From Challenges to Opportunities: A Comprehensive Study of AI-based In-Vehicle Intrusion Detection Systems

Elies Gherbi, Hamza Khemissa, Mohammed Bouchouia, Maxime Ayrault

From Challenges to Opportunities: A Comprehensive Study of AI-based In-Vehicle Intrusion Detection Systems

Elies Gherbi *, Hamza Khemissa†, Mohammed Lamine Bouchouia*, Maxime Ayrault‡
* IRT-SystemX, † Expleo France, ‡ Valeo
Email: {elies.gherbi,mohammed.bouchouia}@irt-systemx.fr, hamza.khemissa@expleogroup.com, maxime.ayrault@valeo.com

***Abstract*—While significant research has been conducted on ML-based In-Vehicle Intrusion Detection Systems (IV-IDS), the practical application of these systems needs further refinement. The safety-critical nature of IV-IDS calls for precise and objective evaluation and feasibility assessment metrics. This paper responds to this need by conducting a rigorous ML-based IV-IDS analysis. We offer a thorough review of recent automotive forensics studies spotlighting the constraints relevant to In-vehicles networks and the associated security/safety requirements to reveal the current gaps in the existing literature. By addressing the limitations of AI in IV-IDS, this paper contributes to the existing research corpus and defines pertinent baseline metrics for in-vehicle networked systems. Essentially, we reconcile the requirements of real-world autonomous vehicles with those of the security domain, enabling an assessment of the viability of AI-based intrusion detection systems.**

***Index Terms*—Machine learning, Intrusion detection, Forensics, in-vehicle network**

I. Introduction

Autonomous Vehicles (AVs) have been rapidly permeating everyday life. Over the past decades, continuous technological advancements have evolved these vehicles into sophisticated entities. AVs offer numerous advanced driver-assistance systems (ADAS) birthed from the progressive integration of Electronic Control Units (ECUs). The growing abundance of ECUs and networks within vehicles, while enhancing capabilities, makes them vulnerable to different possible cyber-attacks. As these AVs become more prevalent, such attacks pose ever-increasing risks to the safety of passengers, pedestrians, and other vehicles.

In the face of these threats, deploying Intrusion Detection Systems (IDS) within vehicles has gained momentum. Such systems serve as vigilant sentinels, detecting unusual or suspect activities and alerting users or systems to potential breaches. By flagging these fraudulent attempts early on, IDS can deter them before they cause substantial damage.

We note the need for a precise definition of automotive forensics. However, a general understanding of principles and processes involved in investigations can be gained by following the guidelines set out in digital forensics, such as ISO/IEC 27043:2015 [1]. However, to enable resilience in these systems, a vehicle must defend itself against attacks and recover swiftly to its optimal operational mode. This is where digital forensics comes into play, to enhance the system's resilience throughout its lifecycle. Digital Forensics has evolved into a crucial part of cyber defense, traditionally understood as collecting, preserving, analyzing, and presenting data post-incident for evidentiary purposes [2]. While the conventional approach has been reactive, responding post-incident, a proactive approach is being adopted increasingly. The proactive modality involves ongoing data collection, protection, detection of suspicious events, evidence acquisition, analysis, and building cases against potential threats [3].

The realm of artificial intelligence (AI)-based IDS addresses new challenges. Given the complex and black-box nature of AI models, the forensic process differs significantly from rule-based systems. AI for IDS requires a nuanced understanding of the principles and processes involved in these investigations, following guidelines, recommendations, and standards in the digital forensics domain. As science evolves, a precise definition and standardization of automotive forensics must be established. Nevertheless, current AI-based IDS do not account for forensic requirements or specific internal automotive needs, which makes the use of the different in-vehicle IDS impractical.

In this article, we aim to build a framework for assessing the viability of IDS based on AI/machine learning (ML) algorithms specifically designed for in-vehicle use. Based on the analysis of current research, we have identified areas of improvement and suggested future research directions. Our main goal is to establish a set of basic evaluation metrics for AI/ML-based IDS that are tailored to the unique requirements of in-vehicle systems and ensure the models' practicality.

