and automate the identification of potential threats and vulnerabilities. ML can assist in identifying patterns and anomalies that may not be evident through traditional approaches.
- **Scenario Analysis**: conduct a comprehensive scenario analysis to evaluate the performance of the cybersecurity measures under various attack scenarios. This helps identify potential weaknesses and prioritize measures that demonstrate robustness across different threats.
- **Stakeholder Engagement**: involve a diverse group of stakeholders, including cybersecurity experts, grid operators, regulators, and end-users, in the decision-making process. Their insights can contribute to a more holistic and informed assessment.
- **Feedback Mechanisms**: implement feedback mechanisms that allow for continuous learning and improvement of the MCDM-AHP model based on the outcomes of previous decisions and their real-world impacts.
- **Interdisciplinary Collaboration**: foster collaboration between cybersecurity experts, power engineers, data scientists, and decision analysts to ensure a well-rounded and multidisciplinary approach to improving MCDM-AHP for smart-grid cybersecurity.

By implementing these strategies, the MCDM-AHP methodology can be enhanced to provide more accurate, adaptable, and effective decision support for selecting optimal cybersecurity measures in smart grids.

4.4. Exploring MCDM Approaches for Evaluating Cybersecurity Options in Smart Grids

There are several other multi-criteria decision-making (MCDM) methods [94] that can be implemented to compare the results obtained from the analytical hierarchy process (AHP) and provide a broader perspective. Here are a few additional MCDM methods:

- **Elimination Et Choix Traduisant la Realite (ELECTRE)**: ELECTRE is a family of MCDM methods that rank alternatives based on outranking relations. It considers multiple criteria and assesses the relative performance of alternatives through pairwise comparisons. The ELECTRE methods are particularly useful when dealing with imprecise or qualitative data.
- **VIseKriterijumska Optimizacija I Kompromisno Resenje (VIKOR)**: VIKOR is a multi-criteria decision-making method that combines compromise programming and outranking techniques. It determines a compromise solution by considering the maximum "group utility" and the minimum "individual regret". VIKOR can handle both quantitative and qualitative criteria.
- **Preference Ranking Organization METHod for Enrichment Evaluations II (PROMETHEE II)**: PROMETHEE II is an extension of the PROMETHEE method that incorporates preference functions and pairwise comparisons. It evaluates alternatives based on the net outranking flows and provides a ranking of alternatives. PROMETHEE II accounts for both positive and negative preference information.
- **Data Envelopment Analysis(DEA)**: DEA is a non-parametric method that evaluates the relative efficiency of alternatives. It considers multiple inputs and outputs to assess the efficiency of the alternatives and identify the most efficient ones. DEA can be particularly useful when there are limited or imprecise data available.
- **Grey Decision-Making Models**: grey decision-making models, such as grey relational analysis (GRA) and grey analytical network process (GANP), consider the uncertainty and limited information available in decision-making processes. These models can handle situations where the data are incomplete or imprecise, providing a different perspective on evaluating alternatives.

- **Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS)**: TOPSIS is a decision-making method that aims to find the alternative that is closest to the ideal solution and farthest from the negative ideal solution. It calculates the relative closeness of the alternatives based on their similarity to the positive ideal solution and their dissimilarity to the negative ideal solution. TOPSIS takes into account both positive and negative aspects of the criteria to determine the ranking of alternatives.
- **Weighted Sum Model (WSM)**: The weighted sum model (WSM) is a straightforward and widely used MCDM method. It involves assigning weights to criteria and aggregating the scores of the alternatives based on these weights. Each criterion is multiplied by its corresponding weight, and the results are summed to obtain a final score for each alternative. The alternative with the highest score is considered the best option. WSM is simple to implement and interpret, but it does not capture the interactions or trade-offs between criteria.

Implementing these additional MCDM methods alongside AHP can provide a comparative analysis and enhance the robustness of the decision-making process in evaluating cybersecurity options for smart grids. It allows for a more comprehensive understanding of the results and aids in making informed decisions.

5. Conclusions

5.1. Research Motivation

Smart grids have revolutionized the power sector through the introduction of transformative technologies, enabling efficient energy management, grid optimization, and the seamless integration of renewable energy sources, thereby fostering a climate-resilient energy transition [213–217]. Nonetheless, this digitization and increased connectivity also render smart grids susceptible to a wide range of cybersecurity threats and attacks.

5.2. Research Questions and Methodology

This article provides a comprehensive examination of cyberattacks and cybersecurity in smart grids, exploring various aspects and proposing optimal solutions.

First, it offers an overview of smart-grid components and applications, highlighting their importance in modern power systems. It delves into the types of cyberattacks that pose threats to smart grids, emphasizing the potential short-term and long-term technological, economic, safety, and social impacts on grid infrastructure and operations. It identifies the vulnerable components in smart grids that are susceptible to cyber threats and highlights the cascading effects that cyberattacks can have on different components of the grid. Quantitative models and metrics are examined to assess the impacts of cyberattacks on smart grids, with real-world case studies of cyberattacks on operational smart grids providing valuable insights. Furthermore, the study examines the short-term and long-term technological, economic, safety, and social implications of implementing cybersecurity measures in smart grids. It emphasizes the importance of confidentiality, integrity, and availability as key aspects of cybersecurity in protecting smart-grid infrastructure. Quantitative models and metrics are explored to assess the implications of cybersecurity measures on smart grids, and real-world examples demonstrate the practical implications of implementing cybersecurity measures on operational smart grids.

Second, the article addresses the challenge of selecting the optimal cybersecurity option using a multi-criteria decision-making (MCDM) approach. Specifically, the analytical hierarchy process (AHP) is employed to weigh and prioritize different cybersecurity options (i.e., access control and authentication, encryption, intrusion detection and prevention systems "IDPS", firewalls, security information and event management "SIEM", vulnerability assessment and penetration testing, security incident response, security monitoring and logging, security awareness and training, data backup and recovery, secure software development lifecycle "SSDL", incident response coordination, compliance and regulatory requirements) based on multiple criteria (i.e., security effectiveness, scalability, integration and compatibility, performance impact, cost-effectiveness, manageability and

usability, compliance and regulatory requirements, resilience and redundancy, vendor support and collaboration, future readiness, network segmentation, patch management, threat intelligence, vendor and supply chain security).

Third, the article explores the distinction between artificial intelligence (AI) and machine learning (ML). It examines their potential in the context of smart-grid cybersecurity, highlighting their roles in threat detection, anomaly detection, and incident response. The challenges associated with implementing AI techniques are also addressed, including issues of data quality, interpretability, and algorithm bias. Moreover, the article employs MCDM-AHP to determine the optimal AI option (i.e., machine learning, deep learning, natural language processing "NLP", genetic algorithms "GA", fuzzy logic, expert systems, swarm intelligence, Bayesian networks, and hybrid approaches) for smart-grid cybersecurity.

5.3. General Findings and Discussion

Based on the relative weights of the criteria, we can categorize them into three groups: criteria with high relative weights (above 10%), including "security effectiveness" with the highest weight, indicating its significant importance; criteria with medium relative weights (between 7% and 10%), such as "cost-effectiveness", "scalability", and "integration and compatibility", which are moderately important; and criteria with low relative weights (below 7%), including "performance impact" and several others (i.e., manageability and usability, compliance and regulatory requirements, resilience and redundancy, vendor support and collaboration, future readiness), which contribute to the overall evaluation but have relatively less influence. While the impact of the lower-weighted criteria is smaller, they should still be considered alongside other factors.

Based on the weighted sums of the alternatives, we can categorize them into three groups: alternatives with high weighted sums (above 5), including "access control and authentication" and "Security Information and Event Management (SIEM)", which are crucial for enhancing smart-grid cybersecurity; alternatives with medium weighted sums (between 5 and 5.5), such as "Intrusion Detection and Prevention Systems (IDPS)" and "security incident response", which offer solid performance in detecting and responding to security incidents; and alternatives with low weighted sums (below 4.5), such as "compliance and regulatory requirements" and "encryption", which provide value in their respective criteria but may not excel as strongly overall.

Based on the relative weights of the criteria, we can categorize them into three groups for evaluating cybersecurity options that incorporate artificial intelligence (AI) techniques in smart grids. The criteria with high relative weights, such as "security effectiveness", emphasize the accuracy of threat detection and the importance of AI in effective security measures. The criteria with medium relative weights, including "integration and compatibility" and "performance impact", highlight the need for seamless integration and the impact on system performance. The criteria with low relative weights, such as "manageability and usability", "cost-effectiveness", "resilience and redundancy", "future readiness", "compliance and regulatory requirements", "scalability", "vendor support and collaboration", "network segmentation", and "explainability and transparency", contribute to the evaluation but have less influence compared to higher-weighted criteria. Overall, security effectiveness, integration and compatibility, and performance impact are key considerations when evaluating AI-based cybersecurity options for smart grids, while also taking into account the other criteria to make well-rounded decisions aligned with smart-grid cybersecurity needs.

