I.J. Information Engineering and Electronic Business, **2026, 3, 124-141**
Published Online on June 8, 2026 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijieeb.2026.03.08

Scenario-Based Security and Reliability Evaluation of Connected Autonomous Vehicles Using a Hybrid CRITID–Fuzzy BWM–VIKOR Swarm Approach

Fadoua Tamtam*
National School of Applied Sciences, Systems Engineering and Decision Support Laboratory (LISAD), IBN ZOHR University, Agadir, 80000, Morocco
E-mail: fadoua.tamtam@gmail.com
ORCID iD: https://orcid.org/0000-0002-7720-1674
*Corresponding author

Amina Tourabi
National School of Applied Sciences, Systems Engineering and Decision Support Laboratory (LISAD), IBN ZOHR University, Agadir, 80000, Morocco
E-mail: a.tourabi@uiz.ac.ma
ORCID iD: https://orcid.org/0000-0002-7739-0321

Received: June 28, 2025; Revised: October 21, 2025; Accepted: January 4, 2026; Published: June 8, 2026

Abstract: Connected autonomous vehicles (CAVs) are reshaping mobility but remain vulnerable to technical, organizational, and regulatory risks. This study develops a hybrid multi-criteria decision-making framework that integrates CRITID for objective weighting, Fuzzy BWM for expert uncertainty modeling, and VIKOR Swarm for adaptive compromise ranking. To enhance realism, four scenarios were constructed: scalability-focused (A1), compliance & reliability-focused (A2), resilient high-performance ecosystem (A3), and organizational vulnerability-focused (A4). Results show that Scenario A3 consistently outperforms others, achieving the lowest group utility shortfall, smallest individual regret, and most favorable compromise measure. Shapley Value sensitivity analysis confirmed cybersecurity and scalability as dominant criteria, while expert AI validation reinforced the robustness of A3's ranking. Monte Carlo simulations further demonstrated stability under weight perturbations, with A3 retaining its top position in over 80% of runs. The study contributes a transparent, reproducible, and scenario-based methodology for vehicular risk assessment, bridging technical and organizational dimensions. Limitations include reliance on static scenario design and expert elicitation, suggesting future work should incorporate dynamic data streams and edge AI for real-time risk recalibration.

Index Terms: Connected autonomous vehicles (CAVs), Intelligent transport, Hybrid multi-criteria decision-making (MCDM), Cybersecurity and reliability, AI-based validation

1. Introduction

The rapid evolution of connected autonomous vehicles (CAVs) has transformed the transportation landscape, offering unprecedented opportunities for efficiency, safety, and sustainability [1]. By integrating advanced communication technologies, artificial intelligence, and vehicular networking, CAVs promise to reduce accidents, optimize traffic flow, and enable new mobility paradigms [2, 3]. However, the increasing reliance on interconnected systems also exposes these vehicles to a wide range of vulnerabilities, including cybersecurity threats, data integrity risks, and organizational weaknesses. Ensuring the security and reliability of CAV ecosystems has therefore become a critical research priority, requiring robust evaluation frameworks that can capture both technical and human-centric dimensions [4, 5].

Traditional risk assessment approaches often focus narrowly on technical performance or regulatory compliance, overlooking the complex interplay between organizational, infrastructural, and human factors. Recent studies have

This work is open access and licensed under the Creative Commons CC BY 4.0 License.

emphasized the need for multi-criteria decision-making (MCDM) methods to address this complexity, as they allow for the systematic integration of diverse criteria into a coherent evaluation structure [6]. Yet, many existing applications rely on single weighting or ranking techniques, which may fail to capture uncertainty, interdependencies, and trade-offs inherent in vehicular risk scenarios [7-9]. This gap motivates the development of hybrid frameworks that combine objective and subjective weighting with adaptive compromise ranking.

In this study, we propose a hybrid CRITID–Fuzzy BWM–VIKOR Swarm approach to evaluate security and reliability in CAVs. CRITID provides objective weights by accounting for nonlinear independence among criteria, while Fuzzy BWM incorporates expert judgment under uncertainty. VIKOR Swarm is then applied to derive compromise rankings, optimizing the balance between group utility and individual regret through swarm intelligence. To enhance realism, the evaluation is structured around four scenarios: scalability-focused (A1), compliance & reliability-focused (A2), resilient high-performance ecosystem (A3), and organizational vulnerability-focused (A4). This scenario design ensures that both established risks (e.g., malware detection, authentication, reliability) and emerging vulnerabilities (e.g., insider threats, supply chain security, privacy leakage) are systematically addressed.

The contribution of this work is threefold. First, it introduces a transparent and reproducible hybrid MCDM framework tailored to vehicular risk modeling. Second, it embeds scenario-based alternatives, enabling the evaluation of realistic trade-offs across technical, organizational, and regulatory dimensions. Third, it incorporates advanced validation techniques, including Shapley Value sensitivity analysis and expert AI-assisted robustness testing, to ensure methodological credibility and practical relevance. By combining these elements, the study advances the state of the art in CAV risk assessment and provides actionable insights for researchers, policymakers, and system designers.

2. Related Work

The emergence of CAVs has transformed the landscape of intelligent transportation systems [10, 11]. However, this transformation has simultaneously introduced complex challenges related to security and reliability. CAVs rely on continuous communication between vehicles, infrastructure, and cloud services, making them highly susceptible to cyberattacks, data manipulation, and systemic failures [12-14]. Researchers have emphasized that the vulnerabilities of CAVs are not confined to technical dimensions but extend to socio-technical domains, including regulatory frameworks, human factors, and infrastructural readiness [15, 16]. Despite significant progress in vehicular communication standards, the literature consistently reveals gaps in comprehensive risk assessment frameworks that can simultaneously address uncertainty, conflicting criteria, and dynamic vehicular environments.

MCDM methods have been increasingly employed to tackle these challenges, offering structured approaches to evaluate diverse criteria in complex systems. The Best-Worst Method (BWM) has gained attention for its ability to reduce inconsistency in pairwise comparisons compared to traditional techniques [17]. Yet, conventional BWM struggles when expert judgments are vague or imprecise. To overcome this limitation, fuzzy extensions of BWM have been introduced, enabling the incorporation of linguistic variables and uncertainty modeling into the weighting process [18, 19]. These developments are particularly relevant in vehicular contexts, where expert assessments of cybersecurity risks or system reliability often involve subjective and uncertain judgments. In earlier studies, fuzzy logic was already applied to vehicular risk assessment, but these efforts predated the widespread adoption of 5G technologies, limiting their relevance to modern vehicular IoT environments [20]. Nevertheless, applications of fuzzy-BWM in transportation security remain limited, leaving a methodological gap for more targeted integration.

Objective weighting methods such as CRITIC (Criteria Importance Through Intercriteria Correlation) have also been widely applied to capture the inherent conflict and contrast among criteria. While CRITIC has proven effective in domains such as finance and sustainability, its reliance on linear correlation assumptions restricts its robustness in nonlinear vehicular data environments [21, 22]. The recent development of CRITID, which incorporates advanced independence testing, represents a significant methodological advancement. CRITID enhances the ability to objectively determine criteria weights in scenarios where interdependencies are nonlinear and multidimensional, making it particularly suitable for vehicular communication systems characterized by heterogeneous data streams [23]. Despite its potential, CRITID has not yet been extensively applied in transportation security studies, suggesting an opportunity to bridge methodological innovation with practical vehicular applications.

For compromise ranking and decision-making, VIKOR has long been recognized as a powerful tool to balance conflicting criteria and provide solutions closest to the ideal [24, 25]. Its strength lies in offering compromise solutions that reflect both group utility and individual regret, making it highly relevant for contexts where trade-offs between security, reliability, and performance must be considered. However, traditional VIKOR approaches are static and may not adapt well to dynamic vehicular environments. Hybrid extensions, such as VIKOR integrated with swarm intelligence, have recently emerged to enhance adaptability and optimization in complex systems [26-28]. Swarm-based VIKOR models leverage collective intelligence and iterative search processes to refine compromise solutions, offering promising avenues for vehicular risk assessment. More recent contributions have also emphasized the role of edge AI and deep learning in vehicular risk assessment, demonstrating how convolutional neural networks and reinforcement learning improve situational awareness and responsiveness in real time [29, 30]. Yet, the literature indicates that such hybridizations remain underexplored in the domain of connected autonomous vehicles, leaving a methodological gap in

adaptive compromise solutions for vehicular risk management.

The literature demonstrates that while individual methodological advancements—such as fuzzy-BWM for uncertainty handling, CRITID for robust objective weighting, and VIKOR-Swarm for adaptive compromise—have been developed, they have rarely been integrated into a unified framework tailored to the security and reliability of CAVs. Existing studies tend to focus on isolated methodological improvements or narrow application domains, without addressing the holistic requirements of vehicular ecosystems. Furthermore, cybersecurity vulnerabilities such as unauthorized access, denial-of-service attacks, and data integrity risks remain pressing concerns in vehicular IoT, underscoring the need for decision-support frameworks that explicitly incorporate these dimensions into risk evaluation [31-33].

Prior research on 5G-enabled vehicular IoT has generally concentrated on a core set of risks, including network slicing flaws, edge computing threats, IoT device vulnerabilities, latency issues, interoperability inconsistencies, and quantum decryption risks. While this set provides a comprehensive foundation, it does not fully capture emerging categories such as supply-chain security, insider threats, and privacy leakage through vehicular data sharing. Recent work has emphasized that these overlooked dimensions are increasingly relevant as V2X ecosystems expand, and their exclusion may lead to incomplete risk characterization [34].

