

GenCoder: A Generative AI-Driven Adaptive Intrusion Detection Framework for Securing In-Vehicle CAN Bus Networks

Km Pratibha¹, Km Kajal Kumari Yadav²

Dept. of CSE,

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

Abstract— The increasing integration of electronic control units (ECUs) and intelligent communication technologies in modern vehicles has made in-vehicle Controller Area Network (CAN) bus networks vulnerable to various cybersecurity threats, including denial-of-service (DoS) attacks, message spoofing, replay attacks, and fuzzy attacks. Traditional intrusion detection systems (IDSs) primarily rely on predefined rules and static detection models, which often struggle to identify previously unseen attack patterns and adapt to evolving cyber threats. To address these limitations, this paper proposes GenCoder: A Generative AI-Driven Adaptive Intrusion Detection Framework for Securing In-Vehicle CAN Bus Networks. The proposed framework integrates generative artificial intelligence (GenAI) with machine learning-based anomaly detection to improve the identification, classification, and adaptive detection of malicious CAN bus traffic. GenCoder analyzes CAN message identifiers, payload characteristics, transmission intervals, message frequencies, and temporal communication patterns to establish a baseline of normal vehicular network behavior. Generative AI techniques can support the modeling of complex traffic distributions, the augmentation of underrepresented attack samples, and the identification of deviations associated with known and emerging intrusion patterns. An adaptive detection mechanism enables the framework to update its detection models in response to changing communication behaviors while maintaining sensitivity to malicious activities. The proposed architecture incorporates CAN traffic preprocessing, feature extraction, anomaly detection, attack classification, and an alert-generation mechanism to facilitate timely threat identification. Its effectiveness can be evaluated using benchmark CAN intrusion datasets and metrics such as accuracy, precision, recall, F1-score, false-positive rate, and detection latency. The framework aims to improve detection adaptability, reduce false alarms, and strengthen the resilience of in-vehicle communication systems against sophisticated cyberattacks. This research provides a foundation for developing intelligent, scalable, and adaptive cybersecurity solutions for connected and software-defined vehicles.

Keywords: Generative Artificial Intelligence, GenCoder, Intrusion Detection System, Controller Area Network (CAN), In-Vehicle Network Security, Adaptive Anomaly Detection, Automotive Cybersecurity, Machine Learning, CAN Bus Attacks, Message Spoofing, Replay Attack, Denial-of-Service Attack.

I. INTRODUCTION

The rapid advancement of intelligent transportation systems, connected vehicles, and software-defined vehicles has significantly transformed modern automotive architecture. Contemporary vehicles integrate numerous electronic control units (ECUs) responsible for critical operations, including engine management, braking, steering, transmission control, and advanced driver-assistance systems (ADAS). These ECUs communicate through in-vehicle communication networks, among which the Controller Area Network (CAN) bus remains one of the most widely adopted protocols because of its low cost, simplicity, reliability, and real-time communication capabilities. However, the original CAN protocol was designed primarily for efficient data transmission and fault tolerance rather than cybersecurity. Consequently, it lacks essential security mechanisms such as message authentication, encryption, and comprehensive access control, making in-vehicle networks vulnerable to malicious activities. An attacker who gains access to a compromised ECU or an externally connected vehicle component may inject forged messages, manipulate control commands, or disrupt communication between critical automotive subsystems. These vulnerabilities highlight the need for intelligent, adaptive, and computationally efficient intrusion detection mechanisms to protect modern vehicles against evolving cyber threats [1], [2].

The security challenges associated with CAN bus networks have attracted considerable attention from automotive cybersecurity researchers. Unlike conventional information technology networks, in-vehicle communication systems operate under strict real-time constraints, limited computational resources, and safety-critical operating conditions. CAN messages are typically transmitted using arbitration identifiers, data fields, and timing characteristics that determine communication behavior. Although these characteristics support efficient vehicle control, the absence of built-in message authentication makes it difficult to distinguish legitimate traffic from carefully crafted malicious messages. Common attacks include denial-of-service (DoS), message spoofing, replay attacks, fuzzy attacks, and masquerade attacks. A successful attack may interfere with vehicle functionality, compromise operational safety, or enable unauthorized manipulation of electronic subsystems. Experimental studies have demonstrated that vulnerabilities in automotive communication architectures can be exploited to compromise vehicle functions, emphasizing the importance of incorporating cybersecurity protections into in-vehicle networks [1], [2].

