energies

MDPI

Article

Decision-Support Framework for Cybersecurity Risk Assessment in EV Charging Infrastructure

Roberts Grants [1,*], Nadezhda Kunicina [1], Rasa Brūzgienė [2], Šarūnas Grigaliūnas [2] and Andrejs Romanovs [3]

[1] Faculty of Computer Science, Information Technology and Energy, Institute of Industrial Electronics, Electrical Engineering and Energy, Riga Technical University, LV-1048 Riga, Latvia; nadezda.kunicina@rtu.lv
[2] Department of Computer Sciences, Faculty of Informatics, Kaunas University of Technology, LT-51368 Kaunas, Lithuania; rasa.bruzgiene@ktu.lt (R.B.); sarunas.grigaliunas@ktu.lt (Š.G.)
[3] Information Technology Institute, Riga Technical University, LV-1048 Riga, Latvia; andrejs.romanovs@rtu.lv
* Correspondence: roberts.grants@rtu.lv

Abstract

Rapid expansion of electric vehicle adoption has led to increased dependence on a charging infrastructure that is tightly integrated with energy distribution systems and digital communication networks. As electric vehicle charging stations evolve into complex cyber–physical systems, cybersecurity risks pose a growing threat to grid reliability and user trust. This paper presents a hybrid decision-support framework for cybersecurity risk assessment in EV charging infrastructure that advances beyond prior multi-criteria decision-making approaches by combining interpretability with data-driven validation. Specifically, the framework integrates the Analytic Hierarchy Process (AHP) for expert-driven weighting of cybersecurity attributes with PROMETHEE for flexible threat prioritization, enabling transparent and auditable risk rankings. The framework categorizes cybersecurity criteria across four infrastructure layers—transmission, distribution, consumer, and electric vehicle charging stations—and assigns relative weights through expert-driven pairwise comparisons. PROMETHEE is then applied to rank potential cyber threats based on these weights, allowing for flexible prioritization of cybersecurity interventions. The methodology is validated using the real-world WUSTL-IIoT-2018 SCADA dataset, which includes simulated reconnaissance (network scanning), device identification, and exploitation attacks. While this dataset does not natively include OCPP 2.0 or ISO 15118 protocols, the experimental results demonstrate strong discrimination power (AUC = 0.99, recall = 95%) and provide a basis for extension to modern EVSE communication standards. The results identify critical metrics such as anomalous source packet behavior and encryption reliability as key vulnerability markers, aligning with documented EV charging attack scenarios. By bridging expert judgment with empirical traffic data, the proposed framework offers both technical robustness and explainability, supporting grid operators, SOC teams, and infrastructure planners in systematically assessing risks, allocating resources, and enhancing the resilience of EV charging ecosystems against evolving cyber threats.

Keywords: cybersecurity; EV charging infrastructure; risk assessment; AHP; PROMETHEE; SCADA; smart grid

Academic Editor: JongHoon Kim

Received: 7 March 2026
Revised: 2 April 2026
Accepted: 4 April 2026
Published: 8 April 2026

1. Introduction

Electric mobility is accelerating worldwide, with electric vehicle (EV) adoption rising sharply under the impetus of environmental goals and policy incentives. This growth

demands a reliable and secure EV-charging infrastructure, which is now a critical component of modern smart grids. Contemporary charging stations are highly connected: they interface with grid-control systems, cloud services, user-facing mobile applications, and IoT-based energy-management platforms. Such pervasive digital interconnectedness dramatically enlarges the attack surface for malicious actors. Recent studies underline that distributed-energy systems and EV-charging networks are especially vulnerable to cyber-attacks owing to (i) ubiquitous remote access, (ii) real-time data exchange, and (iii) complex digital interfaces [1]. EV charging stations, as public cyber–physical gateways to the grid, face threats ranging from unauthorized access and malware injection to payment fraud and protocol tampering [2,3]. Compromise of a station's communication stack can disrupt charging sessions, inject malicious commands, or even introduce cascading instabilities into the wider power system. Indeed, denial-of-service, ransomware, and data-interception campaigns have been highlighted as emergent threats to smart-grid and EV infrastructure [4]. The convergence of cybersecurity and electric-power engineering therefore demands urgent, systematic attention to safeguard grid stability, financial integrity, and consumer safety. Several recent real-world incidents highlight the urgency of this challenge. In 2023, coordinated ransomware campaigns temporarily disabled public charging stations in parts of Europe [5], while in 2024, researchers demonstrated protocol manipulation attacks on ISO 15118 [6] that enabled energy theft and denial of service [7]. In 2025, ENISA and national regulators issued warnings about vulnerabilities in OCPP 2.0 implementations that could allow large-scale remote manipulation of charging sessions [8,9]. These cases illustrate that EV charging infrastructure is no longer a hypothetical attack surface but a critical security concern for grid reliability, financial integrity, and consumer trust.

Traditional qualitative risk assessments are inadequate for such a dynamic, multi-faceted threat landscape. Consequently, there is a clear need for structured, quantitative methodologies that accommodate the complexity and interdependence of EV-charging ecosystems. Multi-Criteria Decision-Making (MCDM) techniques offer a powerful analytical framework to meet this challenge. In particular,

- The Analytic Hierarchy Process (AHP) decomposes a complex cybersecurity problem into a hierarchy of criteria and derives consistent weights via expert pairwise comparisons [10];
- The Preference Ranking Organization Method for Enrichment Evaluations (PROMETHEE) provides an outranking mechanism to prioritize threat scenarios under uncertainty [11].

AHP guarantees traceability and consistency of criteria weighting, whereas PROMETHEE excels at computing preference flows without a rigid hierarchical structure. By combining these two, a hybrid AHP–PROMETHEE approach can synergistically exploit expert knowledge and data-driven evaluation to yield a comprehensive cybersecurity risk assessment.

This work proposes a hybrid AHP–PROMETHEE framework for cybersecurity risk assessment in EV-charging infrastructure. The novelty of the framework lies in (i) explicitly linking cybersecurity attributes to layered EVSE infrastructure, (ii) integrating expert-driven interpretability with empirical traffic validation, and (iii) offering explainability advantages compared with purely machine-learning-based intrusion detection approaches.

The main contributions of this work are as follows:

1. Layered infrastructure modeling by segmenting the EV-charging ecosystem into four cyber–physical layers (transmission, distribution, consumer, and EV charging station) and mapping key cybersecurity attributes to each layer, linking power-system operations with cyber-risk factors.

2. AHP-based weighting by expert judgment (informed by standards and threat reports) that is encoded in pairwise-comparison matrices, yielding a consistent set of attribute weights reflecting each factor's impact on grid reliability and security.
3. PROMETHEE-based ranking of cybersecurity threats using AHP-derived weights, producing a prioritized list based on quantitative traffic metrics and stakeholder preferences.
4. Experimental validation of the proposed framework using the WUSTL-IIoT-2018 ICS/SCADA dataset [12], generated in an industrial control system testbed associated with a water storage and treatment process. While the dataset does not natively include OCPP 2.0 or ISO 15118 [6] protocols, the experiments demonstrate methodological applicability and provide a foundation for extension to modern EVSE communication standards [7–9].

By synthesizing expert knowledge, real network data, and decision-analysis techniques, the proposed solution supports grid operators, policy-makers, and EV-service providers in making transparent, justifiable cybersecurity decisions. Ultimately, this work aims to enhance the security of EV-charging ecosystems as they become a cornerstone of sustainable transportation and future smart-grid operation.

The remainder of this paper is organized as follows. Section 2 presents a literature review on cybersecurity risk assessment in power systems and EV infrastructure. Section 3 describes the proposed methodology, including the layered model and the AHP–PROMETHEE framework. Section 4 presents the results and discussion, including validation, sensitivity analysis, and practical implications. Finally, Section 5 concludes the paper.

2. Literature Review

The protection of power grids and electric vehicle charging infrastructure from cyber threats has become a critical priority as digitalization transforms the energy landscape. This section reviews existing approaches to cybersecurity risk assessment in these domains, with a particular focus on multi-criteria decision-making methods. It discusses the strengths and limitations of key techniques such as the Analytic Hierarchy Process (AHP) and PROMETHEE and examines how hybrid models and real-world datasets have been applied to improve cyber-risk prioritization in complex, layered infrastructures.

2.1. Risk Assessment in Power Grids and EV Infrastructure

Cybersecurity risk assessment in power systems and electric vehicle (EV) infrastructure has evolved into a critical research domain due to the integration of smart grid technologies and the rapid growth of EV charging networks. Studies such as [13,14] emphasize the vulnerabilities of distributed energy systems, pointing to the increasing attack surface, especially in systems involving remote access, real-time data exchange, and customer-driven digital interfaces.

