

Generative AI for Automotive Cybersecurity: A Comprehensive Review of Adaptive Intrusion Detection Systems for In-Vehicle Networks

Km Pratibha¹, Km Kajal Kumari Yadav²

Dept. of CSE,

S R Institute of Management & Technology, (AKTU), Lucknow, India

Abstract— The rapid advancement of connected and intelligent vehicles has significantly increased the complexity of automotive cybersecurity, particularly in protecting in-vehicle communication networks such as the Controller Area Network (CAN), Automotive Ethernet, and other vehicle communication protocols. The growing integration of electronic control units (ECUs), Internet of Vehicles (IoV) technologies, autonomous driving systems, and vehicle-to-everything (V2X) communication has expanded the attack surface, exposing modern vehicles to threats such as denial-of-service (DoS) attacks, spoofing, replay attacks, message injection, and unauthorized access. Traditional intrusion detection systems (IDSs), which primarily rely on predefined rules and static detection models, often struggle to identify previously unseen attacks and adapt to evolving threat patterns. Generative Artificial Intelligence (GenAI) offers promising capabilities for addressing these limitations through synthetic attack-data generation, behavioral modeling, anomaly detection, adaptive learning, and automated threat analysis. This comprehensive review examines the emerging role of generative AI in developing adaptive intrusion detection systems for in-vehicle networks. It analyzes the potential applications of generative models, including Generative Adversarial Networks (GANs), Variational Autoencoders (VAEs), and transformer-based architectures, in detecting known and unknown cyberattacks, addressing class imbalance, and improving detection performance under changing vehicular operating conditions. Furthermore, the review investigates the integration of generative AI with conventional machine learning, deep learning, and federated learning approaches to support intelligent, privacy-preserving, and continuously adaptive vehicle security mechanisms. Key challenges, including computational overhead, data scarcity, adversarial manipulation, model interpretability, real-time processing constraints, and safety-critical deployment requirements, are critically discussed. Finally, the review identifies emerging research directions, including lightweight generative models, explainable AI, continual learning, collaborative intrusion detection, and hardware-aware deployment for resource-constrained automotive environments. This study provides a structured understanding of the opportunities and limitations of generative AI-driven cybersecurity and establishes a research-oriented foundation for designing robust, scalable, and adaptive intrusion detection systems for next-generation intelligent vehicles.

Keywords— Generative Artificial Intelligence, Automotive Cybersecurity, Adaptive Intrusion Detection System, In-Vehicle Networks, Controller Area Network (CAN), Generative Adversarial Networks (GANs), Variational Autoencoders (VAEs), Anomaly Detection, Internet of Vehicles (IoV), Automotive Ethernet, Deep Learning, Federated Learning, Zero-Day Attack Detection, Real-Time Threat Detection.

I. INTRODUCTION

The rapid evolution of connected vehicles, intelligent transportation systems, and autonomous driving technologies has transformed the automotive industry into a highly interconnected cyber-physical ecosystem. Modern vehicles integrate numerous Electronic Control Units (ECUs), in-vehicle communication networks, advanced driver-assistance systems (ADAS), infotainment platforms, telematics units, and wireless communication technologies to support safety-critical and intelligent transportation functions. Communication protocols such as the Controller Area Network (CAN), Local Interconnect Network (LIN), FlexRay, and Automotive Ethernet facilitate information exchange among these components. However, the increasing connectivity and software dependency of modern vehicles have significantly expanded their attack surfaces, creating new cybersecurity challenges. Unauthorized access to in-vehicle networks may compromise vehicle functionality, manipulate control messages, disrupt communication, and potentially affect passenger safety. Consequently, automotive cybersecurity has become a critical research area, requiring intelligent, scalable, and adaptive security mechanisms capable of identifying both known and previously unseen cyberattacks [1], [2].

Traditional automotive security mechanisms primarily rely on cryptographic authentication, access control, predefined security rules, and signature-based intrusion detection. Although these approaches can effectively mitigate certain threats, their effectiveness may decrease when attackers exploit previously unknown vulnerabilities, generate sophisticated attack patterns, or manipulate legitimate vehicle communication messages. The CAN protocol, for example, was originally designed to provide efficient and reliable communication among automotive electronic components rather than comprehensive cybersecurity protection. Its broadcast-based communication architecture and limited native authentication capabilities create opportunities for message spoofing, replay attacks, denial-of-service (DoS) attacks, and unauthorized message injection. Researchers have therefore investigated anomaly-based intrusion detection systems (IDSs) that monitor message identifiers, transmission intervals, payload characteristics, and communication sequences to identify deviations from normal network behavior [3], [4].