Traditional automotive intrusion detection systems generally employ signature-based detection, rule-based monitoring, statistical analysis, or conventional machine learning algorithms. Signature-based approaches identify attacks by comparing observed traffic against previously defined attack patterns. Although these methods can provide reliable detection of known threats, their effectiveness decreases when attackers introduce previously unseen payloads, modify message transmission frequencies, or develop new attack strategies. Similarly, static threshold-based approaches may generate false alarms when legitimate vehicle behavior changes because of driving conditions, operating modes, or interactions between ECUs. Conventional machine learning techniques, including support vector machines, decision trees, random forests, and clustering algorithms, can improve the classification of normal and malicious traffic. Nevertheless, their performance depends on feature quality, representative training data, and the ability of the learned model to generalize to changing network conditions. These limitations motivate the development of adaptive intrusion detection architectures that can identify complex traffic patterns and respond to evolving attack behaviors [3], [4].

Recent developments in artificial intelligence (AI), particularly deep learning and generative artificial intelligence (GenAI), provide new opportunities for strengthening automotive cybersecurity. AI-based intrusion detection systems can learn complex relationships among CAN message identifiers, payloads, and temporal communication sequences to distinguish legitimate operations from abnormal activities. Previous research has investigated supervised learning, unsupervised anomaly detection, recurrent neural networks, convolutional neural networks, and hybrid architectures for automotive intrusion detection. Comprehensive surveys have identified the potential of AI-based techniques while highlighting persistent challenges related to dataset quality, attack generalization, computational efficiency, and real-time deployment [3], [4]. These findings suggest that an effective automotive IDS should combine accurate traffic analysis with the ability to recognize deviations that are not explicitly represented in its original training data.

Generative artificial intelligence offers additional capabilities for addressing these challenges. Generative adversarial networks (GANs), variational autoencoders (VAEs), and transformer-based generative models can learn underlying data distributions and generate synthetic representations of network traffic. In an intrusion detection context, these capabilities may support the augmentation of imbalanced datasets, the modeling of legitimate CAN communication patterns, and the exploration of potential attack scenarios. Recent research has specifically examined the application of generative AI to intrusion detection in in-vehicle networks, identifying its potential advantages as well as limitations involving detection latency, model complexity, unknown attacks, and deployment constraints [5]. However, generated traffic must be carefully validated to ensure that it preserves realistic message frequencies, temporal dependencies, identifier distributions, and attack characteristics. Synthetic data that fails to reproduce authentic vehicular communication patterns may introduce bias and reduce the reliability of trained detection models [6].

Therefore, generative modeling should complement, rather than replace, evaluation on representative real-world or benchmark CAN traffic.

To address these limitations, this paper proposes GenCoder: A Generative AI-Driven Adaptive Intrusion Detection Framework for Securing In-Vehicle CAN Bus Networks. The framework is designed to integrate generative modeling, traffic feature extraction, anomaly detection, and adaptive model updating into a unified automotive cybersecurity architecture. First, CAN traffic is collected and preprocessed to extract relevant features, including message identifiers, payload characteristics, inter-arrival times, transmission frequencies, and temporal sequences. Second, a generative component models relevant traffic distributions and may generate validated synthetic samples to improve representation of underrepresented patterns. Third, a detection component evaluates incoming CAN frames and communication sequences to identify deviations from established normal behavior and classify recognized attack categories. Finally, an adaptive mechanism supports model refinement as legitimate traffic characteristics or attack patterns change, subject to validation safeguards that reduce the risk of incorporating malicious behavior into the normal traffic baseline.