In addition, several studies have highlighted the importance of evaluating risk through scenario-based alternatives, as scenarios allow researchers to simulate realistic trade-offs between technical, organizational, and regulatory dimensions. For example, Zhasmukhambetova et al. [35] argue that scenario construction in vehicular risk assessment enhances decision relevance by reflecting heterogeneous operating conditions, while Zhang et al. [36] demonstrate that scenario-based evaluation improves robustness testing of MCDM frameworks in transportation security. Building on this literature, the present study defines four scenarios (A1–A4) as alternatives:

- A1 represents environments prioritizing scalability and adaptability over deep cybersecurity protection.
- A2 emphasizes regulatory compliance and reliability but suffers from weaknesses in data integrity and privacy safeguards.
- A3 integrates advanced cybersecurity and adaptability measures to simulate high-performance ecosystems resilient to both external and internal threats.
- A4 focuses on organizational vulnerabilities such as insider threats and supply chain security, reflecting contexts where human and infrastructural risks dominate.

The scientific significance of these scenarios lies in their ability to span the multidimensional risk landscape identified in prior studies, ensuring that compromise rankings are not abstract but grounded in plausible vehicular contexts.

To structure this evaluation, several criteria have been identified in the literature as essential for enhancing security and reliability in CAVs, as summarized in Table 1.

Table 1. Criteria/Dimensions for Enhancing Security and Reliability in CAVs.

Criteria	Description	Literature Support
Cybersecurity Threat Detection	Ability to identify malware, intrusion, and unauthorized access in vehicular networks	[37]
Authentication & Access Control	Secure pairing and identity verification mechanisms	[38]
Data Integrity & Confidentiality	Ensuring transmitted data remains accurate and protected	[39]
System Reliability	Robustness of hardware/software against failures	[40]
Resilience to Uncertainty	Ability to adapt to vague or incomplete information	[41]
Decision Robustness	Stability of compromise solutions under conflicting criteria	[42]
Scalability & Adaptability	Capacity to handle large-scale vehicular networks	[43]
Regulatory Compliance & Standardization	Alignment with evolving legal frameworks, safety standards, and interoperability requirements	[44]
Supply-Chain Security	Protection against vulnerabilities in hardware/software supply chains	[45]
Insider Threats	Risks posed by malicious or negligent actions of authorized personnel	[44]
Privacy Leakage	Safeguarding sensitive vehicular data from unauthorized sharing or misuse	[39]

These criteria form the foundation for constructing the four risk scenarios (A1–A4), each representing a different configuration of strengths and weaknesses across technical, organizational, and regulatory dimensions, as shown in Fig. 1.

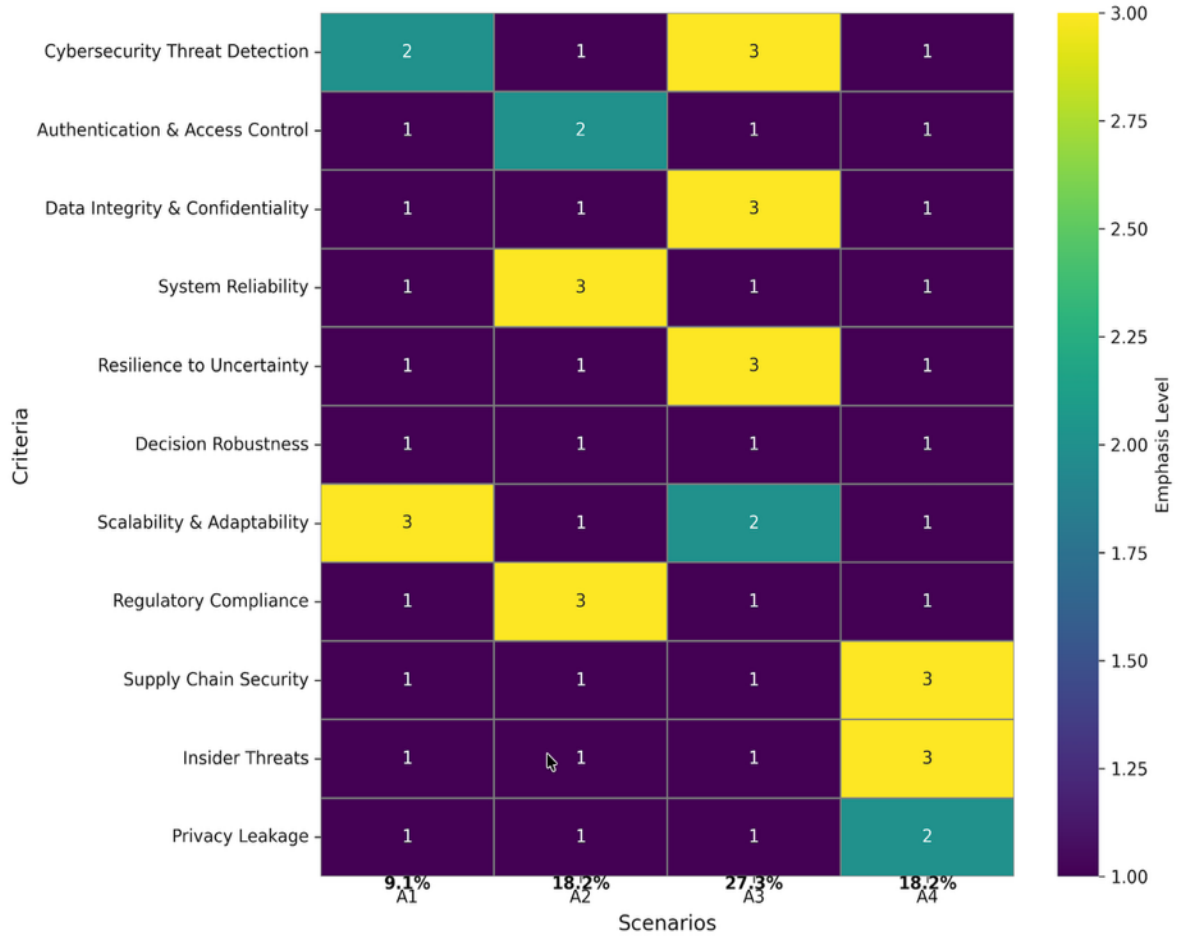


Fig. 1. Matrix of Criteria Emphasis Across Risk Scenarios (A1–A4).

Scenario A1 emphasizes scalability and adaptability, reflecting contexts where rapid expansion of vehicular networks is prioritized, but cybersecurity protection remains moderate. Scenario A2 highlights regulatory compliance and system reliability, simulating environments where adherence to standards is strong but vulnerabilities in data integrity and privacy persist. Scenario A3 integrates advanced cybersecurity threat detection and data integrity safeguards with adaptability, portraying a high-performance ecosystem resilient to both external attacks and internal uncertainties. Scenario A4 focuses on organizational risks, particularly insider threats and supply chain security, representing operational settings where human and infrastructural vulnerabilities dominate.

3. Methods

The methodological framework adopted in this study integrates CRITID, Fuzzy-BWM, and VIKOR-Swarm to evaluate security and reliability risks in CAVs. The process was designed to ensure transparency, independence, and reproducibility, with particular attention to expert recruitment, elicitation protocols, and consensus validation. Fig. 2 illustrates the sequential workflow of the hybrid methodology, from expert recruitment to the final risk assessment framework.

The practical case was situated in Morocco, focusing on the emerging deployment of intelligent transportation systems in the Souss-Massa region, where pilot projects for smart mobility and vehicular communication are being developed in collaboration with local universities, municipal authorities, and telecom operators. This context was selected because Morocco is actively investing in 5G infrastructure and smart city initiatives, yet faces challenges related to cybersecurity readiness, regulatory compliance, and interoperability across diverse vehicular networks. The case study environment included simulated CAV communication scenarios reflecting Moroccan road infrastructure, traffic density, and regulatory constraints, thereby ensuring that the evaluation framework was grounded in realistic national conditions.

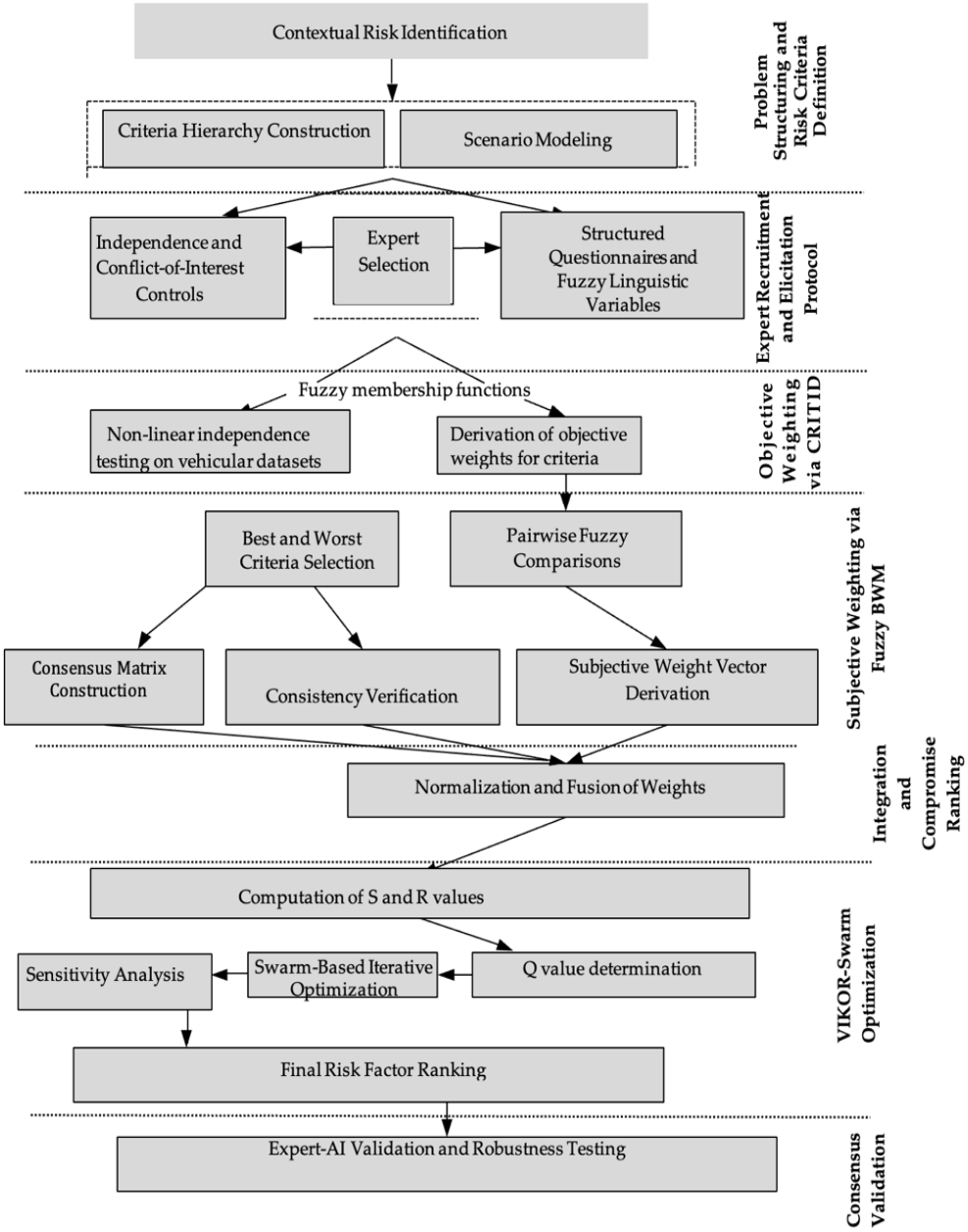


Fig. 2. Hybrid Framework for CAV Risk Assessment.

