Review of the Adoption of an Energy-Efficient Security Mechanism for Neural Networks

Emmanuel U. Usen
Department of Electrical & Electronic Engineering, Pan Atlantic University, Ibeju, Lagos, Nigeria

doi.org/10.64643/IJIRTV12I10-193837-459

Abstract- Neural networks are increasingly embedded in intelligent and connected vehicles to support perception, decision-making, and cooperative functions. While their security is critical for safety, vehicular deployments operate under strict energy and resource constraints. Existing studies broadly address neural network security and energy efficiency in isolation, limiting their practical relevance for vehicle systems. This paper examines how security mechanisms for neural networks can be designed and evaluated with explicit consideration of energy constraints in intelligent and connected vehicles. A Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA)-aligned structured literature review was conducted across major scientific databases, yielding 47 relevant studies. The selected works were analysed using thematic synthesis and classified according to the neural network lifecycle, encompassing model-level, data- and training-level, and deployment-level security mechanisms. Energy implications were assessed based on reported metrics or inferred computational and communication overheads. The review shows that many effective neural network security mechanisms impose substantial energy costs that challenge on-board and edge-based vehicular deployment. Model-level approaches offer energy savings but require robustness-aware design; training-level mechanisms remain computationally intensive; and deployment-level strategies provide practical trade-offs through secure, communication-efficient inference. No single class of mechanisms sufficiently balances security and energy efficiency on its own. The paper then proposes a conceptual framework that integrates security objectives, energy constraints, and vehicular deployment contexts. The framework guides the development of secure, energy-aware neural networks suitable for intelligent and connected vehicle systems by treating energy consumption as a first-order design constraint.

Keywords: Adversarial robustness; Edge-based vehicular computing; Energy-efficient AI; Intelligent and connected vehicles; Neural network security.

I. INTRODUCTION

Neural networks have become a core enabling technology for intelligent and connected vehicles, underpinning key functions such as perception, decision-making, trajectory planning, driver assistance, and cooperative mobility services. Advances in deep learning have significantly improved vehicles' ability to interpret complex sensory data, interact with surrounding infrastructure, and adapt to dynamic traffic environments. As these systems increasingly operate in real-time and safety-critical contexts, neural networks are no longer peripheral components but central decision-making elements within vehicular architectures [1],[2],[4],[57]. Despite these benefits, the growing reliance on neural networks introduces substantial security challenges. Neural models deployed in vehicular environments are vulnerable to a range of attacks, including adversarial manipulation, data poisoning, and model extraction, which can compromise system reliability and safety [6],[7],[27]. These risks are amplified in connected vehicle settings where models interact with external networks, roadside infrastructure, and other vehicles. At the same time, intelligent vehicles operate under strict energy constraints due to limited on-board computational resources, battery capacity, and real-time performance requirements [8],[47],[56].

Existing research on neural network security has largely prioritised robustness and accuracy [2,][9],[33],[35], often overlooking the energy implications of proposed defence mechanisms. Conversely, studies on energy-efficient neural network design tend to focus on model optimisation and inference efficiency without explicitly addressing security threats [16],[17],[19]. This separation has resulted in a fragmented body of knowledge in which security and energy efficiency are treated as independent design objectives. For intelligent and connected vehicles, where both safety assurance and resource efficiency are critical, this lack of integration represents a significant research gap [35],[48],[53].

Against this background, the present study addresses the need for a unified perspective on energy-efficient security mechanisms for neural networks in vehicular applications. The paper aims to systematically examine how security objectives can be achieved while explicitly accounting for energy constraints inherent in intelligent and connected vehicle systems. The scope of the paper is conceptual, focusing on an analytical discussion, a structured classification of existing approaches, and the development of a coherent framework that links security requirements with energy-aware design principles. The paper makes three primary contributions. First, it provides a structured synthesis of security threats relevant to neural networks deployed in intelligent and connected vehicle systems. Second, it critically examines the energy overheads introduced by existing neural network security mechanisms and highlights their implications for resource-constrained vehicular environments. Finally, it proposes a conceptual framework to guide the design and deployment of neural networks that achieve security objectives while remaining energy-efficient in intelligent and connected vehicles.

II. METHODOLOGY

This study employs a PRISMA-aligned structured literature review to ensure transparency, traceability, and analytical rigor in examining energy-efficient security mechanisms for neural networks in intelligent and connected vehicles. The review followed a systematic process of literature identification, screening, eligibility assessment, and synthesis.

2.1 Research Questions

The review was guided by the following research questions:

i. What types of security mechanisms have been proposed for neural networks in intelligent and connected vehicles?

ii. How do these mechanisms impact energy efficiency and computational requirements?

iii. At which stages of the neural network lifecycle (model development, data and training, deployment) are these mechanisms applied, and what are the associated trade-offs?

2.2 Search Strategy

A comprehensive search was conducted across multiple databases, including IEEE Xplore, ACM Digital Library, Scopus, Web of Science, and Google Scholar, to capture peer-reviewed studies on neural network security in vehicular contexts. Search terms combined keywords related to neural network security, energy efficiency, intelligent vehicles, and deployment constraints. Boolean operators and database-specific filters were applied to refine results. A total of 128 records were initially identified.

2.3 Inclusion and Exclusion Criteria

Studies were selected based on specific inclusion and exclusion criteria. Included were works that addressed neural network security mechanisms relevant to intelligent and connected vehicles, particularly those that considered energy or computational efficiency alongside security. Both empirical and theoretical studies applicable to vehicular or other safety-critical systems were considered. Studies were excluded if they focused solely on cloud-based learning without a vehicle deployment context, addressed energy optimization without any security considerations, or lacked sufficient relevance to the research questions. Following an initial screening, eight duplicate records were removed, resulting in 120 unique studies retained for further analysis.

2.4 Study Selection Process

Title and abstract screening excluded 65 studies for irrelevance to neural network security, energy efficiency, or vehicular deployment contexts. The remaining 55 studies underwent full-text assessment based on the eligibility criteria, resulting in 8 further exclusions, producing a final dataset of 47 studies. Figure 1 shows the PRISMA flow diagram illustrating the study identification, screening, and selection process.

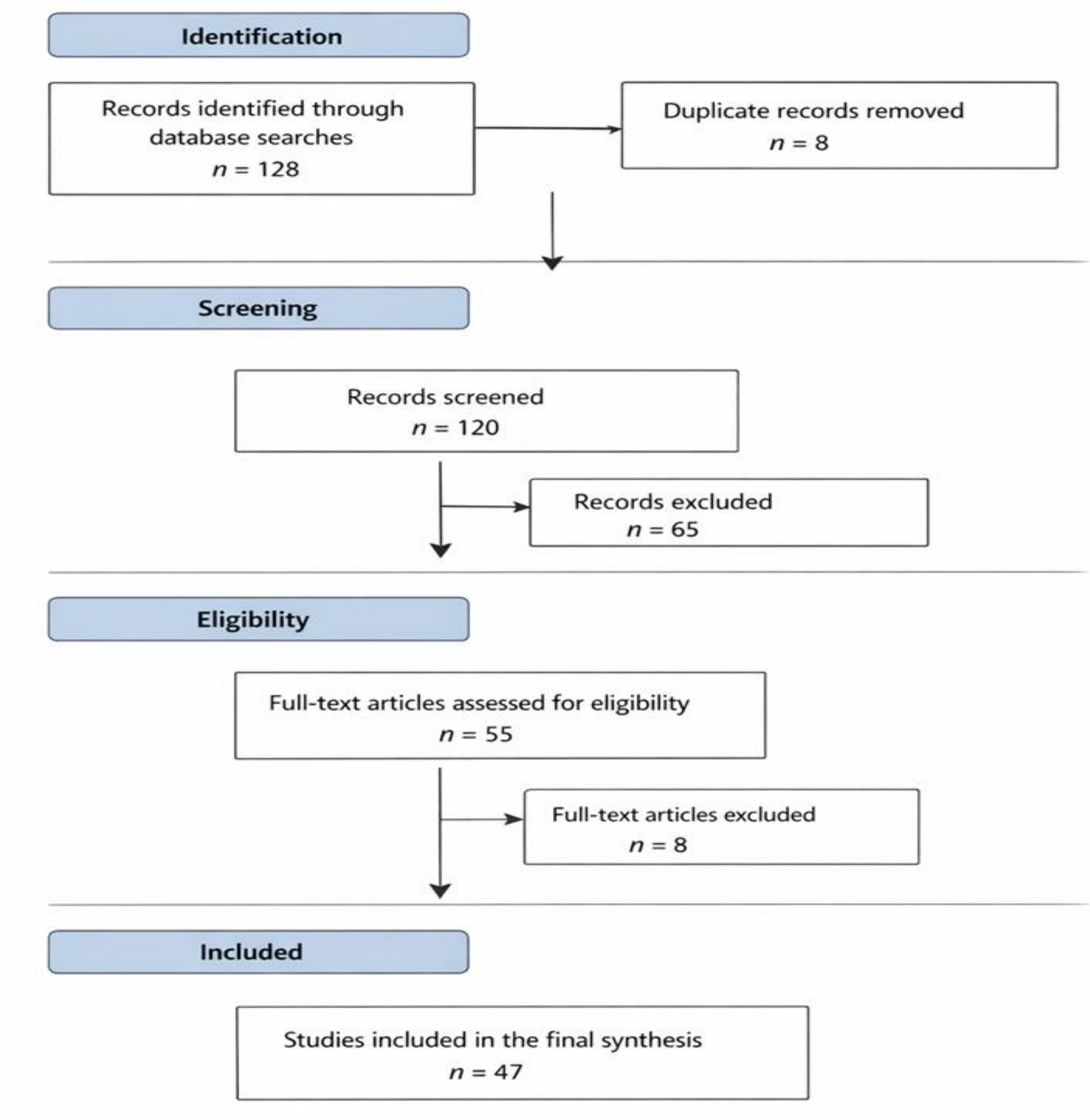
Identification
Records identified through database searches
n = 128
Duplicate records removed
n = 8
Screening
Records screened
n = 120
Records excluded
n = 65
Eligibility
Full-text articles assessed for eligibility
n = 55
Full-text articles excluded
n = 8
Included
Studies included in the final synthesis
n = 47