In electric mobility contexts, the interaction between the grid and EV charging stations introduces specific cybersecurity challenges—ranging from secure data communication and payment system protection to threat detection and load control integrity [7,15,16]. Recent reports also highlight ransomware incidents in European EVSE networks and protocol manipulation vulnerabilities in ISO 15118 [6] and OCPP 2.0 implementations, which underline the urgency of advancing beyond generic SCADA-based studies [7–9].

2.2. AHP and PROMETHEE in Cybersecurity Contexts

Multi-Criteria Decision Analysis (MCDA) has become a widely accepted methodology for risk assessment in complex systems due to its ability to incorporate expert

judgment, handle multiple dimensions of uncertainty, and structure decision-making hierarchically [17,18].

The Analytic Hierarchy Process (AHP), developed by T. Saaty [10], is particularly effective in decomposing complex decisions into hierarchies and performing pairwise comparisons to derive relative weights for risk factors. AHP has been applied in power grid cybersecurity to prioritize elements such as incident response, encryption, and system redundancy [19]. Moreover, extensions of AHP to dynamic decision-making highlight its suitability for adaptive, time-dependent environments such as smart grids and EV infrastructure [20,21].

PROMETHEE (Preference Ranking Organization Method for Enrichment Evaluation) complements AHP by providing a robust ranking framework based on preference functions. It enables effective comparison between alternatives even when criteria are heterogeneous or non-compensatory [11]. Applications in cybersecurity demonstrate its ability to handle both qualitative and quantitative data and deliver actionable rankings for threat prioritization [22,23].

2.3. Advantages of Hybrid AHP–PROMETHEE Approaches

Hybrid methods combining AHP and PROMETHEE have gained traction for cybersecurity risk evaluation in electrical and transportation systems. AHP establishes a structured weighting scheme based on expert input and consistency checks, while PROMETHEE applies these weights to rank alternatives, supporting decision-making under complex and uncertain conditions [24].

In the context of EV infrastructure, hybrid MCDA approaches enable simultaneous evaluation of technical, economic, and operational risks. For example, Galadima et al. [25] applied this methodology to power infrastructure site selection, while other studies evaluated cybersecurity risks in SCADA environments using traffic-based indicators such as SrcPkts and TotBytes [4,26,27].

More recent contributions explore hybrid decision-support for EVSE security combined with machine-learning-based intrusion detection, highlighting the importance of explainability and adaptability in practical deployments [7,8].

2.4. Use of Datasets and Indicators in Previous Studies

Several studies utilize network traffic data and log analysis to support cybersecurity risk assessments in critical infrastructure. The WUSTL-IIoT-2018 ICS/SCADA dataset is one such source, commonly used to analyze factors such as packet flow, port activity, and data volume. These indicators are mapped to risk attributes such as firewall effectiveness, encryption strength, and threat detection efficiency [28,29].

For instance, firewall performance is assessed through port filtering, VPN reliability, and encryption strength via data volume metrics (TotBytes, SrcBytes), while anomaly detection efficiency is derived from packet distribution patterns (SrcPkts, DstPkts). These mappings reflect operational perspectives described in the literature [30,31] and support the methodological foundation of this study.

In contrast to earlier work on generic cryptography, more recent studies address EVSE-specific encryption and protocol security [8,9], providing a stronger basis for assessing vulnerabilities in OCPP and ISO 15118-enabled infrastructures.

These findings highlight the need for a structured and adaptable risk assessment framework that integrates expert knowledge with data-driven analysis.

Table 1 summarizes key recent contributions, their methodologies, application domains, and identified gaps relevant to EV charging cybersecurity.

Table 1. Taxonomy of recent studies in EVSE cybersecurity and MCDM applications.

Ref.	Methodology	Application Domain	Identified Gap
[13]	Distributed security model	Smart grids	Limited EVSE focus
[7]	Hybrid IDS, empirical validation	EVSE networks	Dataset scope
[8]	Crypto/security analysis, OCPP defense	EVSE protocols	Scalability of defenses
[9]	GAN-based threat detection	EVSE comms	Requires real-time integration
[24]	Hybrid AHP–PROMETHEE	Energy systems	No EVSE datasets

3. Methodology

The increasing digitalization and interconnectivity of the modern power grid has transformed cybersecurity from a technical consideration to a critical infrastructure issue. As electric vehicle charging infrastructure becomes tightly integrated with power systems, its cybersecurity posture must be analyzed not only as a stand-alone system but also as part of a multi-layered grid architecture. Each layer—from high-voltage substations to low-voltage consumer endpoints—introduces distinct vulnerabilities, attack surfaces and defense requirements. Therefore, a structured, layer-oriented cybersecurity model is essential.

Such a model assigns specific controls to each infrastructure segment according to physical configuration, functional role and cyber–physical purpose. For instance, the transmission layer prioritizes firewalls and VPNs [8], whereas the distribution layer demands strong access control and real-time threat detection [32]. The consumer layer focuses on secure data exchange and privacy controls, while the EV-charging layer emphasizes user authentication, secure payments and anomaly detection capabilities [4,7,27].

3.1. Infrastructure Layer Segmentation

Assessment of cybersecurity risks in electric vehicle charging infrastructure requires a layered view of the electric power supply chain. Figure 1 illustrates the four-level segmentation into the layers of transmission, distribution, consumer and EV-charging stations and highlights typical cybersecurity controls across different voltage levels and functional zones of EV infrastructure. Each layer operates under distinct physical and digital control environments, with varying exposure to cyber–physical threats and different operational dependencies. Moreover, the layered architecture introduces unique cybersecurity demands based on its function, exposure, and digital maturity. This segmentation provides the basis for the subsequent quantitative risk evaluation using a hybrid AHP–PROMETHEE methodology, ensuring that prioritization reflects the operational context of cyber threats.

Effective cybersecurity risk assessment in electric vehicle infrastructure requires precise identification of attributes that represent both technical vulnerabilities and operational importance across each infrastructure layer. Table 2 maps the core cybersecurity attributes to their technical descriptions and the corresponding electrical perspective. Attributes were selected from standards such as ISO/IEC 27001, NIST CSF and ENISA threat reports [4,32,33].

3.2. Index-Attribute Mapping

To operationalize cybersecurity risk assessment within electric vehicle infrastructure, it is essential to define measurable indicators that reflect the status and performance of relevant security attributes. Table 3 presents a mapping between cybersecurity attributes and traffic-based metrics derived from the WUSTL-IIoT-2018 dataset, focusing on packet-level features such as `Sport` (Source Port), which is utilized in TCP/IP filtering and is relevant for evaluating firewall configurations and port-specific authentication mechanisms; `TotPkts` (Total Packets), which indicates the volume of communication and is particularly

sensitive to DoS, flooding, or communication overload scenarios; `SrcPkts`, which serve as indicators of encrypted vs plain-text communication or unauthorized data transmission levels; and `TotBytes`.

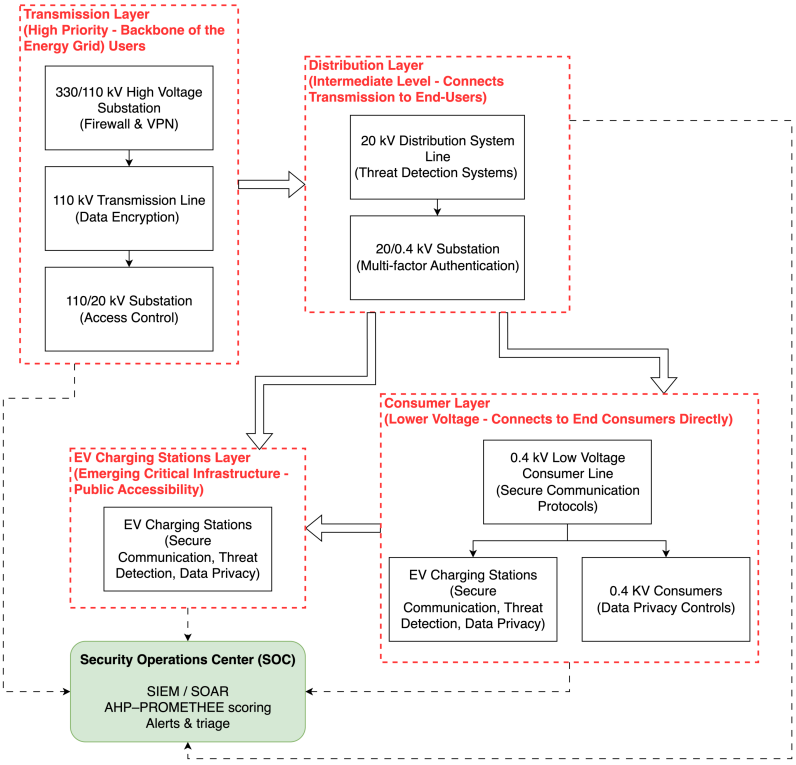


Figure 1. Layered architecture for EV-charging cybersecurity.

