FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 9 No. 12, December, 2025, pp 369 – 380
DOI: https://doi.org/10.33003/fjs-2025-0912-3993

ANOMALY-BASED INTRUSION DETECTION IN VEHICULAR NETWORKS USING GATED RECURRENT UNIT DEEP LEARNING MODEL-- A SYSTEMATIC REVIEW

***[1]Tose E. Oziegbe, [1]Abel E. Edje and [1]Maureen Akazue**

[1]Department of Computer Science, Delta State University Abraka, Nigeria.

*Corresponding authors' email: toseoziegbe@gmail.com

ABSTRACT

Intelligent transportation systems (ITS) have been revitalized by the rapid growth of vehicular networks, namely Vehicular Ad Hoc Networks (VANETs), which have accelerated real-time vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) interactions. However, the progressive and interconnected qualities of these networks create major cybersecurity complications that typical traditional solutions cannot properly handle. Through a survey of peer-reviewed research, this systematic literature review investigates the application of Gated Recurrent Unit (GRU) deep learning architectures for anomaly-based intrusion detection within automotive networks, examining peer-reviewed studies that were released between 2021 and 2025. With an emphasis on GRU implementation, the paper divides deep learning (DL) approaches into five primary categorization divisions: Generative Models, Feed-Forward Neural Networks (FFNN), Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Deep Reinforcement Learning (DRL). Through intricate analysis, this study shows that GRU models are ideally suited for intrusion detection in vehicular networks, capturing temporal connections in contrast to conventional Long Short-Term Memory (LSTM) networks. Findings show that GRU techniques are notably effective at detecting a variety of attack types, such as DoS, fuzzing, spoofing, and impersonation attacks, while preserving low false positive rates (FPR) and computational complexity suitable for real-time deployment in vehicular environments with limited resources. GRU models have continuously outperformed conventional methods in evaluation measures like as accuracy, precision, recall, F1-score, and False Alarm Rate (FAR). According to the review's findings, GRU-based anomaly detection is a viable strategy for achieving vehicle network security with notably optimized efficiency.

Keywords: Gated Recurrent Unit (GRU), Vehicular Ad Hoc Networks (VANETs), Intrusion Detection System (IDS), Anomaly Detection, Deep Learning, Intelligent Transportation Systems (ITS), Recurrent Neural Networks (RNN), Cybersecurity, Controller Area Network (CAN), Real-time Detection

INTRODUCTION

In ITS, the rise of vehicular networks has ushered in a revolutionary era when road safety, traffic management, and growing energy problems are all extensively addressed. According to Ahmad et al., (2024), VANETs allow vehicles to communicate with roadside infrastructure (V2I) as well as with one another (V2V). VANETs are essential for enabling driverless vehicles, smart city projects, and advanced driver assistance systems (ADAS) by facilitating real-time data sharing. However, as automotive networks become more sophisticated and interconnected, they are vulnerable to a variety of security risks, according to Johnson et al., (2024). There are several difficulties in protecting VANETs against cyberattacks because of their intrinsic features. Conventional security measures, such as encryption and firewalls, frequently fall short in identifying complex threats that can evade conventional defences. According to Zhang et al., (2024), there is a growing need for advanced intrusion detection systems (IDS) that can monitor network traffic, identify irregularities, and spot any security breaches. Anomaly-based intrusion detection techniques, which focus on identifying departures from typical patterns of behavior, have drawn significant interest as the best strategy. This approach is based on the idea that attacks will cause observable departures from typical network behavior. According to Patel et al. (2024), one admirable DL model for anomaly detection is the GRU, a kind of recurrent neural network (RNN) that consumes sequential input and learns temporal connections. GRUs effectively detects unusual patterns in vehicle networks when they are improved with cutting-edge methods like domain-specific adjustments or hybrid architectures. In order to take use of GRU's ability to handle time-series data, improve detection accuracy, and reduce false positives, this study presents GRU model for anomaly-based intrusion detection in automotive networks. Additionally, GRUs outperform other RNN variations in terms of computing efficiency, such as LSTM networks, which makes them particularly well-suited for real-time anomaly detection in resource-rich contexts like vehicular networks (Thompson et al., 2024). Among the many benefits of anomaly-based IDS is their ability to detect previously unidentified attacks without relying on previously established attack signatures, which makes them more flexible and appropriate for spotting new, zero-day threats. Specifying Vehicle mobility and the transmission of various data kinds make static rule sets difficult. Anomaly-based IDS are able to identify minute variations that can indicate attacks by continuously learning from typical network activity, Lee et al., (2025). According to Edje et al., (2023), algorithms are fundamental computing processes that allow machine learning (ML) systems to identify patterns in data and generate predictions. They optimize mathematical algorithms that reduce prediction mistakes in order to convert raw data into meaningful models (Edje et al., (2021). The choice of algorithm has a considerable impact on a model's accuracy, training speed, and capacity to generalize to new data (Agboi et al., 2024). For instance, neural networks are very good at recognizing complicated patterns. Different algorithms are better suited for different sorts of problems.