Based on the weighted sums, the alternatives for addressing the cybersecurity needs of smart grids can be categorized into three groups. The alternatives with high weighted sums, such as "deep learning", demonstrate strong potential and favorable performance across multiple criteria. The alternatives with medium weighted sums, including "hybrid approaches", "Bayesian networks", "swarm intelligence", and "machine learning", offer effectiveness and relevance in addressing cybersecurity challenges. The alternatives with low weighted sums, such as "fuzzy logic", "natural language processing (NLP)", "expert

systems", and "genetic algorithms (GA)", may have limited applicability or effectiveness compared to other options. These findings provide insights into the effectiveness and suitability of AI techniques and methods for enhancing smart-grid cybersecurity.

The advantages and limitations of MCDM-AHP are addressed, highlighting its potential shortcomings in capturing the full complexity of cybersecurity decision-making and the subjective nature of assigning weights to criteria. The article also proposes future directions on how to enhance MCDM-AHP for smart-grid cybersecurity and acknowledges the need for alternative MCDM techniques that can provide a more comprehensive and robust assessment. These alternative techniques may include the technique for order of preference by similarity to ideal solution (TOPSIS), preference ranking organization method for enrichment evaluations (PROMETHEE), and others. Each technique offers unique advantages and considerations in evaluating and comparing different cybersecurity options, addressing the limitations of MCDM-AHP.

5.4. Practical Implications

The article's examination of cyberattacks and cybersecurity in smart grids, solving the MCDM problem using AHP for optimal cybersecurity options, and exploring the potential benefits and challenges of AI, has several practical implications:

- **Enhanced Awareness and Preparedness**: the article's overview of smart-grid components, applications, and the types of cyberattacks helps raise awareness about potential vulnerabilities. Grid operators and cybersecurity professionals can use this knowledge to enhance their understanding of the risks and develop proactive measures to protect smart-grid infrastructure.
- **Prioritizing Optimal Cybersecurity Options**: the application of MCDM-AHP to find the optimal cybersecurity option provides a systematic approach for decision-making. Grid operators and policymakers can use this methodology to evaluate and prioritize various cybersecurity options based on multiple criteria, thereby allocating resources efficiently to the most effective solutions.
- **Strengthening Cybersecurity Measures**: the implications of cybersecurity for smart grids underscore the need for robust security measures. Grid operators can leverage the insights from this article to implement access controls, authentication protocols, encryption mechanisms, and other cybersecurity solutions to safeguard critical infrastructure against cyber threats.
- **Leveraging AI for Improved Security**: understanding the difference between AI and exploring its potential and challenges enables grid operators to make informed decisions about leveraging these technologies. By using AI algorithms for threat detection, anomaly detection, and incident response, smart grids can enhance their resilience and response capabilities.
- **Addressing the Limitations and Exploring Alternatives**: Acknowledging the limitations of MCDM-AHP and considering alternative MCDM techniques allows decision-makers to make more comprehensive assessments. This knowledge empowers them to evaluate different cybersecurity options and make well-informed decisions, considering a broader range of factors and trade-offs.

By embracing these practical implications, stakeholders in the smart-grid domain can enhance their cybersecurity posture, minimize vulnerabilities, and improve the overall resilience and reliability of the grid infrastructure in the face of evolving cyber threats.

Funding: This research was supported by the Laboratory of Renewable Energies and Advanced Materials (LERMA) and the College of Engineering and Architecture of the International University of Rabat (IUR).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data used in this study, along with the details of the methodology adopted, are comprehensively described in the methodology section (Section 2) of this article

Acknowledgments: The author extends sincere gratitude to the editorial office and the dedicated reviewers for their insightful feedback and meticulous review, which have enhanced the clarity of this article.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Bouramdane, A.A. *Climate Resilience: Insights from Global Negotiations and Morocco's Path to Sustainability*; Lambert Academic Publishing (LAP): London, UK, 2023; ISBN: 978-620-6-75083-3. Available online: https://www.morebooks.shop/shop-ui/shop/product/9786206750833 (accessed on 3 September 2023).
2. Bouramdane, A.A. Morocco's Road to a Climate-Resilient Energy Transition: Emissions Drivers, Solutions, and Barriers. 2023. Available online: https://www.researchgate.net/publication/368602073_Morocco%27s_Road_to_a_Climate-Resilient_Energy_Transition_Emissions_Drivers_Solutions_and_Barriers?channel=doi&linkId=63efefa531cb6a6d1d0df853&showFulltext=true (accessed on 3 September 2023).
3. Bouramdane, A.A. Assessment of CMIP6 Multi-Model Projections Worldwide: Which Regions Are Getting Warmer and Are Going Through a Drought in Africa and Morocco? What Changes from CMIP5 to CMIP6? *Sustainability* **2023**, *15*, 690. [CrossRef]
4. Bouramdane, A.A. Determining Vulnerable Areas to Warming and Drought in Africa and Morocco Based on CMIP6 Projections: Towards the Implementation of Mitigation and Adaptation Measures. In Proceedings of the EGU General Assembly 2023, Vienna, Austria, 24–28 April 2023; EGU23-2456. [CrossRef]
5. Bouramdane, A.A. Lieux Les Plus Sensibles Au Changement Climatique Nécessitant des Mesures d'Atténuation et d'Adaptation. *Energie/Mines Carrières*, 12 May 2023 . Available online: https://zenodo.org/record/7937556 (accessed on 3 September 2023).
6. Bouramdane, A.A. *Climate Risks and Energy Transition in Morocco: Vulnerability to Climate Losses and Damages and Uncertainty in the Renewable Electricity Mix Under Different Penetration*; Lambert Academic Publishing (LAP): London, UK, 2023; ISBN: 978-620-6-17980-1. Available online: https://www.morebooks.shop/shop-ui/shop/product/9786206179801 (accessed on 3 September 2023).
7. Bouramdane, A.A. Chaleur Caniculaire, Incendies Gigantesques à Répétition: Des Signes du Changement Climatique? *Énergie/Mines Carrières*, 2 August 2022. Available online: https://zenodo.org/record/7594264 (accessed on 3 September 2023).
8. Bouramdane, A.A. Sécheresse: L'extrême Va-t-il Progressivement Devenir la Norme? *Énergie/Mines Carrières*, 12 August 2022. Available online: https://zenodo.org/record/7594311 (accessed on 3 September 2023).
9. Bouramdane, A.A. Quelle est la Relation entre l'Agriculture et le Changement Climatique? *Énergie/Mines Carrières*, 20 February 2023. Available online: https://zenodo.org/record/7730008 (accessed on 3 September 2023).
10. Bouramdane, A.A. Solutions Pour Réduire la Pression sur l'Eau. *Énergie/Mines Carrières*, 26 May 2023. Available online: https://zenodo.org/record/8021765 (accessed on 3 September 2023).
11. Bouramdane, A.A. Préservation des Ressources d'Eau et Transition Énergétique: Point sur le Photovoltaïque Flottant. *Énergie/Mines Carrières*, 26 May 2023. Available online: https://zenodo.org/record/8021774 (accessed on 3 September 2023).
12. Bouramdane, A.A. Scenarios of Large-Scale Solar Integration with Wind in Morocco: Impact of Storage, Cost, Spatio-Temporal Complementarity and Climate Change. Ph.D. Thesis, Physics, Institut Polytechnique de Paris, Paris, France, 2021.
13. Bouramdane, A.-A. RCP 8.5 Climate Change Versus Cost Effect on Optimal Scenario Mixes of Variable and Dispatchable Technologies in Morocco: Climate Model Inter-Comparison. Ph.D. Thesis, Physics, Institut Polytechnique de Paris, Paris, France, 2021. [CrossRef]
14. RUSI. United Services Institute for Defense and Security Studies, "Security a Net-Zero Future: Cyber Risks to the Energy Transition". 2022. Available online: https://rusi.org/explore-our-research/publications/emerging-insights/securing-net-zero-future-cyber-risks-energy-transition (accessed on 4 July 2023).
15. Mo, Y.; Kim, T.H.J.; Brancik, K.; Dickinson, D.P.; Lee, H.; Perrig, A.; Sinopoli, B. Cyber–Physical Security of a Smart Grid Infrastructure. *Proc. IEEE* **2012**, *100*, 195–209.
16. Rekik, M.; Chtourou, Z.; Gransart, C.; Atieh, A. A Cyber-Physical Threat Analysis for Microgrids. In Proceedings of the 2018 15th International Multi-Conference on Systems, Signals & Devices (SSD), Hammamet, Tunisia, 19–22 March 2018; pp. 731–737.
17. Woo, P.S.; Kim, B.H. Methodology of Cyber Security Assessment in the Smart Grid. *J. Electr. Eng. Technol.* **2017**, *12*, 495–501. [CrossRef]
18. Asrari, A.; Ansari, M.; Khazaei, J.; Cecchi, V. Real-time Blackout Prevention in Response to Decentralized Cyberattacks on a Smart Grid. In Proceedings of the 2020 IEEE Texas Power and Energy Conference (TPEC), College Station, TX, USA, 6–7 February 2020; pp. 1–5.
19. Ansari, M.; Asrari, A. Reaction to Detected Cyberattacks in Smart Distribution Systems. In Proceedings of the 2020 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 17–20 February 2020; pp. 1–5.
20. Alkuwari, A.N.; Al-Kuwari, S.M.; Qaraqe, M.K. Anomaly Detection in Smart Grids: A Survey From Cybersecurity Perspective. In Proceedings of the 2022 3rd International Conference on Smart Grid and Renewable Energy (SGRE), Doha, Qatar, 20–22 March 2022; pp. 1–7.