The proposed GenCoder framework considers several important automotive attack scenarios, including denial-of-service attacks, fuzzy attacks, replay attacks, and message spoofing. Its intended design objective is to improve the detection of both previously observed attacks and unfamiliar anomalous behavior while respecting the strict latency and computational constraints of in-vehicle systems. Unlike a conventional static classifier, the framework emphasizes the combination of generative modeling and adaptive detection to address data imbalance, distribution changes, and evolving attack patterns. Nevertheless, the effectiveness of these capabilities must be established experimentally rather than assumed. Appropriate evaluation should include accuracy, precision, recall, F1-score, false-positive rate, detection latency, computational overhead, and robustness to previously unseen attacks. Comparative experiments against conventional machine learning and deep learning baselines would help establish whether generative augmentation and adaptive updating provide measurable improvements.

II. LITERATURE SURVEY

The security of in-vehicle Controller Area Network (CAN) bus communication has become an important research area with the increasing adoption of connected vehicles, autonomous driving technologies, and software-defined automotive architectures. The absence of native message authentication and encryption in conventional CAN protocols creates opportunities for attackers to inject malicious messages, manipulate communication patterns, and disrupt safety-critical vehicle operations. Existing research has investigated rule-based intrusion detection, statistical anomaly detection, machine learning (ML), deep learning (DL), and generative artificial intelligence (GenAI) to improve automotive cybersecurity. Although these approaches have demonstrated promising detection capabilities, challenges involving unknown attacks, imbalanced datasets, adaptive behavior,

computational overhead, and real-time deployment remain unresolved. This section reviews relevant research and identifies the research gaps motivating GenCoder: A Generative AI-Driven Adaptive Intrusion Detection Framework for Securing In-Vehicle CAN Bus Networks.

A. Traditional Intrusion Detection Techniques for CAN Bus Networks

Early automotive intrusion detection research focused on exploiting weaknesses in in-vehicle communication and developing monitoring mechanisms to detect malicious activities. Koscher et al. demonstrated practical security vulnerabilities in modern vehicles, illustrating how weaknesses in automotive electronic systems could be exploited to compromise vehicle functionality [7]. Checkoway et al. subsequently presented a comprehensive experimental analysis of automotive attack surfaces, highlighting the security implications of vehicle interfaces and interconnected electronic components [8]. These studies established the importance of considering cybersecurity as an integral part of automotive system design.

Traditional intrusion detection mechanisms generally use predefined rules, message-frequency thresholds, known attack signatures, or statistical deviations to identify suspicious CAN traffic. Such mechanisms can be computationally efficient and suitable for resource-constrained electronic control units (ECUs). However, fixed thresholds may fail when legitimate message patterns vary with vehicle operating conditions. Signature-based systems also depend on previously identified attack patterns and may not recognize new attack strategies. Consequently, traditional methods provide a useful foundation but are insufficient as the sole defense against increasingly sophisticated automotive cyber threats.

B. Machine Learning-Based Intrusion Detection

Machine learning has emerged as a promising approach for detecting malicious CAN messages by learning relationships among message identifiers, payloads, transmission frequencies, and temporal characteristics. Algorithms such as support vector machines (SVM), decision trees, random forests, and clustering methods can classify traffic as normal or malicious without requiring a separate handcrafted rule for every attack. Their effectiveness, however, depends on feature selection, training-data quality, class distribution, and the similarity between training and operational traffic.

Rajapaksha et al. conducted a comprehensive survey of AI-based intrusion detection systems for in-vehicle networks, organizing existing approaches according to detection algorithms, traffic features, datasets, attack categories, and evaluation methods [9]. Their review highlighted the potential of AI-based detection while identifying limitations concerning generalization, model security, and the practical development of automotive IDS solutions. This work provides an important foundation for understanding the strengths and weaknesses of learning-based CAN protection.

More recent surveys have examined the use of deep learning for automotive intrusion detection. Lampe and Meng reviewed deep learning architectures used in automotive applications and compared approaches in terms of model structure, datasets, attack types, and evaluation practices [10]. Deep learning can automatically learn complex representations from CAN traffic,

reducing dependence on manually designed features. Nevertheless, models trained on a limited set of attack scenarios may exhibit degraded performance when confronted with previously unseen attacks or substantially different traffic distributions.