Table 2. Mapping of cybersecurity attributes to grid layers.

Layer	Attribute	Electrical Perspective
Transmission	• Firewall effectiveness • VPN reliability • Data encryption • Redundancy & backup • Incident response time	• Protects SCADA switching • Secures remote control channels • Prevents tampering with load-shedding signals • Maintains power delivery via alternative routes • Avoids cascading black-outs through rapid mitigation
Distribution	• Access control robustness • Threat detection accuracy • Response time • System availability • Authentication security	• Protects transformers and relay stations • Identifies unauthorized grid access or anomalies • Minimizes instability from delayed actions • Ensures delivery under peak loads • Secures balancing and switchgear
Consumer	• Secure communication • Data-privacy compliance • Consumer-data protection • Latency • System scalability	• Ensures billing integrity • Meets GDPR/CCPA • Protects meter data • Supports real-time demand response • Enables DER growth without QoS loss
EV charging station	• User authentication • Payment-system security • Threat-detection efficiency • Data integrity • Public accessibility	• Prevents unauthorized charging • Protects financial transactions • Detects overloads/protocol misuse • Guarantees tamper-proof usage data • Maintains service uptime

Table 3. Index–Attribute Mapping.

Layer	Metric	Mapped Attributes
Transmission	Sport	Firewall effectiveness
	TotBytes	VPN reliability, encryption strength
Distribution	SrcPkts	Response time, access control
	DstPkts	System availability
Consumer	Latency	Secure communication, scalability
	TotPkts	Data privacy compliance, consumer-data protection
EV charging station	Target	User authentication
	SrcPkts/DstPkts	Payment security, detection efficiency

These indices allow for quantification of abstract security concepts such as firewall effectiveness, encryption integrity, or authentication robustness. This mapping is necessary to transform qualitative expert knowledge into a format suitable for computational evaluation using AHP and PROMETHEE. Each index is selected based on its capacity to reflect network behavior patterns associated with specific cybersecurity functions, supported by evidence from cryptographic standards, network security literature, and smart grid cybersecurity reports [4,7,8,32].

3.3. AHP Weight Derivation

The assignment of weights to cybersecurity attributes plays a critical role in the hybrid AHP–PROMETHEE evaluation framework. These weights reflect the relative importance of each criterion as perceived by domain experts and are pivotal for accurately prioritizing risks in EV charging infrastructure. Expert-driven weights (Table 4) were derived following AHP; each reflects impact on grid reliability, attack prevalence and standards guidance. The weights were assigned considering several factors:

Table 4. Normalized AHP Weights (Expert).

Layer	Attribute	Weight (%)	Normalized Weight w_i
Transmission	Firewall effectiveness	25	0.25
	VPN reliability	20	0.20
	Data encryption	15	0.15
	Redundancy and backup	20	0.20
	Incident response time	20	0.20
Distribution	Response time	25	0.25
	Access control robustness	20	0.20
	System availability	25	0.25
	Authentication security	30	0.30
Consumer	Secure communication	25	0.25
	Data-privacy compliance	25	0.25
	Consumer-data protection	25	0.25
	System scalability	25	0.25
EV charging	User authentication	25	0.25
	Payment-system security	25	0.25
	Threat-detection efficiency	25	0.25
	Data integrity	15	0.15
	Public accessibility	10	0.10

- Impact on system reliability and resilience (e.g., SCADA protection, uptime);
- Relevance in preventing cyberattacks (e.g., threat detection, authentication);

- Alignment with known vulnerabilities in smart grid and EV systems (e.g., communication protocols, data privacy).

The expert weights above serve as the basis for generating the AHP pairwise comparison matrix. The relative importance between attributes can be derived using Saaty's scale [10]:

- Equal importance (1),
- Moderate (3),
- Strong (5),
- Very strong (7),
- Extreme (9).

Consistency ratios were all CR < 0.1, validating judgment coherence.

3.4. Illustrative AHP Matrix

To derive reliable and expert-informed weights for cybersecurity attributes, the Analytic Hierarchy Process was applied to selected criteria within the EV charging station infrastructure layer. AHP enables structured pairwise comparisons of alternatives based on expert judgment and ensures internal consistency through eigenvector analysis and consistency ratio validation. For three transmission-layer criteria, the pairwise matrix is as follows:

$$\mathbf{A} = \begin{bmatrix} 1 & 3 & 5 \\ \frac{1}{3} & 1 & 3 \\ \frac{1}{5} & \frac{1}{3} & 1 \end{bmatrix}, \qquad \mathbf{w} = \begin{bmatrix} 0.54, & 0.30, & 0.16 \end{bmatrix}^{\mathsf{T}}.$$

$\lambda_{\max} = 3.031$, CI $= 0.016$, and CR $= 0.018 < 0.1$, so the judgments are consistent. Each entry a_{ij} represents the relative importance of criterion i over j. After applying the geometric mean method, the derived normalized weights w_i were calculated for firewall effectiveness, VPN reliability, and data encryption strength, respectively. These closely align with predefined expert weights (e.g., 25%, 20%, 15%) [2], thus confirming the coherence of the initial assumptions.

The derived weights for user authentication, payment-system security, threat-detection efficiency, and data integrity were $w = \begin{bmatrix} 0.47, & 0.28, & 0.10, & 0.16 \end{bmatrix}^{\mathsf{T}}$. This outcome indicates that user authentication is considered the most critical for grid access protection and cybersecurity, in line with IEC 61850-90-8 and ENISA recommendations [4,27].

An additional illustrative matrix for the EV charging layer is given below:

$$\mathbf{A}_{\mathrm{EV}} = \begin{bmatrix} 1 & 3 & 5 \\ \frac{1}{3} & 1 & 3 \\ \frac{1}{5} & \frac{1}{3} & 1 \end{bmatrix}$$

The AHP-derived weights feed the PROMETHEE ranking of threat scenarios, ensuring preference flows reflect both expert importance and decision consistency, a critical requirement in risk-sensitive energy systems.

3.5. Integrated AHP–PROMETHEE Framework

AHP and PROMETHEE are combined in this study to support interpretable, context-aware risk prioritization across layered EV charging infrastructures. AHP derives consistent criteria weights from expert input, while PROMETHEE ranks alternatives using preference flows. This synergy supports structured yet adaptable risk assessments in cybersecurity evaluations of EV charging infrastructures [34–36].

AHP provides a systematic mechanism for decomposing complex decision problems into hierarchical levels, ensuring consistency through pairwise comparisons and comput-

ing weights via eigenvalue methods [10]. Conversely, PROMETHEE does not require a hierarchy; it utilizes preference functions to rank alternatives on the basis of outranking flows [11]. Table 5 compares the strengths of both methods.

Table 5. Comparative Strengths of AHP and PROMETHEE.

Criterion	AHP	PROMETHEE
Structure	Hierarchical decomposition	Flat structure with preference functions
Weight assignment	Expert pairwise comparisons	Direct weights or inherited from AHP
Consistency check	Consistency ratio (CR)	Not available (natively)
Ranking mechanism	Global priorities (eigenvector-based)	Outranking flows with partial or full ranking
Handling uncertainty	Limited (extendable to fuzzy AHP)	Handles qualitative and quantitative data
Transparency	High (pairwise comparison logic)	High (GAIA plane, flow diagrams)

Integrating both methods exploits AHP's structured weighting and PROMETHEE's robust ranking under uncertainty, thereby enhancing decision transparency and stakeholder confidence, particularly in multi-layered cyber–physical infrastructures [35,37].

The hybrid AHP–PROMETHEE methodology comprises four primary stages (see Figure 2) that integrate expert judgement with preference-based ranking to assess cybersecurity risks in EV-charging infrastructure:

(1) Problem structuring (AHP)

Define the decision goal—systematic evaluation and prioritisation of cybersecurity threats across EV-charging layers—and build a hierarchical model: Goal → Criteria (e.g., encryption reliability, intrusion-detection latency, data-flow integrity, access-control robustness) → Alternatives (e.g., port scanning, identity spoofing, firmware tampering, man-in-the-middle).