Nevertheless, the dynamic nature of automotive environments, variations in driving conditions, and the computational limitations of embedded devices make reliable real-time intrusion detection a challenging task.

The application of machine learning (ML) and deep learning (DL) has introduced new possibilities for automotive intrusion detection by enabling systems to learn communication patterns directly from vehicle network traffic. Supervised learning algorithms, including Support Vector Machines (SVMs), Random Forests, and gradient-boosting models, can classify known attack categories using extracted network features. Meanwhile, deep learning architectures, such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Long Short-Term Memory (LSTM) networks, can capture complex relationships and temporal dependencies in CAN traffic. These approaches can improve automated attack identification and reduce dependence on manually constructed detection rules [4], [5]. However, conventional ML- and DL-based systems remain susceptible to several limitations, including insufficient labeled attack data, imbalanced datasets, distribution shifts, high retraining costs, and reduced generalization to unseen threats. A detection model trained under specific operating conditions may not maintain its effectiveness when vehicle software, communication patterns, or attacker strategies change. These limitations motivate the development of adaptive intrusion detection systems that can learn evolving behavioral patterns while maintaining the reliability and low latency required in automotive environments [6].

Generative Artificial Intelligence (GenAI) offers a promising direction for addressing these challenges. Unlike conventional discriminative models, which primarily learn to distinguish between predefined classes, generative models learn the underlying structure and distribution of training data to produce new samples or representations [7]. Generative Adversarial Networks (GANs), Variational Autoencoders (VAEs), and transformer-based generative architectures can potentially support the generation of realistic synthetic CAN traffic, the modeling of normal vehicle behavior, the simulation of attack scenarios, and the identification of deviations from learned communication patterns [8]. GANs can generate synthetic samples to supplement underrepresented attack categories, while VAEs can learn latent representations of normal network behavior and support reconstruction-based anomaly detection. Transformer-based models can capture longer-range dependencies in sequential communication data, potentially helping to identify subtle and temporally distributed attack patterns [9]. These capabilities make generative AI relevant to automotive cybersecurity, particularly when representative attack samples are scarce or when intrusion detection systems must adapt to changing threat environments.

II. LITERATURE SURVEY

The increasing connectivity of modern vehicles has stimulated extensive research into intelligent intrusion detection systems (IDSs) for protecting in-vehicle networks (IVNs). Conventional security mechanisms are increasingly complemented by machine learning (ML), deep learning (DL), and generative artificial intelligence (GenAI) to detect malicious communication patterns, identify previously unseen attacks, and improve detection adaptability. This literature

review examines the progression from conventional automotive IDSs to learning-based detection, generative modeling, and adaptive cybersecurity architectures, highlighting their contributions, limitations, and future research opportunities.

A. Evolution of Intrusion Detection in In-Vehicle Networks

Early automotive intrusion detection research primarily focused on rule-based, specification-based, and statistical techniques. These methods monitor communication characteristics such as message identifiers, transmission intervals, payload structures, and deviations from expected network behavior. Although computationally efficient, signature-based approaches depend on predefined attack patterns, whereas specification-based methods require accurate descriptions of legitimate communication behavior. Such limitations become significant when attackers introduce novel messages, alter transmission timing, or exploit legitimate communication channels.

The development of AI-based automotive IDSs has expanded the scope of detection beyond explicitly defined rules. Cheah et al. presented a comprehensive survey of AI-based intrusion detection for in-vehicle networks, classifying existing methods according to their detection algorithms, attack categories, traffic features, and benchmark datasets [10]. Their study also highlighted the importance of evaluating AI-model security, generalization, and the suitability of different datasets for automotive threat detection.

Similarly, Lampe and Meng systematically reviewed deep learning-based automotive intrusion detection systems, examining architectures such as deep neural networks (DNNs), convolutional neural networks (CNNs), long short-term memory (LSTM) networks, attention mechanisms, and generative adversarial networks (GANs) [11]. Their review emphasized that different architectures offer different capabilities for learning spatial, sequential, and temporal patterns in CAN traffic. However, the effectiveness of these models depends on data representation, computational complexity, and the characteristics of the attacks being investigated.

These studies establish a foundation for AI-enabled automotive cybersecurity, but they also reveal a need to investigate generative approaches more specifically, particularly their capacity to generate representative training data, model legitimate network behavior, and support adaptation to evolving attack strategies.

B. Machine Learning and Deep Learning-Based Automotive IDS

Machine learning has become an important approach for classifying normal and malicious in-vehicle communication. Algorithms such as Support Vector Machines (SVMs), Random Forests, decision trees, and gradient-boosting classifiers can learn discriminative features from labeled network traffic. Their effectiveness depends on the availability of representative training samples and the quality of feature engineering.