21. Bhattacharjee, S.; Islam, M.J.; Abedzadeh, S. Robust Anomaly based Attack Detection in Smart Grids under Data Poisoning Attacks. In Proceedings of the 8th ACM on Cyber-Physical System Security Workshop, Nagasaki, Japan, 30 May 2022.
22. Liu, Q.; Hagenmeyer, V.; Keller, H.B. A Review of Rule Learning-Based Intrusion Detection Systems and Their Prospects in Smart Grids. *IEEE Access* **2021**, *9*, 57542–57564. [CrossRef]
23. Gül, Ö. A Research on Cyber Security Intrusion Detection Against Physical Access Cyber Attacks Using Open Source Software for Smart Grids. *Int. Rev. Electr. Eng. Iree* **2021**, *16*, 136–146. [CrossRef]
24. Bertone, F.; Lubrano, F.; Goga, K. Artificial Intelligence Techniques to Prevent Cyber Attacks on Smart Grids. *Ann. Disaster Risk Sci.* **2020**, *3*, 249381. [CrossRef]
25. Alwageed, H.S. Detection of Cyber Attacks in Smart Grids Using SVM-Boosted Machine Learning Models. *Serv. Oriented Comput. Appl.* **2022**, *16*, 313–326. [CrossRef]
26. Bhattarai, B.P.; Paudyal, S.; Luo, Y.; Mohanpurkar, M.U.; Cheung, K.; Tonkoski, R.; Hovsapian, R.; Myers, K.S.; Zhang, R.; Zhao, P.; et al. Big Data Analytics in Smart Grids: State-Of-the-Art, Challenges, Opportunities, and Future Directions. *IET Smart Grid* **2019**, *2*, 141–154. [CrossRef]
27. Colmenares-Quintero, R.F.; Quiroga-Parra, D.J.; Rojas, N.N.V.; Stansfield, K.; Colmenares-Quintero, J.C. Big Data Analytics in Smart Grids for Renewable Energy Networks: Systematic Review of Information and Communication Technology Tools. *Cogent Eng.* **2021**, *8*, 1935410. [CrossRef]
28. Zavala-Diaz, J.; Reyes-Archundia, E.; Olivares-Rojas, J.C.; Chavez-Baez, M.V.; Gutiérrez-Gnecchi, J.A.; Méndez-Patiño, A. Study of Public Key Cryptography Techniques for Authentication in Embedded Devices for Smart Grids. In Proceedings of the IEEE International Autumn Meeting on Power, Electronics and Computing (ROPEC 2021), Ixtapa, Mexico 10–12 November 2021; Volume 5; pp. 1–5.
29. Zhai, F.; Yang, T.; Zhao, B.; Chen, H. Privacy-Preserving Outsourcing Algorithms for Multidimensional Data Encryption in Smart Grids. *Sensors* **2022**, *22*, 4365. [CrossRef]
30. Nyangaresi, V.O.; Alsamhi, S.H. Towards Secure Traffic Signaling in Smart Grids. In Proceedings of the 2021 3rd Global Power, Energy and Communication Conference (GPECOM), Virtual, 5–8 October 2021; pp. 196–201.
31. Dutta, S.; Chukkapalli, S.S.L.; Sulgekar, M.; Krithivasan, S.; Das, P.K.; Joshi, A. Context Sensitive Access Control in Smart Home Environments. In Proceedings of the 2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), Baltimore, MD, USA, 25–27 May 2020; pp. 35–41.
32. Mutsvangwa, A.; Nleya, B.; Nleya, B. Secured Access Control Architecture Consideration for Smart Grids. In Proceedings of the 2016 IEEE PES PowerAfrica, Livingstone, Zambia, 28 June 2016–3 July 2016; pp. 228–233.
33. Wang, H.; Yu, H.; Zheng, H.; Wang, G.; Wang, C.; Li, B. A Secure and Efficient Data Transmission Scheme for Edge Devices in Smart Grids. In Proceedings of the 2020 IEEE International Conference on Progress in Informatics and Computing (PIC), Shanghai, China, 18–20 December 2020; pp. 323–327.
34. Sikeridis, D.; Bidram, A.; Devetsikiotis, M.; Reno, M.J. A Blockchain-Based Mechanism for Secure Data Exchange in Smart Grid Protection Systems. In Proceedings of the 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 10–13 January 2020; pp. 1–6.
35. Genge, B.; Haller, P.; Dumitru, C.D.; Enăchescu, C. Designing Optimal and Resilient Intrusion Detection Architectures for Smart Grids. *IEEE Trans. Smart Grid* **2017**, *8*, 2440–2451. [CrossRef]
36. Höfling, M. Design, Evaluation, and Optimization of Communication Architectures for Smart Grids. Ph.D. Thesis, Universität Tübingen, Tübingen, Germany, 2017.
37. Cheng, A.J.W. Evaluating the Impacts of Centralized and Decentralized Electric Vehicle Smart Charging Algorithms on the Electric Grid. Ph.D. Thesis, UC Irvine, Irvine, CA, USA, 2018.
38. Danzi, P. Communication Architectures for Reliable and Trusted Wireless Systems in Smart Grids. Ph.D. Thesis, Aalborg Universitet, Aalborg, Denmark, 2019.
39. Popovic, M. Redundancy in Communication Networks for Smart Grids. Ph.D. Thesis, École Polytechnique Fédérale de Lausanne, Lausanne, Switzerland, 2016.
40. Santos, A.A.; Rizk, A.; Steinke, F. Flexible Redundancy Generation for Virtual Network Embedding with an Application to Smart Grids. In Proceedings of the Eleventh ACM International Conference on Future Energy Systems, Virtual, 22–26 June 2020.
41. Gavriluta, C.; Boudinet, C.; Kupzog, F.; Gómez-Expósito, A.; Caire, R. Cyber-Physical Framework for Emulating Distributed Control Systems in Smart Grids. *Int. J. Electr. Power Energy Syst.* **2020**, *114*, 105375. [CrossRef]
42. Hammad, E.M.; Farraj, A.K.; Kundur, D. On Cyber-Physical Coupling and Distributed Control in Smart Grids. *IEEE Trans. Ind. Informatics* **2019**, *15*, 4418–4429. [CrossRef]
43. Petrenko, S. Ontology of Cyber Security of Self-Recovering Smart Grid. In *CEUR Workshop*; 2018. Available online: https://ceur-ws.org/Vol-2081/paper21.pdf (accessed on 3 September 2023).
44. Fries, S.; Hof, H.J. Regulations and Standards Relevant for Security of the Smart Grid. Available online: https://books.google.co.jp/books?hl=zh-CN&lr=&id=cgbSBQAAQBAJ&oi=fnd&pg=PA205&dq=Fries,+S.%3B+Hof,+H.J.+Regulations+and+Standards+Relevant+for+Security+of+the+Smart+Grid&ots=O4IQE-OY8W&sig=CBUkLHbDOPFDWh9_HIlvPKmFrIM&redir_esc=y#v=onepage&q&f=false (accessed on 3 September 2023).

