Science World Journal Vol. 21(No 1) 2026 https://dx.doi.org/10.4314/swj.v21i1.37
www.scienceworldjournal.org
ISSN: 1597-6343 (Online), ISSN: 2756-391X (Print)
Published by Faculty of Science, Kaduna State University

Review Article

DEEP LEARNING–BASED INTRUSION DETECTION IN VEHICULAR NETWORKS: A REVIEW OF GATED RECURRENT UNIT APPROACHES

*Tose E. Oziegbe, Abel E. Edje, Maureen Akazue

Department of Computer Science, Delta State University, Abraka, Nigeria

*Corresponding Author Email Address: toseoziegbe@gmail.com

ABSTRACT
With the intention of protecting road users and network facilities, notable security challenges that require robust intrusion detection systems (IDSs) have been identified with the growth of vehicular networks. This systematic review examines recent deep learning (DL) applications to assess their capability to identify anomaly-based intrusions in vehicular networks, with a focus on Gated Recurrent Unit (GRU) architectures. Following a structured literature search and screening protocol, peer-reviewed studies published between 2021 and 2025 were systematically identified, evaluated, and synthesized. GRU networks enable real-time detection with efficient computation and also show remarkable capacity to capture temporal dependencies and sequential patterns in network data. This systematic review finds that GRU-based systems can achieve better performance with fewer parameters and maintain low computational cost by effectively addressing the vanishing gradient issues in conventional RNNs. Some of the reported accuracies exceeded 99% across several benchmark datasets, including CICIDS2017, CICIDS2018, NSL-KDD, and UNSW-NB15. Hybrid GRU-CNN architectures routinely outperform traditional detection algorithms. The efficient utilization of GRUs in resource-constrained vehicle contexts is confirmed by performance tests using evaluation metrics such as precision, recall, F1 Score, and false positive rate (FPR). GRU ensembles, combined with other algorithms such as bidirectional LSTM networks, attention mechanisms, and optimization techniques, have improved detection capabilities against complex attacks such as DoS, blackhole, and zero-day exploits. The results show that GRU is crucial for developing an accurate, lightweight IDS that can be deployed to safeguard transportation infrastructure and current vehicular networks.

Keywords: Gated Recurrent Unit (GRU), Deep Learning (DL), Intrusion Detection System (IDS), Vehicular Networks, Anomaly Detection, Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Everything (V2X), Vehicular Ad-Hoc Networks (VANET)

INTRODUCTION

Vehicular networks have emerged from the rapid adoption of connected and autonomous vehicles, which have revolutionized contemporary transportation systems. Examples of vehicular communications include Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Vehicle-to-Everything (V2X) (Khan et al., 2022). Because vehicular networks are becoming more complex and connected, the attack surfaces they face have increased significantly (Akazue et al., 2024), and the corresponding cybersecurity risks could jeopardise not only the privacy and integrity of data but also the physical safety of drivers and passengers (Tose et al., 2026). The dynamic nature of vehicles has brought about serious threats, exacerbated by inflexible real-time communication requirements, insufficient computational resources in embedded vehicular systems, and the safety-critical nature of automotive applications (Canh et al., 2023). Cyberattacks that plague vehicular networks could be in many different forms; denial-of-service (DoS) attacks make vital communications less effective (Akazue et al., 2023), message injection attacks introduce false information into networks (Edje et al., 2021), spoofing attacks pose as authentic vehicles or infrastructure, and replay attacks retransmit intercepted messages in order to alter system behaviour (Korium et al., 2023). Traditional IDS that works by identifying rules or signatures has become unable to continually detect evolving threat forms in automotive networks (Canh et al., 2023). Some of the challenges they face include a lack of capacity to identify new zero-day threats and high false-positive rates in dynamic vehicle situations.

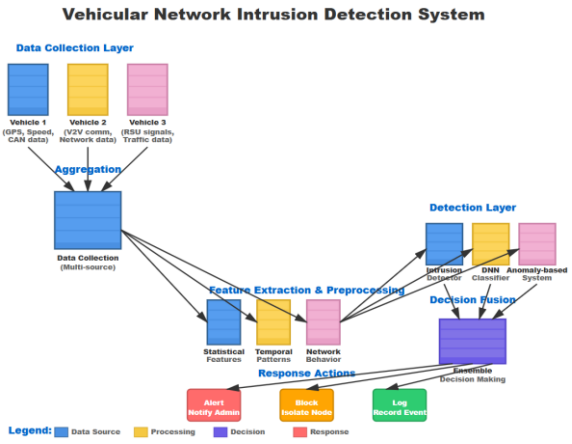

Figure 1: Vehicular Network Intrusion Detection System

Academics have undertaken investigations to develop more intelligent and adaptable solutions based on DL and machine learning (ML) algorithms (Edje et al., 2024) due to the previously mentioned constraints. DL methods automatically extract intricate patterns from unprocessed data without requiring a feature-creation technique; they have become a means for anomaly-based intrusion detection in vehicular networks, which is revolutionary (Alqahtani et al., 2022). Deep neural networks, unlike shallow ML techniques, identify complex relationships and hierarchical representations in high-dimensional network traffic data. They