II. Background and Related Work

In this section, we overview common attacks in AVs context, we revise the definition of resilience, and we outline recent research works on AI-based IDS for AVs.

A. Common Attacks

Over the past few years, Manufacturers have incorporated more driving assistance systems inside vehicles. These systems can control essential functions of the vehicle, which could compromise the driver's safety if misused. Additionally, the

increased connectivity of these systems creates new opportunities for cyber-attacks, potentially compromising the privacy and integrity of the vehicle and its passengers. These attacks can occur in three ways: physically, close to the vehicle, or remotely.

- OBD-II: modifying the vehicle's configuration to unlock new functions , sending messages on the CAN bus.
- USB port: installing malware or ransomware on the vehicle.
- Physical attacks: cutting brakes or steering wires.
- Bluetooth: invading the user's privacy by tracking its movement.
- Wi-Fi: spreading worms to collect privacy data, install malware, or take remote control of the vehicle.
- V2X: taking control of an entire fleet of vehicles.

B. Resilience definition

Resilience is a term that has been used extensively in the fields of psychology, economics, environment, and the medical field. In each of these domains a definition has appeared, giving meaning to this term, yet in the computer field a clear and precise definition has not been established. By merging different definitions that we encountered, we come up with the following definition:

- **Resilience**: being able to defend against an attack as long as possible, and once the defenses have fallen, being able to recover to the nominal operating state as quickly as possible.

Resilience aims to improve the security of the vehicle but without any impact on the safety and limited impacts on the overall performance. To provide trustworthy systems, system architects are looking for a way to apply cyber-resilience concepts into architectures, designs, and operational systems [4]. According to NIST SP 800-160 Vol. 1 [5], cyber resilience metrics can be used as evidence in assurance cases.

C. AI-based IDS for AVs

ISO 26262 mandates the implementation of safety mechanisms in AVs components to maintain their functionality and mitigate known failures/malicious activities. However, AVs failures still occur due to compromised safety mechanisms which require additional countermeasures like IDS. AI-powered systems can analyze large amounts of data, identify patterns, and adapt detection methods in real-time. Many articles explored ML and deep learning (DL) methods to detect cyber threats in AVs.

- In a CNN-based IDS survey [6], the authors compare the capabilities, features, and performance of ML approaches. The result varies depending on the used datasets, network architecture, and feature extraction techniques.
- In an overview of DL-based IDS in an automotive network [7], the authors categorized the different approaches on topology and techniques based on the accuracy, precision, recall, and F1 measures.
- An improvement of in-vehicle security networks by using a hybrid blockchain framework to provide a secure and decentralized way to store and share data related to the in-vehicle network (IVN) has been discussed in [8].
- In a survey on AI/ML-based IDSs and misbehavior detection [9], the authors suggested that despite extensive research, few solutions have been implemented in practical applications. Partly due to the lack of real-world scenarios demonstration and the inadequacy of evaluation metrics used to measure IDS feasibility solutions.

These articles share common points on methods, results, and applications. However, the evaluation is mainly done from a performance viewpoint. Feasibility is assessed based on the execution time and the computational cost. This brought to our attention a significant gap in the current approach to AVs. There is a need for metrics that address specific requirements in this domain. We also find that studies do not consider enough automotive cybersecurity and safety aspects, which are crucial in designing an effective IDS. To address this missing link in current methodologies and elucidate resultant system implications, we extract automotive and cybersecurity domain-specific requirements. Then, we outline the shortcomings of existing AI-based IDS solutions for AVs networks.

III. Architectures constraints and Domain requirements of N-IDS in AVs

In this section, we discuss domain-specific requirements and constraints for building efficient IDS.