45. Cespedes, R. Lessons Learned and Future Challenges for the Development of Smart Grids in Latin America. In Proceedings of the 2012 IEEE PES Innovative Smart Grid Technologies (ISGT), Washington, DC, USA, 16–20 January 2012; p. 1.
46. Ruland, C.; Sassmannshausen, J.; Waedt, K.; Zivic, N.S. Smart Grid Security–An Overview of Standards and Guidelines. *E I Elektrotechnik Und Informationstechnik* **2017**, *134*, 19–25. [CrossRef]
47. Falcis, N.D. Best Sync Practices & Architecture Strategies for Secure, Resilient PNT in Smart Grids. In *The Precise Time and Time Interval Systems and Applications Meeting*; Institute of Navigation (ION): Manassas, VA, USA, 2022.
48. Nicol, D.M.; Belovich, E.; Bohara, A. Smart Grid Network Flows Best Practices Checker. In Proceedings of the 2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Singapore, 25–28 October 2022; pp. 231–237.
49. Tang, S.; Liu, Z.; Wang, L. Power System Reliability Analysis Considering External and Insider Attacks on the SCADA System. In Proceedings of the 2020 IEEE/PES Transmission and Distribution Conference and Exposition (T&D), Chicago, IL, USA, 12–15 October 2020; pp. 1–5.
50. Miller, M.Z.; Griendling, K.; Mavris, D.N. Exploring Human Factors Effects in the Smart Grid System of Systems Demand Response. In Proceedings of the 2012 7th International Conference on System of Systems Engineering (SoSE), Genova, Italy, 16–19 July 2012; pp. 1–6.
51. Collen, A.; Szanto, I.C.; Benyahya, M.; Genge, B.; Nijdam, N.A. Integrating Human Factors in the Visualisation of Usable Transparency for Dynamic Risk Assessment. *Information* **2022**, *13*, 340. [CrossRef]
52. Fredman, D. A Human Side of the Smart Grid: Behavior-Based Energy Efficiency from Renters Using Real-Time Feedback and Competitive Performance-Based Incentives. Ph.D. Thesis, The University of Vermont and State Agricultural College, Burlington, VT, USA, 2018.
53. Szekeres, A.; Snekkenes, E.A. Representing Decision-Makers in SGAM-H: The Smart Grid Architecture Model Extended with the Human Layer. In Proceedings of the GraMSec@CSF, Boston, MA, USA, 22 June 2020.
54. Rodriguez, R.M.; Golob, E.J.; Xu, S. Human Cognition Through the Lens of Social Engineering Cyberattacks. *Front. Psychol.* **2020**, *11*, 1755.
55. Siddiqi, M.A.; Pak, W.; Siddiqi, M.A. A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures. *Appl. Sci.* **2022**, *12*, 6042 . [CrossRef]
56. Ray, J.R. Training Programs to Increase Cybersecurity Awareness and Compliance in Non-Profits. 2014. Available online: https://scholarsbank.uoregon.edu/xmlui/bitstream/handle/1794/19638/Ray2014.pdf (accessed on 3 September 2023).
57. Albediwi, M.; Sadaf, K. A Framework for Cybersecurity Awareness in Saudi Arabia. *J. Eng. Appl. Sci.* **2023**, *10*, 35–35 . [CrossRef]
58. Loi, M.; Christen, M. Ethical Frameworks for Cybersecurity. In *The International Library of Ethics, Law and Technology*; Springer Nature, Switzerland AG: Basel, Switzerland, 2020.
59. Zojer, G. Theorising Security: A Human Security Perspective on Cybersecurity. 2019. Available online: https://lauda.ulapland.fi/bitstream/handle/10024/64113/Zojer.Gerald%20part%202.pdf?sequence=1 (accessed on 3 September 2023).
60. Rahman, M.A.; Manshaei, M.H.; Al-Shaer, E.; Shehab, M. Secure and Private Data Aggregation for Energy Consumption Scheduling in Smart Grids. *IEEE Trans. Dependable Secur. Comput.* **2017**, *14*, 221–234. [CrossRef]
61. Aloulou, R.; Meddeb-Makhlouf, A.; Gassara, B.; Fakhfakh, A. Securing a Power Management Chain for Smart Grids. In Proceedings of the 2020 International Wireless Communications and Mobile Computing (IWCMC), Limassol, Cyprus, 15–19 June 2020; pp. 1713–1718.
62. de Jesus Martins, R.; Knob, L.A.D.; da Silva, E.G.; Wickboldt, J.A.; Filho, A.E.S.; Granville, L.Z. Specialized CSIRT for Incident Response Management in Smart Grids. *J. Netw. Syst. Manag.* **2018**, *27*, 269–285. [CrossRef]
63. Albasrawi, M.N.; Jarus, N.; Joshi, K.; Sarvestani, S.S. Analysis of Reliability and Resilience for Smart Grids. In Proceedings of the International Computer Software and Applications Conference, Vasteras, Sweden, 21–25 July 2014; pp. 529–534.
64. Kanca, A.M.; Sağiroğlu, Ş. Sharing Cyber Threat Intelligence and Collaboration. In Proceedings of the 2021 International Conference on Information Security and Cryptology (ISCTURKEY), Ankara, Turkey, 2–3 December 2021; pp. 167–172.
65. Vakilinia, I. Collaborative Analysis of Cybersecurity Information Sharing. Ph.D. Thesis, University of Nevada, Reno, NV, USA, 2019.
66. Bassiliades, N.; Chalkiadakis, G. Artificial Intelligence Techniques for the Smart Grid. *Adv. Build. Energy Res.* **2018**, *12*, 1–2. [CrossRef]
67. Ahmed, B.; Shuja, M.E.; Mishra, H.M.; Qtaishat, A.; Kumar, M. IoT Based Smart Systems using Artificial Intelligence and Machine Learning: Accessible and Intelligent Solutions. In Proceedings of the 2023 6th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 3–4 March 2023; pp. 1–6.
68. Parati, N.; Amdani, D.S.Y. *Deep Learning for Cyber Security*; Journal of Computer Science: Dubai, United Arab Emirates, 2020.
69. Basodi, S.; Tan, S.; Song, W.; Pan, Y. Data Integrity Attack Detection in Smart Grid: A Deep Learning Approach. *Int. J. Secur. Netw.* **2020**, *15*, 15–24. [CrossRef]
70. Aziz, S.; Irshad, M.; Haider, S.A.; Wu, J.; Deng, D.; Ahmad, S. Protection of a Smart Grid with the Detection of Cyber-Malware Attacks Using Efficient and Novel Machine Learning Models. *Front. Energy Res.* **2022**, *10*, 1102. [CrossRef]
71. Pokhrel, S.; Abbas, R.; Aryal, B. IoT Security: Botnet Detection in IoT Using Machine Learning. *arXiv* **2021**, arXiv:2104.02231.