detect complex attacks that span multiple protocol layers and temporal sequences (Halim et al., 2021). DL structures offers efficient results, from recent studies; autoencoders manages unsupervised anomaly detection, convolutional neural networks (CNNs) executes spatial feature extraction, recurrent neural networks (RNNs) models temporal sequences, hybrid architectures that integrate many paradigms to capitalize on their complimentary capabilities provides critical capacities, and generative adversarial networks (GANs) does adversarial learning (Ullah et al., 2022). GRUs exhibit distinct structural benefits and are renowned for vehicular network intrusion detection compared to other DL algorithms; their gating mechanism is simpler than that of Long Short-Term Memory (LSTM) networks (Tose et al., 2025). On benchmark datasets, researchers have found that GRU models achieve attractive trade-offs between detection performance and processing overhead, with detection accuracies surpassing 99% (Ma et al., 2022; Tang et al., 2024). Hybrid structures that combine CNNs and GRUs have also demonstrated advanced capabilities in extracting temporal and spatial information from network traffic, leading to lower false-positive rates and higher detection rates (Kothai et al., 2024; Wang et al., 2025). These developments suggest that GRU-based approaches offer a promising avenue for creating IDS that are practical, deployable, and capable of functioning within the resource limitations and real-time demands of vehicular networks (Tose et al., 2025).

Research Objectives

The following research goals serve as the basis for this investigation:

(1) to systematically examine state-of-the-art DL techniques used for anomaly-based intrusion detection in vehicular networks, with a focus on GRU architectures;

(2) to evaluate and contrast GRU-based models' performance against other DL architectures using standardized benchmark datasets;

(3) to determine which architectural configurations, optimization techniques, and hybrid frameworks best improve GRU detection performance;

(4) to identify existing limitations, unresolved issues, and promising avenues for future vehicular network security research.

Questions for Research

The following research questions are addressed in this study:

(RQ1) What performance levels have been attained and which DL architectures have been used for anomaly-based intrusion detection in vehicular networks?

(RQ2) In terms of detection accuracy, computational efficiency, and applicability for resource-constrained vehicular contexts, how do GRU-based models compare to other DL architectures?

(RQ3) Which hybrid configurations and optimization strategies improve GRU-based IDS' performance?

(RQ4) What are the current limitations of GRU-based IDS approaches, and what research directions could address these gaps in the context of next-generation vehicular networks?

Scope of the Study

Peer-reviewed journal papers and conference proceedings released between January 2021 and December 2025 are the subject of this review. DL-based anomaly detection systems for vehicular network environments, such as V2V, V2I, V2X, VANET, CAN bus, and Internet of Vehicles (IoV) contexts, are its primary focus. In addition to highlighting GRU architectures and their hybrid variations, the review provides a comparative analytical framework and surveys other DL techniques, including CNNs, LSTMs, autoencoders, and GANs. Excluded were studies that only addressed non-security vehicular applications and standard ML techniques without DL components. This study is intended to serve researchers and practitioners engaged in developing intrusion detection solutions for vehicular networks, connected and autonomous vehicle systems.

MATERIALS AND METHODS

This scoping survey reviews contemporary DL technologies in vehicular networks for intrusion identification, with a significant attention on the GRU approach, which is the focus of the systematic analysis.

Procedure for Review

With a focus on GRU architectures, this scoping review employed a systematic approach to identify and evaluate recent research on DL-based intrusion detection applications in vehicular networks.

Method of Searching

Numerous scholarly databases, including IEEE Xplore, ScienceDirect, Springer Link, ACM Digital Library, and Google Scholar, were searched thoroughly for relevant literature. To capture the most current developments in the subject, the search was limited to peer-reviewed journal papers and conference proceedings published between January 2021 and December 2025. Boolean operators were used in the search strategy to combine pertinent keywords, such as: ("deep learning", "neural network", "GRU", "gated recurrent unit", "LSTM" or "CNN") AND ("vehicular network", "VANET", "V2V", "V2X", "CAN bus" or "Internet of Vehicles") AND ("intrusion detection", "anomaly detection", "cybersecurity" or "attack detection").

Criteria for Inclusion and Exclusion

The following criteria were used to include studies:

(1) proposed or assessed DL models for intrusion detection in vehicular networks; (2) offered empirical results with standard performance metrics; (3) used benchmark datasets for validation; (4) were published in English; and (5) appeared in peer-reviewed venues. Excluded studies were those that: (1) addressed vehicular applications outside the realm of security; (2) lacked experimental validation; (3) were review papers, books, or grey literature; or (4) exclusively focused on classical ML algorithms without DL components.

Data Extraction and Study Selection

250 possibly pertinent items were found in the first search. 120 studies were chosen for full-text review after title and abstract screening. After the criteria for inclusion and exclusion had been applied, 70 studies were kept for more depth examination, With the intention of recording important data, such as author(s), publication year, methodology, datasets, performance metrics (accuracy, precision, recall, F1-score, false positive rate), computing needs, and important conclusions, a standardized data extraction form was created. Two independent reviewers performed the data extraction, and any conflicts were resolved by consensus.

Evaluation of Quality

Among the quality indicators were the clarity of research objectives, an appropriate methodology, the use of standard benchmark datasets, adequate model architecture and hyperparameter descriptions, appropriate train-test split procedures, comparisons with baseline methods, and thorough reporting of various performance metrics.