Figure 1: PRISMA Flow Diagram of Study Selection Process.

2.5 Data Extraction, Analysis, and Synthesis

Key attributes were systematically extracted from each study, focusing on aspects such as security threat models, the neural network lifecycle stages targeted, the nature of the proposed defense mechanisms, and any reported or inferred energy implications. In cases where explicit energy metrics were not provided, the potential energy impact was estimated based on factors like model complexity, training requirements, communication overhead, or dependence on specialized hardware. The collected data were then organized into structured comparison tables to support cross-study analysis. The subsequent analysis applied a thematic synthesis, categorizing security mechanisms according to model-level, data- and training-level, and deployment-level approaches. This framework enabled a detailed examination of energy overheads, robustness trade-offs, and operational feasibility across the various stages of the neural network lifecycle.

2.6 Quality Assessment

Each study was evaluated for both methodological rigor and its relevance to the research questions. Assessment focused on how clearly the security problem was defined, the adequacy of energy or computational evaluations, and the applicability of the approach to vehicular deployment contexts. In addition, the reliability of reported experimental or analytical results was carefully considered. Only studies that met these quality standards were included in the final synthesis.

2.7 Conceptual Framework

Insights from the review informed the development of a conceptual framework integrating security threats, energy constraints, and vehicular deployment contexts. This framework provides a structured basis for evaluating existing mechanisms and guiding future research on secure, energy-aware neural network design.

III. NEURAL NETWORKS AND ENERGY CHALLENGES IN VEHICLES

According to studies by [1],[32],[59], neural networks have been reported to be integral to the operation of intelligent and connected vehicles, providing the computational foundation for perception, decision-making, and control systems. In autonomous driving, convolutional neural networks (CNNs) are widely employed for visual recognition tasks, including object detection, lane detection, and pedestrian recognition, enabling vehicles to navigate complex environments safely and efficiently [7],[13],[40]. Recurrent neural networks (RNNs) and their variants, such as long short-term memory networks (LSTMs), are commonly utilized for temporal data analysis, facilitating the prediction of vehicle trajectories, traffic flow, and driver behaviour [24]. Moreover, graph neural networks and attention-based architectures have emerged in vehicle-to-everything (V2X) systems to model interactions between vehicles, infrastructure, and surrounding environments, thereby enhancing situational awareness and cooperative driving strategies [29]. These applications collectively underpin the advanced functionality of connected and autonomous vehicles, positioning neural networks as indispensable for both safety-critical and performance-critical operations.

Despite their operational significance, neural networks impose significant energy demands, posing substantial challenges in vehicular contexts. On-board deployment, particularly in electric and hybrid vehicles, necessitates careful management of energy consumption to prevent undue drain on vehicle power systems, which can impact both operational range and system longevity [54]. The high computational complexity of deep neural networks results in increased processing requirements, which are often constrained by the limited energy budgets of embedded vehicular hardware, including graphics processing units (GPUs), field-programmable gate arrays (FPGAs), and dedicated neural processing units (NPUs) [9].

Edge and cloud-assisted neural network deployments introduce additional considerations. Offloading computation to edge nodes or cloud servers can reduce on-board processing requirements, yet such strategies incur energy overheads associated with data transmission, communication latency, and network infrastructure [11]. Furthermore, high-bandwidth connectivity is not universally available, leading to variability in energy expenditure and potential performance degradation in areas with limited network coverage. Consequently, energy-efficient design strategies must encompass both local computational optimizations and network-aware considerations, ensuring that security mechanisms integrated with neural networks do not impose prohibitive energy costs.

The interplay among computational complexity, energy efficiency, and vehicular constraints underscores the need for security mechanisms that take energy constraints into account. Without such consideration, robust neural network defenses may inadvertently compromise vehicle operational efficiency, potentially affecting system reliability and user acceptance [5].

IV. SECURITY THREATS TO VEHICULAR NEURAL NETWORKS

The increasing reliance on neural networks to support perception, decision-making, and communication in intelligent and connected vehicles has expanded the system attack surface and introduced new categories of security risk. Unlike conventional software components, neural networks exhibit vulnerabilities arising from both their data-driven training processes and their deployment in highly interconnected, safety-critical vehicular environments. Understanding these threats is essential for assessing the security and energy implications of protective mechanisms.

4.1 Taxonomy of Attacks on Vehicular Neural Networks

Security threats to neural networks can be broadly classified into several categories, each posing distinct challenges in vehicular contexts. Adversarial attacks exploit neural networks' sensitivity to carefully crafted input perturbations, leading to misclassifications or erroneous predictions while remaining imperceptible to human observers. In connected vehicles, such attacks may target perception models responsible for traffic sign recognition, lane detection, or obstacle identification, potentially leading to unsafe control decisions [5],[21].

Data poisoning attacks occur during the training or updating phase of a neural network, where maliciously manipulated data is introduced to corrupt the learned model. This threat is particularly relevant in connected vehicle ecosystems that rely on shared data, federated learning, or over-the-air updates, as attackers may influence training data at the edge or during aggregation [3],[53]. Poisoned models may exhibit degraded performance or targeted misbehaviour under specific conditions.

Another significant category involves inference and model-extraction attacks, in which adversaries attempt to infer sensitive information about the training data or reconstruct model parameters through repeated queries. In vehicular systems, such attacks may compromise proprietary models or reveal sensitive mobility patterns and sensor data, raising both security and privacy concerns [5],[41]. These attacks do not necessarily disrupt immediate functionality but undermine trust, confidentiality, and long-term system integrity. Table 1 summarises the principal categories of attacks targeting neural networks in vehicular environments, highlighting their defining characteristics, affected components, potential impacts on vehicle operation, and the associated energy implications of commonly adopted defence mechanisms.