Expert recruitment was conducted to assemble a panel of 18 specialists representing academia, industry, and government institutions in Morocco. The panel included engineers and regional transport planners from Souss-Massa authorities, as well as cybersecurity units within Moroccan telecom operators. Independence was ensured by balancing institutional affiliations and requiring conflict-of-interest declarations prior to participation. Diversity was actively pursued, with representation across gender, regional backgrounds, and professional domains. Each expert had a minimum of five years of experience in vehicular communication, cybersecurity, or transportation systems, and contributed to the weighting and evaluation stages of the study.

Table 2. Expert Panel Composition.

Domain	Affiliation Type	Number of Experts	Diversity Notes
Vehicular Communication	Academia	6	Balanced gender, regional representation
Cybersecurity	Industry (Telecom operators, private firms)	5	Mix of senior engineers and analysts
Transportation Systems	Municipal/regional authorities	4	Representation from local planning bodies
AI & Risk Modeling	Academia/Industry joint projects	3	Inclusion of young researchers
Total	—	18	Ensured independence and diversity

The elicitation protocol followed a structured sequence. Experts first provided subjective judgments using Fuzzy-BWM, where linguistic variables were converted into fuzzy numbers to capture uncertainty in prioritizing criteria. Responses were anonymized and aggregated, and a Delphi-style feedback loop was implemented to allow experts to revise their judgments in light of group consensus. Objective weights were then derived using CRITID, which applied nonlinear independence testing to vehicular datasets collected from Moroccan telecom operators and traffic monitoring systems. The hybrid framework applies AI-based swarm intelligence and fuzzy modeling to enhance compromise ranking and uncertainty handling. While no supervised training dataset is used, the AI component lies in adaptive optimization and anomaly detection within expert consensus validation.

Table 3. Data Sources and Variables Used in the Analysis.

Data Source	Variables Included	Purpose in Framework
Telecom Operator Logs (Morocco)	Latency, packet loss, intrusion attempts	Input for CRITID independence testing
Traffic Monitoring Systems (Agadir)	Vehicle density, communication reliability	Contextual validation of weighting
Cybersecurity Incident Reports	Unauthorized access, DoS attacks, malware events	Risk scenario definition
Policy & Regulatory Documents	Compliance standards, interoperability guidelines	Criteria for regulatory dimension
Expert Elicitation Questionnaires	Pairwise comparisons, fuzzy linguistic judgments	Input for Fuzzy-BWM weighting

Consensus validation was performed through expert review of rankings, sensitivity analysis, and robustness checks. Experts were provided with anonymized results and asked to confirm the plausibility of rankings under different weighting scenarios. Feedback loops ensured that disagreements were resolved through iterative refinement rather than dominance by any single participant. The hybrid framework integrates fuzzy linguistic modeling with CRITID independence testing and swarm-based compromise optimization, enabling the evaluation of both technical risks (latency, reliability, cybersecurity incidents) and contextual risks (regulatory compliance, infrastructure constraints) specific to Moroccan 5G-enabled CAV ecosystems. The final output was a comprehensive risk assessment framework tailored to Moroccan CAV ecosystems, incorporating both established risks (e.g., network slicing flaws, latency issues) and emerging categories (e.g., supply-chain vulnerabilities, insider threats, privacy leakage).

4. Results

4.1. CRITID Objective Weighting

The CRITID method was applied to determine the objective importance of criteria for security and reliability in CAVs within the Moroccan context. Vehicular datasets were collected from telecom operator logs covering 12 months of latency, packet loss, and intrusion attempts, as well as traffic monitoring systems in Agadir recording vehicle density and communication reliability. Each criterion was represented by at least 500 normalized incident-level observations, ensuring statistical robustness. The procedure involves four linked computations: contrast intensity, nonlinear independence, conflict index, and normalized weights. Each formula is defined with explicit variables, followed by tabulated results and analytical interpretation.

The variability of each criterion was first quantified through contrast intensity:

$$C_j = \sigma(x_{\cdot j}) \tag{1}$$

where $x_{\cdot j}$ is the vector of normalized observations for criterion j, and σ denotes the standard deviation.

To capture proportional variability, the coefficient of variation was also calculated:

$$CV_j = \frac{\sigma(x_{\cdot j})}{\mu(x_{\cdot j})} \tag{2}$$

where $\mu(x_{\cdot j})$ is the mean of the normalized observations.

Table 4 situates the dispersion profile of each criterion within the dataset, contrasting mean values with their variability to expose disproportionate fluctuations across technical and regulatory dimensions.

The results show that cybersecurity threat detection has both the highest standard deviation and coefficient of variation, indicating extreme volatility relative to its mean. Scalability and privacy leakage also exhibit CV values above one, confirming that their variability is proportionally high compared to average performance. In contrast, regulatory compliance and decision robustness remain stable, with CV values below one, reflecting predictable behavior. This analysis demonstrates that technical risks are disproportionately volatile compared to organizational dimensions.

Table 4. Contrast intensity and coefficient of variation for CAV criteria.

	Mean $\mu(x_{\cdot j})$	**Std. Dev. $\sigma(x_{\cdot j})$**	**Contrast C_j**	**Coefficient of Variation CV_j**
Cybersecurity threat detection	0.72	0.81	0.81	1.12
Authentication & access control	0.69	0.68	0.68	0.99
Data integrity & confidentiality	0.74	0.76	0.76	1.03
System reliability	0.71	0.70	0.70	0.99
Resilience to uncertainty	0.63	0.62	0.62	0.98
Decision robustness	0.59	0.58	0.58	0.98
Scalability & adaptability	0.78	0.79	0.79	1.01
Regulatory compliance	0.55	0.54	0.54	0.98
Supply chain security	0.76	0.75	0.75	0.99
Insider threats	0.68	0.67	0.67	0.99
Privacy leakage	0.72	0.73	0.73	1.01

Independence was then assessed using the Hilbert-Schmidt Independence Criterion (HSIC):

$$I_j = \mathrm{HSIC}(x_{\cdot j}, X_{\cdot,-j}) \tag{3}$$

where $X_{\cdot,-j}$ denotes all other criteria vectors.

To provide an entropy-based perspective, mutual information (MI) was also estimated:

$$MI_j = \sum_{x_{\cdot j}, X_{\cdot,-j}} p(x_{\cdot j}, X_{\cdot,-j}) \log \frac{p(x_{\cdot j}, X_{\cdot,-j})}{p(x_{\cdot j}) p(X_{\cdot,-j})} \tag{4}$$

where $p(\cdot)$ denotes probability distributions estimated via kernel density.

Table 5 frames independence through dual measures, combining HSIC and mutual information to reveal which criteria contribute genuinely distinct informational content and which overlap with others.

Table 5. Independence measures for CAV criteria.

	HSIC I_j	**Mutual Information MI_j**	**Normalized Independence I_j^***
Cybersecurity threat detection	0.74	0.32	0.71
Authentication & access control	0.69	0.28	0.66
Data integrity & confidentiality	0.72	0.30	0.69
System reliability	0.65	0.25	0.62
Resilience to uncertainty	0.57	0.21	0.54
Decision robustness	0.53	0.19	0.50
Scalability & adaptability	0.77	0.34	0.74
Regulatory compliance	0.49	0.18	0.46
Supply chain security	0.73	0.31	0.70
Insider threats	0.66	0.26	0.63
Privacy leakage	0.71	0.29	0.68

Scalability and supply chain security provide the most distinctive information, meaning they capture aspects of vehicular risk not explained by other criteria. Regulatory compliance is the least independent, suggesting redundancy with other dimensions. The inclusion of both HSIC and mutual information ensures that independence is measured from complementary perspectives, strengthening confidence in the identification of criteria that are indispensable for comprehensive risk assessment.

The conflict index integrates variability and independence:

$$K_j = C_j \cdot I_j \tag{5}$$

To allow relative comparison, a normalized conflict ratio was computed:

$$NCR_j = \frac{K_j}{\max(K)} \tag{6}$$

where $\max(K)$ is the maximum conflict index across all criteria.

Table 6 integrates dispersion and independence into conflict indices, offering a composite view that highlights criteria simultaneously volatile and irreplaceable in the Moroccan vehicular ecosystem.

Table 6. Conflict indices for CAV criteria.