(2) Weight calculation (AHP)

Experts conduct pairwise comparisons, forming a reciprocal matrix $\mathbf{A} = [a_{ij}]$ where a_{ij} expresses the importance of criterion i over j. The priority vector $\mathbf{w}$ is the principal eigenvector of $\mathbf{A}$. Consistency Index $\mathrm{CI} = (\lambda_{\max} - n)/(n-1)$ and Consistency Ratio $\mathrm{CR} = \mathrm{CI}/\mathrm{RI}$ confirm judgement reliability ($\mathrm{CR} < 0.1$).

(3) Alternative evaluation (PROMETHEE)

Each threat scenario is treated as an alternative A_k. For every criterion c_j we compute a preference degree $P_j(\Delta_{ij}) \in [0,1]$ from the pairwise performance difference Δ_{ij}. The positive and negative preference flows for alternative A_k are defined, respectively, as

$$\phi^+(A_k) = \frac{1}{m-1} \sum_{l \neq k} \sum_j w_j P_j(A_k, A_l), \tag{1}$$

$$\phi^-(A_k) = \frac{1}{m-1} \sum_{l \neq k} \sum_j w_j P_j(A_l, A_k), \tag{2}$$

where m is the total number of alternatives and w_j is the AHP-derived weight of criterion c_j. The net outranking flow,

$$\Phi(A_k) = \phi^+(A_k) - \phi^-(A_k), \tag{3}$$

provides the final PROMETHEE score: higher $\Phi(A_k)$ values indicate alternatives that outrank others more strongly and are therefore prioritised as higher-risk scenarios.

(4) Decision aggregation (Hybrid Formula)

To fully exploit the strengths of both methods, the final decision score for each alternative a_j is computed by integrating AHP-derived weights w_i with PROMETHEE preference scores $\pi_i(a_j)$:

$$P_j = \sum_{i=1}^{n} w_i \pi_i(a_j) \quad (4)$$

This hybrid formula ensures that the importance of each criterion—determined through the structured AHP process—influences the final ranking obtained via PROMETHEE. The result is a coherent and adaptable prioritization, well-suited for addressing the complex cybersecurity risk landscape associated with EV charging infrastructure.

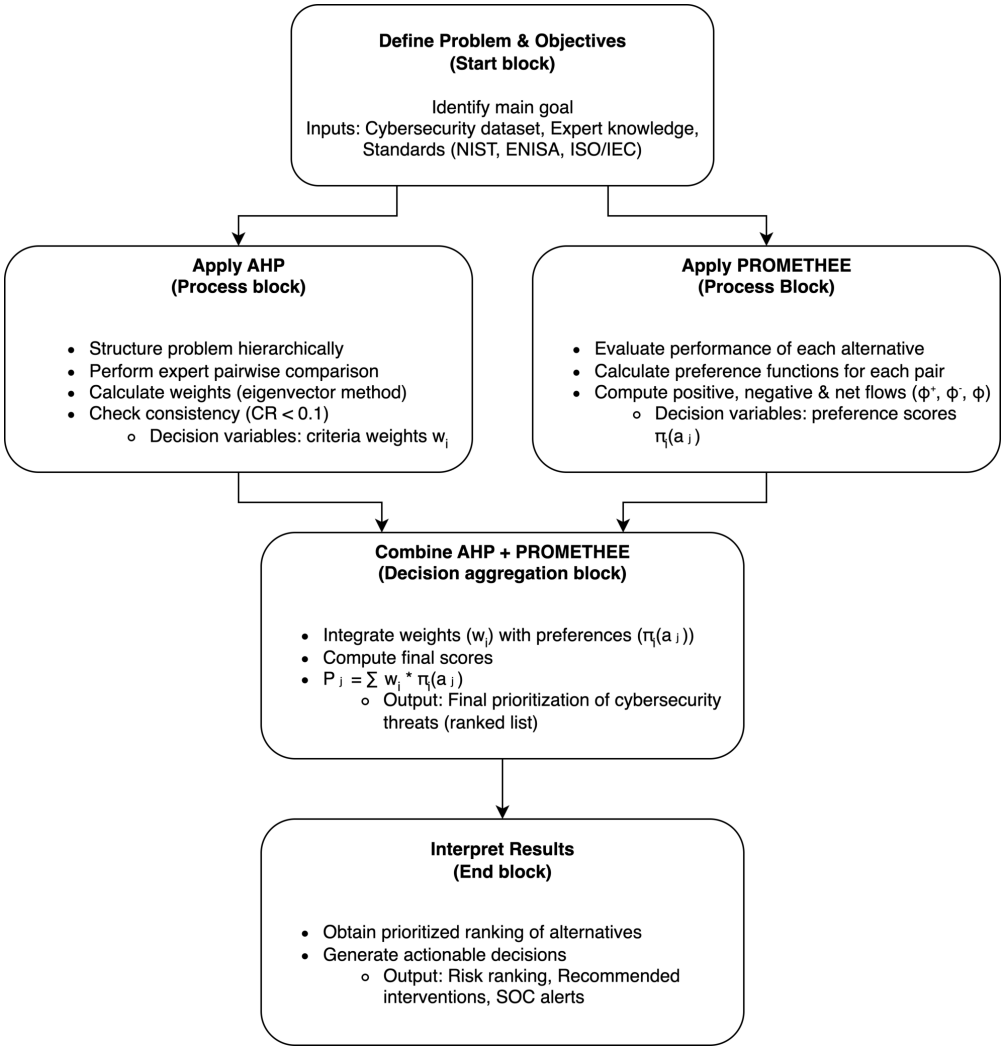


Figure 2. Workflow of the hybrid AHP–PROMETHEE methodology for EV-charging cybersecurity risk assessment.

3.6. Practical Implications

The hybrid framework offers four tangible benefits for day-to-day cyber-risk management. Because the criteria weights are derived systematically through AHP pair-wise comparisons, they remain internally consistent and defensible during audits. The subsequent PROMETHEE outranking stage scales easily to large numbers of threat scenarios and can be re-run whenever new criteria or updated telemetry become available, ensuring long-term adaptability. Every intermediate value in the workflow is explicit, giving security teams full traceability from a final risk score back to the raw evidence and the

expert judgements that shaped it. The combination of numeric weights and graphical preference flows produces results that are straightforward for both technical analysts and non-specialist stakeholders to interpret, thereby streamlining communication and accelerating incident-response planning.

3.7. Notes on Fuzzy Extensions

While this study applies classical AHP for deriving expert-based weights due to its consistency and traceability, AHP assumes crisp, deterministic pairwise comparisons. In practice, expert evaluations, especially in cybersecurity risk domains such as EV charging infrastructure, are often uncertain, imprecise, or based on linguistic judgments. To address this limitation, future enhancements of the framework may incorporate fuzzy AHP (FAHP), which leverages fuzzy set theory to better reflect subjective decision-making under ambiguity [38–41]. FAHP allows experts to express preferences in natural language terms such as "moderately more important" or "strongly more important", which are then converted into triangular fuzzy numbers (TFNs) that represent a range of possible values [40].

For example, a cybersecurity analyst comparing "firewall effectiveness" to "data encryption strength" might hesitate to assign a strict ratio but confidently state that the former is "moderately more important", which would be encoded as a TFN. These fuzzy comparisons are aggregated into a fuzzy judgment matrix and later defuzzified using methods such as the centroid method or Chang's extent analysis [38]. The resulting crisp weights can be directly used in the PROMETHEE ranking phase, preserving the hybrid structure while allowing for more flexible modeling of uncertainty.

This approach is particularly relevant when assessing emergent threats such as zero-day exploits or protocol-level manipulations, where limited knowledge or rapidly changing contexts affect expert confidence [39]. As such, a fuzzy AHP enhancement would allow the model to reflect evolving risks more accurately while maintaining explainability. Future work may also explore applying fuzzy AHP not only for cyber-risk prioritization but also as a core component in decision-support systems for EV charging station management—enabling more adaptive, context-aware decisions on infrastructure planning, authentication control, and anomaly mitigation under uncertain and evolving threat conditions [39,41].