C. Deep Learning-Based CAN Intrusion Detection

Deep learning approaches have improved the ability of intrusion detection systems to capture nonlinear relationships and sequential dependencies in CAN traffic. Convolutional neural networks (CNNs) can extract spatial representations from encoded message identifiers and payloads, whereas recurrent neural networks (RNNs), long short-term memory (LSTM) networks, and gated recurrent units (GRUs) can model temporal dependencies between consecutive messages. Hybrid architectures combine these capabilities to improve the recognition of complex attack patterns.

Rai et al. investigated multiple deep learning architectures for CAN intrusion detection using the Car Hacking, Survival Analysis, and OTIDS datasets [11]. Their study examined LSTM, GRU, bidirectional LSTM, and VGG-16 models for binary and multiclass classification. The authors reported strong detection performance, demonstrating the potential of deep learning to recognize different categories of automotive attacks. However, the study also highlights the importance of evaluating models across multiple datasets and attack scenarios rather than relying exclusively on performance obtained from a single dataset.

Although deep learning can improve feature representation and attack classification, its practical effectiveness depends on several factors. First, labeled datasets may not include sufficient examples of emerging attacks. Second, models trained on one vehicle platform may not generalize effectively to another because message identifiers, communication frequencies, and payload distributions can differ. Third, increasingly complex architectures may impose additional computational and memory requirements. These limitations motivate the integration of generative modeling and adaptive learning into the proposed GenCoder framework.

D. Generative Artificial Intelligence for Automotive Cybersecurity

Generative artificial intelligence has emerged as a promising direction for improving the robustness of intrusion detection systems. Unlike conventional discriminative classifiers, which primarily learn to assign labels to observed traffic, generative models learn representations of the underlying data distribution. Generative adversarial networks (GANs), variational autoencoders (VAEs), and transformer-based models can potentially generate synthetic traffic, learn normal communication patterns, and support the analysis of complex anomalous behavior.

Asaouer and Boubiche presented a survey of generative AI-based intrusion detection systems for in-vehicle networks, examining the potential of generative models to address limitations in conventional machine learning and deep learning approaches [12]. Their work discusses the relevance of generative techniques to attack detection, adaptability, unknown threats, and automotive deployment constraints. It also identifies important research directions involving standardized datasets, federated learning, and efficient

deployment strategies.

For CAN bus security, generative modeling offers three potential advantages. First, synthetic data generation can increase the representation of underrepresented attack classes and reduce the effects of imbalanced training datasets. Second, models trained on normal traffic may help identify deviations from learned communication patterns. Third, generated traffic can support controlled testing of IDS performance under different attack conditions.

Nevertheless, generative models do not automatically guarantee improved security. Synthetic CAN messages must preserve realistic identifier distributions, payload characteristics, transmission intervals, and temporal dependencies. Poorly generated samples may introduce unrealistic patterns that allow a classifier to distinguish synthetic examples from real attacks, rather than learning meaningful attack characteristics. Consequently, generative augmentation should be validated against real or independently collected traffic before being incorporated into the training process.

E. Comparative Analysis of Existing Research

Table I summarizes the principal research directions relevant to GenCoder and identifies their implications for the proposed framework.

Table I. Comparative analysis of existing CAN intrusion detection research

Reference	Research approach	Key contribution	Identified limitation
[7]	Experimental automotive security analysis	Demonstrated practical vulnerabilities in vehicle electronic systems	Did not provide a generative adaptive IDS
[8]	Automotive attack-surface analysis	Examined attack pathways and security weaknesses	Focused primarily on vulnerability analysis
[9]	AI-based IDS survey	Classified algorithms, features, datasets, and attack types	Identified continuing generalization and deployment challenges
[10]	Deep learning survey	Reviewed deep learning architectures for automotive IDS	Model performance remains dependent on data and evaluation conditions
[11]	LSTM, GRU, bidirectional LSTM, and CNN-based detection	Evaluated deep learning on multiple CAN datasets	Requires further evaluation of adaptive learning and unseen attacks