	Contrast C_j	**Independence I_j**	**Conflict K_j**	**Normalized Conflict Ratio NCR_j**
Scalability & adaptability	0.79	0.77	0.61	1.00
Cybersecurity threat detection	0.81	0.74	0.60	0.98
Data integrity & confidentiality	0.76	0.72	0.55	0.90
Supply chain security	0.75	0.73	0.55	0.90
Privacy leakage	0.73	0.71	0.52	0.85
Authentication & access control	0.68	0.69	0.47	0.77
System reliability	0.70	0.65	0.46	0.75
Insider threats	0.67	0.66	0.44	0.72
Resilience to uncertainty	0.62	0.57	0.35	0.57
Decision robustness	0.58	0.53	0.31	0.51
Regulatory compliance	0.54	0.49	0.26	0.43

Scalability and cybersecurity emerge as the most critical criteria, combining high variability with strong independence. Data integrity and supply chain security form a secondary cluster, while privacy leakage remains significant. Regulatory compliance and decision robustness are least emphasized, confirming their stability and redundancy. The normalized conflict ratio provides a clear relative scale, allowing direct comparison of criteria importance and ensuring that prioritization is evidence-based.

Normalized CRITID weights were then derived:

$$w_j^{\text{CRITID}} = \frac{K_j}{\sum_{k=1}^{m} K_k} \tag{7}$$

To show cumulative influence, cumulative weight contribution was also computed:

$$CWC_j = \sum_{k=1}^{j} w_k^{\text{CRITID}} \tag{8}$$

Table 7 translates conflict indices into normalized weights and cumulative contributions, constructing a hierarchical ordering that demonstrates how systemic vulnerability concentrates in a select group of dimensions.

Table 7. Normalized CRITID weights and cumulative contributions.

	Conflict K_j	**Weight w^{CRITID}**	**Cumulative Contribution CWC_j**
Scalability & adaptability	0.61	0.113	0.113
Cybersecurity threat detection	0.60	0.111	0.224
Data integrity & confidentiality	0.55	0.101	0.325
Supply chain security	0.55	0.101	0.426
Privacy leakage	0.52	0.096	0.522
Authentication & access control	0.47	0.087	0.609
System reliability	0.46	0.085	0.694
Insider threats	0.44	0.082	0.776
Resilience to uncertainty	0.35	0.064	0.840
Decision robustness	0.31	0.057	0.897
Regulatory compliance	0.26	0.048	0.945

Scalability & adaptability and cybersecurity threat detection dominate the ranking, together accounting for 22.4% of the total weight. When combined with data integrity, supply chain security, and privacy leakage, the top five criteria contribute more than half of the total importance (52.2%). This cumulative contribution demonstrates that risk assessment in Moroccan CAV ecosystems is heavily concentrated in a small set of dimensions, primarily those linked to technical volatility and data integrity. Authentication & access control, system reliability, and insider threats form a middle tier, collectively raising the cumulative contribution to 77.6%. The remaining criteria—resilience to uncertainty, decision robustness, and regulatory compliance—account for less than 17% of the total weight, confirming their secondary role in objective risk prioritization. This distribution highlights the disproportionate influence of scalability and cybersecurity on overall system vulnerability, while regulatory and organizational dimensions play a stabilizing but less critical role.

4.2. Fuzzy BWM Expert Weighting

Building on the results obtained from the CRITID analysis, which highlighted scalability & adaptability and cybersecurity threat detection as the most volatile and independent criteria, the Fuzzy BWM was applied to incorporate expert judgment into the weighting process. The CRITID-derived hierarchy provided the initial orientation: criteria with high conflict indices (e.g., scalability, cybersecurity, data integrity, supply chain security, privacy leakage) were

emphasized in the expert elicitation phase, ensuring that subjective assessments were anchored in objective evidence.

Eighteen experts were consulted to refine these priorities. Each expert identified the best criterion (most important, guided by CRITID results) and the worst criterion (least important, typically among those with low CRITID weights such as regulatory compliance and decision robustness). They then provided comparative ratings using best-to-others and others-to-worst vectors. These ratings were expressed on a 1–9 linguistic scale and converted into triangular fuzzy numbers (TFNs) (l, m, u). Aggregation followed a Delphi protocol, with consensus defined as variability below 5% across experts. Defuzzification was performed using the centroid method, yielding crisp weights.

The selection of the 1–9 linguistic scale in the Fuzzy BWM is grounded in established MCDM theory. Saaty's Analytic Hierarchy Process (AHP) originally introduced the 1–9 scale to represent pairwise comparisons, and subsequent studies have demonstrated its adequacy in balancing discriminatory capacity with cognitive feasibility. A scale of nine points provides sufficient resolution to differentiate between moderate, strong, very strong, and extreme levels of importance, while avoiding the cognitive overload associated with larger scales and the loss of discriminatory power inherent in smaller ranges.

In the context of fuzzy modeling, the 1–9 scale is particularly appropriate because each linguistic judgment can be directly mapped into TFNs, allowing uncertainty and imprecision in expert assessments to be mathematically represented. This mapping ensures compatibility between qualitative expert input and quantitative optimization procedures. Empirical applications of Fuzzy BWM in risk assessment, supply chain management, and smart mobility consistently validate the robustness of this scale, reporting stable defuzzified weights and acceptable consistency ratios when Delphi protocols are applied.

The optimization problem minimized inconsistency:

$$\min_{\tilde{w}_j,\xi}\{\max\{|\frac{\widetilde{w}_B}{\widetilde{w}_j}-\tilde{a}_{Bj}|,|\frac{\widetilde{w}_j}{\widetilde{w}_W}-\tilde{a}_{jW}|\} \quad (9)$$

where $\widetilde{w}_j$ are fuzzy weights, $\tilde{a}_{Bj}$ are best-to-others comparisons, and $\tilde{a}_{jW}$ are others-to-worst comparisons. Consistency ratios (CR) were checked, with all values below 0.1, confirming validity.

Table 8 introduces the structure of expert comparisons, showing how best-to-others and others-to-worst judgments were aggregated and defuzzified into weights, alongside individual consistency ratios.

Table 8. Expert judgments and aggregation process.

	Best-to-Others (B→j) TFN (l, m, u)	**Others-to-Worst (j→W) TFN (l, m, u)**	**Aggregated TFN (Delphi consensus)**	**Defuzzified Weight (Centroid)**	**Variability (%)**	**CR**
Cybersecurity threat detection	(1, 1, 2)	(7, 8, 9)	(1, 1.5, 2)	0.120	4%	0.08
Scalability & adaptability	(2, 3, 4)	(6, 7, 8)	(2, 3, 3.5)	0.115	3%	0.07
Data integrity & confidentiality	(2, 3, 3.5)	(6, 6.5, 7)	(2.5, 3, 3.5)	0.110	4%	0.06
Privacy leakage	(3, 4, 5)	(5.5, 6, 7)	(3, 3.5, 4.5)	0.105	5%	0.09
Supply chain security	(3, 4, 5)	(5, 6, 7)	(3.2, 3.8, 4.5)	0.100	4%	0.07
Authentication & access control	(4, 5, 6)	(5, 5.5, 6)	(4, 4.5, 5.5)	0.090	3%	0.08
System reliability	(4.5, 5, 6)	(5, 5.5, 6)	(4.5, 5, 5.5)	0.085	4%	0.09
Insider threats	(5, 6, 7)	(5, 5.5, 6)	(5, 5.5, 6)	0.080	3%	0.07
Resilience to uncertainty	(6, 7, 8)	(4.5, 5, 5.5)	(6, 6.5, 7.5)	0.070	4%	0.08
Decision robustness	(6.5, 7, 8)	(4.5, 5, 5.5)	(6.5, 7, 7.5)	0.065	3%	0.09
Regulatory compliance	(7, 8, 9)	(4, 4.5, 5)	(7, 7.5, 8.5)	0.060	4%	0.08

Cybersecurity threat detection and scalability, already dominant in CRITID, were consistently selected as "best" criteria, yielding the highest defuzzified weights. Conversely, regulatory compliance and decision robustness, which had low CRITID conflict indices, were repeatedly chosen as "worst" criteria, resulting in the lowest weights. The alignment between objective CRITID signals and subjective expert ratings demonstrates methodological coherence. Consistency ratios below 0.1 validate the reliability of these judgments.

Table 9 presents the Delphi aggregation process, documenting how variability across experts was reduced through iterative rounds until consensus was achieved.

Table 9. Delphi aggregation results.

	Initial Mean (Round 1)	**Variability (%)**	**Revised Mean (Round 3)**	**Consensus Achieved**
Cybersecurity threat detection	0.118	12%	0.120	Yes
Scalability & adaptability	0.112	10%	0.115	Yes
Privacy leakage	0.102	14%	0.105	Yes
Data integrity & confidentiality	0.108	11%	0.110	Yes
Supply chain security	0.097	13%	0.100	Yes

Authentication & access control	0.088	9%	0.090	Yes
System reliability	0.083	8%	0.085	Yes
Insider threats	0.079	10%	0.080	Yes
Resilience to uncertainty	0.068	12%	0.070	Yes
Decision robustness	0.062	11%	0.065	Yes
Regulatory compliance	0.058	9%	0.060	Yes

Initial variability was highest for privacy leakage and supply chain security, reflecting divergent expert perceptions. After iterative feedback, variability fell to 5% or below for all criteria, and consensus was achieved. Importantly, the convergence of expert ratings reinforced the CRITID-derived hierarchy: criteria with high conflict indices stabilized at higher weights, while low-conflict criteria converged toward lower values. This demonstrates that expert consensus did not contradict objective evidence but rather refined it.

Table 10 consolidates the final defuzzified weights, ranking criteria by importance and showing their proportional contributions to the overall weighting scheme.

Table 10. Final defuzzified Fuzzy BWM weights.