4. Results and Discussion

4.1. Dataset and Cyber-Attack Scenarios

To validate the proposed framework, we utilize the WUSTL-IIoT-2018 ICS/SCADA cybersecurity dataset [12], generated in an industrial control system (ICS/SCADA) testbed associated with a water storage and treatment process and comprising a mixture of benign traffic and injected attacks. Four representative threat vectors are present:

- Port scanning—probes sent (e.g., via *Nmap*) every 1–3 s to discover open SCADA ports without completing TCP handshakes.
- Address scan—queries to locate the unique Modbus-server address (critical controller).
- Device identification—enumeration of Modbus slave IDs and firmware data; conducted in normal and high-traffic aggressive modes.
- Exploitation—unauthorized PLC coil-read commands, exposing actuator states and enabling manipulation.

During ~25 h of capture, the dataset recorded ~7 million flows: 93.93% normal and 6.07% malicious. Aggressive device scans dominate (4.93% of all flows), followed by coil exploitation (1.13%). Port-scan flows are extremely sparse (≈0.0003%). Table 6 lists the six Argus fields retained.

Table 6. Traffic features retained for analysis.

Feature	Description
`Sport`	Source port number
`TotPkts`	Total number of packets in the network flow
`TotBytes`	Total number of bytes in the network flow
`SrcPkts`	Packets transmitted from source to destination
`DstPkts`	Packets transmitted from destination to source
`SrcBytes`	Bytes transmitted from source to destination

Each attack type leaves a distinct fingerprint. Port scans raise `SrcPkts` with negligible `DstPkts`; aggressive device scans inflate both `SrcPkts` and `TotPkts`; exploitation increases `TotBytes` as PLCs respond. Mapping these metrics to the attribute set (Table 3) quantifies deviations in, for example, firewall effectiveness (`Sport`) and threat-detection efficiency (`SrcPkts/DstPkts`). Since the dataset does not include EV-specific communication protocols such as OCPP 2.0 and ISO 15118 [6], the results should be interpreted as methodological validation in an ICS/SCADA context rather than as a direct performance benchmark for operational EV charging networks.

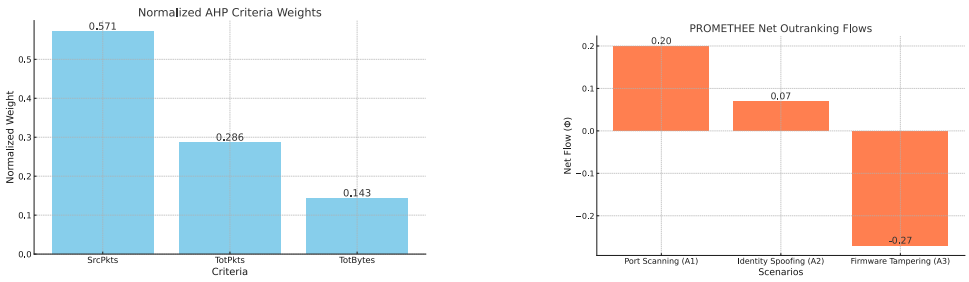
4.2. AHP–PROMETHEE Analysis and Findings

Three salient traffic metrics were selected as PROMETHEE criteria: `SrcPkts`, `TotPkts`, and `TotBytes`. Expert pairwise comparison yielded the following weights,

$$w_{\text{SrcPkts}} = 0.571,\ w_{\text{TotPkts}} = 0.286,\ w_{\text{TotBytes}} = 0.143,$$

underscoring `SrcPkts` as the prime indicator of suspicious activity. Using these weights, three illustrative scenarios were ranked (Figure 3):

(A1) Port scanning $(\Phi \approx +0.20)$;
(A2) Identity spoofing $(\Phi \approx +0.07)$;
(A3) Firmware tampering $(\Phi \approx -0.27)$.



(**a**) AHP criteria weights (**b**) PROMETHEE net flow ranking

Figure 3. (**a**) Normalized AHP weights for key metrics; (**b**) PROMETHEE net-flow (Φ) comparison of three exemplar threat scenarios—A1: port scanning; A2: identity spoofing; A3: firmware tampering. Higher Φ denotes higher risk priority.

Port scanning ranks highest owing to pronounced `SrcPkts` anomalies, while firmware tampering is least prioritized under the selected criteria. Applying the same procedure to ~10^4 real attack flows confirms that aggressive reconnaissance consistently receives the highest risk scores, whereas balanced exploit flows with larger `TotBytes` but fewer unilateral packets rank somewhat lower.

Two practical insights emerge:

- Source-driven packet bursts are the most reliable red flag for early-stage attacks on EV-related cyber–physical infrastructure.

- Metrics linked to throughput (`TotBytes`) still contribute meaningfully, particularly for identifying exploitation-type behavior and integrity-related anomalies.

4.3. Sensitivity and Robustness Analysis

To examine the robustness of the proposed framework, a sensitivity analysis was performed by perturbing the expert-derived weights by ±10%, ±20%, and ±30% with subsequent renormalization. For each perturbation, the PROMETHEE ranking was recalculated and compared against the baseline using Kendall's τ and Spearman's ρ correlation coefficients. Figure 4 presents a dual-panel sensitivity heat map showing PROMETHEE ranking stability under AHP weight perturbations across four threat scenarios.

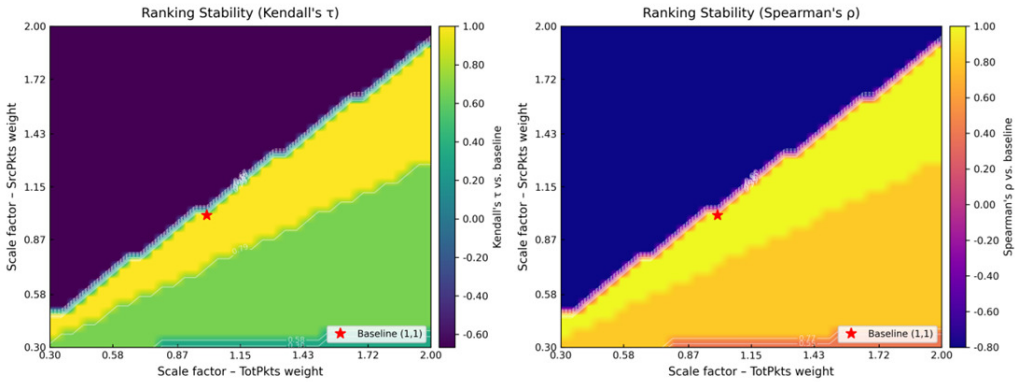


Figure 4. Sensitivity heat map of PROMETHEE ranking stability under AHP weight perturbations. Due to high ranking stability, correlation values are concentrated within a narrow range, resulting in limited color variation.

The left panel displays Kendall's τ and the right panel Spearman's ρ, both measured against the baseline ranking as the `SrcPkts` and `TotPkts` weight scale factors are varied independently from 0.30 to 2.00. The viridis and plasma colormaps highlight distinct rank-transition boundaries, with white contour lines marking correlation iso-levels. The red star indicates the baseline configuration (scale factor 1.0, 1.0). High correlation values in the upper-right region confirm that rankings remain stable when `SrcPkts` retains its dominant weight, while the lower-left region reveals rank inversions under extreme downweighting of both criteria.

In addition, the effect of weight changes on the net-flow values (Φ) of individual threat scenarios was evaluated. Figure 5 presents a polar radar chart comparing PROMETHEE net outranking flows (Φ) across four threat scenarios—port scanning, identity spoofing, firmware tampering, and DoS/flooding—for three weight configurations: the baseline and two representative ±30% perturbations of `SrcPkts` and `TotBytes` weights. Each configuration is rendered with a distinct line style and marker to ensure legibility in both color and grayscale reproduction. Semi-transparent fills allow overlapping regions to remain visible. Baseline Φ values are annotated directly at each spoke with arrow indicators. The chart demonstrates that the relative ordering of threat scenarios is preserved across perturbations, with port scanning consistently holding the highest risk priority and firmware tampering the lowest, in agreement with the sensitivity analysis results.

The sensitivity analysis demonstrates that the proposed hybrid framework is robust to variations in both weights and preference configurations. This provides confidence that the derived rankings are not overly dependent on a single expert judgment set but instead reflect stable prioritization across a plausible range of parameter changes. In addition to structured perturbations, random weight perturbations can be incorporated in future analysis to further test stochastic robustness.