Table 1. Taxonomy of attacks on vehicular neural networks

Attack type	Description	Targeted neural network component	Potential impact on vehicles	Energy implications of defence	References
Adversarial attacks	Exploit the sensitivity of neural networks to carefully crafted input perturbations that induce misclassification while remaining largely imperceptible.	Input layer, feature extraction layers, perception models	Unsafe perception outcomes, such as incorrect traffic sign recognition, lane detection errors, or obstacle misidentification, potentially lead to hazardous control decisions	Defences often require additional computation during training or inference (e.g., adversarial training, input sanitisation), increasing on-board energy consumption	Guesmi et al., 2023; Alobaid et al., 2025
Data poisoning attacks	Introduce malicious or manipulated data during training or model updating to	Training data pipeline, model parameters	Degraded model accuracy or targeted mis-behaviour under specific conditions, undermining the reliability of	Mitigation techniques such as data validation, redundancy, or robust aggregation add energy and	Sun et al., 2022; Aljanabi et al., 2024

	corrupt learned representations.		vehicular decision-making	communication overhead, particularly in distributed learning settings.	
Inference and model extraction attacks	Infer sensitive training data or reconstruct model parameters through repeated queries or side-channel observations.	Output layer, decision boundaries, model responses	Compromise of proprietary models, leakage of sensitive mobility or sensor data, and erosion of trust in connected vehicle systems	Defences such as query limiting, noise injection, or secure enclaves may increase inference latency and energy usage	Alobaid et al., 2025; Mohamed, 2025

4.2 Attack Surfaces in Connected Vehicle Systems

The connected nature of modern vehicular systems amplifies neural network vulnerabilities by exposing multiple attack surfaces across sensing, communication, and computation layers. On-board sensors, including cameras, lidar, and radar, represent a primary entry point for adversarial manipulation, as neural networks often rely directly on raw or lightly processed sensor data. Communication interfaces used for vehicle-to-vehicle and vehicle-to-infrastructure interactions further extend the attack surface, enabling remote or distributed attacks that may affect multiple vehicles simultaneously [12],[14].

Edge and cloud-assisted computation introduce additional risks, particularly when neural network models or updates are transmitted over wireless channels or executed on shared infrastructure. In such settings, attackers may exploit insecure communication protocols, compromised roadside units, or insufficiently protected update mechanisms to inject malicious inputs or extract model information [46]. The heterogeneity of hardware platforms and software stacks in connected vehicle ecosystems further complicates threat mitigation, as uniform security guarantees are difficult to enforce.

4.3 Safety and Reliability Implications

The consequences of successful attacks on vehicular neural networks extend beyond conventional cybersecurity concerns and directly affect system safety and operational reliability. Erroneous perceptions or decisions induced by adversarial manipulation may lead to incorrect vehicle responses, increasing the risk of collisions or traffic disruptions. Even subtle degradations in model performance can have disproportionate effects in time-critical driving scenarios, where decisions must be made within strict latency constraints.

From a reliability perspective, compromised neural networks undermine the predictability and robustness required for large-scale deployment of intelligent and connected vehicles. Persistent or undetected attacks may erode user trust and hinder regulatory acceptance, particularly if failures cannot be easily explained or traced. Moreover, many existing security countermeasures introduce computational overhead that increases energy consumption, conflicting with the limited power budgets and reliability requirements of vehicular and edge-based systems [50]. Consequently, securing vehicular neural networks requires approaches that account for both adversarial threats and operational constraints inherent in intelligent and connected vehicles.

V. ENERGY-EFFICIENT SECURITY MECHANISMS: REVIEW AND CLASSIFICATION

Security mechanisms for neural networks deployed in intelligent and connected vehicles must address two tightly coupled constraints: robustness against adversarial threats and strict resource constraints. Conventional security solutions for neural networks often prioritise robustness or accuracy without sufficient consideration of energy overhead, rendering them impractical for vehicular and edge-based deployments. This section reviews and classifies existing energy-efficient security mechanisms across three analytical levels: model-level, data- and training-level, and deployment-level approaches. The classification highlights how security objectives can be aligned with energy efficiency requirements in vehicle-centric environments.

5.1 Model-Level Approaches

Model-level approaches focus on modifying neural network structure or representation to reduce computational complexity while maintaining acceptable security properties. Lightweight neural network architectures are widely adopted in vehicular systems to enable real-time inference under power constraints. Architectures such as compact convolutional networks and depth-efficient models reduce parameter counts and arithmetic operations, thereby lowering energy consumption during both training and inference [37],[42]. From a security perspective, such architectures also reduce the attack surface for model extraction and inversion attacks, though overly simplified models may become more susceptible to adversarial manipulation if robustness is not explicitly addressed.

Pruning-aware security mechanisms extend this principle by removing redundant or low-importance parameters while preserving the network's defensive capabilities. Structured pruning techniques, when integrated with robustness constraints, can reduce energy usage without significantly degrading resistance to adversarial inputs [30],[37]. In vehicular applications, pruning-aware defences are particularly relevant because they allow security enhancements to coexist with strict latency and power budgets.

Quantisation-compatible security mechanisms further improve energy efficiency by reducing numerical precision during computation. Quantised neural networks consume less power and memory, making them suitable for embedded vehicle hardware. However, naively applying security mechanisms to quantised models can introduce instability or weaken robustness guarantees. Recent studies have therefore explored security-aware quantisation strategies that preserve defensive properties while reducing energy consumption [13],[39],[43]. Such approaches are increasingly relevant for intelligent vehicles, where inference is often performed on specialised low-power accelerators.

5.2 Data and Training Level Approaches

Data- and training-level approaches aim to enhance robustness during the learning phase while minimising the energy cost of defensive training procedures. Adversarial training remains one of the most effective strategies for improving neural network security, but it is computationally intensive and energy-demanding, particularly for large-scale models [22]. This limitation poses challenges for vehicular systems, where retraining or continual learning may be required under constrained resources.

Energy-aware adversarial robustness strategies seek to mitigate this overhead by reducing the frequency, complexity, or scope of adversarial perturbations used during training. Techniques such as selective adversarial training, curriculum-based robustness learning, and lightweight adversarial example generation have been proposed to balance robustness with computational efficiency [58]. These methods aim to achieve acceptable security guarantees while lowering energy consumption, making them more suitable for vehicle-related applications.

Additionally, data-efficient learning strategies, including transfer learning and federated learning, can indirectly support energy-efficient security. By leveraging pre-trained models or distributed learning paradigms, vehicular systems can reduce local training effort and energy expenditure while still incorporating security-aware updates. However, these approaches introduce new security concerns, such as poisoned updates or communication-based attacks, which must be addressed within an energy-aware framework.

5.3 Deployment-Level Approaches

Deployment-level approaches address security and energy efficiency during inference and real-time operation. In intelligent and connected vehicles, neural networks are often deployed at the edge, either on board the vehicle or within nearby roadside infrastructure. Secure and energy-efficient inference mechanisms, therefore, play a critical role in ensuring reliable operation.

Techniques such as secure inference protocols, model partitioning, and hardware-assisted security aim to protect neural network execution while minimizing power consumption. Trusted execution environments and lightweight cryptographic protections can safeguard inference processes without incurring the high overhead associated with full homomorphic encryption or complex secure multiparty computation [26]. These approaches are particularly relevant for latency-sensitive vehicular applications, where excessive energy use directly affects system viability.

Communication-efficient deployment strategies further reduce energy consumption by limiting data exchange among vehicles, edge nodes, and cloud services. By reducing redundant transmissions and localising security-critical computations, these mechanisms lower both communication energy costs and exposure to network-based attacks [49]. Such strategies align closely with the operational requirements of connected vehicle ecosystems. Figure 2 presents a classification of energy-efficient security mechanisms for neural networks in intelligent and connected vehicles, illustrating the different approaches and their application across the model development, training, and deployment stages.