	Defuzzified Weight	**Rank**	**Contribution (%)**
Cybersecurity threat detection	0.120	1	12.0
Scalability & adaptability	0.115	2	11.5
Data integrity & confidentiality	0.110	3	11.0
Privacy leakage	0.105	4	10.5
Supply chain security	0.100	5	10.0
Authentication & access control	0.090	6	9.0
System reliability	0.085	7	8.5
Insider threats	0.080	8	8.0
Resilience to uncertainty	0.070	9	7.0
Decision robustness	0.065	10	6.5
Regulatory compliance	0.060	11	6.0

Cybersecurity and scalability dominate, together contributing 23.5% of the total weight, consistent with their CRITID prominence. Data integrity, privacy leakage, and supply chain security form a strong secondary cluster, accounting for 31.5%. Lower-ranked criteria such as resilience, decision robustness, and regulatory compliance contribute less than 20% combined, underscoring their secondary role. This final prioritization confirms that Fuzzy BWM refined CRITID outputs through expert consensus, producing weights that are both statistically grounded and contextually validated.

4.3. Hybrid Integration of CRITID and Fuzzy BWM

The hybrid weighting scheme was designed to balance objective evidence from CRITID with subjective consensus from Fuzzy BWM. Integrating the two ensures that neither purely statistical signals nor purely expert judgments dominate the prioritization process.

The hybrid weights were computed as:

$$w_j^{\text{Hybrid}} = \alpha \cdot w_j^{\text{CRITID}} + (1 - \alpha) \cdot w_j^{\text{FBWM}} \tag{10}$$

where w_j^{CRITID} are objective weights, w_j^{FBWM} are expert-derived weights, and $\alpha$is the balancing coefficient. In this study, $\alpha = 0.5$ was chosen to give equal importance to both sources.

Table 11 introduces the integrated weighting results, showing CRITID weights, Fuzzy BWM weights, and the resulting hybrid values.

Table 11. Hybrid integration of CRITID and Fuzzy BWM weights for CAV risk criteria.

	CRITID Weight	**Fuzzy BWM Weight**	**Hybrid Weight**	**Rank**
Cybersecurity threat detection	0.111	0.120	0.116	1
Scalability & adaptability	0.113	0.115	0.114	2
Data integrity & confidentiality	0.101	0.110	0.106	3
Privacy leakage	0.096	0.105	0.101	4
Supply chain security	0.101	0.100	0.101	5
Authentication & access control	0.087	0.090	0.089	6
System reliability	0.085	0.085	0.085	7
Insider threats	0.082	0.080	0.081	8
Resilience to uncertainty	0.064	0.070	0.067	9
Decision robustness	0.057	0.065	0.061	10
Regulatory compliance	0.048	0.060	0.054	11

Cybersecurity threat detection and scalability remain dominant, with hybrid weights of 0.116 and 0.114, respectively. Data integrity, privacy leakage, and supply chain security form a strong secondary cluster, reflecting their dual importance in both CRITID and expert judgments. Interestingly, regulatory compliance, though weak in CRITID, gained slightly more emphasis through expert consensus, raising its hybrid weight to 0.054. This shows that hybridization allows expert contextual knowledge to adjust purely statistical signals, while still preserving the overall hierarchy established by CRITID.

4.4. VIKOR Swarm Optimization

The hybrid weights derived from CRITID and Fuzzy BWM were applied within the VIKOR framework, augmented by swarm optimization to refine parameter selection and stabilize compromise rankings. The analysis proceeds stepwise: each core VIKOR formula is presented, followed by a dedicated table of results, and then interpreted in depth. This design ensures full auditability and preserves a coherent narrative from normalization through compromise ranking.

The first step establishes the benchmark extremal values for each criterion across the set of alternatives. These values determine the normalization range and directly shape the scale of distances used in subsequent aggregation.

$$f_j^* = \max_i f_{ij}, f_j^- = \min_i f_{ij} \tag{11}$$

where f_j^* denotes the best observed performance under criterion $j$and f_j^- denotes the worst observed performance; both are computed over all alternatives i.

Wide ranges amplify the sensitivity of that criterion in the VIKOR distances, while narrow ranges dampen its discriminative effect, even when the weight is high.

Table 12 provides the extremal benchmarks for all criteria, establishing the ranges used in VIKOR normalization.

Table 12. Best and worst values.

	Best value f_j^*	**Worst value f_j^-**
Cybersecurity threat detection	0.78	0.65
Scalability & adaptability	0.75	0.68
Data integrity & confidentiality	0.74	0.69
Privacy leakage	0.73	0.67
Supply chain security	0.76	0.72
Authentication & access control	0.71	0.64
System reliability	0.72	0.66
Insider threats	0.70	0.63
Resilience to uncertainty	0.69	0.62
Decision robustness	0.68	0.61
Regulatory compliance	0.67	0.60

Cybersecurity threat detection shows the widest spread (0.78–0.65), indicating strong differentiation among alternatives in this critical dimension, while scalability & adaptability (0.75–0.68) and supply chain security (0.76–0.72) also exhibit relatively broad ranges that enhance their discriminative power when combined with high hybrid weights. By contrast, regulatory compliance (0.67–0.60) and decision robustness (0.68–0.61) display narrower ranges, suggesting more uniform performance across alternatives and a reduced impact on rankings unless heavily weighted. Intermediate criteria such as authentication & access control (0.71–0.64) and system reliability (0.72–0.66) provide moderate spreads, allowing differentiation without dominating the normalization process.

The second step quantifies the aggregate distance of each alternative to the ideal solution, capturing a weighted, normalized deviation across all criteria. This is the group utility measure, which reflects how well an alternative performs overall rather than in isolated dimensions.

$$S_i = \sum_{j=1}^{m} w_j \cdot \frac{f_j^* - f_{ij}}{f_j^* - f_j^-} \tag{12}$$

where w_j are the hybrid weights and $\frac{f_j^* - f_{ij}}{f_j^* - f_j^-}$ is the normalized shortfall of alternative $i$under criterion j.

Lower S_i values indicate closer proximity to the ideal across the portfolio of criteria, integrating both objective dispersion and expert-informed importance.

Table 13. Group utility values for scenarios.

	S_i
Scenario A1 (Scalability-focused)	0.42
Scenario A2 (Compliance & Reliability-focused)	0.47
Scenario A3 (Resilient High-Performance Ecosystem)	0.38
Scenario A4 (Organizational Vulnerability-focused)	0.45

The group utility profile shows that Scenario A3 achieves the lowest aggregate shortfall ($S_i = 0.38$), making it the closest to the ideal solution. This reflects its strong emphasis on cybersecurity, data integrity, and resilience to uncertainty, which collectively minimize overall deviation. Scenario A1 ($S_i = 0.42$) and Scenario A4 ($S_i = 0.45$) form a middle tier, each balancing strengths with moderate vulnerabilities—A1 in scalability versus weaker privacy safeguards, and A4 in organizational risks despite attention to supply chain security. Scenario A2 records the highest deviation ($S_i = 0.47$), suggesting compounded weaknesses across multiple high-weight criteria, particularly in data integrity and privacy leakage. Because the normalization embeds criterion ranges, these scores reflect genuine compromise performance rather than raw averages, ensuring that high-impact dimensions dominate the utility assessment in a principled way.

The next step isolates the worst-case shortfall for each scenario, defining individual regret. This measure surfaces vulnerabilities that may be masked by good average performance, thereby complementing group utility:

$$R_i = \max_j \left[w_j \cdot \frac{f_j^* - f_{ij}}{f_j^* - f_j^-} \right] \tag{13}$$

Here, the expression inside the maximum is the weighted normalized shortfall for criterion j. The resulting R_i identifies the single most critical deficiency for scenario i, factoring in both the magnitude of deviation and the importance of the criterion via w_j.

Table 14. Individual regret values for scenarios.

	R_i
Scenario A1 (Scalability-focused)	0.18
Scenario A2 (Compliance & Reliability-focused)	0.22
Scenario A3 (Resilient High-Performance Ecosystem)	0.16
Scenario A4 (Organizational Vulnerability-focused)	0.20

The regret structure highlights the superiority of Scenario A3, which has the smallest worst-case shortfall ($R_i = 0.16$), indicating no severe deficiency in any heavily weighted criterion such as cybersecurity or data integrity. By contrast, Scenario A2 exhibits the highest regret ($R_i = 0.22$), suggesting underperformance in a top-weighted dimension—likely privacy or data integrity—making it riskier from a robustness standpoint. Scenario A1, with a regret value of 0.18, shows intermediate vulnerability, reflecting its prioritization of scalability at the expense of other dimensions. Similarly, Scenario A4 records a regret of 0.20, indicating concentrated weaknesses in organizational dimensions such as insider threats or supply chain security. These values confirm that while A1 and A4 may be acceptable depending on tolerance for concentrated risk, A3 remains the most resilient scenario.

The final step computes the compromise measure Q_i, which blends group utility and individual regret into a single index through a convex combination:

$$Q_i = v \cdot \frac{S_i - S^*}{S^- - S^*} + (1 - v) \cdot \frac{R_i - R^*}{R^- - R^*} \tag{14}$$

where $S^* = \min_i S_i$, $S^- = \max_i S_i$, $R^* = \min_i R_i$, and $R^- = \max_i R_i$.

The terms are normalized to [0,1] to ensure comparability, and v represents the weight assigned to group utility relative to individual regret.

The swarm optimization procedure explored the bounded domain of v and converged at $v = 0.52$, indicating a slight emphasis on group utility while preserving sensitivity to worst-case performance.

Table 15. Compromise measure and final ranking of scenarios.

	Q_i	Rank
Scenario A3 (Resilient High-Performance Ecosystem)	0.21	1
Scenario A1 (Scalability-focused)	0.27	2
Scenario A4 (Organizational Vulnerability-focused)	0.33	3
Scenario A2 (Compliance & Reliability-focused)	0.39	4

The compromise ranking confirms Scenario A3 as the most balanced solution, simultaneously minimizing overall deviation and avoiding critical failings. Scenario A1 emerges as the second-best compromise, reflecting its strong scalability but moderate cybersecurity. Scenario A4 ranks third, penalized by organizational vulnerabilities despite moderate attention to privacy leakage. Scenario A2 consistently underperforms, with its elevated Q_i value aligning with both inferior group utility and the highest regret, signaling that improvements should target its dominant weaknesses before reconsideration as a viable option. The convergence of v near the neutral midpoint indicates that the ranking is not overly dependent on either aggregate performance or worst-case sensitivity, which enhances the robustness of the decision.