Synthesis Method

The results were arranged and presented using a narrative synthesis approach (Popay et al., 2006). We examined the specific approaches, datasets used, performance results, and computational factors pertinent to vehicular network environments for each DL category considered.

Covered DL Methodologies

DL-based intrusion detection addresses specific issues in vehicular network security; recent research has subdivided it into distinct structural frameworks. They are: Generative Adversarial Networks (GANs), Autoencoders (AEs), Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Hybrid Architectural Paradigms (HAPs).

***CNNs*:** Extract spatial information from network traffic data and represent it as images or matrices. CNN-based models identify intrusions in controller area network (CAN) bus traffic successfully (Aldhyani et al., 2022), and feature engineering is addressed by convolutional layers, where they automatically learn hierarchical features from raw traffic patterns while retaining computation efficiency that is appropriate for vehicle edge devices (Hossain et al., 2023).

***RNNs*:** Captures temporal patterns in sequential vehicle streams of data. Time-series communication trends are ordered and managed by LSTM networks from one vehicle to another; these networks identify flooding and message injection attacks in an organized and efficient manner (Sharma et al., 2023). Long-term dependencies are preserved by the memory cells in LSTM networks; these networks detect complex attacks at different stages that take a long time to manifest (Yang et al., 2024).

***Autoencoders*:** Reduce data dimensionality from high to low, learn them, and perform unsupervised anomaly identification. Ahmed et al. (2023) identified cases of high reconstruction errors in VANETs as anomalies by training a variational autoencoder (VAE) to reconstruct relevant communication patterns during training. Since AEs learn only from benign traffic, this method is particularly helpful in vehicle settings where labelled attack data is limited (Li et al., 2024).

***GANs*:** Use adversarial training that exists between the generator and discriminator networks to execute analysis on acquired traffic distributions and identify deviations. Zhang et al. (2023) developed a GAN-based IDS that outperforms supervised techniques for identifying zero-day attacks by training the discriminator to distinguish normal from abnormal vehicle interactions. There is no need for retraining in a fixed format; the adversarial framework supports adaptation to continually evolving attack patterns (Kumar et al., 2024).

***HAPs*:** Much of the focus of recent studies has been on hybrid algorithms that combine many DL techniques. A CNN-LSTM structure that extracts spatial features using CNNs and employs LSTMs for temporal modelling was developed by Wang et al. (2024). Their detection accuracy was 99.2%, and their FPR was low. The integration of self-attention techniques into transformer designs has demonstrated potential to capture crucial dependencies in vehicular data from multiple sources (Chen et al., 2024). Federated learning techniques solve data sovereignty issues in vehicular networks by enabling cooperative model training across dispersed vehicles while protecting privacy (Nguyen et al., 2023).

GRUs Methodical Significance

GRU data validation pipeline excels in neural network problems; it represents a profound improvement over RNN design, resolving pronounced limitations that reduce the latter's performance (Kothai et al., 2024). GRU's architecture addresses the vanishing gradient problem, a major concern in deep recurrent networks, and it performs detection with fewer parameters and lower computational overhead. Processing vast volumes of network traffic is therefore fast, which is critical for real-time attack detection. GRUs are well-suited for use in circumstances where storage and processing capabilities should be conserved; their gating mechanisms capture long-term dependencies excellently in communication patterns that may span multiple message interfaces (Almahadin et al., 2023).

Performance Metrics and Datasets

Evaluation of DL models for vehicular network intrusion detection is performed using standard metrics such as false positive rate, F1 score, accuracy, recall, and precision. The Receiver Operating Characteristic (ROC) curve, Area Under Curve (AUC), and confusion matrices are widely used to evaluate classifier performance across varying decision thresholds. Some frequently used datasets for intrusion detection research include UNSW-NB15, NSL-KDD, CICIDS2017, CICFlowmeter, CSE-CIC-IDS-2018, VeReMi, CAN-HCRL, CAN-Intrusion, Car Hacking, Network Traffic, and Road Traffic.

FINDINGS

Security plays a vital role in data transmission, as various security attacks directly affect the safety of vehicular road users. Although DL architectures yield promising outcomes, as shown in *Table 1,* recent research has demonstrated that GRU networks offer significant advantages for anomaly-based intrusion detection in vehicular environments by capturing temporal dependencies and sequential patterns in network traffic data (Tose et al., 2026). GRU has an intricate structure that is well-suited to building lightweight systems for vehicular networks and CAN IDSs in real time. A lightweight real-time IDS was designed by Ma et al. (2022) to enable deployment on embedded computing devices in vehicles. It was suitable for vehicle-mounted CAN and could perform online intrusion detection of network message data in real time, identify intrusion messages, and secure vehicle-mounted CAN. It also had deployment possibilities.