A. Physical constraints

Connected vehicles may offer a range of new functionalities, thanks to a large ECUs integration within their architecture, but they are nevertheless embedded systems with limited computing power. Most embedded ECUs within the vehicle are small 8- or 16-bit microcontrollers with only one simple task to perform, with no space or computing power to detect attacks or defend themselves. The ECU's available memory is more in the order of Kb than Gb, as on a conventional system making it complicated to implement defense processes.

So in order to defend such a system, an in-depth architecture has been implemented. The vehicle's various functionalities are grouped into domains, each with its own sub-network for communicating with each other. The sub-network is managed by a Domain Controller (DC), which handles traffic within the domain. Inter-domain communications are handled by a Secure Gateway with greater computing power, enabling the network to be monitored and various types of system defense to be implemented.

B. Resilience and forensics requirements

CAVs are critical embedded systems, which require efficient techniques to ensure safety. Mechanisms for threats detection and investigation methods are very important in the design of the vehicle architecture's defenses.

In order to strengthen the resilience level of a system, some cyber resiliency metrics established by MITRE can be used [10]. From the selected metrics, we identified some approaches related to the metrics.

- **Analytic monitoring:** checking the system's integrity.
- **Substantiated integrity:** detecting adversary's attempts to deliver compromised data, software, and hardware.
- **Contextual awareness:** situational awareness, revealing patterns or trends in adversary behavior.
- **Deception:** misleading the adversary or hiding critical assets from the adversary.
- **Adaptive Response:** optimizing the ability to react appropriately to adverse conditions.
- **Non-Persistence:** limiting an adversary intrusion time.
- **Redundancy:** using hardware or software replication in a system.

Unfortunately, those approaches are tailored for forensic experts, and AI cannot take those directly into consideration. Thus, we discuss in the following section a new design to define AI applicable metrics.

IV. AI/ML-Based IDS Techniques in IVN

In this section, we introduce our taxonomy for AI/ML-based IDS techniques in IVN and an overview clarifying the decisions made throughout the various stages of constructing an AI model. This can assess the detection system efficacy and the suggested approaches practicality.

Our taxonomy presented in Figure 1 is divided into three parts: *1)* data and monitoring, *2)* modeling and learning tasks, and *3)* deployment and detection strategies.

A. Data and monitoring

The necessity of well-curated datasets for effective anomaly detection in ML-based IDS is widely acknowledged. We aim to examine this relationship, structuring our investigation into two clear segments.

1) Data sources and modalities

AVs are complex machines, comprised of sensors, ECU, and actuators. Those parts are interconnected through a variety of intra-vehicle networks that enable AVs monitoring and control. There are currently five primary intra-vehicle networks in use (LIN, CAN, FlexRay, Ethernet, and MOST), in addition to other V2X communication like WIFI and Bluetooth. There have been many proposed datasets for in vehicles communication [11]–[13], which mainly focuses on capturing CAN traffic. Those datasets are usually recorded through the vehicle diagnostics port (OBD-II), or simulation software such as Simulink. In a study by [11], the authors provide a comprehensive analysis of security-focused datasets, based on three primary factors: covered technology, attack types, and overall characteristics. In [12] the authors also explore several automotive IDS datasets and identify some issues, including inaccurate documentation or labeling and noisy attacks that can be easily detected through simple methods. Meanwhile, in [14] the authors recently conducted a survey of automotive security datasets and evaluated each data-set based on 11 criteria. They recommend specific datasets for use in in-vehicle and inter-vehicle ML-based IDSs.

2) Information types and preprocessing

The extraction of relevant features from raw in-vehicle data is pivotal for effective attack detection using ML algorithms. IDS detects intrusions at two levels of inspections: flow-based and payload-based. Flow-based approaches group packets together based on their common properties during a specific period, considering the arbitration IDs' frequencies, timing, and sequencing. Payload-based approaches, on the other hand, focus on the information carried by the packets and reflect the behavior of the vehicle's ECUs. The message content can be represented either by the data frame (strings of bits) without explicitly recovering the signals that these bits represent or by the signal, which requires decoding the raw data field bits [12]. Other works use physical layer attributes such as voltage.