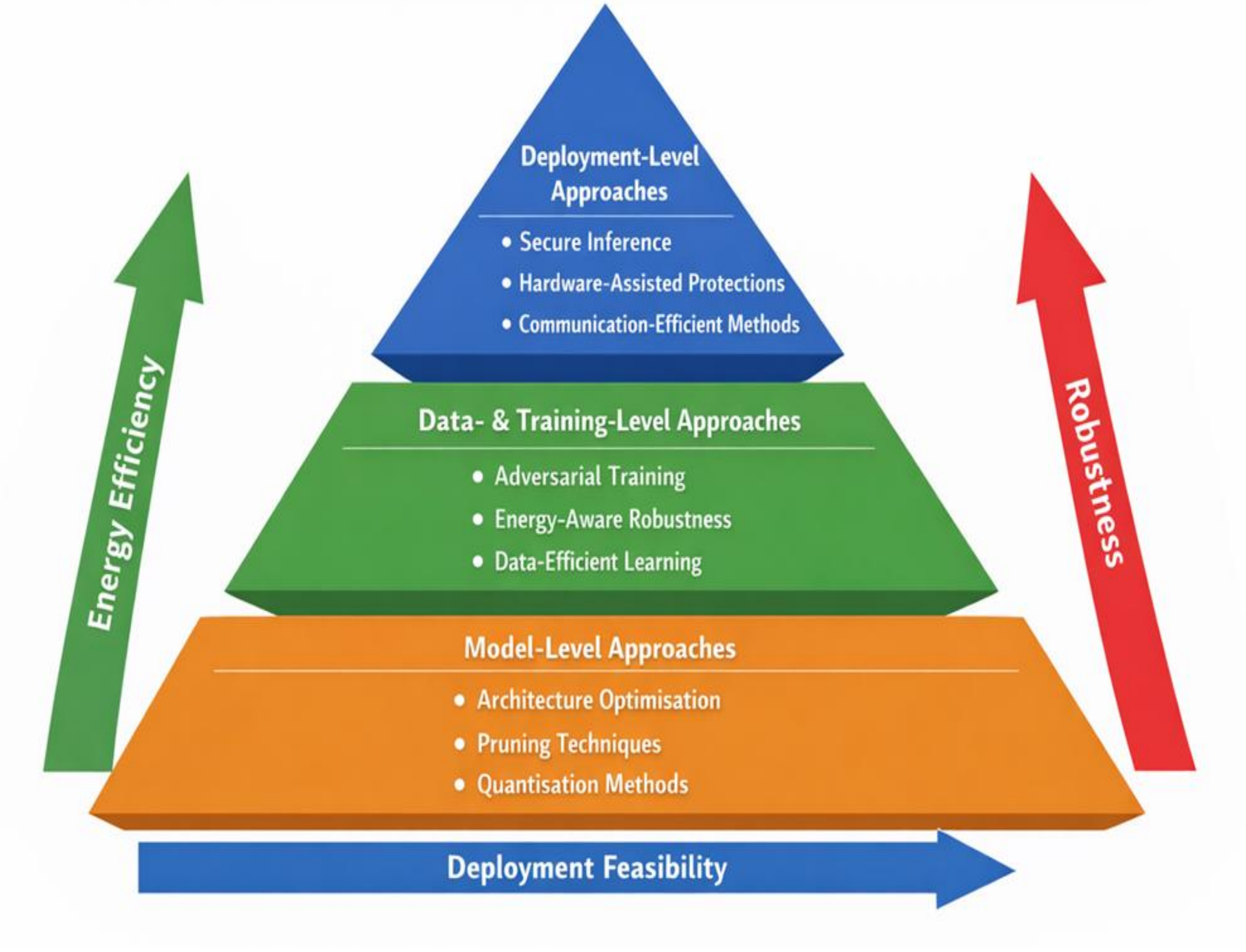
Deployment-Level Approaches
• Secure Inference
• Hardware-Assisted Protections
• Communication-Efficient Methods
Data- & Training-Level Approaches
• Adversarial Training
• Energy-Aware Robustness
• Data-Efficient Learning
Model-Level Approaches
• Architecture Optimisation
• Pruning Techniques
• Quantisation Methods
Energy Efficiency
Robustness
Deployment Feasibility

Figure 2: Classification of Energy-Efficient Security Mechanisms for Neural Networks in Intelligent and Connected Vehicles.

The figure illustrates the three levels of approaches: model-level, data- and training-level, and deployment-level, showing representative techniques for each. Model-level approaches focus on architecture optimization, pruning, and quantisation to reduce computational load. Data- and training-level approaches include adversarial training, energy-aware robustness strategies, and data-efficient learning methods. Deployment-level approaches cover secure inference, hardware-assisted protections, and communication-efficient strategies. The figure highlights the trade-offs among energy efficiency, robustness, and deployment feasibility, showing how each contributes to securing vehicular neural networks under resource constraints.

5.4 Comparative Discussion: Applicability to Intelligent and Connected Vehicles

A comparative assessment of energy-efficient security mechanisms shows that no single approach fully addresses the operational constraints of intelligent and connected vehicle systems. Table 2 summarises these mechanisms across model-, training-, and deployment-level approaches, each targeting distinct stages of the system lifecycle. Model-level strategies reduce network complexity and computational demand, offering immediate energy savings for on-board intelligence, though they require robustness-aware design to avoid increased vulnerability to adversarial manipulation. Data- and training-level approaches strengthen robustness at the foundational level during learning. Still, their adoption is limited by the time and energy costs of training and by sensitivity to threat assumptions in dynamic environments. Deployment-level mechanisms secure inference and communication during real-time operation, particularly in edge-based contexts, maintaining system responsiveness without excessive energy overhead.

Together, these insights highlight the need for an integrated, cross-layer security perspective. By combining complementary strategies across all three levels, it is possible to achieve energy-efficient neural network security that meets the robustness, efficiency, and operational demands of future intelligent and connected vehicles.

Table 2: Conceptual synthesis of energy-efficient security mechanisms for neural networks in intelligent and connected vehicles

Level of approach	Primary objective	Typical techniques	Energy efficiency implications	Security implications	Relevance to intelligent and connected vehicles	References
Model-level	Reduce computational and structural complexity while maintaining robustness.	Lightweight architectures, pruning-aware defences, quantisation-compatible security	Lower inference and memory energy consumption through reduced parameters and precision	Smaller attack surface, but potential vulnerability if robustness is not explicitly preserved	Highly suitable for on-board and embedded vehicular systems with strict power and latency constraints	Liu and Xu, 2025; Musa et al., 2025; Kandasamy and Roseline, 2025; He et al., 2024; Marwan et al., 2024; Navaz et al., 2025
Data- and training-level	Enhance robustness during learning with minimal training overhead	Energy-aware adversarial training, selective robustness strategies, and transfer learning	Reduced training-time energy consumption compared to complete adversarial training	Improved resistance to adversarial manipulation, dependent on threat model assumptions	Relevant for periodic updates, cooperative learning, and adaptive vehicular intelligence	Guo et al., 2024; Yan et al., 2024
Deployment-level	Secure inference and	Secure inference protocols,	Energy savings through	Protection against	Critical for edge-based	Hua et al., 2022; Sha et

	communication under real-time constraints	hardware-assisted security, and communication-efficient strategies	localised computation and reduced communication overhead	inference-time and network-based attacks	vehicular deployment and vehicle-to-infrastructure interactions	al., 2025
Integrated perspective	Balance security, energy efficiency, and operational feasibility	Cross-layer security design combining model, training, and deployment strategies	Optimised energy use across the lifecycle of neural network deployment	Holistic security coverage across multiple attack surfaces	Most appropriate for safety-critical, dynamically connected vehicle environments	Liu and Xu, 2025; Guo et al., 2024; Hua et al., 2022

VI. RESULTS AND DISCUSSION

The structured review yielded 47 primary studies addressing energy-efficient security mechanisms for neural networks deployed in intelligent and connected vehicle environments. The analyzed works span model-level, data- and training-level, and deployment-level strategies, allowing comparative assessment of how energy efficiency and security are jointly addressed across the neural network lifecycle.

6.1 Model-Level Mechanisms

At the model level, the results show a strong convergence toward lightweight architectures, pruning-aware defenses, and quantisation-compatible security mechanisms as dominant approaches for reducing energy consumption while preserving robustness. Lightweight convolutional and depth-efficient architectures consistently demonstrated reductions in parameter count and inference energy without substantial loss of predictive accuracy [37],[42],[60]. These findings reinforce established evidence that architectural efficiency is a primary driver of energy savings in embedded vehicular platforms.

Pruning-aware security mechanisms further contributed to energy reduction by eliminating redundant parameters while maintaining defensive performance against adversarial threats [28],[31]. Unlike naive pruning, these approaches explicitly account for robustness during parameter removal, addressing concerns raised in prior studies regarding the vulnerability of aggressively simplified models. Similarly, quantisation-aware security techniques were shown to improve computational efficiency on vehicle-grade hardware while preserving robustness properties when properly integrated into the defense design [13],[39],[43].

These observations align with broader literature on model compression and low-power deep learning, which emphasizes the inherent trade-off between efficiency and security [31],[34],[45]. Several studies caution that excessive simplification can inadvertently increase susceptibility to adversarial manipulation unless robustness constraints are explicitly embedded in the compression process [17],[55]. The reviewed evidence supports this view, suggesting that energy-efficient model design must be security-aware rather than purely performance-driven.

6.2 Data- and Training-Level Mechanisms

At the data and training level, adversarial training remains the most widely adopted robustness enhancement technique. However, the review confirms that its high computational and energy demands pose significant challenges for vehicular deployment [22]. In response, several studies propose energy-aware adversarial training variants, including selective perturbation strategies and curriculum-based robustness learning. These approaches reduce training overhead while maintaining acceptable security guarantees [58], indicating that robustness need not come at prohibitive energy cost when adaptively applied.