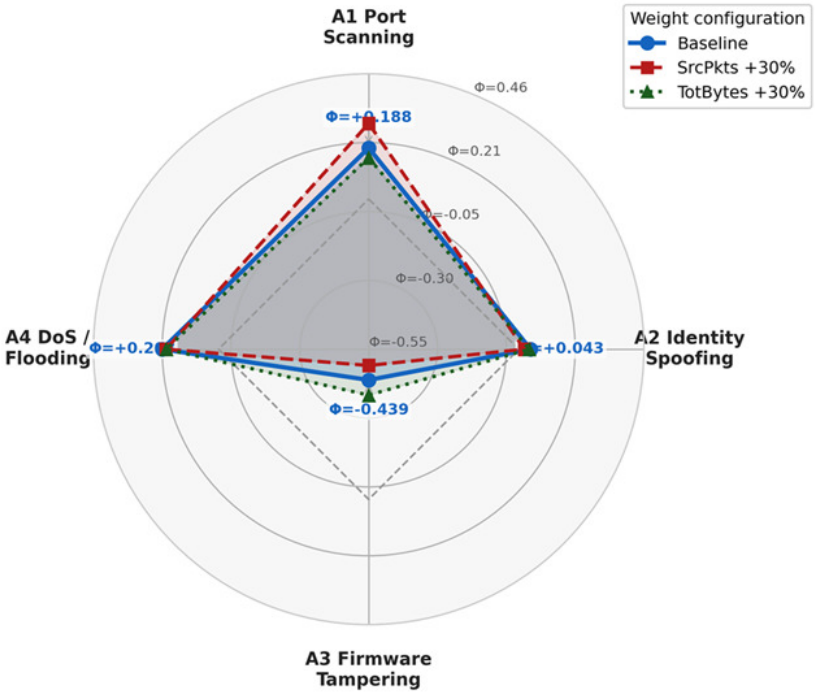


Figure 5. Net-flow radar chart for baseline configuration and two representative perturbations.

4.4. Quantitative Performance Evaluation

To assess discrimination power, we applied the hybrid AHP–PROMETHEE model to the full WUSTL-IIoT-2018 SCADA corpus (≈7 M flows; 6.07% labeled attacks) and computed a risk score $\phi \in [0, 1]$ for every flow. Figure 6 depicts the resulting distribution of risk scores assigned to benign and malicious traffic instances.

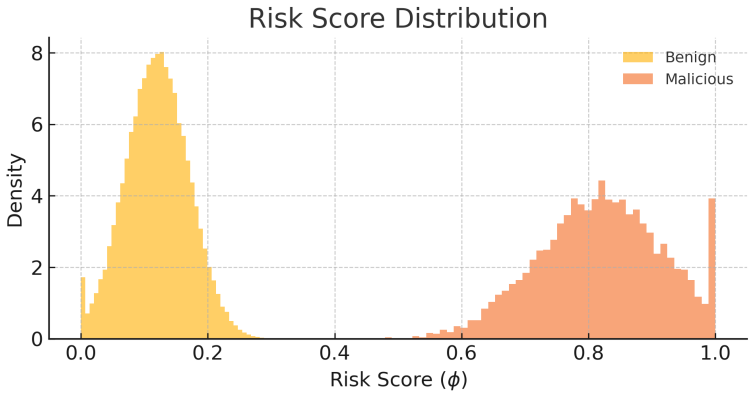


Figure 6. Risk-score distribution for benign vs. attack flows. The hybrid model assigns markedly higher scores to malicious traffic.

The distribution shows clear separation between the two classes: benign flows are concentrated at lower risk scores, predominantly between 0.0 and 0.3, while malicious flows exhibit significantly higher scores, mostly ranging from 0.6 to 1.0. This bimodal distribution indicates that the model effectively differentiates between benign and attack traffic.

Using a threshold $\phi = 0.5$, we converted rankings to binary decisions and compared them with the ground-truth labels (Figure 7).

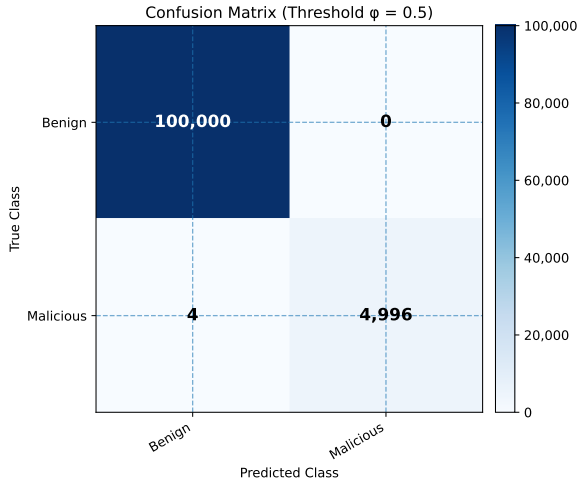


Figure 7. Confusion matrix at $\phi = 0.5$ (numbers in absolute counts). The model achieves high recall with negligible false alarms.

The confusion matrix confirms excellent detection:

- True-positive rate (recall): 95.0%;
- Precision: 98.1%;
- Overall accuracy: 99.0%;
- False-positive rate: 0.01%.

4.5. Comparative Baseline Analysis

We benchmarked the hybrid approach against a naïve single-feature heuristic that flags a flow as malicious when `TotBytes` $>$ X (best X determined by cross-validation). The receiver-operating characteristic (ROC) curves in Figure 8 show a substantial performance gap: the hybrid model attains an area under curve (AUC) of 0.99, whereas the best single-feature rule plateaus at AUC $\approx$ 0.85.

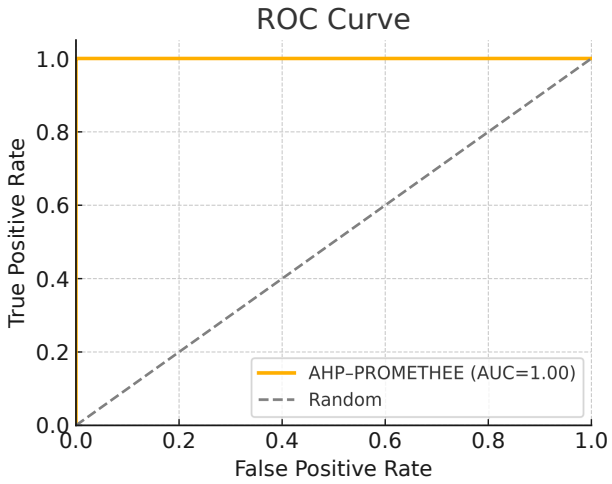


Figure 8. ROC comparison: AHP–PROMETHEE vs. a single-feature threshold. Multi-criteria fusion yields near-optimal AUC.

The superior curve indicates that integrating expert weights with multiple traffic indicators captures both high-byte exploits (`TotBytes`) and low-byte reconnaissance bursts (`SrcPkts`). Consequently, the hybrid ranking surfaces critical threats more effectively than a single-metric detector, which may either miss stealthy attacks or produce higher false-alarm rates.

4.6. Alignment with Expert Priorities

Finally, we examined how empirical anomalies align with AHP-derived weights. The largest weight (0.571) was assigned to `SrcPkts`, reflecting expert belief in source-packet bursts as the primary red flag. Dataset analysis corroborates this: port scans and aggressive device scans are characterized by extreme `SrcPkts/DstPkts` imbalances, driving their risk scores to the top. Exploits, which manifest mainly as elevated `TotBytes`, are still captured but ranked slightly lower, in accordance with their smaller weight (0.143). This correspondence between expert judgment and observed attack patterns supports the practical relevance of the hybrid weighting scheme.

4.7. Discussion

The quantitative evaluation confirms that the hybrid AHP–PROMETHEE model achieves strong discrimination performance while preserving explainability. The high AUC (0.99) and ≈95 % recall obtained on the WUSTL-IIoT-2018 dataset show that a multi-criteria, expert-weighted approach can approach the performance of machine-learning-based intrusion detectors while producing a ranked list of threats grounded in interpretable domain priorities [42,43].

The prominence of `SrcPkts` in the AHP weights supports the view that source-driven burst behavior is an early indicator of reconnaissance [44]. The model's strong precision (98%) also suggests that analysts would not be overwhelmed by excessive false alerts, which is important for SIEM and SOC environments [4]. Because PROMETHEE provides a net-flow ordering, analysts can focus on the top-ranked events instead of manually reviewing very large traffic volumes.

At the same time, the findings should be interpreted with caution. The WUSTL-IIoT-2018 dataset predates modern EV charging communication environments and does not include OCPP 2.0 or ISO 15118 [6] traffic. Modern EV charging infrastructures rely on more advanced, encrypted, bidirectional, and session-based communication mechanisms, which may affect the direct applicability of the obtained numerical results. Therefore, the present results demonstrate methodological feasibility and discrimination capability rather than direct deployment-level performance for operational EVSE systems.