Some attacks, such as flooding attacks, can be identified by analyzing the communication flow as they significantly impact it. However, other types of attacks can only be detected by examining the payload. Therefore, detecting various types of attacks require analyzing both the flow and payload levels.

Besides the inspection level, preprocessing converts network traffic into a series of observations, represented as feature vectors. There are two modeling scenarios: point-wise and window-wise. Point-wise labels each packet as normal or malicious, while window-wise gives the network state over a specific time frame. However, outputting for each data point is impractical in real-time environments like IVN. Despite this, many in-vehicle ML-IDS methods use point-wise modeling [15], [16].

B. Modeling and learning tasks

In-vehicle IDS increasingly utilize DL and ML techniques. Many methods have been employed, from supervised to unsupervised anomaly detection. Various architectures have been implemented to showcase the effectiveness of DL in detecting attacks, compared to classical ML techniques [9]. These techniques include traditional neural networks and newer transformers, GPT [17], and diffusion models [18], which have been used to improve the quality of intrusion detection. Although numerous techniques are available, there remains a considerable disparity between their application and practicality in real-world scenarios, especially in in-vehicle cybersecurity, forensics, and safety. This is because these methods must incorporate specific requirements as constraints in their modeling or evaluation processes and address the architectural limitations of in-vehicle systems, which have limited resources. Another critical factor is the need to reduce the "black box" aspect of deep neural networks to make forensic and investigation processes easier, which is the main goal of an IDS. Therefore, adapting and improving these methods is essential to meet the demands and challenges of the in-vehicle system and cybersecurity domains. To achieve this, the design of these approaches needs to consider the following aspects:

1) Explainability and interpretability

Entrusting crucial decisions to a system without explanation presents apparent risks. The lack of transparency further exac-

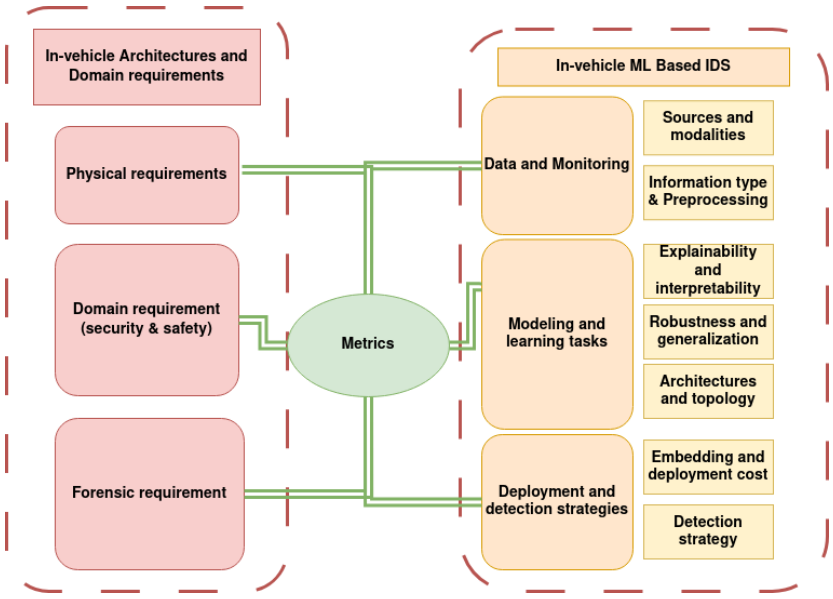

Fig. 1. AI-based In-vehicle IDS requirements

erbates the problem in the field of Cybersecurity. In [19], the authors provide an in-depth examination of the application of XAI in Cybersecurity and analyze the main Cybersecurity application fields concluding that machine-human integration is possible under one condition: the former must be explainable to the latter. Authors in [20] explore the decision tree algorithm for malicious node identification by applying it to an openly available dataset. The resulting model generates rules that are understandable and help network security personnel enhance trust by taking a possible course of action in case of malicious traffic identification. In [21], the authors consider human-in-the-loop, which can be used as a guideline when designing an X-IDS and introduce the use of SHAP (SHapley Additive exPlanations) in the field of IDS to generate explanations.