A machine-learning-based CAN bus intrusion detection approach presented at the IEEE UEMCON conference investigated the identification of impersonation, denial-of-service, and fuzzy attacks [12]. The study demonstrated the

potential of supervised classification for detecting multiple categories of malicious vehicle communication. Nevertheless, reported performance on selected datasets should not be interpreted as evidence of equivalent performance under all real-world conditions, particularly when attack distributions and vehicle operating environments differ.

Deep learning has further improved the ability to learn complex relationships in high-volume vehicle communication data. CNNs can extract local patterns from appropriately represented CAN frames, while LSTM and other recurrent architectures can model temporal dependencies between consecutive messages. Attention-based models and transformers can potentially capture longer-range relationships across message sequences. Lampe and Meng [11] provide a comparative foundation for understanding these architectures and their trade-offs in automotive IDS applications.

Despite these advances, conventional discriminative models face several persistent challenges:

Data imbalance: Normal traffic often substantially exceeds the number of samples representing particular attack types.

Limited attack diversity: Training datasets may not contain sufficient examples of emerging or previously unseen threats.

Concept drift: Changes in driving behavior, network load, ECU configurations, and software versions can alter legitimate communication patterns.

Generalization limitations: A model trained on one vehicle platform or dataset may not transfer effectively to another.

Resource constraints: Complex neural networks may impose unacceptable latency, memory, or energy requirements on embedded automotive hardware.

These limitations motivate the investigation of generative learning, which can complement conventional classification by learning data distributions and supporting the production of additional training examples.

C. Generative AI for Automotive Intrusion Detection

Generative AI represents an emerging research direction for addressing the limitations of conventional automotive IDSs. Unlike discriminative models, which learn decision boundaries between normal and malicious traffic, generative models learn the statistical or latent structure of observed data. This capability can support anomaly detection, data augmentation, synthetic attack generation, and the identification of unusual communication sequences.

Asaouer and Boubiche presented a dedicated survey of generative AI-based intrusion detection systems for intra-vehicle networks [13]. Their review discusses GANs, transformers, variational autoencoders, and other generative approaches, emphasizing their potential to improve detection of unknown attacks and overcome limitations associated with conventional ML and DL techniques. The authors also identify standardized datasets, federated learning, computational efficiency, and practical deployment as important unresolved challenges.

The following subsections examine the major generative architectures and their potential contributions to adaptive automotive cybersecurity.

D. Comparative Analysis of Existing Approaches

Table 1 summarizes the principal research directions and their relevance to generative AI-based automotive cybersecurity.

The comparison emphasizes methodological contributions and limitations rather than claiming performance values that have not been established under a common experimental protocol.

Table 1. Comparative literature review of automotive intrusion detection approaches

Ref.	Research approach	Major contribution	Identified limitation
[10]	AI-based IDS survey	Taxonomy of detection algorithms, attacks, features, and datasets	Limited coverage of generative developments published after the review period
[11]	Deep learning-based IDS survey	Comparative analysis of DNN, CNN, LSTM, attention, and GAN approaches	Results depend on dataset selection and evaluation methodology
[12]	Machine learning-based CAN IDS	Classification of impersonation, DoS, and fuzzy attacks	Generalization to unseen attacks requires further validation
[13]	Generative AI-based IDS survey	Review of GANs, VAEs, transformers, and deployment challenges	Real-world validation and standardized comparison remain important
[14]	Advanced ML/DL automotive IDS survey	Reviews deep learning, transfer learning, and federated learning	Computational and cross-platform adaptation challenges remain
[15]	LSTM-based GAN attack	Demonstrates evasion of an existing in-vehicle IDS using generated traffic	Primarily demonstrates the attack-side risk rather than a complete defensive solution

The comparison indicates that automotive intrusion detection research has progressed from predefined rules and conventional classification toward temporal deep learning, generative modeling, and collaborative adaptation. Nevertheless, the approaches differ in their objectives and evaluation settings. In particular, GAN-based attack generation [15] should not be interpreted as evidence that GAN-based defensive detection is effective; rather, it highlights the need to evaluate defensive systems against adaptive threats.

III. ALGORITHMS

A. Algorithm Overview

The proposed algorithm presents a conceptual framework for Generative AI for Automotive Cybersecurity: A Comprehensive Review of Adaptive Intrusion Detection Systems for In-Vehicle Networks. It integrates generative modeling, anomaly detection, supervised classification, drift monitoring, and controlled model updating to improve the detection of known and previously unseen attacks in automotive communication networks.