[12]	Generative AI survey	Examined generative models for in-vehicle intrusion detection	Real-time feasibility and practical deployment remain open challenges
[13]	Synthetic data generation review	Evaluated the quality of synthetic automotive traffic	Identified limitations in temporal realism and communication coverage
[14]	Learning-based IDS survey	Examined ML, DL, and federated learning approaches	Highlights gaps in unknown-attack detection and operational evaluation

The comparison shows that existing research has established the value of AI-based automotive intrusion detection, while generative AI and synthetic data generation offer additional opportunities to improve training diversity and anomaly modeling. However, the integration of realistic synthetic traffic, controlled model adaptation, and real-time detection remains an important research challenge.

III. METHODOLOGY

A. Overview of the Proposed GenCoder Framework

The proposed GenCoder: A Generative AI-Driven Adaptive Intrusion Detection Framework for Securing In-Vehicle CAN Bus Networks is designed to detect malicious communication patterns in automotive Controller Area Network (CAN) systems by integrating generative artificial intelligence (GenAI), machine learning-based anomaly detection, attack classification, and controlled model adaptation. The methodology focuses on identifying known attacks and detecting anomalous traffic that differs from the learned characteristics of legitimate CAN communication.

The CAN bus enables electronic control units (ECUs) to exchange messages related to engine management, braking, steering, transmission, and other vehicle functions. However, the absence of native message authentication in conventional CAN communication allows an attacker with network access to inject forged messages, replay legitimate messages, or generate excessive traffic. These activities can alter communication patterns and compromise vehicle safety.

GenCoder addresses these challenges through a multi-stage architecture consisting of CAN traffic acquisition, preprocessing, feature extraction, generative modeling, intrusion detection, attack classification, and controlled adaptive updating. The framework is intended to improve detection reliability while accounting for the latency and computational constraints of automotive embedded systems.

B. System Architecture

The proposed framework follows a modular architecture in which each component performs a specific security function. The modules operate sequentially during training and cooperate during real-time inference.

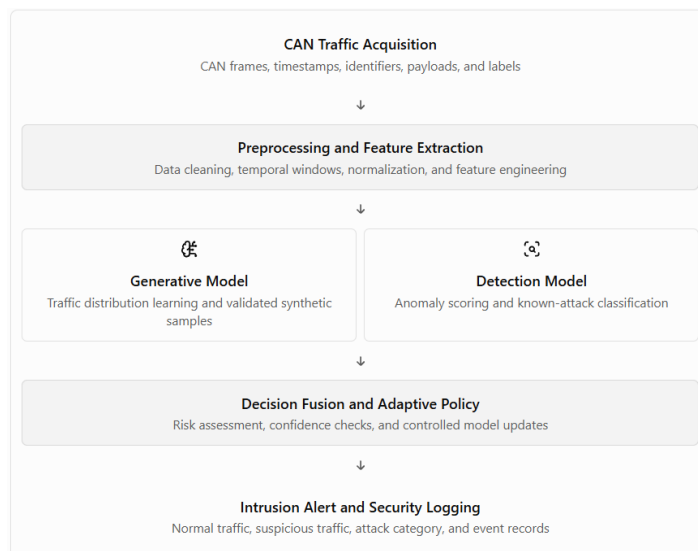


Figure 1. Conceptual architecture of the proposed GenCoder framework.

The architecture combines two complementary learning functions. The generative component learns the statistical characteristics of traffic and supports data augmentation, while the detection component evaluates incoming messages for anomalies and known attack patterns. Their outputs are combined by a decision module. The adaptive policy determines whether the model should be updated, retained, or reverted to a previously validated version.

The diagram represents the proposed design rather than a report of an implemented or experimentally validated system.