XAI in Cybersecurity can be a double-edged sword, as it can leave the system vulnerable to adversary attacks, meaning that, malicious actors that understand how the X-IDS works can exploit it to craft attacks challenging its robustness.

2) Robustness and generalization

Recent years have witnessed a surge in research focusing on adversarial ML, a field that explores the vulnerabilities of ML models to adversarial attacks [22]. This is particularly relevant in the context of in-vehicle IDS, where the robustness of ML models is critical to ensure the safety and integrity of vehicular systems [23]. Several methods have been proposed to enhance the robustness of ML models against adversarial attacks. However, these methods often involve a trade-off between adversarial robustness and detection accuracy, which may not be acceptable in certain domains where high detection accuracy is paramount. Given the current challenges, there is a requirement for strong and suitable methods to enhance the adversarial robustness of ML models while still retaining their detection accuracy. Additionally, it is essential to develop metrics that can evaluate the effectiveness of these methods and guide future research in this area, specifically for in-vehicle IDS.

To sum up, although adversarial ML has made notable advancements, its usage in the in-vehicle sector is still in its early stages [24], [25]. Further research should concentrate on defining the characteristics of adversarial attacks in this area, creating resilient approaches, and setting benchmarks for evaluating adversarial strength.

3) Architectures and topology

An important aspect that has been overlooked in current research is the unique architecture of future IVNs [26]. These networks are naturally distributed and hierarchical, with isolated probes for security purposes. This type of architecture requires a different approach when creating IDS models due to challenges related to communication overhead and information loss, mainly when compressing data. The impact of a distributed architecture on communication overhead is a crucial factor to consider. The difference between centralized and distributed models regarding communication cost can be substantial. Centralized models, while potentially more straightforward to implement, may suffer from high communication costs and increased latency due to the need to transmit data across the network. On the other hand, distributed models can reduce communication costs and latency by processing data locally. However, they may face challenges related to information loss, particularly when data compression is involved. Moreover, the fact that IVNs comprise multiple sub-networks, each with its modality and behaviors, introduces another layer of complexity. This scenario is reminiscent of the challenges faced in multi-modal ML, an advanced domain that seeks to harmonize different data modalities [27]. IDS for IVN could draw inspiration from this field, aiming to harmonize the behaviors of different sub-networks within the system.

C. Detection and deployment strategies

When implementing AI-based IV-IDS, it is crucial to consider various factors. One key factor is the detection strategy. For instance, in a distributed setting, assessing the uncertainty of each probe's result is important. Cooperative aspects of the IDS output and different update strategies can help manage this uncertainty [28], [29]. In [29], the authors present a cooperative ML-IDS that leverages the output of the IDS by using a consensus algorithm that considers the uncertainty of the results from each probe. In [30], the authors proposed a distributed framework for IVN anomaly detection that utilizes multi-dimensional temporal and data properties. They suggest deploying it on a mobile edge for additional computational resources, which could cause delays and hinder real-time attack detection.

Another aspect to consider is the deployment of DL-based Embedded Intrusion Detection Systems (EIDS) in automotive applications. These systems need to be designed carefully considering the computational and memory costs. In the study [31], a lightweight DL model was proposed for automotive systems. The model was designed to minimize CPU and memory costs while maintaining high detection accuracy.

D. Discussion

Creating comprehensive automotive datasets is difficult due to various network technologies, leading to limited features for robust IDS models. More datasets are needed for cellular and Bluetooth communications. Incomplete datasets impact the evaluation of IDS approaches, making it hard to compare and benchmark ML-based in-vehicle IDS approaches. The absence of suitable data makes it challenging to reproduce research findings and develop dependable in-vehicle IDS.