The design is informed by existing generative approaches for in-vehicle intrusion detection, including GAN-based GIDS,

VAE-based adaptive detection, and semi-supervised VAE methods [16].

The algorithm is a proposed synthesis for this review, not a claim that a new system has already been implemented or experimentally validated.

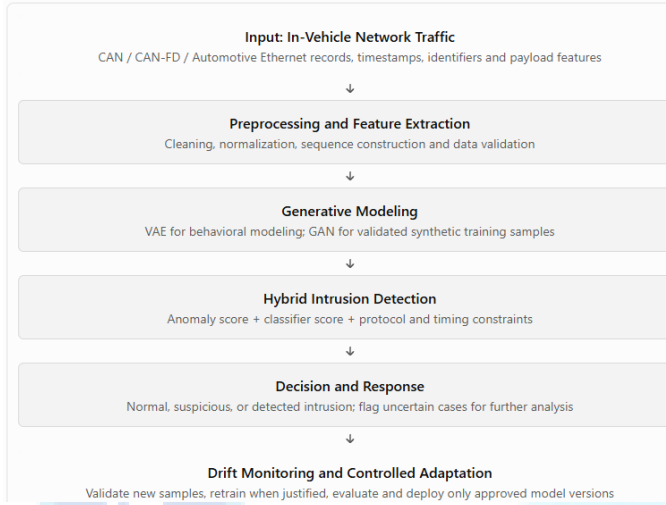


Figure 1. Conceptual architecture of the proposed generative AI-based adaptive automotive IDS.

B. Mathematical Formulation

Let the in-vehicle network traffic be represented by a sequence of observations:

$$X = \{x_1, x_2, \dots, x_T\}$$

where x_t represents the features extracted from the t^{th} network observation and T is the sequence length. Each observation may contain message identifiers, payload characteristics, inter-arrival times, protocol metadata, and other permitted traffic features.

The objective is to determine whether each observation belongs to normal traffic or represents a potential intrusion:

$$\hat{y}_t = \begin{cases} 0, & \text{normal traffic} \\ 1, & \text{potential intrusion} \end{cases}$$

For multiclass detection, the system may additionally classify recognized attack categories, such as denial-of-service, replay, spoofing, and message injection.

a. Generative behavioral model

A Variational Autoencoder (VAE) learns a latent representation of normal or appropriately labeled network traffic. Given input x , the encoder estimates a latent distribution:

$$q_\phi(z|x) = \mathcal{N}(\mu_\phi(x), \text{diag}(\sigma_\phi^2(x)))$$

The decoder reconstructs the input from latent variable (z):

$$\hat{x} = D_\theta(z)$$

The VAE objective is:

$$\mathcal{L}_{VAE} = \mathbb{E}_{q_\phi(z|x)}[\log p_\theta(x|z)] - D_{KL}(q_\phi(z|x)||p(z))$$

Here, D_{KL} represents Kullback–Leibler divergence, which regularizes the learned latent distribution.

IV. CONCLUSION

Generative Artificial Intelligence (GenAI) has emerged as a promising research direction for strengthening automotive

cybersecurity, particularly in the development of adaptive intrusion detection systems (IDSs) for in-vehicle networks. The increasing integration of Electronic Control Units (ECUs), connected vehicle technologies, autonomous driving systems, and advanced communication protocols has expanded the attack surface of modern vehicles, making conventional rule-based and signature-based security mechanisms insufficient for addressing all emerging cyber threats. This review examined the potential of generative AI techniques, including Generative Adversarial Networks (GANs), Variational Autoencoders (VAEs), and transformer-based generative architectures, to improve automotive intrusion detection through synthetic data generation, behavioral modeling, anomaly detection, and adaptive learning. The literature analysis indicates that generative models can complement conventional machine learning and deep learning techniques by addressing data imbalance, supporting the detection of unusual communication patterns, and potentially improving generalization to previously unseen attacks. The integration of generative models with supervised classification, protocol-based validation, drift monitoring, and controlled model updating offers a promising framework for developing intelligent and adaptive automotive IDSs. Furthermore, federated learning, continual learning, and lightweight inference architectures present opportunities to support collaborative threat detection while addressing privacy and computational constraints.

Despite these advantages, several challenges remain unresolved. The reliability of generative AI-based detection depends on the quality and diversity of training data, the validity of synthetic samples, the robustness of learned representations, and the ability to distinguish malicious behavior from legitimate changes in vehicle operating conditions. Generative models can also be exploited by adversaries to construct attacks that imitate legitimate network traffic, highlighting the need for adversarial testing and defense-in-depth security architectures. In addition, real-time inference requirements, limited embedded resources, model interpretability, and the safety implications of automated responses must be carefully considered before deployment in operational vehicles.