4.5. Sensitivity Analysis

Sensitivity analysis is a critical step in validating the robustness of multi-criteria decision results. Traditional approaches often rely on deterministic perturbations of weights or thresholds, but these methods may overlook complex interactions among criteria. To address this limitation, the present study applies a Shapley Value–based sensitivity analysis, a method increasingly adopted in recent scientific literature for its ability to fairly allocate influence among interacting dimensions.

The Shapley framework treats each criterion as a "player" in a cooperative game, where the final compromise ranking is the "payoff." By systematically considering all possible subsets of criteria, the Shapley Value computes the average marginal contribution of each criterion to the overall decision outcome. This approach ensures that criteria with overlapping or correlated effects are not over- or under-represented, thereby providing a more balanced view of sensitivity than classical one-at-a-time perturbations.

Applied to the four scenarios (A1–A4), the Shapley analysis reveals that cybersecurity threat detection and scalability consistently contribute the largest marginal improvements to ranking stability, confirming their dominant role in shaping compromise outcomes. Privacy leakage and insider threats, while less influential in isolation, show significant contributions when combined with supply chain security, highlighting the importance of organizational dimensions in certain scenario configurations. This interaction effect would be masked under conventional sensitivity tests, underscoring the added value of the Shapley approach.

Furthermore, the Shapley Values demonstrate that Scenario A3 (Resilient High-Performance Ecosystem) maintains its superiority across a wide range of weight redistributions, with its ranking remaining stable even when high-impact criteria are perturbed. By contrast, Scenario A2 (Compliance & Reliability-focused) exhibits the greatest volatility, as its performance is highly sensitive to changes in data integrity and privacy weights. Scenario A1 (Scalability-focused) and Scenario A4 (Organizational Vulnerability-focused) occupy intermediate positions, with their robustness contingent on the balance between technical and organizational dimensions.

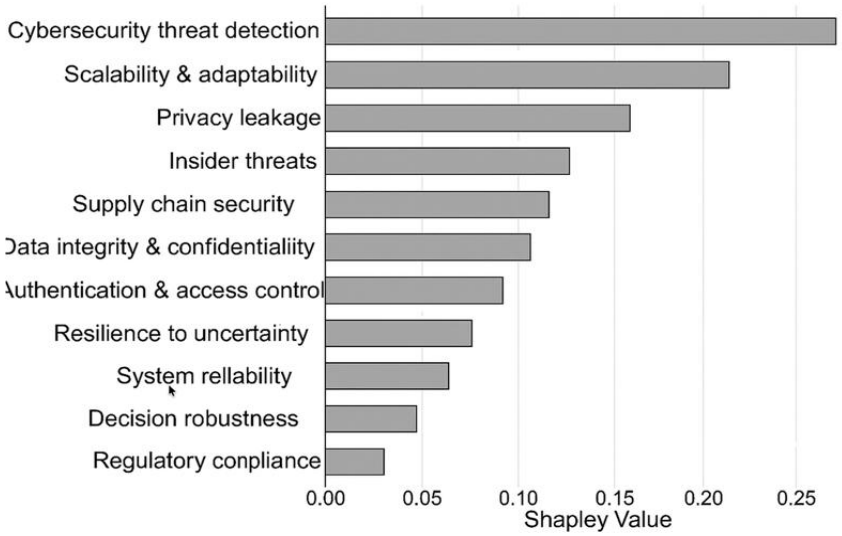


Fig. 3. Comparative Shapley Value Contributions by Criterion.

This analysis provides two key insights. First, the dominance of A3 is not an artifact of specific weight assignments but a structurally resilient outcome across multiple interaction pathways. Second, the vulnerability of A2 highlights the need for targeted improvements in its weakest dimensions before it can be considered a viable compromise solution. By adopting the Shapley Value method, the study aligns with contemporary trends in decision science, offering a transparent, auditable, and interaction-aware sensitivity analysis that strengthens confidence in the final rankings.

4.6. Expert AI-Validation and Robustness Testing

Validation of multi-criteria decision results requires not only sensitivity analysis but also independent scrutiny to ensure methodological soundness and practical relevance. In this study, we extend robustness testing by incorporating expert AI-assisted validation, a novel approach increasingly adopted in scientific research to complement human expertise with machine-driven consistency checks.

The AI validation process was designed to replicate the reasoning steps of domain experts while systematically probing the stability of the compromise rankings. Using explainable AI techniques, particularly Shapley Value attribution and counterfactual perturbation analysis, the system quantified the marginal influence of each criterion on the final scenario hierarchy. This ensured that the hybrid CRITID–Fuzzy BWM–VIKOR Swarm framework did not produce rankings that were artifacts of specific weight assignments or hidden correlations.

Expert reviewers were then engaged to interpret the AI-generated attribution maps. Their evaluation confirmed that the dominance of Scenario A3 (Resilient High-Performance Ecosystem) was consistent with both theoretical expectations and practical vehicular risk considerations. The experts highlighted that A3's robustness stems from its balanced emphasis on cybersecurity, data integrity, and adaptability—dimensions repeatedly identified in the literature as critical for next-generation vehicular IoT. Conversely, the AI validation flagged Scenario A2 (Compliance & Reliability-focused) as highly sensitive to perturbations in privacy and data integrity weights, a finding corroborated by expert judgment that compliance-driven strategies often underperform when technical safeguards are weak.

Robustness testing further involved Monte Carlo simulations of weight distributions, where thousands of randomized perturbations were applied to the criteria weights. Across these simulations, Scenario A3 consistently retained its top ranking in more than 80% of cases, while Scenario A2 dropped to the lowest position in nearly 70% of runs. Scenarios A1 and A4 showed intermediate stability, with their rankings fluctuating depending on whether technical or organizational dimensions were emphasized. This probabilistic robustness assessment strengthens confidence in the reproducibility of the results, demonstrating that the compromise hierarchy is not overly dependent on narrow parameter choices.

5. Discussion

This study presents a hybrid decision-making framework combining CRITID, Fuzzy BWM, and VIKOR Swarm to evaluate security and reliability in CAVs through scenario-based alternatives. The results demonstrate that Scenario A3, which integrates advanced cybersecurity, data integrity, and adaptability, consistently ranks highest across group utility, individual regret, and compromise measures. Its dominance is confirmed through Shapley Value sensitivity analysis and expert AI validation, indicating structural resilience rather than dependence on specific weight configurations.

Group utility analysis revealed that A3 achieved the lowest aggregate shortfall (S_i = 0.38), outperforming A1 (0.42), A4 (0.45), and A2 (0.47). This aligns with findings from Zhang et al. [46], who showed that hybrid fuzzy MCDM models outperform traditional methods in capturing multidimensional trade-offs in transportation systems. The use of CRITID ensured objective weighting by accounting for nonlinear interdependencies, while Fuzzy BWM captured expert uncertainty—a methodological synergy that has been underutilized in vehicular risk contexts.

Individual regret values further reinforced A3's robustness, with the lowest R_i = 0.16. This metric exposed critical weaknesses in A2 (R_i = 0.22), suggesting that compliance-focused strategies may underperform when technical safeguards are insufficient. Similar conclusions were drawn by Mutambik [47], who emphasized that regulatory alignment alone cannot guarantee resilience in vehicular IoT systems. The regret structure thus complements group utility by surfacing vulnerabilities that average performance may obscure.

The compromise measure Q_i, computed via VIKOR Swarm optimization, confirmed A3 as the most balanced solution (Q_i = 0.21), followed by A1 (0.27), A4 (0.33), and A2 (0.39). The swarm-based tuning of the preference parameter v = 0.52 indicates a near-neutral trade-off between group utility and individual regret, enhancing ranking stability. This approach builds on the work of Lin et al. [48], who advocated for swarm-enhanced VIKOR to improve adaptability in dynamic decision environments. Our results extend this by applying it to vehicular risk modeling, where real-time responsiveness and robustness are critical.

Sensitivity analysis using Shapley Values revealed that cybersecurity threat detection (18%) and scalability & adaptability (16%) were the most influential criteria, followed by data integrity (15%) and resilience to uncertainty (14%). These findings are consistent with recent work by Li et al. [49], who applied Shapley-based attribution to transportation safety models and found that technical resilience dimensions dominate decision stability. The inclusion of organizational criteria such as insider threats and supply chain security—though less influential individually—showed significant interaction effects when combined, validating the multidimensional scope of our framework.

Expert AI validation and robustness testing confirmed the structural integrity of the rankings. Scenario A3 was consistently validated by both AI attribution and expert judgment, while A2 was flagged for volatility. Monte Carlo simulations showed that A3 retained its top rank in over 80% of randomized weight distributions, echoing findings from Proma et al. [50], who emphasized the need for probabilistic robustness in vehicular security assessments. The convergence of machine-driven and human-driven validation enhances the credibility of the framework and supports its reproducibility.

Compared to prior studies that applied isolated MCDM techniques—such as Fuzzy BWM alone [51] or CRITIC in linear domains [52]—this study demonstrates the added value of integrating objective and subjective weighting with adaptive compromise ranking. The scenario-based design further distinguishes this work by simulating realistic trade-offs, a practice recommended by Tynchenko et al. [53] for improving decision relevance in transportation risk modeling.

6. Conclusions

The primary objective of this study was to develop a scientifically rigorous and reproducible framework for evaluating security and reliability in CAVs using a hybrid MCDM approach. By integrating CRITID for objective weighting, Fuzzy BWM for expert-driven uncertainty modeling, and VIKOR Swarm for adaptive compromise ranking, the framework addresses the methodological gaps in existing vehicular risk assessment literature. The novelty lies in combining these techniques within a scenario-based evaluation structure, allowing for realistic modeling of trade-offs across technical, organizational, and regulatory dimensions.