Data-efficient learning paradigms, particularly transfer learning and federated learning, were also shown to reduce local training energy consumption by leveraging shared or pre-trained knowledge [3],[53]. However, the results highlight new security risks introduced by these methods, such as poisoned model updates and communication-based attacks. This finding reinforces prior concerns that energy-efficient collaborative learning mechanisms require additional safeguards to ensure integrity and trustworthiness.

These results corroborate existing research emphasizing the need to balance robustness and efficiency during training [2],[48]. The reviewed studies collectively suggest that adaptive, selective, or context-aware training strategies offer a practical pathway toward energy-efficient security in vehicular neural networks.

6.3 Deployment-Level Mechanisms

At the deployment level, the reviewed studies emphasize the importance of secure inference, hardware-assisted protection, and communication-efficient strategies for real-time edge operation. Trusted execution environments and lightweight cryptographic protocols were frequently employed to provide runtime security without incurring excessive energy or latency overhead [26],[49]. Additionally, minimizing communication frequency and payload size was shown to significantly reduce energy costs associated with vehicle-to-vehicle and vehicle-to-infrastructure interactions.

These findings are consistent with prior work on edge-based neural network deployment, which stresses that security mechanisms must be computationally lightweight and latency-aware to meet vehicular real-time constraints [9],[12]. The reviewed evidence indicates that deployment-level optimizations play a critical role in sustaining energy-efficient security beyond model and training design.

6.4 Cross-Layer Implications

An integrated analysis across all levels reveals that no single mechanism sufficiently addresses both energy efficiency and security in isolation. Instead, the most effective solutions adopt cross-layer strategies that combine optimized model design, energy-aware training, and secure, lightweight deployment mechanisms. Such holistic approaches consistently achieve better trade-offs between robustness, energy consumption, and latency.

This conclusion aligns with earlier observations by [47],[48], who argue that energy-conscious, system-level design is essential for safety-critical and connected vehicle applications. The results of this review reinforce the need for coordinated design choices across the neural network lifecycle.

While the reviewed literature demonstrates that energy-efficient security for vehicular neural networks is achievable, several gaps persist. These include the lack of standardized metrics for evaluating energy-security trade-offs, limited end-to-end threat modeling across the neural network lifecycle, and insufficient consideration of heterogeneous vehicle hardware and networking environments. Addressing these challenges is critical for translating current research advances into deployable, robust, and energy-aware neural network systems for connected and autonomous vehicles.

VII. CONCEPTUAL FRAMEWORK FOR ENERGY-EFFICIENT SECURITY

The conceptual framework presented in Figure 3 offers a structured view of energy-efficient security for neural networks in intelligent and connected vehicles. It encompasses three interconnected layers—model-level, data- and training-level, and deployment-level—that illustrate the interplay among security objectives, energy constraints, and operational contexts. By mapping security threats, energy implications, and feedback loops across these layers, the framework provides a comprehensive perspective on the trade-offs involved in designing robust yet energy-efficient vehicular neural networks. Central to this approach is recognizing energy consumption as a primary constraint, guiding the selection and deployment of security mechanisms while ensuring reliability and responsiveness in real-world driving conditions.

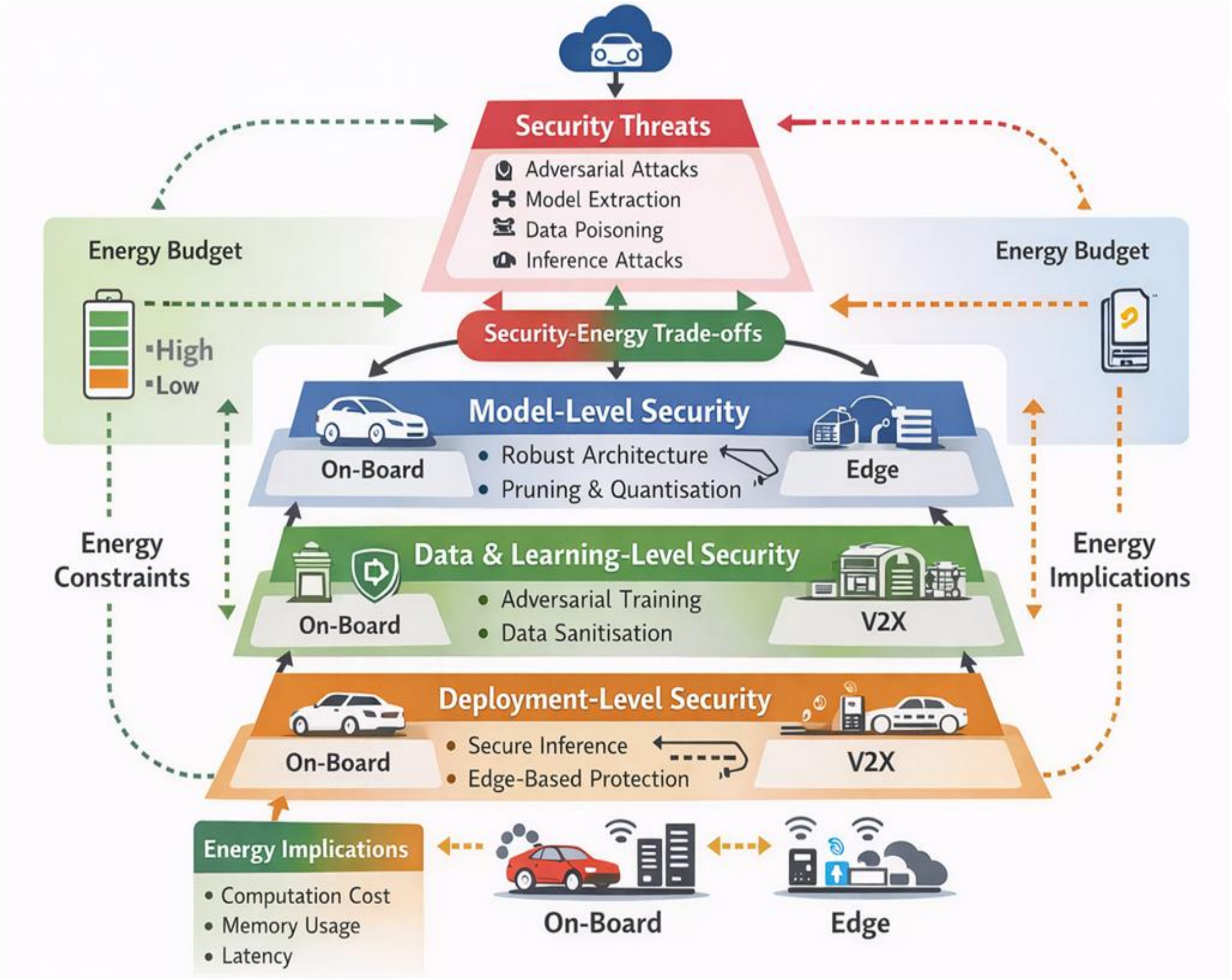

Figure 3: Conceptual Framework for Energy-Efficient Security in Intelligent & Connected Vehicles.

7.1 Integrating Security Objectives and Energy Constraints

Neural networks deployed in intelligent and connected vehicles operate under stringent energy, latency, and reliability requirements. Unlike cloud-based systems, vehicular platforms rely on embedded processors, edge devices, and battery-dependent power sources, making energy efficiency a critical design consideration. At the same time, these systems face diverse security threats, including adversarial manipulation of inputs, model extraction, data poisoning, and inference attacks, which can compromise safety-critical decision-making processes [10],[44].

The proposed framework conceptualises security and energy efficiency as interdependent dimensions rather than competing objectives. The framework, therefore, positions energy consumption as a first-order constraint that shapes the selection, design, and deployment of security mechanisms.

At the core of the framework is a layered perspective comprising three interrelated components: the neural network model, the data and learning process, and the deployment environment. Each layer is associated with specific security objectives and energy implications. By analysing these layers jointly, the framework enables a holistic assessment of how security measures affect overall system efficiency and operational feasibility in intelligent and connected vehicles.

7.2 Design Principles for Energy-Efficient Neural Network Security

Based on this integrated perspective, several design principles emerge to guide the development of energy-efficient security mechanisms.

First, proportional security is emphasised, whereby the level of protection is aligned with the criticality of the vehicular function and the severity of the threat model. Safety-critical tasks such as perception and control may justify higher security overheads, whereas auxiliary functions may require lighter-weight protections to conserve energy. This principle reflects the need to balance risk mitigation with resource constraints in heterogeneous vehicular systems [38].