Science World Journal Vol. 21(No 1) 2026 https://dx.doi.org/10.4314/swj.v21i1.37
www.scienceworldjournal.org
ISSN: 1597-6343 (Online), ISSN: 2756-391X (Print)
Published by Faculty of Science, Kaduna State University

Figure 2: Research Timeline and Evolutionary Trend

GRU outperforms other RNNs and their combinations in terms of anomaly recognition accuracy and training cost, while also exhibiting generalization ability. Tang et al. (2024), using GRU, resolved the problems of capturing the temporal dimension's patterns and evolution within trajectory data, thereby adequately identifying the behavioural inertia of the target group. GRUs effectively detect high intrusion frequencies; when used with Gabor high-resolution feature extraction, it efficiently performed intrusion detection using high- and low-frequency data injection settings in real-world and synthetic environments (Islam et al., 2023). GRUs, when combined with other DL algorithms, possess increased capacities. They offer significant advantages in model lightweighting, making them especially suitable for real-time monitoring of vehicular network security. The GRU model developed by Wang et al. (2025) reduced the number of parameters and computational overhead for vehicular networks, making it very useful for IoV environments where resources are limited. GRU--CNN hybrid was used by Kothai et al. (2024) to solve overfitting and low-velocity problems. Their IDS protected the ad hoc network and detected several attacks, therefore safeguarding vehicle users. The results showed that the proposed model outperformed other traditional detection mechanisms. The GBiL model, comprising GRU and bidirectional LSTM (BiLSTM) networks, has shown significant effectiveness in detecting black hole attacks. Its performance was over that of conventional DL models, such as CNN, LSTM, and GRU. The major components of the methodology that helped increase intrusion detection efficiency in VANETs include feature selection and optimisation, data augmentation, a trust detection module, and real-time simulations. The model's effectiveness was notably improved by leveraging PSO methods and SMOTETomek (Shobana et al., 2025). GRU--CNN algorithm achieves high detection rates. This was demonstrated by Imrana et al. (2024) in their evaluation of the hybrid technique using the NSL-KDD and UNSW-NB15 datasets. They extracted spatial and temporal features using the algorithm, then compared their model against seven baseline algorithms on both datasets. The proposed CNN-GRU-FF model obtained the best performance in accuracy, detection rates, precision, F-score, and false alarm rates at the time. The GRU--CNN mechanism possesses strong feature-extraction capability, high detection accuracy, and a low false-alarm rate when dealing with large-scale, high-dimensional network data. This was demonstrated by Cao et al. (2022), who addressed incomplete feature extraction and general multi-classification effects that network IDSs (NIDS) suffer from.

Table 1: Comparison of Deep Learning Architectures for Vehicular Network Intrusion Detection

References	Architectural Algorithm	Temporal Modeling	Computational Cost	Edge Suitability	Typical Accuracy (%)	Datasets	Key Limitation
Wang et al. (2025). Shobana et al. (2025)	**GRU**	High	Low	High	93–99.99	HCRL-OTIDS, CIC-IDS2018, Car Hacking Datasets, SUMO, NS-3 Synthetic	Limited spatial feature extraction; limited interpretability
Khan et al. (2024). Tippannavar et al. (2023)	**LSTM**	Very High	Moderate–High	Moderate	92–99.4	Application-Layer DoS Attack Dataset, NAIST CAN dataset	High parameter count; slower training; resource-intensive for edge deployment
Saravanan et al. (2025); Salek et al. (2023)	**CNN**	Low	Low–Moderate	High	92–99.9	Car hacking dataset, CSE-CIC-IDS2018 dataset	Poor temporal dependency capture; requires input

							to be structured as images/matrices.
Kothai et al. (2024); Imrana et al. (2024)	**GRU–CNN Hybrid**	High	Moderate	Moderate–High	99.6–99.99	**Unspecified, NSL-KDD,** and **UNSW-NB15** datasets	Increased architectural complexity; harder to tune and deploy on resource-constrained devices
Xu et al. (2025); Althunayyan et al. (2024)	**Autoencoder**	Low–Moderate	Moderate	Moderate	85–97	Car-hacking and CIC-IoV 2024	Unsupervised; lower precision; no labelled attack data needed, but higher FPR
Xu et al. (2025); Mahmoudi (2025)	**GAN**	Moderate	High	Low	80–96	Framework For Misbehavior Detection (F2MD), **CICIDS2017** ,UNSW-NB15 and CSE-CIC-IDS2018dataset	Training instability; high compute; difficult real-time deployment
Umer et al. (2025); Xi et al. (2024)	**Transformer**	Very High (attention)	Very High	Low	93–99.5	UNSW-NB15, NSL-KDD, CIC-DDoS 2019 dataset	Very high memory and compute demands; limited suitability for embedded vehicular systems

Note: Edge suitability refers to deployability on resource-constrained embedded vehicular platforms.

Table 2: Comparative Performance of GRU-Based Models For (Vehicular Network) Intrusion Detection

Authors	**Problems solved**	**Model**	**Datasets**	**F1-score**	**Recall**	**Precision**	**Accuracy**
Honnappa et al., (2024)	Network attacks detection & classification	Bi-GRU_ALF-SOA	CICIDS2018	99.25	99.30	99.64	99.90
			CICIDS2019	99.26	99.52	99.90	99.91
			UNSW-NB15	98.79	98.89	98.85	99.15

Science World Journal Vol. 21(No 1) 2026 https://dx.doi.org/10.4314/swj.v21i1.37
www.scienceworldjournal.org
ISSN: 1597-6343 (Online), ISSN: 2756-391X (Print)
Published by Faculty of Science, Kaduna State University