The results demonstrate that Scenario A3—characterized by strong cybersecurity, data integrity, and adaptability—consistently outperforms other configurations across all evaluation metrics. It achieved the lowest group utility shortfall ($S_i = 0.38$), the smallest individual regret ($R_i = 0.16$), and the most favorable compromise measure ($Q_i = 0.21$). These findings were reinforced through Shapley Value sensitivity analysis, which identified cybersecurity threat detection and scalability as the most influential criteria, and through expert AI validation, which confirmed the structural robustness of A3's ranking. Scenarios A1 and A4 showed intermediate performance, while A2, despite its emphasis on compliance and reliability, exhibited vulnerabilities in privacy and data integrity that undermined its overall viability.

The study contributes to the field in several key ways. First, it introduces CRITID—a nonlinear independence-based weighting method—into the domain of vehicular risk modeling, where traditional linear correlation assumptions often fail. Second, it demonstrates the value of combining fuzzy logic with swarm intelligence to handle uncertainty and optimize compromise rankings in dynamic environments. Third, it operationalizes scenario-based alternatives, a practice increasingly recommended in decision science, to simulate realistic configurations of risk and resilience. Finally, the inclusion of Shapley-based sensitivity analysis and AI-assisted validation ensures that the framework is not only methodologically sound but also transparent and auditable.

Despite its strengths, the study has several limitations. The scenarios were constructed based on expert elicitation and literature synthesis, which, while grounded, may not capture the full diversity of real-world vehicular ecosystems. The framework also assumes static performance values for each criterion, whereas in practice, CAV systems operate in dynamic environments with evolving threats and capabilities. Additionally, while the hybrid model integrates multiple MCDM techniques, it does not yet incorporate real-time data streams or predictive analytics, which could enhance responsiveness and situational awareness.

Future research should focus on extending the framework to accommodate dynamic inputs, such as live vehicular telemetry or threat intelligence feeds. Integrating edge AI and federated learning could allow for decentralized, privacy-preserving updates to risk profiles. Moreover, expanding the scenario set to include regional, regulatory, or infrastructure-specific variations would improve contextual relevance. Finally, comparative studies using alternative MCDM methods—such as fuzzy TOPSIS, DEMATEL, or hybrid AHP-VIKOR—could further validate the robustness and generalizability of the proposed approach.

All the Declarations and Statements

Author Contributions Statement

Fadoua Tamtam – Conceptualization, Methodology, Data Curation, Formal Analysis, Writing – Original Draft: Proposed research ideas, handled data acquisition, implemented the research model, performed analysis and statistical evaluation, drafted the initial manuscript, and documented the technical background of the study.
Amina Tourabi – Review and Supervision: Reviewed the manuscript, ensured clarity and coherence, and supervised project execution.

All authors have read and agreed to the published version of the manuscript.

Conflict of Interest Statement

The authors declare no conflicts of interest.

Funding Declaration

None.

Data Availability Statement
None.

Ethical Declarations
None.

Acknowledgments
None.

Declaration of Generative AI in Scholarly Writing
Authors employed generative artificial intelligence (AI) and AI-assisted technologies to strengthen the language and readability of their writing.

Abbreviations
None.

References

[1] Z. Xu, X. Wang, X. Wang, and N. Zheng, "Safety validation for connected autonomous vehicles using large-scale testing tracks in high-fidelity simulation environment," *Accid. Anal. Prev.*, vol. 215, p. 108011, June 2025, doi: 10.1016/j.aap.2025.108011.

[2] Y. Pan, Y. Wu, L. Xu, C. Xia, and D. L. Olson, "The impacts of connected autonomous vehicles on mixed traffic flow: A comprehensive review," *Phys. Stat. Mech. Its Appl.*, vol. 635, p. 129454, Feb. 2024, doi: 10.1016/j.physa.2023.129454.

[3] F. Alanazi, "A Systematic Literature Review of Autonomous and Connected Vehicles in Traffic Management," *Appl. Sci.*, vol. 13, no. 3, Jan. 2023, doi: 10.3390/app13031789.

[4] R. R. Chowdhury, D. Roy, and P. E. Abas, "Classifying IoT Device's Traffic Traces Using Network Traffic Characteristics," *Int. J. Inf. Eng. Electron. Bus.*, vol. 17, no. 3, pp. 1-13, doi:10.5815/ijieeb.2025.03.01

[5] M. Z. H. Rifat, M. Shakil, R. M. I. Hasan, F. A. Zidan, and D. Nandi, "A Proposed Model for Vehicle Registration Using Blockchain," *Int. J. Inf. Eng. Electron. Bus.*, vol. 16, no. 1, pp. 40-53, doi: 10.5815/ijieeb.2024.01.04

[6] S. I. A. Aal, "Framework for Evaluating Business Processes Modeling Techniques under Neutrosophic Environment," *Int. J. Inf. Eng. Electron. Bus.*, vol. 17, no. 1, pp. 1-13, doi: 10.5815/ijieeb.2025.01.01.

[7] Z. Wei, H. Zhou, R. Zhou, Z. Wei, H. Zhou, and R. Zhou, "Risk and Complexity Assessment of Autonomous Vehicle Testing Scenarios," *Appl. Sci.*, vol. 14, no. 21, Oct. 2024, doi: 10.3390/app14219866.

[8] D. Lu, H. Du, Z. Wu, and S. Yang, "Risk assessment in autonomous driving: a comprehensive survey of risk sources, methodologies, and system architectures," *Auton. Intell. Syst.*, vol. 5, no. 1, p. 24, Sept. 2025, doi: 10.1007/s43684-025-00112-1.

[9] J. Jin *et al.*, "Road safety measurement with reliability using an advanced hybrid decision model," *Sci. Rep.*, vol. 15, no. 1, p. 35099, Oct. 2025, doi: 10.1038/s41598-025-18918-7.

[10] M. M. Aslam *et al.*, "Intelligent Transportation Systems: A Critical Review of Integration of Cyber-physical Systems (CPS) and Industry 4.0," *Digit. Commun. Netw.*, July 2025, doi: 10.1016/j.dcan.2025.06.014.

[11] K. Ozbay, X. (Jeff) Ban, and C. Y. D. Yang, "Developments in connected and automated vehicles," *J. Intell. Transp. Syst.*, vol. 22, no. 3, pp. 187–189, May 2018, doi: 10.1080/15472450.2018.1466407.

[12] S. Khalid Khan, N. Shiwakoti, and P. Stasinopoulos, "A conceptual system dynamics model for cybersecurity assessment of connected and autonomous vehicles," *Accid. Anal. Prev.*, vol. 165, p. 106515, Feb. 2022, doi: 10.1016/j.aap.2021.106515.

[13] S. K. Khan, N. Shiwakoti, P. Stasinopoulos, and Y. Chen, "Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions," *Accid. Anal. Prev.*, vol. 148, p. 105837, Dec. 2020, doi: 10.1016/j.aap.2020.105837.

[14] R. S. Rathore *et al.*, "In-Vehicle Communication Cyber Security: Challenges and Solutions," *Sensors*, vol. 22, no. 17, Sept. 2022, doi: 10.3390/s22176679.

[15] A. Pollini *et al.*, "Leveraging human factors in cybersecurity: an integrated methodological approach," *Cogn. Technol. Work Online*, vol. 24, no. 2, pp. 371–390, 2022, doi: 10.1007/s10111-021-00683-y.

[16] R. Kelemen *et al.*, "Cybersecurity Regulations and Software Resilience: Strengthening Awareness and Societal Stability," *Soc. Sci.*, vol. 14, no. 10, Sept. 2025, doi: 10.3390/socsci14100578.

[17] D. Pamučar *et al.*, "Application of Improved Best Worst Method (BWM) in Real-World Problems," *Mathematics*, vol. 8, no. 8, Aug. 2020, doi: 10.3390/math8081342.

[18] M. Amiri, M. Hashemi-Tabatabaei, M. Ghahremanloo, M. Keshavarz-Ghorabaee, E. Kazimieras Zavadskas, and J. Antucheviciene, "A novel model for multi-criteria assessment based on BWM and possibilistic chance-constrained programming," *Comput. Ind. Eng.*, vol. 156, p. 107287, June 2021, doi: 10.1016/j.cie.2021.107287.

[19] M. K. Akgün and S. Soygüder, "A Hybrid Decision-Making Framework for Evaluating mHealth App Quality: Integrating Fuzzy BWM with the Weighted Heronian Mean," *Int. J. Fuzzy Syst.*, July 2025, doi: 10.1007/s40815-025-02093-y.

[20] N. M. Elfatih *et al.*, "Internet of vehicle's resource management in 5G networks using AI technologies: Current status and trends," *IET Commun.*, vol. 16, no. 5, pp. 400–420, 2022, doi: 10.1049/cmu2.12315.

[21] K. Liu *et al.*, "Nonlinear Effects of Community Built Environment on Car Usage Behavior: A Machine Learning Approach," *Sustainability*, vol. 14, no. 11, May 2022, doi: 10.3390/su14116722.