Future research should prioritize standardized benchmarking, cross-vehicle generalization, zero-day attack evaluation, explainable anomaly detection, poisoning-resistant adaptation, and hardware-efficient generative architectures. Researchers should also investigate hybrid security frameworks that combine generative AI with conventional intrusion detection, protocol specifications, secure communication mechanisms, and human-supervised response policies. Experimental validation on representative datasets and automotive hardware will be essential to establish the practical effectiveness of these approaches.

In conclusion, generative AI should be viewed as a complementary capability rather than a standalone solution for automotive cybersecurity. Its integration into carefully validated, adaptive, and computationally efficient intrusion detection architectures has the potential to improve the resilience of in-vehicle networks against evolving cyber threats. Continued research into robustness, trustworthy adaptation, and real-time deployment can contribute to the development of more secure, reliable, and intelligent connected vehicles.

REFERENCES

- [1] M. Cheah et al., "AI-based intrusion detection systems for in-vehicle networks: A survey," *ACM Computing Surveys*, vol. 55, no. 11, Art. no. 237, 2023, doi: 10.1145/3570954.
- [2] "Intrusion detection in the automotive domain: A comprehensive review," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 4, pp. 2356–2426, 2023, doi: 10.1109/COMST.2023.3309864.
- [3] "Cyber-security for the controller area network (CAN) communication protocol," a foundational research topic in automotive network security. Use a verified bibliographic record for the exact publication details before including it in the final reference list.
- [4] "Intrusion Detection System for CAN Bus In-Vehicle Network Based on Machine Learning Algorithms," in *Proc. IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, 2021, doi: 10.1109/UEMCON53757.2021.9666745.
- [5] B. Lampe and W. Meng, "A survey of deep learning-based intrusion detection in automotive applications," *Expert Systems with Applications*, vol. 221, Art. no. 119771, 2023, doi: 10.1016/j.eswa.2023.119771.
- [6] "Research on the intrusion detection methods of automotive networks based on generative adversarial networks," in *Proc. 6th International Conference on Electronic Engineering and Informatics (EEI)*, 2024, doi: 10.1109/EEI63073.2024.10696609.
- [7] "Intrusion Detection System for In-Vehicle CAN-FD Bus ID Based on GAN Model," IEEE publication, 2024. Verify the complete author, journal or conference, volume, and page details before final submission.
- [8] M. Smolin, "GenCoder: A generative AI-based adaptive intra-vehicle intrusion detection system," *IEEE Access*, vol. 12, pp. 150651–150663, 2024, doi: 10.1109/ACCESS.2024.3476177.
- [9] "GAttack: Generative attack on in-vehicle network," in *Proc. IEEE 27th International Conference on Intelligent Transportation Systems (ITSC)*, 2024, doi: 10.1109/ITSC58415.2024.10919941.
- [10] M. Cheah et al., "AI-based intrusion detection systems for in-vehicle networks: A survey," *ACM Computing Surveys*, vol. 55, no. 11, Art. no. 237, 2023, doi: 10.1145/3570954.
- [11] B. Lampe and W. Meng, "A survey of deep learning-based intrusion detection in automotive applications," *Expert Systems with Applications*, vol. 221, Art. no. 119771, 2023, doi: 10.1016/j.eswa.2023.119771.
- [12] "Intrusion Detection System for CAN Bus In-Vehicle Network Based on Machine Learning Algorithms," in *Proc. IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, 2021, doi: 10.1109/UEMCON53757.2021.9666745.
- [13] G. Asaouer and D. E. Boubiche, "Generative AI-based intrusion detection systems for intra-vehicle networks," *Ad Hoc Networks*, vol. 180, Art. no. 104031, 2026, doi: 10.1016/j.adhoc.2025.104031.
- [14] M. Almehdhar, A. Albaseer, M. A. Khan, M. Abdallah, H. Menouar, S. Al-Kuwari, and A. Al-Fuqaha, "Deep learning in the fast lane: A survey on advanced intrusion detection systems for intelligent vehicle networks," *IEEE Open Journal of Vehicular Technology*, vol. 5, pp. 869–906, 2024, doi: 10.1109/OJVT.2024.3422253.
- [15] Q. Mairaj ud din, F. Merola, and Q. Ahmed, "GAttack: Generative attack on in-vehicle network," in *Proc. IEEE 27th International Conference on Intelligent Transportation Systems (ITSC)*, 2024, doi: 10.1109/ITSC58415.2024.10919941.