72. McDonald, C.; Hogue, C.M.; Ashley, J.; Blejski, B.; Barraza, A.; Donner, P.; Leary, T.; Evangelista, P.F.; Leger, A.S. Investigating Machine Learning for Anomaly Detection in Phasor Measurement Unit Data. In Proceedings of the 2020 52nd North American Power Symposium (NAPS), Tempe, AZ, USA. 11–13 April 2021; pp. 1–6.
73. Sun, S.; Liu, C.; Zhu, Y.; He, H.; Xiao, S.; Wen, J. Deep Reinforcement Learning for the Detection of Abnormal Data in Smart Meters. *Sensors* **2022**, *22*, 8543. [CrossRef]
74. Li, X.J.; Ma, M.D.; Sun, Y. An Adaptive Deep Learning Neural Network Model to Enhance Machine-Learning-Based Classifiers for Intrusion Detection in Smart Grids. *Algorithms* **2023**, *16*, 288. [CrossRef]
75. Yu, T.; Da, K.; Wang, Z.; Ling, Y.; Li, X.; Bin, D.; Yang, C. An Advanced Accurate Intrusion Detection System for Smart Grid Cybersecurity Based on Evolving Machine Learning. *Front. Energy Res.* **2022**, *10*, 903370. [CrossRef]
76. de Oliveira Saraiva, F.; Asada, E.N. Decision Making in Intelligent Electrical Systems Using Distributed Artificial Intelligence and Heuristic Methods.In Proceedings of the 2013 IEEE PES Conference on Innovative Smart Grid Technologies (ISGT Latin America), Sao Paulo, Brazil, 15–17 Apri l 2013.
77. Biaojun, L.; Chuantao, Y.; Feng, Z.; Lin, W.H.; Jiashui, D.; Quanzhou, X. Intelligent Decision Support System for Business Forecasting Using Artificial Intelligence. *Arab. J. Sci. Eng.* **2021**, *48*, 4113.
78. Mohana, P.; Muthuvinayagam, M.; Umasankar, P.; Muthumanickam, T. Automation Using Artificial Intelligence Based Natural Language Processing. In Proceedings of the 2022 6th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 29–31 March 2022; pp. 1735–1739.
79. Lee, J.; Kim, M.; Park, K.; Noh, S.; Bisht, A.; Das, A.K.; Park, Y. Blockchain-Based Data Access Control and Key Agreement System in IoT Environment. *Sensors* **2023**, *23*, 5173. [CrossRef]
80. Abdulwahid, A.H. Artificial Intelligence-based Control Techniques for HVDC Systems. *Emerg. Sci. J.* **2023**, *7*, 643–653. [CrossRef]
81. Kulkarni, Y.; SayfHussain, Z.; Ramamritham, K.; Somu, N. EnsembleNTLDetect: An Intelligent Framework for Electricity Theft Detection in Smart Grid. In Proceedings of the 2021 International Conference on Data Mining Workshops (ICDMW), Auckland, New Zealand, 7–10 December 2021; pp. 527–536.
82. Bao, H.; Ren, B.; Li, B.; Kong, Q. BBNP: A Blockchain-Based Novel Paradigm for Fair and Secure Smart Grid Communications. *IEEE Internet Things J.* **2022**, *9*, 12984–12996. [CrossRef]
83. Gope, P.; Sikdar, B.K. Privacy-Aware Authenticated Key Agreement Scheme for Secure Smart Grid Communication. *IEEE Trans. Smart Grid* **2019**, *10*, 3953–3962. [CrossRef]
84. Sri, P.L.; Krishna, C.N.; Sai, A.D.; Roshini, S. Concealing the Data Using Cryptography. In Proceedings of the 2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS), Coimbatore, India, 2–4 February 2023; pp. 368–372.
85. Raghavasimhan, T.V.; Manoj, S.; Sweetlin, J.D.; Rakshit, S. Preventing Cryptographic Attacks Using AI-hard Password Authentication. In Proceedings of the 2023 International Conference on Networking and Communications (ICNWC), Chennai, India, 5–6 April 2023; pp. 1–6.
86. Choi, I.S.; Hong, J.; Kim, T. Multi-Agent Based Cyber Attack Detection and Mitigation for Distribution Automation System. *IEEE Access* **2020**, *8*, 183495–183504. [CrossRef]
87. Alatwi, H.A.; Morisset, C. Adversarial Machine Learning In Network Intrusion Detection Domain: A Systematic Review. *arXiv* **2021**, arXiv:abs/2112.03315.
88. Janjić, A.; Savic, S.M.; Velimirovic, L.Z.; Nikolić, V. Renewable Energy Integration in Smart Grids-Multicriteria Assessment Using the Fuzzy Analytical Hierarchy Process. *Turk. J. Electr. Eng. Comput. Sci.* **2015**, *23*, 1896–1912. [CrossRef]
89. Omar, F.; Bushby, S.T.; Williams, R.D. Assessing the Performance of Residential Energy Management Control Algorithms: Multi-Criteria Decision Making Using the Analytical Hierarchy Process. *Energy Build.* **2018**, *199*, 537–546. [CrossRef]
90. Alilou, M.; Gharehpetian, G.B.; Ahmadiahangar, R.; Rosin, A.; Anvari-Moghaddam, A. Day-Ahead Scheduling of Electric Vehicles and Electrical Storage Systems in Smart Homes Using a Novel Decision Vector and AHP Method. *Sustainability* **2022**, *14*, 11773. [CrossRef]
91. Ashari, S.; Setiawan, E.A. Optimization of Advanced Metering Infrastructure (AMI) Customer Ecosystem by Using Analytic Hierarchy Process Method. In Proceedings of the 2022 10th International Conference on Smart Grid (icSmartGrid), Istanbul, Turkey, 27–29 June 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 240–248.
92. Petrova, V.A. The Hierarchical Decision Model of Cybersecurity Risk Assessment. In Proceedings of the 2021 12th National Conference with International Participation (ELECTRONICA), Sofia, Bulgaria, 27–28 May 2021; pp. 1–4.
93. Ungkap, P.; Daengsi, T. Cybersecurity Awareness Modeling Associated with Influential Factors Using AHP Technique: A Case of Railway Organizations in Thailand. In Proceedings of the 2022 International Conference on Decision Aid Sciences and Applications (DASA), Chiangrai, Thailand., 23–25 March 2022; pp. 1359–1362.
94. Taherdoost, H.; Madanchian, M. Multi-Criteria Decision Making (MCDM) Methods and Concepts. *Encyclopedia* **2023**, *3*, 77–87. [CrossRef]
95. Piwowarski, M.; Nermend, K. Issues of Multi-Criteria Methods Applicability Supporting Complex Business Process Decision-Making in Management. In Proceedings of the International Conference on Knowledge-Based Intelligent Information & Engineering Systems, Verona, Italy, 7–9 September 2022.
96. Kumar, V.; Vrat, P.; Shankar, R. Prioritization of Strategies to Overcome the Barriers in Industry 4.0: A Hybrid MCDM Approach. *OPSEARCH* **2021**, *58*, 711–750. [CrossRef]

97. Youssef, M.I.; Webster, B. A Multi-Criteria Decision Making Approach to the New Product Development Process in Industry. *Rep. Mech. Eng.* **2022**, *3*, 83–93. [CrossRef]
98. Zavadskas, E.K.; Turskis, Z. Multiple Criteria Decision Making (MCDM) Methods in Economics: An Overview. *Technol. Econ. Dev. Econ.* **2011**, *17*, 397–427. [CrossRef]
99. Dymowa, L. *MCDM with Applications in Economics and Finance*; Springer Nature: Berlin/Heidelberg, Germany, 2011.
100. Ayag, Z. A Comparison Study of Fuzzy-Based Multiple-Criteria Decision-Making Methods to Evaluating Green Concept Alternatives in a New Product Development Environment. *Int. J. Intell. Comput. Cybern.* **2021**, *14*, 412–438. [CrossRef]
101. Macêdo-Júnior, R.O.; Serpa, F.S.; Santos, B.L.P.; Vasconcelos, C.R.D.; Silva, G.F.; Ruzene, D.S.; Silva, D.P. Produced Water Treatment and Its Green Future in the Oil and Gas Industry: A Multi-Criteria Decision-Making Study. *Int. J. Environ. Sci. Technol.* **2022**, *20*, 1369–1384. [CrossRef]
102. Osintsev, N. Multi-Criteria Decision-Making in Transport and Logistics. *Transp. Ural.* **2021**, *4*, 3–17 . [CrossRef]
103. Hajduk, S. Multi-Criteria Analysis in the Decision-Making Approach for the Linear Ordering of Urban Transport Based on TOPSIS Technique. *Energies* **2021**, *15*, 274. [CrossRef]
104. Kumar, A.; Sah, B.; Singh, A.R.; Deng, Y.; He, X.; Kumar, P.; Bansal, R.C. A Review of Multi Criteria Decision Making (MCDM) Towards Sustainable Renewable Energy Development. *Renew. Sustain. Energy Rev.* **2017**, *69*, 596–609. [CrossRef]
105. Lenarczyk, A.; Jaskólski, M.; Bućko, P. The Application of a Multi-Criteria Decision-Making for Indication of Directions of the Development of Renewable Energy Sources in the Context of Energy Policy. *Energies* **2022**, *15*, 9629. [CrossRef]
106. Shimray, B.A.; Singh, K.M.; Mehta, R.K. A Survey of Multi-Criteria Decision Making Technique Used in Renewable Energy Planning. *Int. J. Comput.* **2017**, *4523*, 124–140.
107. Witt, T.; Klumpp, M. Multi-Period Multi-Criteria Decision Making under Uncertainty: A Renewable Energy Transition Case from Germany. *Sustainability* **2021**, *13*, 6300. [CrossRef]
108. Bouramdane, A.A. Identifying Large-Scale Photovoltaic and Concentrated Solar Power Hot Spots: Multi-Criteria Decision-Making Framework. *World Acad. Sci. Eng. Technol. Int. J. Energy Power Eng.* **2023**, *17*. [CrossRef]
109. Bouramdane, A.A. Spatial Suitability Assessment of Onshore Wind Systems Using the Analytic Hierarchy Process . *World Acad. Sci. Eng. Technol. Int. J. Energy Power Eng.* **2023**, *17*. [CrossRef]
110. Bouramdane, A.A. Site Suitability of Offshore Wind Energy: A Combination of Geographic Referenced Information and Analytic Hierarchy Process. *World Acad. Sci. Eng. Technol. Int. J. Energy Power Eng.* **2023**, *17*. [CrossRef]
111. Bouramdane, A.A. *Potential Site for Offshore Floating Photovoltaic Systems in Morocco: Evaluation Criteria Required Considering Climate Change Effects to Achieve the Energy Trilemma*; Lambert Academic Publishing (LAP): London, UK, 2023. ISBN: 978-620-6-15964-3. Available online: https://www.morebooks.shop/shop-ui/shop/product/9786206159643 (accessed on 3 September 2023).
112. Sariyildiz, A.Y. Evaluation of the Health Performances of the Regions Affiliated to the Ministry of Health by Multi-Criteria Decision Making Techniques. *J. Health Sci. Med.* **2022**, *5*, 1562–1567 . [CrossRef]
113. Ardalan, S.A.; Mirzaie, A.; Begloo, A.G. Prioritizing the Factors Affecting Adoption of E-Commerce Using Multi-Criteria Decision Making Techniques in Tehran Hospitals in 2021. *J. Fam. Med. Prim. Care* **2022**, *11*, 7842–7849.
114. Castro-Lopez, A.; Cervero, A.; Galve-González, C.; Puente, J.; Bernardo, A.B. Evaluating Critical Success Factors in the Permanence in Higher Education Using Multi-Criteria Decision-Making. *High. Educ. Res. Dev.* **2021**, *41*, 628–646. [CrossRef]
115. Xu, S.; Yeyao, T.; Shabaz, M. Multi-Criteria Decision Making for Determining Best Teaching Method Using Fuzzy Analytical Hierarchy Process. *Soft Comput.* **2022**, *27*, 2795–2807. [CrossRef]
116. Thakkar, N.; Paliwal, P. A State-of-the-Art Review on Multi-criteria Decision Making Approaches for Micro-grid Planning. In *Algorithms for Intelligent Systems*; Springer Nature: Berlin/Heidelberg, Germany, 2022.
117. Omar, F. A Residential Energy Control Algorithm Assessment Tool forSmart Grid: Multi-Criteria Decision Making Using the AnalyticalHierarchy Process. Ph.D. Thesis, Faculty of the School of Engineering and Applied Science, Department of Electrical and Computer Engineering, University of Virginia, Charlottesville, VA, USA, 2019.
118. Zou, X.; Ma, S.D.; Xin, S. An Analytical Hierarchy Process Approach for Smart City Assessment in Japan. *Int. Rev. Spat. Plan. Sustain. Dev.* **2022**, *10*, 58–72. [CrossRef]
119. Saaty, T.L. Decision Making for Leaders: The Analytical Hierarchy Process for Decisions in a Complex World. 1982, 291. Available online: https://api.semanticscholar.org/CorpusID:53771268 (accessed on 3 September 2023).
120. Saaty, T.L. Decision Making with the Analytic Hierarchy Process. *Int. J. Serv. Sci.* **2008**, *1*, 83–98. [CrossRef]
121. Saaty, T.L. A Scaling Method for Priorities in Hierarchical Structures. *J. Math. Psychol.* **1977**, *15*, 234–281. [CrossRef]
122. Saaty, T.L. How to Make a Decision: The Analytic Hierarchy Process. *Interfaces* **1990**, *24*, 19–43. [CrossRef]
123. Saaty, T.L. The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation. 1990. Available online: https://api.semanticscholar.org/CorpusID:120643630 (accessed on 3 September 2023).
124. Saaty, R.W. The Analytic Hierarchy Process—What It Is and How It Is Used. *Math. Model.* **1987**, *9*, 161–176. [CrossRef]
125. Saaty, T.L. *What is the Analytic Hierarchy Process*; Springer: Berlin/Heidelberg, Germany, 1988.
126. Saaty, T.L. *Fundamentals of Decision Making and Priority Theory With the Analytic Hierarchy Process*; RWS Publications: Ellsworth Ave Pittsburgh, PA, USA, 2000.
127. Mancarella, P. Smart Multi-Energy Grids: Concepts, Benefits and Challenges. In Proceedings of the 2012 IEEE Power and Energy Society General Meeting, San Diego, CA, USA, 22–26 July 2012; pp. 1–2.
128. Abdullah, A.A.; Hassan, T.M. Smart Grid (SG) Properties and Challenges: An Overview. *Discov. Energy* **2022**, *2* , 8. [CrossRef]