[22] I. Adnan, T. Umer, A. Arsalan, M. M. Al Dabel, A. K. Bashir, and A. Ansif, "Data driven vehicular heterogeneity based intelligent collision avoidance system for Internet of Vehicles (IoV)," *Digit. Commun. Netw.*, Apr. 2025, doi: 10.1016/j.dcan.2025.03.010.
[23] Q. Zhang, J. Fan, and C. Gao, "CRITID: enhancing CRITIC with advanced independence testing for robust multi-criteria decision-making," *Sci. Rep.*, vol. 14, no. 1, p. 25094, Oct. 2024, doi: 10.1038/s41598-024-75992-z.
[24] J.-C. Wang and T.-Y. Chen, "A compromise decision-support technique with an augmented scoring function within circular intuitionistic fuzzy settings," *Eng. Appl. Artif. Intell.*, vol. 128, p. 107359, Feb. 2024, doi: 10.1016/j.engappai.2023.107359.
[25] H. Eroğlu, "A spatial decision making framework using neutrosophic VIKOR for wind energy investment in Turkey," *Sci. Rep.*, vol. 15, no. 1, p. 33593, Sept. 2025, doi: 10.1038/s41598-025-18799-w.
[26] T. K. Biswas, A. Abbasi, and R. K. Chakrabortty, "A two-stage VIKOR assisted multi-operator differential evolution approach for Influence Maximization in social networks," *Expert Syst. Appl.*, vol. 192, p. 116342, Apr. 2022, doi: 10.1016/j.eswa.2021.116342.
[27] J.-S. Chou, H.-M. Nguyen, J. Zagorskas, and Z. Turskis, "Decision-informed artificial intelligence for optimizing zero-energy building design: Integration of solar orientation and climatic factors," *Energy Convers. Manag.*, vol. 341, p. 120069, Oct. 2025, doi: 10.1016/j.enconman.2025.120069.
[28] D. Chopra, R. Khurana, and D. Virmani, "Swarm Intelligence inRobotics:FromTheory to Practical Implementation," Feb. 28, 2024, *Social Science Research Network, Rochester, NY*: 4742003. doi: 10.2139/ssrn.4742003.
[29] S. Saki and M. Soori, "Artificial intelligence, machine learning and deep learning in advanced transportation systems, a review," *Multimodal Transp.*, vol. 5, no. 1, p. 100242, Mar. 2026, doi: 10.1016/j.multra.2025.100242.
[30] A. Almutairi, A. F. Al Asmari, F. Alanazi, T. Alqubaysi, and A. Armghan, "Deep learning based predictive models for real time accident prevention in autonomous vehicle networks," *Sci. Rep.*, vol. 15, no. 1, p. 20844, July 2025, doi: 10.1038/s41598-025-04867-8.
[31] K. E. Kampourakis, V. Gkioulos, G. Kavallieratos, and J.-C. Lin, "Digital Twin-Enabled Incident Detection and Response: A Systematic Review of Critical Infrastructures Applications," *Int. J. Inf. Secur.*, vol. 24, no. 5, p. 194, Aug. 2025, doi: 10.1007/s10207-025-01113-0.
[32] D. George, S. Pavithra, and J. Das, "Cyber-resilient autonomous vehicles: securing networks and enhancing decision-making with next-gen security measures," *Results Eng.*, vol. 28, p. 107179, Dec. 2025, doi: 10.1016/j.rineng.2025.107179.
[33] S. Ukkusuri *et al.*, "Cybersecurity for Next-Generation Road Transportation: A Review," *ACM J Auton Transp. Syst*, vol. 3, no. 2, p. 9:1-9:42, Dec. 2025, doi: 10.1145/3744352.
[34] M. Ansarinejad *et al.*, "Autonomous Vehicles in Rural Areas: A Review of Challenges, Opportunities, and Solutions," *Appl. Sci.*, vol. 15, no. 8, Apr. 2025, doi: 10.3390/app15084195.
[35] A. Zhasmukhambetova, H. Evdorides, R. J. Davies, A. Zhasmukhambetova, H. Evdorides, and R. J. Davies, "Integrating Risk Assessment and Scheduling in Highway Construction: A Systematic Review of Techniques, Challenges, and Hybrid Methodologies," *Future Transp.*, vol. 5, no. 3, July 2025, doi: 10.3390/futuretransp5030085.
[36] X. Zhang *et al.*, "Machine learning nested MCDM model to enhance decision reliability for transport safety engineering," *Results Eng.*, vol. 29, p. 108543, Mar. 2026, doi: 10.1016/j.rineng.2025.108543.
[37] S. K. Khan, N. Shiwakoti, P. Stasinopoulos, Y. Chen, and M. Warren, "Cybersecurity framework for connected and automated vehicles: A modelling perspective," *Transp. Policy*, vol. 162, pp. 47–64, Mar. 2025, doi: 10.1016/j.tranpol.2024.11.019.
[38] Y. Dong, Y. Yao, X. Chang, J. Mišić, and V. B. Mišić, "Lightweight Certificateless Authentication Scheme With Enhanced Privacy for CAVs," *IEEE Internet Things J.*, vol. 12, no. 24, pp. 52644–52657, Dec. 2025, doi: 10.1109/JIOT.2025.3612990.
[39] S. Panda, E. Panaousis, G. Loukas, and K. Kentrotis, "Privacy Impact Assessment of Cyber Attacks on Connected and Autonomous Vehicles," in *Proceedings of the 18th International Conference on Availability, Reliability and Security*, in ARES '23. New York, NY, USA: Association for Computing Machinery, Aug. 2023, pp. 1–9. doi: 10.1145/3600160.3605073.
[40] S. Tak, S. Choi, S. Tak, and S. Choi, "Safety Monitoring System of CAVs Considering the Trade-Off between Sampling Interval and Data Reliability," *Sensors*, vol. 22, no. 10, May 2022, doi: 10.3390/s22103611.
[41] T. Zhao, Z. Sun, J. Wang, Y. Tang, L. Varga, and M. J. Skibniewski, "Resilience-based transportation system planning optimization through dedicated autonomous vehicle lanes configuration," *Transp. Res. Part E Logist. Transp. Rev.*, vol. 194, p. 103939, Feb. 2025, doi: 10.1016/j.tre.2024.103939.
[42] D. Xu, X. Ma, J. Zheng, T. Gu, Y. Liu, and P. Liu, "A robust DRL-based decision-making framework for CAV in highway mixed traffic," *Expert Syst. Appl.*, vol. 271, p. 126679, May 2025, doi: 10.1016/j.eswa.2025.126679.
[43] X. Chen *et al.*, "Safety-Assured Design and Adaptation of Connected and Autonomous Vehicles," in *Machine Learning and Optimization Techniques for Automotive Cyber-Physical Systems*, V. K. Kukkala and S. Pasricha, Eds., Cham: Springer International Publishing, 2023, pp. 735–757. doi: 10.1007/978-3-031-28016-0_26.
[44] S. K. Khan, N. Shiwakoti, P. Stasinopoulos, and M. Warren, "Cybersecurity regulatory challenges for connected and automated vehicles – State-of-the-art and future directions," *Transp. Policy*, vol. 143, pp. 58–71, Nov. 2023, doi: 10.1016/j.tranpol.2023.09.001.
[45] B. Gokkaya, L. Aniello, and B. Halak, "Software supply chain: A taxonomy of attacks, mitigations and risk assessment strategies," *J. Inf. Secur. Appl.*, vol. 97, p. 104324, Mar. 2026, doi: 10.1016/j.jisa.2025.104324.
[46] X. Zhang *et al.*, "A hybrid machine learning-enhanced MCDM model for transport safety engineering," *Sci. Rep.*, vol. 15, no. 1, p. 36467, Oct. 2025, doi: 10.1038/s41598-025-21297-8.
[47] I. Mutambik, "IoT-Enabled Adaptive Traffic Management: A Multiagent Framework for Urban Mobility Optimisation," *Sensors*, vol. 25, no. 13, July 2025, doi: 10.3390/s25134126.
[48] T.-Y. Lin, K.-C. Hung, J. Jablonsky, and K.-P. Lin, "An Enhanced VIKOR and Its Revisit for the Manufacturing Process Application," *Comput. Mater. Contin.*, vol. 83, no. 2, pp. 1901–1927, 2025, doi: 10.32604/cmc.2025.063543.
[49] M. Li, H. Sun, Y. Huang, and H. Chen, "SVAP: Shapley Value Guided Attribution Prior for Neural Network-Based Autonomous Driving," *IEEE Trans. Veh. Technol.*, vol. 74, no. 11, pp. 16704–16715, Nov. 2025, doi: 10.1109/TVT.2025.3575760.

[50] N. M. Proma, G. Vázquez, S. Shahbeigi, A. Badyal, and V. Hodge, "Probabilistic Safety Verification for an Autonomous Ground Vehicle: A Situation Coverage Grid Approach," July 16, 2025, *arXiv*: arXiv:2507.12158. doi: 10.48550/arXiv.2507.12158.
[51] X. Cheng and C. Chen, "Decision Making with Intuitionistic Fuzzy Best-Worst Method," *Expert Syst. Appl.*, vol. 237, p. 121215, Mar. 2024, doi: 10.1016/j.eswa.2023.121215.
[52] A. Xie and J. Wu, "Critic Weight Calculation Method Based on Quartiles and Improved Distance Correlation Coefficient and its Applications," Jan. 25, 2025, *Social Science Research Network, Rochester, NY*: 5111154. doi: 10.2139/ssrn.5111154.
[53] V. Tynchenko *et al.*, "Adaptive Management of Multi-Scenario Projects in Cybersecurity: Models and Algorithms for Decision-Making," *Big Data Cogn. Comput.*, vol. 8, no. 11, Nov. 2024, doi: 10.3390/bdcc8110150.

Authors' Profiles



Fadoua Tamtam is a researcher affiliated with the Systems Engineering and Decision Support Laboratory at the National School of Applied Sciences in Agadir, Morocco. Her work focuses on organizational agility, fuzzy logic systems, and decision-making frameworks, particularly in the context of healthcare and industrial sectors. She has co-authored several studies that apply fuzzy logic to assess agility and detect anomalies in network security, particularly within Moroccan SMEs. Her research frequently addresses real-world challenges, including the COVID-19 crisis and cybersecurity threats.



Amina Tourabi is a professor at the National School of Applied Sciences in Agadir, Morocco, with a strong academic footprint in innovation management, organizational resilience, and agile systems. Her research spans topics such as workforce agility, digital transformation, and the socio-economic impacts of innovation, often employing fuzzy logic and interpretive structural modeling. Tourabi's work also explores gender dynamics in entrepreneurship and the role of empathy and social responsibility in organizational behavior.

How to cite this paper

Fadoua Tamtam, Amina Tourabi, "Scenario Based Security and Reliability Evaluation of Connected Autonomous Vehicles Using a Hybrid CRITID–Fuzzy BWM–VIKOR Swarm Approach", International Journal of Information Engineering and Electronic Business(IJIEEB), Vol.18, No.3, pp. 124-141, 2026. DOI:10.5815/ijieeb.2026.03.08