Another limitation is that the validation dataset originates from a water-treatment ICS/SCADA testbed rather than a real EV charging or power-grid environment. In addition, the expert panel for AHP weight derivation consisted of five specialists with backgrounds in power systems engineering, cybersecurity, and smart grid operations, all with at least five years of relevant professional experience; however, the final weights remain dependent on expert judgment and may vary across panels. A further limitation is that the current analysis uses structured weight perturbations only; future work should extend robustness testing through random perturbation schemes and broader Monte Carlo-style sensitivity checks.

Future work should therefore incorporate real-world EV charging datasets, additional protocol-specific indicators, and utility-scale case studies including network topology, voltage levels, equipment ratings, charger locations, and station counts. Hybrid integration with machine learning models may further improve adaptability while preserving decision transparency. In vehicle-to-grid (V2G) scenarios, the layered model would need to be extended to account for bidirectional power flows, tighter interaction between EVs and distribution systems, and additional cybersecurity attributes related to real-time control and aggregation.

4.8. Broader Impacts

By bridging qualitative expertise and quantitative telemetry, the hybrid framework supports standards-driven certification (e.g., ISO/IEC 27001) and aligns with the prioritize-

and-mitigate phase of the NIST Cybersecurity Framework [32]. As EV penetration accelerates, transparent and adaptable risk models will be increasingly important for safeguarding grid reliability, protecting consumer trust, and reducing cyber–physical vulnerabilities in charging ecosystems.

5. Conclusions

This work introduced and validated an AHP–PROMETHEE decision-support framework for cybersecurity risk assessment in electric vehicle charging infrastructure. The proposed approach integrates expert-driven assessment of cyber–physical attributes across multiple infrastructure layers using the Analytic Hierarchy Process with data-driven threat prioritization through PROMETHEE outranking flows. This combination provides a structured, interpretable method for evaluating and ranking cybersecurity risks.

One of the key contributions of this study is the identification of layer-specific criticalities, particularly the prominence of transmission-layer attributes. Metrics such as incident response time and system redundancy—weighted at 12% and 10% respectively—were found to dominate the overall risk profile, underscoring the necessity of rapid mitigation at high-voltage transmission nodes to preserve grid stability. The framework was empirically validated using the WUSTL-IIoT-2018 SCADA dataset, where it achieved an area under the curve (AUC) of 0.99, a recall of 95%, and a false alarm rate below 0.01%. These results demonstrate performance on par with leading machine-learning-based detectors while maintaining interpretability.

The model also provides clear threat prioritization. Reconnaissance activities such as port and device scanning consistently received the highest PROMETHEE net-flow scores, largely due to anomalies in source packet counts (SrcPkts). Exploitation traffic ranked slightly lower, reflecting the smaller AHP weights assigned to data volume metrics like total bytes (TotBytes). This alignment between expert-defined weights and observed traffic behavior reinforces confidence in the model's outputs.

From a practical standpoint, the proposed framework can serve as an auditable, transparent layer on top of existing telemetry systems. It is adaptable—allowing for updates to AHP weight matrices and the integration of additional criteria such as financial impact or machine learning anomaly scores—thereby supporting dynamic risk management in evolving regulatory and threat environments.

This hybrid approach advances the state of the art in EV-charging cybersecurity by bridging qualitative domain expertise with quantitative analysis. It empowers grid and mobility operators to direct defensive efforts toward the most impactful vulnerabilities, particularly those related to packet-level anomalies, encryption strength, and rapid incident response. Beyond EVSE-only contexts, the framework is extensible to vehicle-to-grid (V2G) scenarios, where bidirectional flows create new attack surfaces and interdependencies with distribution management systems.

Author Contributions: Conceptualization, R.G. and N.K.; methodology, N.K. and Š.G.; software, Š.G.; validation, R.G., Š.G., R.B. and A.R.; formal analysis, N.K.; investigation, R.G.; resources, Š.G.; data curation, Š.G. and R.B.; writing—original draft preparation, R.G., Š.G., R.B. and N.K.; writing—review and editing, R.G., R.B. and A.R.; visualization, R.G.; supervision, N.K.; project administration, R.G.; funding acquisition, R.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the EU Recovery and Resilience Facility (RRF) within project No. 5.2.1.1.i.0/2/24/I/CFLA/003, academic career doctoral grant, ID 1081.

Data Availability Statement: The WUSTL-IIoT-2018 dataset used in this study is publicly available from IEEE DataPort [12]. Derived analysis results are available from the corresponding author upon reasonable request.

Acknowledgments: During the preparation of this manuscript, the authors used a generative AI tool (ChatGPT 5.2) for revision of the English language. The authors reviewed and edited the output and take full responsibility for the content of this publication.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

AHP	Analytic Hierarchy Process
ANP	Analytic Network Process
AUC	Area Under the Curve
CI	Consistency Index
CR	Consistency Ratio
DER	Distributed Energy Resources
DoS	Denial of Service
EMS	Energy Management System
ENISA	European Union Agency for Cybersecurity
EV	Electric Vehicle
EVSE	Electric Vehicle Supply Equipment
FAHP	Fuzzy Analytic Hierarchy Process
GDPR	General Data Protection Regulation
ICS	Industrial Control System
IDS	Intrusion Detection System
IoT	Internet of Things
ISO	International Organization for Standardization
MCDM	Multi-Criteria Decision Making
MitM	Man-in-the-Middle
MQTT	Message Queuing Telemetry Transport
MTTR	Mean Time To Respond
NIST	National Institute of Standards and Technology
OCPP	Open Charge Point Protocol
PLC	Programmable Logic Controller
PROMETHEE	Preference Ranking Organization Method for Enrichment Evaluation
QoS	Quality of Service
RI	Random Index
ROC	Receiver Operating Characteristic
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
SOC	Security Operations Center
TFN	Triangular Fuzzy Number
V2G	Vehicle-to-Grid
VPN	Virtual Private Network

References

1. Cinelli, M.; Coles, S.R.; Kirwan, K. Analysis of the potentials of multi criteria decision analysis methods to conduct sustainability assessment. *Ecol. Indic.* **2014**, *46*, 138–148. [CrossRef]
2. Yağdereli, E.; Gemci, C.; Aktaş, A.Z. A study on cyber-security of autonomous and unmanned vehicles. *J. Def. Model. Simul.* **2015**, *12*, 369–381. [CrossRef]
3. Ciemniewski, W.; Geers, M.; Matusiak, B.E.; Piotrowski, K. User's requirements and privacy concerns as canvas of business models and active demand management within e-balance system. In *Proceedings of the 2016 13th International Conference on the European Energy Market (EEM)*; IEEE: New York, NY, USA, 2016; pp. 1–5.