129. Miroshnyk, O.; Moroz, O.; Shchur, T.; Chepizhnyi, A.; Qawaqzeh, M.Z.; Kocira, S. Investigation of Smart Grid Operation Modes with Electrical Energy Storage System. *Energies* **2023**, *16*, 2638. [CrossRef]
130. Simes, M.G.; Farret, F.A. *Stand Alone and Grid-Connected Inverters*; Wiley-IEEE Press: Hoboken, NJ, USA, 2017; pp. 177–202. [CrossRef]
131. Ahmetović, H.; Bosovic, A.; Merzic, A.; Music, M. Analysis of Microgrid Operation in Stand-Alone Mode - Sustainable Smart Tourist Village Case Study. *B H Electr. Eng.* **2020**, *14*, 35–42. [CrossRef]
132. Chankaya, M.; Ahmad, A.; Hussain, I. Smart Grid-Tied PV-Battery Storage System Operation under Dynamic Conditions. In Proceedings of the 2022 1st International Conference on Sustainable Technology for Power and Energy Systems (STPES), Srinagar, India, 4–6 July 2022; pp. 1–6.
133. Abdukhakimov, A.; Bhardwaj, S.; Gashema, G.; Kim, D.S. Reliability Analysis in Smart Grid Networks Considering Distributed Energy Resources and Storage Devices. *Int. J. Electr. Electron. Eng. Telecommun.* **2019**, *8*, 233–237. [CrossRef]
134. Xu, G.; Yu, W.; Griffith, D.W.; Golmie, N.; Moulema, P. Toward Integrating Distributed Energy Resources and Storage Devices in Smart Grid. *IEEE Internet Things J.* **2017**, *4*, 192–204. [CrossRef]
135. Al-Hallaj, S.; Wilke, S.K.; Schweitzer, B. Energy Storage Systems for Smart Grid Applications. 2017. Available online: https://link.springer.com/chapter/10.1007/978-3-319-48920-9_8 (accessed on 3 September 2023).
136. Gellings, C.W.; Gellings, C.W. *The Smart Grid: Enabling Energy Efficiency and Demand Response*; CRC press: Boca Raton, FL, USA, 2020.
137. Shakeri, M.; Pasupuleti, J.; Amin, N.; Rokonuzzaman, M.; Low, F.W.; Yaw, C.T.; Asim, N.; Samsudin, N.A.; Tiong, S.K.; Hen, C.K.; et al. An Overview of the Building Energy Management System Considering the Demand Response Programs, Smart Strategies and Smart Grid. *Energies* **2020**, *13*, 3299. [CrossRef]
138. Nawaz, F.; Ahmad, G.; Ihsanullah.; Javed, K.; Khan, I.; Khan, W. An optimal Home Energy Management System Based on Time of Use pricing Scheme in Smart Grid. *Int. J. Sci. Eng. Res.* **2017**, *8*, 882–894.
139. Das, S.; Acharjee, P.; Bhattacharya, A. Charging Scheduling of Electric Vehicle Incorporating Grid-to-Vehicle and Vehicle-to-Grid Technology Considering in Smart Grid. *IEEE Trans. Ind. Appl.* **2021**, *57*, 1688–1702. [CrossRef]
140. Shebanow, A. The Efficacy and Challenges of SCADA and Smart Grid Integration. *J. Cyber Secur. Inf. Syst.* **2016**, *1*, 1–7.
141. Tanwar, S.; Tyagi, S.; Kumar, S. *The Role of Internet of Things and Smart Grid for the Development of a Smart City*; Springer: Singapore, 2018.
142. Winanda, M.; Satriawan, A.; Gondokaryono, Y.S. Smart Grid Secure Data Transmission for High Voltage Grid. In Proceedings of the 2014 International Conference on Information Technology Systems and Innovation (ICITSI), Bandung, Indonesia, 24–27 November 2014; pp. 70–75.
143. Zolin, D.; Ryzhkova, E. Wide Area Monitoring System (WAMS) Application in Smart Grids. In Proceedings of the 2021 3rd International Youth Conference on Radio Electronics, Electrical and Power Engineering (REEPE), Moscow, Russia, 11–13 March 2021; pp. 1–6.
144. Vijayalakshmi, S.; Kavitha, D. Optimal Placement of Phasor Measurement Units for Smart Grid Applications. In Proceedings of the 2018 National Power Engineering Conference (NPEC), Madurai, India, 9–10 March 2018; pp. 1–6.
145. Peng, F.Z. Flexible AC Transmission Systems (FACTS) and Resilient AC Distribution Systems (RACDS) in Smart Grid. *Proc. IEEE* **2017**, *105*, 2099–2115. [CrossRef]
146. Wall, R.L. *Intelligent Application of Flexible AC Transmission System Components in an Evolving Power Grid*; University of Arkansas: Fayetteville, AR, USA, 2018.
147. Abrahamsen, F.E.; Ai, Y.; Cheffena, M. Communication Technologies for Smart Grid: A Comprehensive Survey. *Sensors* **2021**, *21*, 8087. [CrossRef] [PubMed]
148. Mohtashami, S.; Pudjianto, D.; Strbac, G. Strategic Distribution Network Planning With Smart Grid Technologies. *IEEE Trans. Smart Grid* **2017**, *8*, 2656–2664. [CrossRef]
149. Sachdeva, P. The Role of Advanced Distribution Automation in Smart Grid. *Int. J. Eng. Res.* **2020**, *9*. [CrossRef]
150. Nasrallah, M.; Ismeil, M.A. Smart Grid - Reliability, Security, Self-Healing Standpoint, and State of the Art. *Svu-Int. J. Eng. Sci. Appl.* **2022**, *3*, 87–92. [CrossRef]
151. Sarathkumar, D.; Srinivasan, M.; Stonier, A.A.; Samikannu, R.; Dasari, N.R.; Raj, R.A. A Technical Review on Self-Healing Control Strategy for Smart Grid Power Systems. *IOP Conf. Ser. Mater. Sci. Eng.* **2021**, *1055*, 012153. [CrossRef]
152. Halle, P.D.; S., S. SRAMI: Secure and Reliable Advanced Metering Infrastructure Protocol for Smart Grid 2021. Available online: https://assets.researchsquare.com/files/rs-791353/v1_covered.pdf?c=1632234486 (accessed on 3 September 2023).
153. Ghosal, A.; Conti, M. Key Management Systems for Smart Grid Advanced Metering Infrastructure: A Survey. *IEEE Commun. Surv. Tutorials* **2018**, *21*, 2831–2848. [CrossRef]
154. Bouramdane, A.A. *How to Manage Vulnerabilities in the Renewable Energy Environment?* Leadvent Group, Renewable Energy Cyber Security Forum: Berlin, Germany, 2023. [CrossRef]
155. Lázaro, J.; Astarloa, A.; Rodríguez, M.; Bidarte, U.; Jiménez, J. A Survey on Vulnerabilities and Countermeasures in the Communications of the Smart Grid. *Electronics* **2021**, *10*, 1881. [CrossRef]
156. Gajanan, L.S.; Kirar, M.K.; Raju, M. Cyber-Attacks on Smart Grid System: A Review. In Proceedings of the 2022 IEEE 10th Power India International Conference (PIICON), New Delhi, India, 25–27 November 2022; pp. 1–6.