Second, security mechanisms should be architecture-aware. Neural network architectures designed for vehicular applications increasingly favour compact and efficient models, such as lightweight convolutional or compressed deep learning architectures. Security techniques that are compatible with such models, including pruning-aware defences or quantisation-friendly protections, are more likely to achieve acceptable energy-performance trade-offs [51].

Third, energy-aware deployment is central to the framework. Security mechanisms should account for where neural network inference and decision-making occur, whether on-board the vehicle, at the roadside edge, or within cooperative vehicular networks. Distributing security functions across these layers can reduce local energy consumption while maintaining acceptable levels of robustness, provided that communication and latency costs are carefully managed [20].

Finally, adaptability is a key principle. Intelligent and connected vehicles operate in dynamic environments with varying threat levels and energy availability. The framework, therefore, supports adaptive security strategies that adjust protection mechanisms in response to contextual factors, such as driving conditions, connectivity status, and remaining energy resources.

7.3 Mapping the Framework to Vehicular Applications

The proposed conceptual framework is directly applicable to a range of neural-network-driven vehicular applications. In perception systems, for example, energy-efficient security mechanisms can be integrated into lightweight vision models to mitigate adversarial input manipulation without significantly increasing inference cost. In cooperative driving and vehicle-to-everything (V2X) scenarios, the framework supports the allocation of security functions between vehicles and edge infrastructure, reducing on-board energy expenditure while preserving trust in shared information.

More broadly, the framework provides a structured basis for evaluating existing security approaches and guiding future theoretical and empirical research. By explicitly linking security objectives to energy constraints and deployment contexts, it addresses a critical gap in the literature on neural network security for intelligent and connected vehicles. This integrative perspective is particularly relevant as vehicular systems continue to incorporate increasingly complex learning-based components under strict efficiency and sustainability requirements [23].

Thus, the conceptual framework advances understanding of how to jointly address energy efficiency and security in neural networks for intelligent and connected vehicles. It offers a coherent foundation for the design of practical, scalable, and context-aware security mechanisms that align with the operational realities of modern vehicular systems.

VIII. IMPLICATIONS AND FUTURE DIRECTIONS

8.1 Deployment considerations, scalability, and regulatory aspects

The deployment of energy-efficient security mechanisms for neural networks in real-world systems raises practical considerations that extend beyond algorithmic design. In intelligent and connected vehicle ecosystems, neural networks are increasingly embedded in resource-constrained environments, including on-board electronic control units, edge devices, and roadside infrastructure.

Scalability represents a further challenge. As neural networks are deployed across fleets of vehicles and interconnected infrastructures, security mechanisms must scale across heterogeneous hardware platforms and varying operating conditions. Energy-efficient designs that rely on adaptive or modular security components offer advantages in this regard, enabling selective activation of protection mechanisms based on contextual risk or available resources. However, achieving consistent security guarantees at scale remains complex, especially in distributed and cooperative vehicular settings where models may be updated, shared, or partially executed across multiple nodes.

Regulatory and standardisation considerations also play a critical role in shaping deployment pathways. Intelligent and connected vehicles operate within tightly regulated environments, where safety, data protection, and cybersecurity requirements are increasingly formalised through national and international standards. Emerging regulatory frameworks emphasise robustness, explainability, and resilience of AI systems, which may impose additional constraints on security mechanisms for neural networks. Energy-efficient security approaches must therefore be designed with compliance in mind, ensuring that reductions in computational or energy overhead do not compromise transparency, auditability, or safety certification processes. Alignment with evolving standards for automotive cybersecurity and AI governance is likely a prerequisite for widespread adoption.

8.2 Research gaps and opportunities for theoretical or interdisciplinary development

Despite growing interest in secure and efficient neural network design, several research gaps remain. A central limitation of existing work lies in the fragmented treatment of security and energy efficiency as largely independent objectives. There is a need for more unified theoretical frameworks that explicitly model the trade-offs between robustness, performance, and energy consumption, particularly in safety-critical domains such as intelligent transportation systems. Formalising these trade-offs could support principled design choices and enable more precise comparison between competing security strategies.

Opportunities also exist for interdisciplinary research that bridges computer science, electrical engineering, and transportation studies. Insights from low-power hardware design, vehicular systems engineering, and control theory may inform the development of security mechanisms that are better aligned with real-world deployment constraints. Similarly, collaboration with legal and policy scholars could support integrating regulatory requirements into the early stages of system design, reducing the risk of misalignment between technical innovation and governance expectations.

Finally, future research would benefit from greater attention to long-term adaptability. As attack strategies evolve and vehicular systems become increasingly autonomous and interconnected, static security solutions are unlikely to remain effective. Energy-efficient mechanisms that support continual learning, adaptive defence, or risk-aware operation represent a promising direction, but remain underexplored in the current literature. Addressing these challenges will be essential for ensuring that neural networks can be deployed securely and sustainably within next-generation intelligent and connected vehicle systems.

IX. CONCLUSION

This study examined how security mechanisms for neural networks in intelligent and connected vehicles can be designed with explicit consideration of energy constraints. The findings demonstrate that security and energy efficiency are inseparable design considerations in vehicular environments, where neural networks operate under strict power, latency, and reliability requirements. Approaches that emphasise robustness without accounting for energy overhead are unlikely to be viable in real-world deployments, while energy-focused optimisations that overlook security can introduce new vulnerabilities. These results highlight the necessity of balancing protection strength with operational feasibility.

The study shows that energy overheads emerge at multiple stages of the neural network lifecycle and therefore require coordinated responses tailored to each stage by synthesising existing literature. Model-level techniques such as lightweight architectures, pruning, and quantisation can reduce computational demand, but must be developed with robustness awareness to avoid increased susceptibility to adversarial attacks. At the training stage, energy-aware and selective robustness strategies offer more practical alternatives to exhaustive adversarial training in resource-constrained vehicular settings. During deployment, secure inference and communication-efficient mechanisms are essential for protecting real-time operation without imposing excessive energy costs. Collectively, these findings indicate that effective security for vehicular neural networks arises from the careful integration of complementary mechanisms rather than reliance on any single approach.

Accordingly, this study recommends that security mechanisms for vehicular neural networks be selected and combined across model, training, and deployment stages based on their proportional energy costs and contextual risk exposure. It further recommends that energy efficiency be treated as a primary design constraint in the development and deployment of neural network defences for intelligent vehicles.

The study contributes a conceptual framework that unifies security objectives, threat models, and energy considerations within a single analytical perspective. By embedding energy efficiency directly into the evaluation of security mechanisms, the framework offers a structured basis for decision-making in intelligent and connected vehicle systems, where neural networks support safety-critical perception, control, and coordination functions.

At the same time, the analysis reveals important limitations in the existing body of research. Energy consumption is not consistently measured or reported, and many proposed security mechanisms lack validation on realistic vehicular hardware and workloads. These gaps restrict the ability to assess practical trade-offs and deployment readiness. Future research should therefore prioritise empirical benchmarking that jointly evaluates robustness, energy use, and latency, as well as the development of adaptive security mechanisms capable of responding to dynamic operational and threat conditions.

Thus, this study advances understanding of energy-efficient neural network security in intelligent and connected vehicles by clarifying key trade-offs and providing a coherent framework for reasoning about them. By aligning security design with energy-aware principles, it lays a foundation for neural network systems that are not only robust but also practical and sustainable for next-generation vehicular applications.

REFERENCES

[1] Abiodun, O.I., Jantan, A., Omolara, A.E., Dada, K.V., Mohamed, N.A. and Arshad, H. (2018), “State-of-the-art in artificial neural network applications: A survey”, *Heliyon*, Elsevier, Vol. 4 No. 11, p. e00938.

[2] Al Hwaitat, A.K. and Fakhouri, H.N. (2024), “Adaptive Cybersecurity Neural Networks: An Evolutionary Approach for Enhanced Attack Detection and Classification”, *Applied Sciences*, Multidisciplinary Digital Publishing Institute (MDPI), Vol. 14 No. 19, p. 9142.

[3] Aljanabi, M., Omran, A.H., Mijwil, M.M., Abotaleb, M., El-Kenawy, E.-S.M., Mohammed, S.Y. and Ibrahim, A. (2024), “Data poisoning: issues, challenges, and needs”, *IET Conference Proceedings*, Institution of Engineering and Technology, Vol. 2023 No. 44, pp. 359–363.