Related Works

Significant innovations has been utilized in vehicular IDS research by Graph Neural Networks (GNN). In order to find correlations between network traffic changes and upgrade detection accuracy, Xiao et al. (2022) used a GNN architecture with Control Area Network Graph Attention Networks (CAN-GAT). Although this method produced encouraging results in identifying important network connections, it had drawbacks when it came to handling fixed point counts and high computing complexity. Various academics have concentrated on obtaining lightweight and optimal IDS solutions in order to identify computational limits in vehicle contexts. Wang et al., (2025) suggested a lightweight intrusion detection system that combines shallow CNN and GRU. It is specifically made for VANET real-time monitoring and offers significant advantages in model optimization. Binarized Neural Networks (BNN) were used by Zhang et al., (2022) to improve in-vehicle network intrusion detection while lowering power consumption, detection delay, and memory needs. In contrast to full-precision networks, this method required trade-offs between representational capacity and accuracy. Using straightforward RNN algorithms, Kristianto et al., (2023) developed a lightweight and sustainable domain-based intrusion detection system that acquired in-vehicle network training with a reduced memory footprint and compute resources. These methods show continuous attempts to strike a compromise between realistic deployment constraints and detection efficiencies. The use of GANs in vehicle IDS is a new area of study. Deng and associates (2022) developed N-GAN, a revolutionary anomaly-based network IDS that uses GAN and outperforms baseline models in both particular attack class identification and general anomaly detection. Chen et al., (2021) achieved real-time detection capabilities with noteworthy comprehensive performance by implementing Auxiliary Classifier GANs (ACGAN) for CAN network intrusion detection. However, when training several network components at once becomes sophisticated, GAN-based methods encounter training stability issues. Recognizing that single-technique approaches would not adequately meet contemporary vehicle security threat convolutions is reflected in the development toward hybrid systems. Numerous studies have looked into hybridizing different DL architectures to capitalize on their complementing advantages. In order to successfully resolve the complexity of encryption and authentication attacks, Lo et al., (2022) developed the CNN-LSTM hybrid technique for spatial-temporal representation of in-vehicle network data. However, scarce data and optimization issues brought on by architectural complexity resulted in performance decrease in their model. Important ensemble techniques have been investigated in recent work. Using feature fusion and stacking-based ensemble learning, Alqahtani et al., (2022) created an IDS-IVN system that demonstrated enhanced detection capabilities for in-vehicle network traffic. An adaptive learning factor-based sandpiper optimization algorithm fused with Bi-GRU was proposed by Honnappa et al. (2024), demonstrating favorable efficiency while reducing computational convolution. Temporal dependencies in automotive network traffic can be effectively captured by LSTM networks and their variants. Yu et al., (2022) successfully determined the validity of emergency messages by using LSTM in false message detection for time series classification for VANETs. However, their methodology demonstrated susceptibility to overfitting and lengthy sequences that are difficult. In the field of vehicle intrusion detection research, CNN has emerged as a leading methodology. Numerous research have shown how successful CNN is at removing spatial details from network traffic data. Hu et al., (2022) presented the mosaic-coded CNN technique, which enhanced discrimination and reliability capability while satisfying real-time detection needs for vehicular networks. When compared to LSTM, GRU-based algorithms are more computationally efficient while yet achieving comparable results. In order to achieve low false alarm rates and effective feature extraction capabilities, Almahadin et al., (2023) implemented a GRU-based DL model for VANET anomaly detection. Hybrid GRU techniques have produced noteworthy results. For example, Islam et al., (2024) used GRU algorithms to create a comprehensive frequency-agnostic intrusion detection system that demonstrated remarkable performance in high-frequency intrusion detection.