Although there have been many studies on in-vehicle IDS, some fail to assess the effectiveness of their ML/DL solutions because the available datasets need to be aligned with the needs of AVs. Furthermore, more appropriate metrics must be used to evaluate and validate datasets and their preprocessing while considering the architecture and domain requirements of IVN IDS as mentioned in the preceding section III. A critical issue revolves around the semantic gap between the detection results produced by ML-based IDS and the actionable interpretations needed by network operators III-B. While these systems can identify potential security threats, translating these detections into practical, implementable defense strategies remains problematic. This gap stems primarily from the intricate nature of these systems, characterized by complex algorithmic processes and layers of abstraction that makes it difficult to interpret the outcomes in a human-understandable form. Also, Due to the opacity of their decision-making process, ML-based IDS can lead to false positives that may have severe implications for network operators, resulting in considerable hesitance to act based solely on their detection results. The root of these issues can be traced back to the lack of explainability. Explainability in AI refers to the degree to which a human can understand a system's reasoning. The need for explainability is pressing, particularly in IDSs where understanding the reasons behind an alert is crucial for effective response and mitigation. Current explanation methodologies developed for ML-based systems have been proven inadequate for In-vehicle IDS due to their inability to manage historical inputs and complex feature dependencies inherent in structured data. future research must explore ways to enhance the explainability of ML-based IDS. This would serve a dual purpose: firstly, to provide human operators with actionable insights for rapid forensic intervention, and secondly, to inform the development of automated defensive mechanisms. By addressing the fundamental root cause of the issues above, such efforts can significantly improve the effectiveness and reliability of ML-based IDS, bringing us closer to robust, AI-enabled network security.

While significant strides have been made in improving the accuracy of IDS through various machine-learning architectures, there is a pressing need to consider the unique characteristics of IVNs. Future research should address the challenges posed by these networks' distributed and hierarchical nature, the communication overhead, and the need for harmonization across different network modalities.

ML-based IDS deployment and detection strategies need to consider various aspects, including managing output uncertainty, cooperative aspects, update strategy, and computational and memory costs. Integrating DL methods can further enhance the performance and security of these systems.

V. Metrics for evaluating the Viability of a practical AI based IDS

When it comes to using AI, particularly ML and DL, for IVN IDS, many challenges and complexities must be addressed to make these systems more dependable and effective for AVs. In order to evaluate and tackle these challenges, it is essential to identify specific metrics. The following section outlines a set of metrics, each designed to address a particular issue mentioned in the previous section IV. These metrics serve as both a diagnostic tool to identify and quantify problems and a performance indicator to track improvements and interventions. Understanding the relevance of each metric and the issues they address is crucial in the context of IVN IDS.

- **Data Adequacy:** measures datasets available quantity and quality for IDS models training. Used to assess limited and incomplete datasets.
- **Data Compatibility:** evaluates the compatibility of datasets with AVs' needs. Address the problem of misaligned datasets.
- **Harmonization:** measures the system's ability to work harmoniously across different network modalities. Harmonization across different network modalities.
- **Evaluation Metric Suitability:** measures evaluation metrics appropriateness used to validate datasets and preprocessing techniques.
- **Explainability:** quantifies the extent to which a human can understand a system's reasoning. Assess the lack of explainability in DL-NIDS.

- **Communication Overhead:** assesses the additional data being transmitted due to IDS implementation. Evaluate the challenges posed by the distributed and hierarchical nature of IVNs.
- **Output Uncertainty Management:** evaluates the system's ability to handle and communicate the output uncertainty, given the need to manage output uncertainty in ML IDS.
- **Adversarial Robustness:** assesses IDS resilience against adversarial attacks. Quantifies the system's ability to correctly identify threats even for inputs intentionally designed to deceive or mislead the system.
- **Cooperation Level:** measures system collaboration with other systems and parts of the vehicle.
- **Update Efficiency:** how effectively the system can update itself.
- **Computational and Memory Costs:** quantifies computational resources required for running the IDS and the amount of used memory.
- **Detection Latency:** measures the time taken to detect an intrusion.