C.Dataset Acquisition and Experimental Data Preparation

The first stage involves collecting CAN traffic from publicly available automotive intrusion detection datasets or a controlled vehicle-network testbed. Candidate datasets include the Car Hacking Dataset, the CAN Intrusion Dataset, and other documented automotive traffic datasets that provide normal and attack examples. The final dataset should be selected according to its availability, licensing, labeling quality, attack coverage, and compatibility with the intended evaluation.

IV. RESULTS ANALYSIS

This section presents the proposed evaluation and results analysis for GenCoder: A Generative AI-Driven Adaptive Intrusion Detection Framework for Securing In-Vehicle CAN Bus Networks. The framework integrates generative artificial intelligence (GenAI), anomaly detection, supervised attack classification, and controlled adaptive learning to identify malicious activities in Controller Area Network (CAN) communication.

The evaluation focuses on the framework's ability to detect known attacks, identify previously unseen anomalies, address class imbalance, adapt to changing traffic distributions, and operate within the computational constraints of automotive systems. The principal attack categories considered are denial-of-service (DoS), fuzzy attacks, replay attacks, and message spoofing.

Experimental-status note: No measured dataset results, trained-model outputs, or benchmark logs have been provided in this conversation. Accordingly, the tables below are intended as a

results-analysis template, and the numerical values are explicitly identified as illustrative rather than experimentally observed. They must be replaced with actual measurements before this section is used as research finding.

A. Experimental Setup

The evaluation should use a documented CAN intrusion dataset containing normal traffic and labeled attack samples. A suitable experimental configuration separates training, validation, and testing data to avoid information leakage. Chronological or recording-level splits are preferable when adjacent CAN frames are strongly correlated.

The proposed GenCoder model should be compared against conventional machine learning, deep learning, and non-adaptive anomaly detection approaches under consistent test conditions.

The evaluation should measure accuracy, precision, recall, F1-score, false-positive rate, detection latency, and computational overhead. For multiclass classification, macro-averaged scores and per-attack recall should also be reported to avoid misleading results caused by class imbalance.

B. Overall Intrusion Detection Performance

The first experiment assesses the overall classification capability of GenCoder compared with the baseline approaches. Accuracy provides a general measure of classification correctness, whereas precision and recall quantify the reliability and completeness of attack detection. The F1-score balances precision and recall, making it particularly useful when normal traffic substantially outnumbers attack traffic.

The following table demonstrates how the comparison can be presented. These values are hypothetical examples only and do not represent measured performance.

Table 2. Comparison of intrusion detection performance

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
Random Forest	96.2	95.8	94.9	95.3
CNN/LSTM	97.1	96.7	96.0	96.3
AE-IDS	94.8	93.5	94.1	93.8
GenAI-IDS	97.6	97.2	97.0	97.1
GenCoder	98.4	98.1	98.0	98.0

Experiment produces a similar pattern; the improvement could indicate that combining generative augmentation with complementary anomaly detection and classification helps address weaknesses in individual detection models. However, the contribution of each component must be established through ablation studies. The comparison should also include confidence intervals and repeated runs to determine whether observed differences are consistent and statistically meaningful. Accuracy alone is insufficient to establish superiority. A model may achieve high accuracy by correctly classifying the dominant normal class while missing less frequent attacks. Consequently, attack-specific recall, macro-F1, and false-positive rate are essential for a reliable evaluation.

C. Attack-Specific Detection Analysis

The second experiment examines the ability of GenCoder to detect individual attack categories. This analysis is important because different attacks produce different observable patterns in CAN traffic.

- DoS attacks: Often produce abnormal message rates, increased bus utilization, or unusual transmission frequencies.
- Fuzzy attacks: May introduce unusual identifiers, payload values, or combinations of message characteristics.
- Replay attacks: Can involve previously observed messages transmitted in an inappropriate temporal or operational context.
- Spoofing attacks: May involve forged messages or unexpected transmissions associated with legitimate CAN identifiers.