157. Roy, S. Denial of Service Attack on Protocols for Smart Grid Communications. In *Research Anthology on Combating Denial-of-Service Attacks*; IGI Global: Hershey, PA, USA, 2021.
158. Said, D. Quantum Computing and Machine Learning for Cybersecurity: Distributed Denial of Service (DDoS) Attack Detection on Smart Micro-Grid. *Energies* **2023**, *16*, 3572. [CrossRef]
159. Monday, H.N.; Li, J.P.; Nneji, G.U.; Yutra, A.Z.; Lemessa, B.D.; Nahar, S.; James, E.C.; ul Haq, A. The Capability of Wavelet Convolutional Neural Network for Detecting Cyber Attack of Distributed Denial of Service in Smart Grid. In Proceedings of the 2021 18th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), Chengdu, China, 17–19 December 2021; pp. 413–418.
160. Eder-Neuhauser, P.; Zseby, T.; Fabini, J. Malware Propagation in Smart Grid Networks: Metrics, Simulation and Comparison of Three Malware Types. *J. Comput. Virol. Hacking Tech.* **2018**, *15*, 109–125. [CrossRef]
161. Akhtar, T.; Gupta, B.B.; Yamaguchi, S. Malware Propagation Effects on SCADA System and Smart Power Grid. In Proceedings of the 2018 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 12–14 January 2018; pp. 1–6.
162. Li, P.; an Yu, S.; Xiao, L. Smart Grid Worm Detection Based on Deep Reinforcement Learning. In Proceedings of the 2022 IEEE/CIC International Conference on Communications in China (ICCC), Foshan, China, 11–13 August 2022; pp. 684–689.
163. AlMajali, A.; Dweik, W. Analysing and Modelling Worm Propagation Speed in the Smart Grid Communication Infrastructure. *Int. J. Embed. Syst.* **2019**, *11*, 11–21. [CrossRef]
164. Jenkins, A.M. Device-Centric Ransomware Detection using Machine Learning-Based Memory Forensics for Smart Inverters 2022. Available online: https://www.acsac.org/2022/workshops/icss/2022-icss-jenkins.pdf (accessed on 3 September 2023).
165. Alvee, S.R.B.; Ahn, B.; Kim, T.; Su, Y.; Youn, Y.W.; Ryu, M.H. Ransomware Attack Modeling and Artificial Intelligence-Based Ransomware Detection for Digital Substations. In Proceedings of the 2021 6th IEEE Workshop on the Electronic Grid (eGRID), New Orleans, LA, USA, 8–10 November 2021 ; pp. 1–5.
166. SonicWall Cyber Threat Report: Charting Cybercrime's Shifting Frontlines. 2023. Available online: https://www.sonicwall.com/2023-cyber-threat-report/ (accessed on 3 September 2023).
167. Cybercrime Magazine, Global Ransomware Damage Costs Predicted to Reach 20 Billion (USD) by 2021. Available online: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/ (accessed on 3 September 2023).
168. Lamble, B. Of Nesting Dolls and Trojan Horses: A Survey of Legal and Policy Issues Attendant to Vehicle-to-Grid Battery Electric Vehicles. *Chicago-Kent* **2011**, *86*, 193.
169. Ozen, A. Malware in Smart Grid. Ph.D. Thesis, Iowa State University, Ames, IA, USA, 2017.
170. Pepin, L.; Wang, L.; Wang, J.; Han, S.; Pishawikar, P.; Herzberg, A.; Zhang, P.; Miao, F. Botnets Breaking Transformers: Localization of Power Botnet Attacks Against the Distribution Grid. *arXiv* **2022**, arXiv:2203.10158.
171. Yang, H.; Cheng, L.; Chuah, M.C. Detecting Peer-to-Peer Botnets in SCADA Systems. In Proceedings of the 2016 IEEE Globecom Workshops (GC Wkshps), Washington, DC, USA, 4–8 December 2016; pp. 1–6.
172. AV-TEST Award 2022: Tested and Award-Winning Security. Available online: https://www.av-test.org/en/news/av-test-award-2022-tested-and-award-winning-security/ (accessed on 3 September 2023).
173. Holm, H.; Flores, W.R.; Ericsson, G. Cyber Security for a Smart Grid—What About Phishing? In Proceedings of the IEEE PES ISGT Europe 2013, Lyngby, Denmark, 6–9 October 2013; pp. 1–5.
174. The 2021 Verizon Data Breach Investigations Report. Available online: https://www.verizon.com/about/news/verizon-2021-data-breach-investigations-report (accessed on 3 September 2023).
175. Stanojevic, M.; Capko, D.; Lendák, I.; Stoja, S.; Jelacic, B. Fighting Insider Threats, with Zero-Trust in Microservice-based, Smart Grid OT Systems. In *Acta Polytechnica Hungarica*; Óbuda University: Budapest, Hungary, 2023.
176. Li, B.; Lu, R.; Xiao, G.; Bao, H.; Ghorbani, A.A. Towards Insider Threats Detection in Smart Grid Communication Systems. *IET Commun.* **2019**, *13*, 1728–1736. [CrossRef]
177. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). Available online: https://www.industrialcybersecuritypulse.com/iiot-cloud/key-takeaways-from-2020-ics-cert-vulnerabilities/ (accessed on 3 September 2023).
178. Wlazlo, P.; Sahu, A.; Mao, Z.; Huang, H.; Goulart, A.E.P.; Davis, K.R.; Zonouz, S. Man-in-The-Middle Attacks and Defense in a Power System Cyber-Physical Testbed. *IET Cyper-Phys. Syst. Theory Appl.* **2021**, *6*, 164–177. [CrossRef]
179. Tharzeen, A.; Natarajan, B.; Srinivasan, B. Phasor Data Correction and Transmission System State Estimation Under Man-in-the-Middle Attack. In Proceedings of the 2023 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 16–19 January 2023; pp. 1–5.
180. Akuffo-Badoo, E.B. Understanding Advanced Persistent Threats. *Adv. Multidiscip. Sci. Res. J. Publ.* **2022**. Available online: https://api.semanticscholar.org/CorpusID:251140813 (accessed on3 September 2023). [CrossRef]
181. Stylianou, L.; Hadjidemetriou, L.; Asprou, M.; Zacharia, L.; Michael, M.K. A Behavioral Model to Detect Data Manipulation Attacks of Synchrophasor Measurements. In Proceedings of the 2021 IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe), Espoo, Finland, 18–21 October 2021 ; pp. 1–6.
182. Duman, O.; Wang, L.; Au, M.; Kassouf, M.; Debbabi, M. Hardening Substations Against Supply Chain Attacks Under Operational Constraints. In Proceedings of the 2022 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), New Orleans, LA, USA, 24–28 April 2022; pp. 1–5.