VI. Conclusion

In this paper, we examine the difficulties posed by AI/ML applications in IV-IDS. We take into account the constraints within the vehicle and the requirements of cybersecurity forensics. We identify several critical issues, including insufficient data, lack of transparency, and the requirement for protection against adversarial attacks. We propose a set of metrics to measure and tackle these challenges, which could guide improvements in system design and implementation. Future efforts should focus on creating appropriate benchmarks and enhancing the transparency of the system. This will enable effective detection and response strategies against intrusion. Overall, this study provides a solid foundation for researchers and practitioners, outlining essential considerations and potential directions for developing robust, AI-based IV-IDS.

References

[1] "International Organization for Standardization (ISO), "ISO/IEC 27043:2015 Information Technology - Security Techniques - Incident Investigation Principles and Processes," ISO Office," 2015.

[2] K. K. G. Buquerin, C. Corbett, and H.-J. Hof, "A generalized approach to automotive forensics," *Forensic Science International: Digital Investigation*, vol. 36, p. 301111, 2021.

[3] P. Sharma and J. Gillanders, "Cybersecurity and forensics in connected autonomous vehicles: A review of state-of-the-art," *IEEE Access*, 2022.

[4] D. J. Bodeau, R. D. Graubart, R. M. McQuaid, and J. Woodill, "Cyber resiliency metrics, measures of effectiveness, and scoring," *Enabling Systems Engineers and Program Managers to Select the Most Useful Assessment Methods*, 2018.

[5] R. Ross, M. McEvilley, and M. Winstead, "Nist sp 800-160 vol1revision 1 engineering trustworthy secure systems initial public draft," 2022.

[6] L. Mohammadpour, T. C. Ling, C. S. Liew, and A. Aryanfar, "A survey of cnn-based network intrusion detection," *Applied Sciences*, 2022.

[7] B.Lampe and W.Meng, "A survey of deeplearning-based intrusion detection in automotive application," *ExpertSystem with Application*, 2023.

[8] N. Khatri, R. Shrestha, and S. Y. Nam, "Security issues with in-vehicle networks, and enhanced countermeasures based on blockchain," *Electronics*, vol. 10, no. 8, p. 893, 2021.

[9] O. Ajibuwa, B. Hamdaoui, and A. A. Yavuz, "A survey on ai/ml-driven intrusion and misbehavior detection in networked autonomous systems: Techniques, challenges and opportunities," *arXiv preprint*, 2023.

[10] D. J. Bodeau, R. D. Graubart, R. M. McQuaid, and J. Woodill, "Cyber resiliency metrics catalog," *The MITRE Corporation, Bedford,MA*, 2018.

[11] G. Karopoulos, G. Kambourakis, E. Chatzoglou, J. L. Hernández-Ramos, and V. Kouliaridis, "Demystifying in-vehicle intrusion detection systems: A survey of surveys and a meta-taxonomy," *Electronics*, 2022.

[12] M. E. Verma, M. D. Iannacone, R. A. Bridges, S. C. Hollifield, P. Moriano, B. Kay, and F. L. Combs, "Addressing the lack of comparability & testing in can intrusion detection research: A comprehensive guide to can ids data & introduction of the road dataset," 2022.

[13] A. Vahidi, T. Rosenstatter, and N. I. Mowla, "Systematic evaluation of automotive intrusion detection datasets," in *Proceedings of the 6th ACM Computer Science in Cars Symposium*, ser. CSCS '22. New York, NY, USA: Association for Computing Machinery, 2022.

[14] D. Swessi and H. Idoudi, "A comparative review of security threats datasets for vehicular networks," in *2021 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, 2021, pp. 746–751.