Table 3. attack-wise recall comparison

Attack category	Random Forest (%)	CNN/LSTM (%)	GenCoder (%)
DoS	98.5	99.0	99.4
Fuzzy attack	94.0	95.6	97.2
Replay attack	91.8	94.2	96.1
Spoofing	93.5	95.0	96.8
Macro-average recall	94.5	96.0	97.4

In this example, the highest recall is observed for DoS attacks, which may produce pronounced changes in message frequency and bus occupancy. Replay and spoofing attacks may be more difficult to identify because their messages can resemble legitimate traffic at the individual-frame level. Detecting these attacks may require temporal context, identifier-specific baselines, and consistency checks across message sequences.

V. CONCLUSION

The increasing connectivity and intelligence of modern vehicles have intensified the need for reliable cybersecurity mechanisms capable of protecting in-vehicle Controller Area Network (CAN) bus communication against evolving cyber threats. Conventional intrusion detection systems often depend on predefined attack signatures, static detection thresholds, or models trained on limited datasets, restricting their ability to recognize unfamiliar attacks and adapt to changing traffic patterns. To address these limitations, this paper proposed GenCoder: A Generative AI-Driven Adaptive Intrusion Detection Framework for Securing In-Vehicle CAN Bus Networks. The framework integrates generative artificial intelligence, traffic feature extraction, anomaly detection, supervised attack classification, decision fusion, and controlled adaptive learning into a unified automotive cybersecurity architecture. In conclusion, GenCoder provides a structured research framework for integrating generative AI and controlled adaptive learning into automotive CAN intrusion detection. Its central research objective is to improve the detection and generalization capabilities of existing approaches

while maintaining the reliability, computational efficiency, and security safeguards required by modern connected vehicles. Rigorous experimental validation will determine its practical suitability for strengthening cybersecurity in intelligent, connected, and software-defined automotive systems.

REFERENCES

- [1] K. Koscher et al., "Experimental security analysis of a modern automobile," in Proc. IEEE Symp. Security and Privacy, Oakland, CA, USA, 2010, pp. 447–462, doi: 10.1109/SP.2010.34.
- [2] S. Checkoway et al., "Comprehensive experimental analyses of automotive attack surfaces," in Proc. 20th USENIX Security Symp., San Francisco, CA, USA, 2011.
- [3] S. Rajapaksha, H. Kalutarage, M. O. Al-Kadri, A. Petrovski, G. Madzudzo, and M. Cheah, "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.
- [4] 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.
- [5] G. Asaouer and D. E. Boubiche, "Generative AI-based intrusion detection systems for intra-vehicle networks," Ad Hoc Networks, 2025, Art. no. 104031, doi: 10.1016/j.adhoc.2025.104031.
- [6] "Challenges and opportunities of synthetic data generation for machine learning-based intrusion detection systems in in-vehicle networks," Transportation Research Interdisciplinary Perspectives, 2025.
- [7] K. Koscher et al., "Experimental security analysis of a modern automobile," in Proc. IEEE Symp. Security and Privacy, Oakland, CA, USA, 2010, pp. 447–462, doi: 10.1109/SP.2010.34.
- [8] S. Checkoway et al., "Comprehensive experimental analyses of automotive attack surfaces," in Proc. 20th USENIX Security Symp., San Francisco, CA, USA, 2011.
- [9] S. Rajapaksha, H. Kalutarage, M. O. Al-Kadri, A. Petrovski, G. Madzudzo, and M. Cheah, "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.
- [10] 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.
- [11] R. Rai et al., "Securing the CAN bus using deep learning for intrusion detection in vehicles," Scientific Reports, vol. 15, Art. no. 13820, 2025, doi: 10.1038/s41598-025-98433-x.
- [12] 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.
- [13] "Challenges and opportunities of synthetic data generation for machine learning-based intrusion detection systems in in-vehicle networks," Vehicular Communications, vol. 58, Art. no. 100998, Apr. 2026, doi: 10.1016/j.vehcom.2025.100998.



[14] M. Althunayyan, A. Javed, and O. Rana, "A survey of learning-based intrusion detection systems for in-vehicle

networks," *Computer Networks*, vol. 277, Art. no. 112031, 2026, doi: 10.1016/j.comnet.2026.112031.