Islam et al., (2023)	Real-world attacks detection	GRU_Gabor filter	BMW	100.00	100.00	100.00	
			KIA	100.00	100.00	100.00	
			TESLA	100.00	100.00	100.00	
Wang et al., (2025)	Real-time attacks detection	GRU_CNN	Car_Hacking	99.99	99.99	99.99	99.99
			OTIDS	99.32	99.32	99.32	99.32
			CICIDS2018	99.66	99.66	99.67	99.66
Shobana et al., (2025)	Sybil, black hole, and wormhole attacks.	GRU_Bi-LSTM	NS-3, SUMO	95.75		96.44	96.01
Imrana et al. (2024).	Network traffic analysis complexity	GRU_CNN_FF	NSL-KDD	99.68		99.68	99.86
			UNSW_NB15	98.28		98.40	99.54
Cao et al., (2022)	Low accuracy of IDS & data detection	GRU_CNN	NSL-KDD	99.70	99.69	99.65	99.69
			CICIDS_2017	99.64	99.65	99.63	99.65
Sagu et al., (2025)	DoS & BotNet attacks.	GRU_CNN	UNSW_NB15	93.69		90.94	93.37
			BoT-IoT	92.79		93.00	92.97

DISCUSSION

The findings from this scoping review make it clear that GRU networks are a highly effective architecture for detecting anomaly-based intrusions in vehicular networks. The improved performance of GRU-based models is due to their architectural efficiency in handling sequential data while maintaining computational tractability (Almahadin et al., 2023; Kothai et al., 2024). When they are combined with other DL models, they exhibit more advanced critical capacities. The results in Table 2 show high performance across several datasets, with some accuracy rates exceeding 99% in many implementations. The Bi-GRU_ALF-SOA model achieved accuracies of 99.90% on CICIDS2018 and 99.91% on CICIDS2019 when tested on benchmark datasets (Honnappa et al., 2024). This improved performance demonstrates that using optimisation algorithms such as the Artificial Life Form-Seagull Optimization Algorithm (ALF-SOA) enhances feature selection and model convergence. The integration of GRU with CNN has proven particularly advantageous for vehicular IDSs. Wang et al. (2025) reported that the GRU-CNN model they developed achieved near-perfect detection, achieving 99.99% accuracy on the Car_Hacking dataset while maintaining a lightweight design suitable for Internet of Vehicles (IoV) environments with limited computational resources. The detection rates reported by Islam et al. (2023) were a benchmark: 100% for precision, recall, and F1-score. For the BMW, KIA, and TESLA vehicle datasets, they combined GRU with Gabor filtering to develop a high-frequency intrusion detection system.

Figure 3: Problem Areas Where Attacks Have Been Detected

This performance they achieved in real-world settings suggests that GRU structures can generalize well, from the training data to novel attack vectors encountered in operational vehicular environments. GRU networks capture temporal anomalies and detect data injection attacks, which are challenging and occur frequently (Tang et al., 2024). In vehicular networks, where real-time data processing is essential, GRUs are computationally efficient. A lightweight GRU-based IDS was successfully

implemented by Ma et al. (2022) on embedded computing devices in vehicles. The model they developed supported online intrusion detection of CAN bus messages with reduced latency. The minimal parameter count of GRUs and their lower computational overhead compared to LSTM networks make them well-suited for edge computing environments with limited processing power and energy consumption (Wang et al., 2025). The effectiveness of GRU-based systems in detecting specific attack types, such as blackhole, Sybil, and wormhole attacks in VANETs, demonstrates their versatility across different threat models.

The GBiL model, developed by Shobana et al. (2025), was a hybrid of BiLSTM and GRU networks. NS-3 and SUMO simulators were used, achieving 96.01% detection accuracy. Particle Swarm Optimization (PSO) and SMOTE-Tomek techniques, used for feature optimization and data augmentation, have further enhanced detection efficiency. This addresses the class imbalance problem that intrusion detection datasets commonly face, in which normal traffic instances far outnumber attack samples. Based on GRU, there are still a few limitations in IDS that warrant careful consideration, irrespective of these developments. First, GRU might perform worse on tasks with extremely long dependency ranges, but LSTM has more intricate gating mechanisms that offer enhanced representational capacity. Though when parameter efficiency is considered, GRU performs better than LSTM (Tose et al., 2025). Second, although the datasets have been standardized, the vast majority of assessed studies relied on publicly accessible datasets (such as CICIDS2017, NSL-KDD, UNSW-NB15, and Car_Hacking) that may not adequately capture the dynamic, heterogeneous nature and real-time constraints of operational vehicular settings. The improved capacity of GRU is further explained by comparing it with other well-known DL architectures, as shown in Table 1. Transformer models perform better on tasks that require global attention across long sequences. However, they are not well-suited for embedded vehicular deployment, as they must be properly compressed due to their high memory and processing requirements. CNNs rely on pre-processing to represent traffic data as spatial structures, as they lack native temporal modelling capabilities, despite providing outstanding spatial feature extraction at low computational cost (Imrana et al., 2024). Although standard LSTMs are good at modelling temporal dependencies (Tippannavar et al., 2023), they require critically more parameters than GRU, which increases inference delay and training time. Though autoencoders have the clear benefit of operating without labelled attack data, they usually produce results with higher false-positive rates than supervised methods. GANs have demonstrated potential for zero-day attack detection through adversarial training (Zhang et al., 2023; Kumar et al., 2024), but the application of GANs with GRU architectures has not been sufficiently examined. Their high computational requirements limit their real-time application. As a result, GRU occupies a good middle ground: it has better edge deployment properties than Transformers and GANs. It offers significant temporal modelling capacity at a lower computational cost than LSTM. Adaptive learning algorithms that allow GRU-based IDS to continuously update their detection models in response to new threats without requiring full retraining should be the subject of future research. More research is needed to apply federated learning strategies to GRU-based architectures explicitly. However, methods have been proposed to enable cooperative model training among dispersed vehicles while maintaining data privacy (Nguyen et al., 2023). The reviewed studies have presented impressive quantitative performance metrics, but the attention given to explaining how GRU networks arrive at their classification decisions has been limited. Attention mechanisms and explainable AI techniques, when incorporated into model development, can enhance the transparency of GRU-based IDS. As a result, security analysts can identify the temporal patterns and features that contribute most to attack detection (Chen et al., 2024). Despite these challenges, the reviewed literature consistently demonstrates that GRU-based models achieve strong, reliable performance across diverse datasets and attack scenarios. The ongoing evolution of hybrid architectures that combine GRU with complementary DL paradigms, reinforced by optimization algorithms and robust feature engineering, continues to advance the detection capabilities and operational readiness of vehicular network IDS solutions. The examined research consistently shows that GRU-based models achieve robust, dependable performance across various datasets and attack scenarios, despite these difficulties. The detection capacity and operational preparedness of vehicular network IDS solutions are being improved by the continuous development of hybrid architectures that combine GRU with complementary DL paradigms, strengthened by robust feature engineering and optimization methods.