183. Zhang, H.; Liu, B.; Wu, H. Smart Grid Cyber-Physical Attack and Defense: A Review. *IEEE Access* **2021**, *9*, 29641–29659. [CrossRef]
184. Wadhawan, Y.; AlMajali, A.; Neuman, C. A Comprehensive Analysis of Smart Grid Systems against Cyber-Physical Attacks. *Electronics* **2018**, *7*, 249. [CrossRef]
185. Gowtham, M.; Pramod, H.B. Semantic Query-Featured Ensemble Learning Model for SQL-Injection Attack Detection in IoT-Ecosystems. *IEEE Trans. Reliab.* **2022**, *71*, 1057–1074.
186. Stellios, I.; Kotzanikolaou, P.; Psarakis, M. Advanced Persistent Threats and Zero-Day Exploits in Industrial Internet of Things. In *Security and Privacy Trends in the Industrial Internet of Thing;* Springer: Cham, Switzerland, 2019.
187. Fursov, I.; Yamkovyi, K.; Shmatko, O. Smart Grid and Wind Generators: An Overview of Cyber Threats and Vulnerabilities of Power Supply Networks. *Radioelectron. Comput. Syst.* **2022**, *4*, 50–63. [CrossRef]
188. Gumrukcu, E.; Arsalan, A.; Muriithi, G.M.; Joglekar, C.; Aboulebdeh, A.; Zehir, M.A.; Papari, B.; Monti, A. Impact of Cyber-Attacks on EV Charging Coordination: The Case of Single Point of Failure. In Proceedings of the 2022 4th Global Power, Energy and Communication Conference (GPECOM), Cappadocia, Turkey, 14–17 June 2022; pp. 506–511.
189. Drayer, E.; Routtenberg, T. Cyber Attack Localization in Smart Grids by Graph Modulation (Brief Announcement). In Proceedings of the International Conference on Cyber Security Cryptography and Machine Learning, Be'er Sheva, Israel, 27–28 June 2019.
190. Salehpour, A.; Al-Anbagi, I.S.; Yow, K.C.; Cheng, X. Modeling Cascading Failures in Coupled Smart Grid Networks. *IEEE Access* **2022**, *10*, 81054–81070. [CrossRef]
191. Novikov, O.; Vedmedenko, G.; Stopochkina, I.; Ilin, M. Cyber Attacks Cascading Effects Simulation for Ukraine Power Grid. In Proceedings of the International Conference on Intelligent Tutoring Systems, Virtual Event, 7–11 June 2021.
192. 2015 Ukraine Power Grid Hack. Available online: https://en.wikipedia.org/wiki/2015_Ukraine_power_grid_hack (accessed on 3 September 2023).
193. DRAGOS 2017, Crashoverride: Analyzing the Malware that Attacks Power Grids. Available online: https://www.wired.com/story/crash-override-malware/ (accessed on 3 September 2023).
194. Industrial Cybersecurity Pulse 2021, Throwback Attack: BlackEnergy Attacks the Ukrainien Power Grid. Available online: https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-blackenergy-attacks-the-ukrainian-power-grid/ (accessed on 3 September 2023).
195. Cyberattaque NotPetya. Available online: https://fr.wikipedia.org/wiki/Cyberattaque_NotPetya (accessed on 3 September 2023).
196. Berserk Bear. Available online: https://en.wikipedia.org/wiki/Berserk_Bear (accessed on 3 September 2023).
197. INSIDER 2016, Hackers are Hitting Israel's Energy Sector with a 'Severe Cyber Attack. Available online: https://www.businessinsider.com/israel-electric-cyberattack-2016-1 (accessed on 3 September 2023).
198. Semertzis, I.; Rajkumar, V.S.; Stefanov, A.; Fransen, F.; Palensky, P. Quantitative Risk Assessment of Cyber Attacks on Cyber-Physical Systems using Attack Graphs. In Proceedings of the 2022 10th Workshop on Modelling and Simulation of Cyber-Physical Energy Systems (MSCPES), Milan, Italy, 3 May 2022; pp. 1–6.
199. Chai, K.Y.; Zolkipli, M.F.B. Review on Confidentiality, Integrity and Availability in Information Security. *J. Ict Educ.* **2021**, *8*, 34–42. [CrossRef]
200. Edwards, N.; Kiser, S.B.; Haynes, J.B. Answering the Cybersecurity Issues: Confidentiality, Integrity, and Availability. *J. Strateg. Innov. Sustain.* **2020**, *15*, 10–14.
201. Ding, J.; Qammar, A.; Zhang, Z.; Karim, A.; Ning, H. Cyber Threats to Smart Grids: Review, Taxonomy, Potential Solutions, and Future Directions. *Energies* **2022**, *15*, 6799. [CrossRef]
202. Gusrialdi, A.; Qu, Z. Smart Grid Security: Attacks and Defenses. In *Smart Grid Control*; Springer: Cham, Switzerland, 2018.
203. Smit, T.; van Haastrecht, M.; Spruit, M.R. The Effect of Countermeasure Readability on Security Intentions. *J. Cybersecur. Priv.* **2021**, *1*, 675–703. [CrossRef]
204. FORTINET, Fortinet Security Fabric Enables Digital Innovation: Broad, Integrated, and Automated. Available online: https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-security-fabric.pdf (accessed on 3 September 2023).
205. NIST, Cybersecurity for Smart Grid Systems. Available online: https://www.nist.gov/programs-projects/cybersecurity-smart-grid-systems (accessed on 3 September 2023).
206. Faquir, D.; Chouliaras, N.; Sofia, V.; Olga, K.; Maglaras, L. Cybersecurity in Smart Grids, Challenges and Solutions. *Aims Electron. Electr. Eng.* **2021**, *5*, 24–37.
207. Bleier, M.T.; Langer, D.L.; Skopik, F. *Smart Grid Cybersecurity Standards: Today and Tomorrow*; Computer Science, Engineering; 2013. Available online: https://api.semanticscholar.org/CorpusID:31361949 (accessed on 3 September 2023).
208. Nvidia. What's the Difference Between Artificial Intelligence, Machine Learning and Deep Learning? 2016. Available online: https://blogs.nvidia.com/blog/2016/07/29/whats-difference-artificial-intelligence-machine-learning-deep-learning-ai/ (accessed on 3 September 2023).
209. Srihith, I.V.D.; Kumar, I.V.S.; Varaprasad, R.; Mohan, Y.R.; Srinivas, T.A.S.; Sravanthi, Y. Future of Smart Cities: The Role of Machine Learning and Artificial Intelligence. *South Asian Res. J. Eng. Technol.* **2022**, *4*, 110–119. [CrossRef]

210. Pullum, L.L.; Jindal, A.; Roopaei, M.; Diggewadi, A.; Andoni, M.; Zobaa, A.F.; Alam, A.; Bani-Ahmed, A.; Ngo, Y.; Vyas, S.; et al. Big Data Analytics in the Smart Grid: Big Data Analytics, Machine Learning and Artificial Intelligence in the Smart Grid: Introduction, Benefits, Challenges and Issues. 2017. Available online: https://api.semanticscholar.org/CorpusID:66344530 (accessed on 3 September 2023).
211. Szczepaniuk, H.; Szczepaniuk, E.K. Applications of Artificial Intelligence Algorithms in the Energy Sector. *Energies* **2022**, *16*, 347. [CrossRef]
212. Khazaii, J. Analytical Hierarchy Process (AHP); In *Advanced Decision Making for HVAC Engineers*; Springer: Cham, Switzerland, 2016. [CrossRef]
213. Bouramdane, A.A. Hydrogène, Captage et Stockage du CO2 et Sobriété Énergétique : Tour d'Horizon. *Énergie/Mines Carrières*, 27 March 2023. Available online: https://zenodo.org/record/7774592 (accessed on 3 September 2023).
214. Bouramdane, A.A. Mix Électrique Marocain : Défis Face à l'Urgence Climatique. *Énergie/Mines Carrières*, 26 December 2022. Available online: https://zenodo.org/record/7594427 (accessed on 3 September 2023).
215. Bouramdane, A.A. PV, CSP et Éolien au Maroc: Intégration à Géométrie Variable. *Énergie/Mines Carrières*, 15 July 2022. Available online: https://zenodo.org/record/7594221 (accessed on 3 September 2023).
216. Bouramdane, A.A. Production d'hydrogène vert au Maroc: Quelle technologie est la plus adaptée à différents niveaux de pénétration renouvelable? *Énergie/Mines Carrières*, 5 July 2023. Available online:https://zenodo.org/record/8144588 (accessed on 3 September 2023).
217. Bouramdane, A.A. Pourquoi l'Atténuation et l'Adaptation aux Changements Climatiques sont Complémentaires? *Énergie/Mines Carrières*, 10 November 2022. Available online: https://zenodo.org/record/7594404 (accessed on 3 September 2023).