[4] Aljehane, N.O. (2024). A Study to Investigate the Role and Challenges Associated with the Use of Deep Learning in Autonomous Vehicles. *World Electric Vehicle Journal*, 15(11), p.518. doi:https://doi.org/10.3390/wevj15110518.

[5] Alobaid, A., Bonny, T. and Alrahhal, M. (2025), “Disruptive attacks on artificial neural networks: A systematic review of attack techniques, detection methods, and protection strategies”, *Intelligent Systems with Applications*, Elsevier, Vol. 26, p. 200529.

[6] Aloraini, F., Javed, A. and Rana, O. (2024), “Adversarial Attacks on Intrusion Detection Systems in In-Vehicle Networks of Connected and Autonomous Vehicles.”, *Sensors (Basel, Switzerland)*, Multidisciplinary Digital Publishing Institute (MDPI), Vol. 24 No. 12, p. 3848.

[7] Álvarez-Silva, S., Mujica Vargas, D. and Arenas Muñiz, A.A. (2025), “Lane Detection Using Computer Vision and Convolutional Neural

Networks for Autonomous Vehicles”, *International Journal of Combinatorial Optimization Problems and Informatics*, Int Journal Combinatorial Optimization Problems & Informatics, Vol. 16 No. 3, pp. 170–194.

[8] Carlini, N. and Wagner, D. (2017), “Towards Evaluating the Robustness of Neural Networks”, institute of electrical electronics engineers, pp. 39–57.

[9] Cheshfar, M., Maghami, M.H., Amiri, P., Garakani, H.G. and Lavagno, L. (2024), “Comparative Survey of Embedded System Implementations of Convolutional Neural Networks in Autonomous Cars Applications”, *IEEE Access*, IEEE, Vol. 12, pp. 182410–182437.

[10] Daghero, F., Poncino, M. and Pagliari, D.J. (2020), “Energy-efficient deep learning inference on edge devices”, Elsevier, pp. 247–301.

[11] Eang, C., Ros, S., Kang, S., Song, I., Tam, P., Math, S. and Kim, S. (2024), “Offloading Decision and Resource Allocation in Mobile Edge Computing for Cost and Latency Efficiencies in Real-Time IoT”, *Electronics*, Multidisciplinary Digital Publishing Institute (MDPI), Vol. 13 No. 7, p. 1218.

[12] Escapa Gordón, P., Matellán Olivera, V. and Suárez Corona, A. (2025), “Vehicle-to-Vehicle Secure Communication Protocol Based on Digital Vehicle Identification Number.”, *Sensors (Basel, Switzerland)*, Multidisciplinary Digital Publishing Institute (MDPI), Vol. 25 No. 19, available at: https://doi.org/10.3390/s25195954.

[13] Farhat, W., Rhaiem, O.B., Faiedh, H. and Souani, C. (2025), “Optimized deep learning for pedestrian safety in autonomous vehicles”, *International Journal of Transportation Science and Technology*, Keai Publishing Ltd, available at: https://doi.org/10.1016/j.ijtst.2025.04.002.

[14] Farsimadan, E., Moradi, L. and Palmieri, F. (2025), “A Review on Security Challenges in V2X Communications Technology for Vanets”, *IEEE Access*, IEEE, Vol. 13, pp. 31069–31094.

[15] Fernández-Llorca, D., Hamon, R., Junklewitz, H., Grosse, K., Kunze, L., Seiniger, P., Swaim, R., *et al.* (2025), “Testing autonomous vehicles and AI: perspectives and challenges from cybersecurity, transparency, robustness and fairness”, *European Transport Research Review*, Springer Nature, Vol. 17 No. 1, available at: https://doi.org/10.1186/s12544-025-00732-x.

[16] Fesu, A., Shone, N., Macdermott, Á., Zhou, B. and Eiza, M. (2025), “Comparative Analysis of SNN and CNN Models for Energy Efficient Intrusion Detection”, institute of electrical electronics engineers, pp. 1–7.

[17] Gao, M. (2022), “An Artificial Neural Network-Based Approach to Optimizing Energy Efficiency in Residential Buildings in Hot Summer and Cold Winter Regions.”, *Computational Intelligence and Neuroscience*, Hindawi London, United Kingdom, Vol. 2022, pp. 1–7.

[18] Gao, P. and Adnan, M. (2025), “Overview of emerging electronics technologies for artificial intelligence: A review”, *Materials Today Electronics*, Elsevier, Vol. 11, p. 100136.

[19] Ghoneim, O., Dobias, P. and Romain, O. (2025), “Survey of neural network optimization methods for sustainable AI: From data preprocessing to hardware acceleration”, *Machine Learning with Applications*, Elsevier, Vol. 22, p. 100762.

[20] Grover, H., Alladi, T., Chamola, V., Singh, D. and Choo, K.-K.R. (2021), “Edge Computing and Deep Learning Enabled Secure Multitier Network for Internet of Vehicles”, *IEEE Internet of Things Journal*, Institute of Electrical Electronics Engineers, Vol. 8, No. 19, pp. 14787–14796.

[21] Guesmi, A., Hanif, M.A. and Shafique, M. (2023), “AdvRain: Adversarial Raindrops to Attack Camera-Based Smart Vision Systems”, *Information*, Multidisciplinary Digital Publishing Institute (MDPI), Vol. 14 No. 12, p. 634.

[22] Guo, R., Chen, Q., Liu, H. and Wang, W. (2024), “Adversarial Robustness Enhancement for Deep Learning-Based Soft Sensors: An Adversarial Training Strategy Using Historical Gradients and Domain Adaptation.”, *Sensors (Basel, Switzerland)*, Multidisciplinary Digital Publishing Institute (MDPI), Vol. 24 No. 12, p. 3909.

[23] Halgamuge, M.N. and Niyato, D. (2024), “Adaptive edge security framework for dynamic IoT security policies in diverse environments”,

Computers & Security, Elsevier, Vol. 148, p. 104128.

[24] He, P., Zhou, Y. and Qin, X. (2024), "A Survey on Energy-Aware Security Mechanisms for the Internet of Things", *Future Internet*, Multidisciplinary Digital Publishing Institute (Mdpi), Vol. 16 No. 4, p. 128.

[25] He, Y., Huang, P., Hong, W., Luo, Q., Li, L. and Tsui, K.-L. (2024), "In-Depth Insights into the Application of Recurrent Neural Networks (RNNs) in Traffic Prediction: A Comprehensive Review", *Algorithms*, Multidisciplinary Digital Publishing Institute (MDPI), Vol. 17 No. 9, p. 398.

[26] Hua, W., Umar, M., Zhang, Z. and Suh, G.E. (2022), "GuardNN", association for computing machinery, pp. 349–354.

[27] Igenewari, L.S. and Okoh E.O. (2025). Adversarial Attacks and Defenses in AI Systems: Challenges, Strategies, and Future Directions. *International Journal of Research and Innovation in Applied Science*, X(VI), pp.996–1022. doi:https://doi.org/10.51584/ijrias.2025.10060075.

[28] Isenkul, M.E. (2025). Energy-aware deep learning for real-time video analysis through pruning, quantization, and hardware optimization. *Journal of Real-Time Image Processing*, 22(3). doi:https://doi.org/10.1007/s11554-025-01703-0.

[29] Ji, M., Wu, Q., Fan, P., Cheng, N., Chen, W., Wang, J. and Letaief, K. (2024), "Graph Neural Networks and Deep Reinforcement Learning Based Resource Allocation for V2X Communications", 9 July, available at: https://doi.org/10.48550/arxiv.2407.06518.

[30] Kandasamy, V. and Roseline, A.A. (2025), "Harnessing advanced hybrid deep learning model for real-time detection and prevention of man-in-the-middle cyber attacks", *Scientific Reports*, Springer Nature, Vol. 15 No. 1, available at: https://doi.org/10.1038/s41598-025-85547-5.

[31] Karathanasis, A., Violos, J. and Kompatsiaris, I. (2025). A Comparative Analysis of Compression and Transfer Learning Techniques in DeepFake Detection Models. *Mathematics*, [online] 13(5), pp.887–887. doi:https://doi.org/10.3390/math13050887.

[32] Khanmohamadi, M. and Guerrieri, M. (2025), "Smart Intersections and Connected Autonomous Vehicles for Sustainable Smart Cities: A Brief Review", *Sustainability*, Multidisciplinary Digital Publishing Institute (MDPI), Vol. 17 No. 7, p. 3254.