Conclusion

This systematic review provides exceptional results for GRU networks, indicating that these results could be replicated by other researchers who utilize GRU in their research. This is so because this approach is very effective for anomaly-based intrusion detection in vehicular networks. The studies reviewed consistently achieved accuracy rates exceeding 99% across various benchmarks and real-world datasets. This study's main contributions are as follows: first, it offers a thorough synthesis of GRU-based and related DL approaches for vehicular IDS published between 2021 and 2025; second, it presents structured comparative tables that allow direct performance comparison across models, datasets, and DL architectures; third, it provides a critical comparative analysis of GRU against LSTM, CNN, Transformer, Autoencoder, and GAN architectures, highlighting the distinct advantages and trade-offs of each; and fourth, outlining the main obstacles to future research. Despite these achievements, several drawbacks are acknowledged in this assessment. Only peer-reviewed English-language literature is included in the analysis; non-English publications and pertinent grey material were not. While the reviewed models report strong benchmark performance, independent replication and testing on proprietary or novel vehicular traffic datasets remain limited. Additionally, rather than evaluating GRU-based IDS in fully functional, real-world vehicular network deployments, most of the examined research was conducted under controlled simulation settings. There are several intriguing avenues for future research on vehicular network intrusion detection. First, privacy-preserving collaborative model training across dispersed vehicle fleets would be advanced by using federated learning frameworks tailored to GRU-based architectures. This would allow for continual improvement without centralizing sensitive traffic data. Second, by incorporating explainable AI (XAI) techniques into GRU-based IDS, the ability to interpret models would be greatly improved, allowing security operators to comprehend better changing threat trends and link detection decisions to specific temporal traffic features. Third, GRU-based models could dynamically update their detection capabilities in response to new zero-day threats without full model

retraining if adaptive, continuous learning methods were developed. Taken as a whole, these paths offer a logical research agenda for improving the dependability, transparency, and usefulness of anomaly-based intrusion detection in next-generation vehicular networks.

REFERENCES

Aidil Redza Khan; Mohd Faizal Jamlos; Nurmadiha Osman; Muhammad Izhar Ishak: "DSRC Technology in Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) IoT System for Intelligent Transportation System (ITS): A Review". January 2022. https://doi.org/10.1007/978-981-33-4597.-3_10

Akazue M., Ashie J., & Edje A. (2024). An Intelligent Fuzzy Logic Automobile Fault Diagnostic System. International Journal of Innovative Science and Research Technology. Volume 9, Issue 2. ISSN No:2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24FEB1293

Tose, E. Oziegbe, Abel E. Edje & Maureen Akazue (2026). Enhanced Gated Recurrent Unit Deep Learning Model for Vehicular Networks Anomaly-Based Intrusion Detection. FUDMA Journal of Sciences (FJS). ISSN online: 2616-1370 ISSN print: 2645 - 2944 Vol. 10 No. 2, January, 2026, pp 38 – 44. https://doi.org/10.33003/fjs-2026-1002-4351.

Thanh Nguyen Canh; Xiem HoangVan: "Machine Learning-Based Malicious Vehicle Detection for Security Threats and Attacks in Vehicle Ad-Hoc Network (VANET) Communications". Corpus ID: 267028266. https://doi.org/10.1109/RIVF60135.2023.10471804

Akazue M., Clive A., Edje A., Omede E. & Ufiofio E. Cybershield: Harnessing Ensemble Feature Selection Technique for Robust Distributed Denial Of Service Attacks Detection. KZYJC ISSN: 1001-0920 Volume 38, Issue 03, July 2023.

Edje A. E., Latiff S. M. & Chan H. W. Enhanced Non-parametric Sequence-based Learning Algorithm for Outlier Detection in the Internet of Things—Neural Processing Letters (2021) 53:1889–1919 https://doi.org/10.1007/s11063-021-10473-2.