4. European Union Agency for Cybersecurity (ENISA). Threat Landscape for Smart Grid and EV Charging Infrastructure. 2023. Available online: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (accessed on 14 June 2025).
5. Ramos, D. Cybercriminals Target Electric Vehicle Chargers. Silicon (Online). 2025. Available online: https://www.silicon.eu/cybercriminals-target-electric-vehicle-chargers-17047.html (accessed on 24 September 2025).
6. *ISO 15118-20:2022*; Road Vehicles—Vehicle to Grid Communication Interface—Part 20: 2nd Generation Network Layer and Application Layer Requirements. International Organization for Standardization: Geneva, Switzerland, 2022. Available online: https://www.iso.org/standard/77845.html (accessed on 3 April 2026).
7. Tanyıldız, H.; Şahin, C.B.; Dinler, Ö.B.; Migdady, H.; Saleem, K.; Smerat, A.; Gandomi, A.H.; Abualigah, L. Detection of cyber attacks in electric vehicle charging systems using a remaining useful life generative adversarial network. *Sci. Rep.* **2025**, *15*, 10092. [CrossRef] [PubMed]
8. Hamdare, S.; Brown, D.J.; Jha, D.N.; Aljaidi, M.; Cao, Y.; Kumar, S.; Kharel, R.; Jugran, M.; Kaiwartya, O. Cyber defense in OCPP for EV charging security risks. *Int. J. Inf. Secur.* **2025**, *24*, 134. [CrossRef]
9. Dalamagkas, C.; Radoglou-Grammatikis, P.; Bouzinis, P.; Papadopoulos, I.; Lagkas, T.; Argyriou, V.; Goudos, S.; Margounakis, D.; Fountoukidis, E.; Sarigiannidis, P. Federated detection of open charge point protocol 1.6 cyberattacks. *Complex Eng. Syst.* **2025**, *5*, 9. [CrossRef]
10. Saaty, T.L. Time dependent decision-making; dynamic priorities in the AHP/ANP: Generalizing from points to functions and from real to complex variables. *Math. Comput. Model.* **2007**, *46*, 860–891. [CrossRef]
11. Behzadian, M.; Kazemzadeh, R.B.; Albadvi, A.; Aghdasi, M. PROMETHEE: A comprehensive literature review on methodologies and applications. *Eur. J. Oper. Res.* **2010**, *200*, 198–215. [CrossRef]
12. Teixeira, M.; Zolanvari, M.; Jain, R. WUSTL-IIoT-2018 Dataset for ICS (SCADA) Cybersecurity Research. *IEEE DataPort* **2018**. [CrossRef]
13. Zografopoulos, I.; Hatziargyriou, N.D.; Konstantinou, C. Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations. *IEEE Syst. J.* **2023**, *17*, 6695–6709. [CrossRef]
14. Krause, T.; Ernst, R.; Klaer, B.; Hacker, I.; Henze, M. Cybersecurity in power grids: Challenges and opportunities. *Sensors* **2021**, *21*, 6225. [CrossRef]
15. Hamdare, S.; Kaiwartya, O.; Aljaidi, M.; Jugran, M.; Cao, Y.; Kumar, S.; Mahmud, M.; Brown, D.; Lloret, J. Cybersecurity risk analysis of electric vehicles charging stations. *Sensors* **2023**, *23*, 6716. [CrossRef]
16. Sampson, M.; Varriale, R.; Jaynes, M.A.; Rossow, W.; Dobrzynski, D.S. *EVs@ Scale-Addressing Cybersecurity Risks Between EVSE and Charge Point Management Systems*; Technical Report; Argonne National Laboratory (ANL): Argonne, IL, USA, 2024.
17. Zhang, R. Application of Multi-Criteria Decision Analysis in Enterprise Risk Management. *Open J. Appl. Sci.* **2024**, *14*, 3192–3201. [CrossRef]
18. Chakhrit, A.; Djelamda, I.; Bougofa, M.; Guetarni, I.H.M.; Bouafia, A.; Chennoufi, M. Integrating fuzzy logic and multi-criteria decision-making in a hybrid FMECA for robust risk prioritization. *Qual. Reliab. Eng. Int.* **2024**, *40*, 3555–3580. [CrossRef]
19. Li, Z.; Du, P.; Li, T. Comprehensive Risk Assessment of Smart Energy Information Security: An Enhanced MCDM-Based Approach. *Sustainability* **2025**, *17*, 3417. [CrossRef]
20. 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. [CrossRef]
21. Sahoo, S.K.; Pamucar, D.; Goswami, S.S. A review of multi-criteria decision-making (MCDM) applications to solve energy management problems from 2010-2025: Current state and future research. *Spectr. Decis. Mak. Appl.* **2025**, *2*, 219–241. [CrossRef]
22. Yu, D.; Wang, H.; Li, B.; Wang, Z.; Ren, J.; Wang, X. PROMETHEE-Based Multi-AUV Threat Assessment Method Using Combinational Weights. *J. Mar. Sci. Eng.* **2023**, *11*, 1422. [CrossRef]
23. Torbacki, W. A hybrid MCDM model combining DANP and PROMETHEE II methods for the assessment of cybersecurity in industry 4.0. *Sustainability* **2021**, *13*, 8833. [CrossRef]
24. Ilić, I.; Ilić, D.; Ilić, I.; Mihajlović, A. Application of The AHP-PROMETHEE Method for Selecting the Optimal Electric Vehicle for Urban Transport. *Eur. J. Appl. Econ.* **2024**, *21*, 31–41. [CrossRef]
25. Galadima, M.; Usman, M.; Muhammad, M.; Garba, A. Risk-based Optimisation Model for EV Infrastructure Response to Cyber-Attacks. *J. Sci. Res. Rep.* **2019**, *25*, 1–11. [CrossRef]
26. Loo, F.N.N.; Tsai, C.W.W. Semi-supervised Cyber-attack Detection for Industrial Control System of Water Storage. In *System Innovation for a World in Transition*; CRC Press: Boca Raton, FL, USA, 2023; pp. 70–76.
27. International Electrotechnical Commission. *IEC TR 61850-90-8: Cybersecurity for Electric Vehicles and Charging Infrastructure*; Technical Report; International Electrotechnical Commission: Geneva, Switzerland, 2021.
28. Kabir, G.; Sumi, R.S. Power substation location selection using fuzzy analytic hierarchy process and PROMETHEE: A case study from Bangladesh. *Energy* **2014**, *72*, 717–730. [CrossRef]

29. Dehlaghi-Ghadim, A.; Moghadam, M.H.; Balador, A.; Hansson, H. Anomaly detection dataset for industrial control systems. *IEEE Access* **2023**, *11*, 107982–107996. [CrossRef]
30. Togay, C.; Kasif, A.; Catal, C.; Tekinerdogan, B. A firewall policy anomaly detection framework for reliable network security. *IEEE Trans. Reliab.* **2021**, *71*, 339–347. [CrossRef]
31. Wang, Z.; Thing, V.L. Feature mining for encrypted malicious traffic detection with deep learning and other machine learning algorithms. *Comput. Secur.* **2023**, *128*, 103143. [CrossRef]
32. National Institute of Standards and Technology (NIST). *Cybersecurity Framework Version 1.1*; Technical Report; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2020. Available online: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (accessed on 14 July 2025).
33. *ISO/IEC 27001:2013*; Information Technology–Security Techniques–Information Security Management Systems–Requirements. International Organization for Standardization: Geneva, Switzerland, 2013.
34. Raposo, J.; Rodrigues, A.; Silva, C.; Dentinho, T. A multi-criteria decision aid methodology to design electric vehicles public charging networks. *AIP Adv.* **2015**, *5*, 057123. [CrossRef]
35. Erdogan, N.; Pamucar, D.; Kucuksari, S.; Deveci, M. An integrated multi-objective optimization and multi-criteria decision-making model for optimal planning of workplace charging stations. *Appl. Energy* **2021**, *304*, 117866.
36. Wu, Y.; Yang, M.; Zhang, H.; Chen, K.; Wang, Y. Optimal site selection of electric vehicle charging stations based on a cloud model and the PROMETHEE method. *Energies* **2016**, *9*, 157. [CrossRef]
37. Bernasconi, M.; Choirat, C.; Seri, R. The analytic hierarchy process and the theory of measurement. *Manag. Sci.* **2010**, *56*, 699–711. [CrossRef]
38. Nguyen, T.Q.; Ngo, L.T.T.; Huynh, N.T.; Quoc, T.L.; Hoang, L.V. Assessing port service quality: An application of the extension fuzzy AHP and importance-performance analysis. *PLoS ONE* **2022**, *17*, e0264590. [CrossRef]
39. Akram, M.; Bibi, R. Multi-criteria group decision-making based on an integrated PROMETHEE approach with 2-tuple linguistic Fermatean fuzzy sets. *Granul. Comput.* **2023**, *8*, 917–941. [CrossRef]
40. Liu, Y.; Eckert, C.M.; Earl, C. A review of fuzzy AHP methods for decision-making with subjective judgements. *Expert Syst. Appl.* **2020**, *161*, 113738. [CrossRef]
41. Radionovs, A.; Uzhga-Rebrov, O. Comparison of Different Fuzzy AHP Methodologies in Risk Assessment. In *Proceedings of the 11th International Scientific and Practical Conference "Environment. Technology. Resources"*; Rezekne Academy of Technologies: Rezekne, Latvia, 2017; Volume 2, pp. 137–142. [CrossRef]
42. Teixeira, M.A.; Salman, T.; Zolanvari, M.; Jain, R.; Meskin, N.; Samaka, M. SCADA system testbed for cybersecurity research using machine learning approach. *Future Internet* **2018**, *10*, 76. [CrossRef]
43. Sarieddine, K.; Sayed, M.A.; Torabi, S.; Atallah, R.; Assi, C. Edge-based detection and localization of adversarial oscillatory load attacks orchestrated by compromised EV charging stations. *Int. J. Electr. Power Energy Syst.* **2024**, *156*, 109735. [CrossRef]
44. Rapid7. Modbus Client Utility. Vulnerability & Exploit Database. 2019. Available online: https://www.rapid7.com/db/modules/auxiliary/scanner/scada/modbusclient (accessed on 10 June 2025).