[33] Khedher, M.I., Houda, J. and El-Yacoubi, M. (2023). On the Formal Evaluation of the Robustness of Neural Networks and Its Pivotal Relevance for AI-Based Safety-Critical Domains. *International Journal of Network Dynamics and Intelligence*, pp.100018–100018. doi:https://doi.org/10.53941/ijndi.2023.100018.

[34] Kim, G.I., Hwang, S. and Jang, B. (2025). Efficient Compressing and Tuning Methods for Large Language Models: A Systematic Literature Review. *ACM Computing Surveys*, 57(10), pp.1–39. doi:https://doi.org/10.1145/3728636.

[35] Li, B., Hu, W., Da, L., Wu, Y., Wang, X., Li, Y. and Yuan, C. (2024). Over-the-air upgrading for enhancing security of intelligent connected vehicles: a survey. *Artificial Intelligence Review*, 57(11). doi:https://doi.org/10.1007/s10462-024-10968-z.

[36] Lin, R., Zhou, Q., Wu, B. and Nan, X. (2022), "Robustness evaluation for deep neural networks via mutation decision boundaries analysis", *Information Sciences*, Elsevier, Vol. 601, pp. 147–161.

[37] Liu, L. and Xu, Z. (2025), "Optimizing lightweight neural networks for efficient mobile edge computing", *Scientific Reports*, Springer Nature, Vol. 15 No. 1, available at: https://doi.org/10.1038/s41598-025-04652-7.

[38] Luo, F., Hou, S., Zhang, X., Yang, Z. and Pan, W. (2020), "Security Risk Analysis Approach for Safety-Critical Systems of Connected Vehicles", *Electronics*, Multidisciplinary Digital Publishing Institute (MDPI), Vol. 9 No. 8, p. 1242.

[39] Marwan, M., Ait Temghart, A., Ouhmi, S. and Lazaar, M. (2024), "Security, QoS and energy aware optimization of cloud-edge data centers using game theory and homomorphic encryption: Modeling and formal verification", *Results in Engineering*, Elsevier, Vol. 24, p. 102902.

[40] Miller, T., Durlik, I., Kostecka, E., Borkowski, P. and Łobodzińska, A. (2024), "A Critical AI View

on Autonomous Vehicle Navigation: The Growing Danger", *Electronics*, Multidisciplinary Digital Publishing Institute (MDPI), Vol. 13 No. 18, p. 3660.

[41] Mohamed, N. (2025), "Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms", *Knowledge and Information Systems*, Springer Nature, Vol. 67 No. 8, pp. 6969–7055.

[42] Musa, A., Kakudi, H., Hassan, M., Hamada, M., Umar, U. and Salisu, M. (2025), "Lightweight Deep Learning Models For Edge Devices—A Survey", *International Journal of Computer Information Systems and Industrial Management Applications*, Machine Intelligence Research Labs, Vol. 17, p. 18.

[43] Navaz, K., Shanmugasundaram, G. and Regin Bose, K. (2025), "Reducing energy consumption and enhancing security in WSNs using Sea Lion Optimization and ensemble voting", *Sādhanā*, Springer Nature, Vol. 50 No. 4, available at: https://doi.org/10.1007/s12046-025-02938-0.

[44] Ngo, D., Park, H.-C. and Kang, B. (2025), "Edge Intelligence: A Review of Deep Neural Network Inference in Resource-Limited Environments", *Electronics*, Multidisciplinary Digital Publishing Institute (MDPI), Vol. 14 No. 12, p. 2495.

[45] Paula, E., Soni, J., Upadhyay, H. and Lagos, L. (2025). Comparative analysis of model compression techniques for achieving carbon efficient AI. *Scientific Reports*, [online] 15(1). doi:https://doi.org/10.1038/s41598-025-07821-w.

[46] Rupanetti, D. and Kaabouch, N. (2024), "Combining Edge Computing-Assisted Internet of Things Security with Artificial Intelligence: Applications, Challenges, and Opportunities", *Applied Sciences*, Multidisciplinary Digital Publishing Institute (MDPI), Vol. 14 No. 16, p. 7104.

[47] Sarkar, S., Shafaei, S., Jones, T.S. and Totaro, M.W. (2025), "Secure Communication in Drone Networks: A Comprehensive Survey of Lightweight Encryption and Key Management Techniques", *Drones*, Multidisciplinary Digital Publishing Institute (MDPI), Vol. 9 No. 8, p. 583.

[48] Sever, T. and Contissa, G. (2024), "Automated driving regulations – where are we now?", *Transportation Research Interdisciplinary Perspectives*, Elsevier, Vol. 24, p. 101033.

[49] Sha, Z., Li, C., Yue, W. and Yu, J. (2025), "Integrated Sensing, Communication and Computing for Targeted Dissemination: A Service-Aware Strategy for Internet of Vehicles", *IEEE Transactions on Vehicular Technology*, IEEE, Vol. 74 No. 3, pp. 4273–4288.

[50] Sheikh, A.M., Islam, M.R., Habaebi, M.H., Zabidi, S.A., Bin Najeeb, A.R. and Kabbani, A. (2025), "A Survey on Edge Computing (EC) Security Challenges: Classification, Threats, and Mitigation Strategies", *Future Internet*, Multidisciplinary Digital Publishing Institute (MDPI), Vol. 17 No. 4, p. 175.

[51] Sinha, P., Sahu, D., Prakash, S., Rathore, R.S., Dixit, P., Pandey, V.K. and Hunko, I. (2025), "An efficient data-driven framework for intrusion detection in wireless sensor networks using deep learning.", *Scientific Reports*, Springer Nature, Vol. 15 No. 1, available at: https://doi.org/10.1038/s41598-025-12867-x.

[52] Sun, G., Cong, Y., Dong, J., Wang, Q., Lyu, L. and Liu, J. (2022), "Data Poisoning Attacks on Federated Machine Learning", *IEEE Internet of Things Journal*, Institute of Electrical Electronics Engineers, Vol. 9 No. 13, pp. 11365–11375.

[53] Sun, B., Yang, S., Wang, Y., Lu, J., Pang, Z., Feng, X., Guang, H. and Cao, Y. (2025). A fusion safety and security analysis framework for intelligent and connected vehicles. *PLOS One*, [online] 20(9), p.e0332050. doi:https://doi.org/10.1371/journal.pone.0332050.

[54] Tarout, H., Zaki, H., Chahbouni, A., Ennajih, E. and Louragli, E.M. (2025), "Optimizing Energy Consumption in Electric Vehicles: A Systematic and Bibliometric Review of Recent Advances", *World Electric Vehicle Journal*, Multidisciplinary Digital Publishing Institute (MDPI), Vol. 16 No. 10, p. 577.

[55] Villegas-Ch, W., Jaramillo-Alcázar, A. and Luján-Mora, S. (2024). Evaluating the Robustness of Deep Learning Models against Adversarial Attacks: An Analysis with FGSM, PGD and CW. *Big data and cognitive computing*, 8(1), pp.8–8. doi:https://doi.org/10.3390/bdcc8010008.

[56] Wang, Z., Wei, H., Wang, J., Zeng, X. and Chang, Y. (2022). Security Issues and Solutions for Connected and Autonomous Vehicles in a Sustainable City: A Survey. *Sustainability*, 14(19), p.12409. doi:https://doi.org/10.3390/su141912409.

[57] Xiao, D., Hu, Y. and He, Z. (2024). Research on Autonomous Driving Scenario and Decision-making based on Deep Neural Network. *2024 3rd International Conference on Electronics and Information Technology (EIT)*, pp.755–758. doi:https://doi.org/10.1109/eit63098.2024.10761988.

[58] Yan, K., Yang, L., Yang, Z. and Ren, W. (2024), “Enhancing Adversarial Robustness through Stable Adversarial Training”, *Symmetry*, Multidisciplinary Digital Publishing Institute (Mdpi), Vol. 16 No. 10, p. 1363.

[59] Yu, X., Huang, Y., Liu, C. and Zhou, S. (2025), "Convolutional Neural Network-Based Autonomous Perception and Intelligent Decision System for Cabin Cleaning Machines", Springer Nature Singapore, pp. 1297–1313.

[60] Zhang, L., Krestinskaya, O., Fouda, M.E., Eltawil, A.M. and Salama, K.N. (2025). Quantized convolutional neural networks: a hardware perspective. *Frontiers in Electronics*, 6.doi:https://doi.org/10.3389/felec.2025.1469802.