Mohamed Selim Korium; Mohamed Sabre; Alexander Beattie; Arun Narayanan; Subham Sahoo; Pedro H.J. Nardelli: " Intrusion detection system for cyberattacks in the Internet of Vehicles environment". Ad Hoc Networks. https://doi.org/10.1016/j.adhoc.2023.103330

Omede E. U., Edje A., Akazue M. I.,Utomwen H, & Ojugo A. A. (2024). IMANoBAS: An Improved Multi-Mode Alert Notification IoT-based Anti-Burglar Defence System. Journal of Computing Theories and Applications ISSN:3024-9104. https://doi.org/10.62411/jcta.9541

Hamed Alqahtani; Gulshan Kumar: "A deep learning-based intrusion detection system for in-vehicle networks". Computers and Electrical Engineering, 2022, p. 108447. https://doi.org/10.1016/j.compeleceng.2022.108447

Abd Munim Abd Halim; Mohd Hamizan Yaacob; Muhamad Husaini; Pranesh Krishnan: "Anomaly Vehicle Detection Using Deep Neural Network". Progress in Engineering Technology III (pp.47–57), January 2021. https://doi.org/10.1007/978-3-030-67750-3_5

Safi Ullah; Muazzam A. Khan Khattak; Jawad Ahmad; William J Buchanan: "A Hybrid Deep Learning Architecture for Intrusion Detection in the Internet of Vehicles". February 2022.22(4). https://doi.org/10.3390/s22041340

Tose, E. Oziegbe, Abel E. Edje & Maureen Akazue (2025). Anomaly-Based Intrusion Detection In Vehicular Networks Using Gated Recurrent Unit Deep Learning Model-- A Systematic Review. FUDMA Journal of Sciences (FJS) ISSN online: 2616-1370 ISSN print: 2645 - 2944 Vol. 9 No. 12, December, 2025, pp 369 – 380 8. https://doi.org/10.33003/fjs-2025-0912-3993.

Ma, H., Cao, J., Mi, B., Wang, X., & Xia, X. (2022). A GRU-based lightweight system for CAN intrusion detection in real time. *Security and Communication Networks*, *2022*, Article ID 5827056. https://doi.org/10.1155/2022/5827056.

Tang, G., Zhao, H., & Yu, B. (2024). Low-cost and high-performance abnormal trajectory detection based on the GRU model with deep spatiotemporal sequence analysis in cloud computing.Journal of Cloud Computing: Advances, Systems and Applications. https://doi.org/10.1186/s13677-024-00611-1

Kothai, G., & Poovammal, E. (2024). A hybrid CNN-GRU-based intrusion detection system for secure communication in vehicular ad hoc networks. *Information Security Journal: A Global Perspective*, 34(2), 115–125. https://doi.org/10.1080/19393555.2024.2361244.

Wang, S., Cheng, J., Wang, Y., Li, S., Kang, L., & Dai, Y. (2025). ConvGRU: A Lightweight Intrusion Detection System for Vehicle Networks Based on Shallow CNN and GRU. IEEE *Access.* http://doi.org/10.1109/ACCESS.2025.3563908.

Aldhyani, T. H. H., & Alkahtani, H. (2022). Cyber security for detecting distributed denial of service attacks in agriculture 4.0: Deep learning model. *Mathematics*, 10(21), 4046. https://doi.org/10.3390/math10214046

Hossain, M. S., Rahman, A., & Islam, M. K. (2023). CNN-based real-time intrusion detection for in-vehicle networks. *Vehicular Communications*, 41, 100598. https://doi.org/10.1016/j.vehcom.2023.100598.

Sharma, R., Gupta, D., & Kumar, N. (2023). LSTM-based anomaly detection framework for V2V communication security. *Ad Hoc Networks*, 145, 103167. https://doi.org/10.1016/j.adhoc.2023.103167

Yang, Z., Liu, K., & Wei, X. (2024). Bidirectional LSTM networks for temporal attack pattern recognition in VANETs. *Journal of Network and Computer Applications*, 218, 103701. https://doi.org/10.1016/j.jnca.2024.103701.

Ahmed, S., Khan, M. A., & Rahman, M. (2023). Variational autoencoder-based anomaly detection for vehicular ad-hoc networks. *IEEE Transactions on Vehicular Technology*, 72(8), 10234–10247. https://doi.org/10.1109/TVT.2023.3267891.

Li, W., Zhao, H., & Zhang, J. (2024). Sparse autoencoder-based intrusion detection for vehicular sensor networks. *Sensors*, 24(4), 1205. https://doi.org/10.3390/s24041205.

Zhang, H., Wu, J., & Li, F. (2023). Adversarial learning for zero-day attack detection in vehicular cyber-physical systems. *IEEE Internet of Things Journal*, 10(15), 13456–13469. https://doi.org/10.1109/JIOT.2023.3265432.

Kumar, P., Singh, A., & Gupta, R. (2024). GAN-driven anomaly detection for intelligent transportation systems. *Computer Networks*, 238, 110087. https://doi.org/10.1016/j.comnet.2024.110087

Wang, L., Chen, S., & Zhou, X. (2024). Hybrid CNN-LSTM model for enhanced intrusion detection in connected vehicles. *IEEE Transactions on Network and Service Management*, 21(2), 1876-1890. https://doi.org/10.1109/TNSM.2024.3367892.