MATERIALS AND METHODS

This study used a systematic literature review (SLR) methodology in accordance with accepted standards (Kitchenham, 2004). One kind of literature review that compiles and evaluates a variety of research projects or publications in a specific field is called a systematic analysis. The following inquiries are the focus of the study:

RQ1: According to anomaly-based intrusion detection in vehicular networks, which DL implementation techniques have been applied?

RQ2: What are deep learning algorithms' advantages and disadvantages?

RQ3: Which IDE environments, benchmark datasets, and programming languages are most frequently utilized for VANET IDS?

RQ4: Which assessment measures are most important for GRUs and which have been applied to deep learning approaches?

RQ5: What are the main infiltration issues that GRU specifically addresses in vehicle networks?

To address each study issue, a comprehensive comprehensive literature review (SLR) was conducted. For RQ1, we examined each paper's overall context in relation to the implementation strategy it suggested. We described the intrusion detection techniques employed in each paper. We examined each paper's accomplishments and any unmet needs for RQ2. We examined commonly used programming languages, IDEs, benchmark datasets, and assessment criteria for VANET IDS while taking RQ3 and RQ4 into account. We categorized deep learning algorithms into five groups: CNN, RNN, FFNN, DRL, and generative models.

RESULTS AND DISCUSSION

The SLR produced 35 publications that were further categorized by titled deep learning approaches, as well as by issues addressed, methods, accomplishments, gaps, measurements, tools, and benchmarks. The diagram in figure 2 illustrate types of DL distribution.