[15] H. Ma, J. Cao, B. Mi, D. Huang, Y. Liu, S. Li, and C. Chen, "A gru-based lightweight system for can intrusion detection in real time," *Sec. and Commun. Netw.*, vol. 2022, jan 2022.

[16] E. Seo, H. M. Song, and H. K. Kim, "GIDS: GAN based intrusion detection system for in-vehicle network," *CoRR*, 2019.

[17] M. Nam, S.Park, and D.Kim, "Intrusion detection method using bidirectional gpt for in-vehicle controller area networks," *IEEEAccess*, 2021.

[18] B. Tang, Y. Lu, Q. Li, Y. Bai, J. Yu, and X. Yu, "A diffusion model based on network intrusion detection method for industrial cyber-physical systems," *Sensors*, vol. 23, no. 3, 2023.

[19] N. Capuano, G. Fenza, V. Loia, and C. Stanzione, "Explainable artificial intelligence in cybersecurity: A survey," *IEEE Access*, 2022.

[20] B. Mahbooba, M. Timilsina, R. Sahal, and M. Serrano, "Explainable artificial intelligence (xai) to enhance trust management in intrusion detection systems using decision tree model," *Complexity*, 2021.

[21] S. Neupane, J. Ables, W. Anderson, S. Mittal, S. Rahimi, I. Banicescu, and M. Seale, "Explainable intrusion detection systems (x-ids): A survey of current methods, challenges, and opportunities," *IEEE Access*, 2022.

[22] T. Bai, J. Luo, J. Zhao, B. Wen, and Q. Wang, "Recent advances in adversarial training for adversarial robustness," 2021.

[23] K. He, D. D. Kim, and M. R. Asghar, "Adversarial machine learning for network intrusion detection systems: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 1, pp. 538–566, 2023.

[24] C. S.Wickramasinghe, D. L.Marino, H. S.Mavikumbure, V. Cobilean, T. D.Pennington, B. J.Varghese, C. Rieger, and M. Manic, "Rx-ads: Interpretable anomaly detection using adversarial ml for electric vehicle can data," 2022.

[25] K. Sauka, G.-Y. Shin, D.-W. Kim, and M.-M. Han, "Adversarial robust and explainable network intrusion detection systems based on deep learning," *Applied Sciences*, vol. 12, no. 13, 2022.

[26] A. G. Mariño, F. Fons, and J. M. M. Arostegui, "The future roadmap of in-vehicle network processing: A hw-centric (r-)evolution," *IEEE Access*, vol. 10, pp. 69 223–69 249, 2022.

[27] T. Baltrusaitis, C. Ahuja, and L. Morency, "Multimodal machine learning: A survey and taxonomy," *CoRR*, vol. abs/1705.09406, 2017.

[28] M. Abdar, F. Pourpanah, S. Hussain, D. Rezazadegan, L. Liu, M. Ghavamzadeh, P. Fieguth, X. Cao, A. Khosravi, U. R. Acharya, V. Makarenkov, and S. Nahavandi, "A review of uncertainty quantification in deep learning: Techniques, applications and challenges," *Information Fusion*, vol. 76, pp. 243–297, 2021.

[29] A. Abusitta, M. Bellaiche, M. Dagenais, and T. Halabi, "A deep learning approach for proactive multi-cloud cooperative intrusion detection system," *Future Generation Computer Systems*, pp. 308–318, 2019.

[30] K. Zhu, Z. Chen, Y. Peng, and L. Zhang, "Mobile edge assisted literal multi-dimensional anomaly detection of in-vehicle network using lstm," *IEEE Transactions on Vehicular Technology*, no. 5, 2019.

[31] H. Ma, J. Cao, B. Mi, D. Huang, Y. Liu, and S. Li, "A gru-based lightweight system for can intrusion detection in real time," *Security and Communication Networks*, vol. 2022, 06 2022.