Chen, Y., Liu, X., & Wang, H. (2024). Transformer-based intrusion detection for connected and autonomous vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 25(3), 2341–2355. https://doi.org/10.1109/TITS.2024.3358721

Nguyen, T. D., Pham, C., & Le, A. (2023). Federated learning for privacy-preserving intrusion detection in vehicular networks. *IEEE Access*, 11, 89234–89248. https://doi.org/10.1109/ACCESS.2023.3304521

ALMahadin, G., Aoudni, Y., Shabaz, M., Agrawal, A. V., Yasmin, G., Alomari, E. S., Al-Khafaji, H. M. R., Dansana, D., & Maaliw, R. R. (2023). VANET Network Traffic Anomaly Detection Using GRU-Based Deep Learning Model. *IEEE Transactions on Consumer Electronics*, 69(4), 1128–1139. https://doi.org/10.1109/TCE.2023.3326384.

Islam, M.R., Sahlabadi, M., Kim, K., Kim, Y., & Yim, K. (2023). CF-AIDS: Comprehensive Frequency-Agnostic Intrusion Detection System on In-Vehicle Network. IEEE VEHICULAR TECHNOLOGY SOCIETY SECTION, http://doi.org/10.1109/ACCESS.2023.3346943.

Shobana, G., Nathan, A. T., Sivakumar, D. S., & Annie, R. A. X. (2025). GBiL: A hybrid gated recurrent units (GRU) and bidirectional long short-term memory (BiLSTM) model with Particle Swarm Optimization for a Robust VANET IDS. EURASIP Journal on Wireless Communications and Networking. https://doi.org/10.1186/s13638-025-02467-8.

Imrana, Y., Xiang, Y., Ali, L., Noor, A., Sarpong, K., & Abdullah, M. A. (2024). CNN-GRU-FF: a double-layer feature fusion-based network intrusion detection system using a convolutional neural network and gated recurrent units. *Complex & Intelligent Systems*, 10(3), 3353–3370. https://doi.org/10.1007/s40747-023-01313-y.

Cao, B., Li, C., Song, Y., Qin, Y., & Chen, C. (2022). Network intrusion detection model based on CNN and GRU. *Applied Sciences*, 12(9), Article 4184. https://doi.org/10.3390/app12094184.

Wang, S., Cheng, J., Wang, Y., Li, S., Kang, L., & Dai, Y. (2025). ConvGRU: A Lightweight Intrusion Detection System for Vehicle Networks Based on Shallow CNN and GRU. IEEE Access. https://doi.org/10.1109/ACCESS.2025.3563908

Khan, F. M., Rahman, T., Zeb, A., Haider, Z. A., Khan, I. U., Bilal, H., Khan, M. A., & Ullah, I. (2024). Vehicular Network Security Through Optimized Deep Learning Model with Feature Selection Techniques. ICCK Transactions on Sensing, Communication, and Control, 1(2), 136–153. https://doi.org/10.62762/TSCC.2024.626147

Tippannavar, S. S., Vanditha M., & Prerana N. (2023). Smart Intrusion Detection System for CAN Network Implemented using LSTM Strategy. International Journal of Innovative Research in Advanced Engineering. Volume 10, Issue 03, pages 98–105. ISSN: 2349–2163. https://doi.org/10.26562/ijirae.2023.v1003.08

Saravanan, R., Balaji, S., Ganesan, M., et al. (2025). An optimal attention deep learning based in-vehicle intrusion detection and classification model on CAN messages. Scientific Reports, 15, 33952. https://doi.org/10.1038/s41598-025-10637-3

Wang, Z., & Ghaleb, F. A. (2023). An Attention-Based Convolutional Neural Network for Intrusion Detection Model. IEEE Access. https://doi.org/10.1109/ACCESS.2023.3271408

Xu, H., Fang, L., Dong, J. *et al.* An efficient vehicular network anomaly detection framework based on an encoder and dynamic threshold adjustment. *Peer-to-Peer Netw. Appl.* **18**, 265 (2025). https://doi.org/10.1007/s12083-025-02093-7

Althunayyan, M., Javed, A., & Rana, O. (2024). A robust multi-stage intrusion detection system for in-vehicle network security using hierarchical federated learning. Vehicular Communications, 49, 100837. https://doi.org/10.1016/j.vehcom.2024.100837

Bingfeng Xu, Jincheng Zhao, Bo Wang, Gaofeng He (2025). Detection of zero-day attacks via sample augmentation for the Internet of Vehicles. Vehicular Communications. Volume 52. https://doi.org/10.1016/j.vehcom.2025.100887

Mahmoudi, I.; Boubiche, D.E.; Athmani, S.; Toral-Cruz, H.; Chan-Puc, F.I. Toward Generative AI-Based Intrusion Detection Systems for the Internet of Vehicles (IoV). *Future Internet* **2025**, *17*, 310. https://doi.org/10.3390/fi17070310

Umer, M., Tahir, M., Sardaraz, M., et al. (2025). Network intrusion detection model using wrapper-based feature selection and multi-head attention transformers. Scientific Reports, 15, 28718. https://doi.org/10.1038/s41598-025-11348-5

Xi, C., Wang, H., & Wang, X. (2024). A novel multi-scale network intrusion detection model with a transformer. Scientific Reports, 14, 23239. https://doi.org/10.1038/s41598-024-74214-w