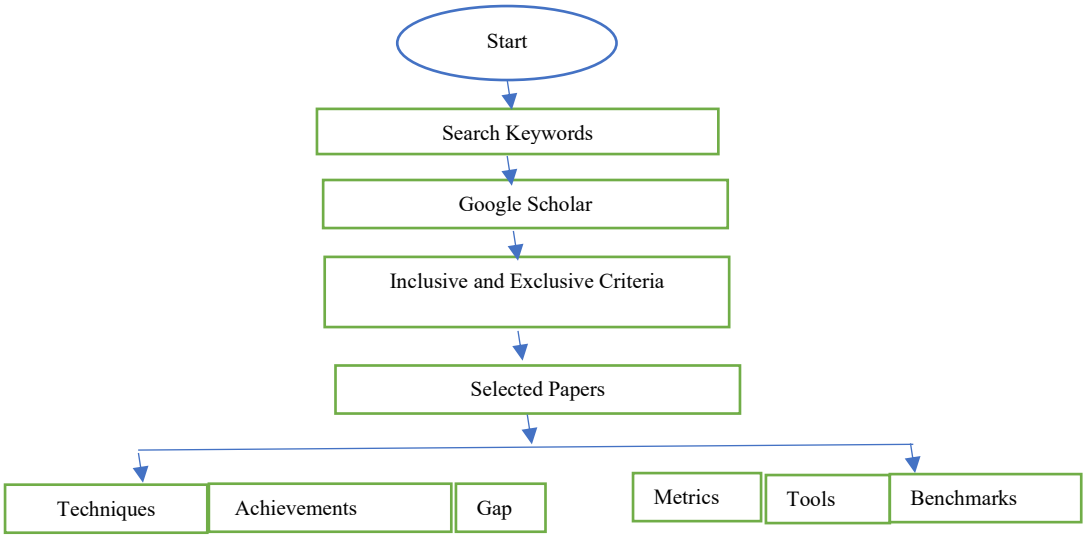

Figure 1: Research Methodology

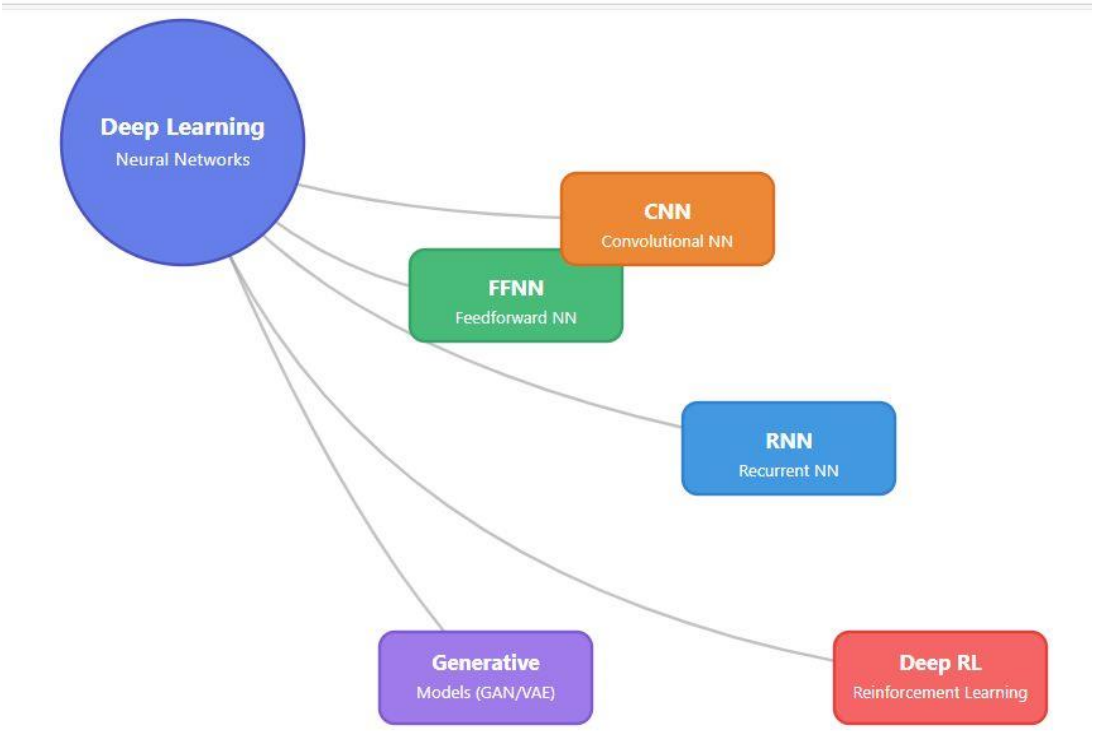

Figure 2: Deep Learning Techniques Distribution (Lecun et al 2015)

Table 1: Comparative Performance of Generative Models for Intrusion Detection in Vehicular Networks

References	Problem	Techniques	Achievement	Weakness	Metrics	Tools	Benchmark
Nabil et al., (2024). Securing VANETs: Multi-Objective Intrusion Detection With Variational Autoencoders (VAE)	Criticality of diverse and evolving nature of potential VANETs threats.	VAE Algorithm, AGE-MOEA Algorithm, R-NSGA-III Algorithm.	Captures and analyzes broadcast vehicular data sequences.	Intricacy of unrealistic generated outputs, mode collapse and training instability.	Precision, Recall, Accuracy.	Python IDE and Programming Language	Car-Hacking Dataset, ROAD Dataset.
Chenyun et al., (2024). Vehicle Network Intrusion Detection Based on K-nearest Neighbor VA Using Contrastive Learning	Lack of information encryption and message authentication in CAN.	VAE Algorithm.	Detects DoS, Fuzzy, gear, and RPM vehicular network attacks.	Complexity of computation for large datasets.	Accuracy, Precision, F1-score	Python IDE and Programming Language	Car-Hacking Dataset.
Junman et al., (2024). GPIDS: GAN Assisted Contextual Pattern-Aware IDS for IVN	Convolution of extra bandwidth and computational resources utility	GAN Algorithm	Effectively addressed SOME (Same Origin Method Exécution) attacks.	Criticality of training Instability: and generator/ discriminator imbalance.	Precision, Accuracy, F1-score		CIC-IDS2018, NSL-KDD Datasets.
Pradeep et al., (2024). Anomaly Detection in IoV CAN Bus Traffic Using Variational Autoencoder-LSTM with Attention Mechanism	Complication in transmitting data between ECUs in in-vehicle networks due to various cyberattacks.	VA Algorithm, LSTM Algorithm.	Strong detection of unusual behaviour and flexible IoV cybersecurity solution.	Complexity of computation for large dataset	F1-score, Accuracy, Recall, Precision.	Python IDE and Programming Language	CICIoV2024 Dataset.
Abizar et al., (2024). Artificial Intelligence-based intrusion detection system for V2V communication in VANETs.	Vehicular communications are susceptible to a number of attacks, especially when they occur between vehicles (V2V).	Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) Algorithm and BiGAN Algorithm	Demonstrates superior performance compared to traditional methods.	Convolution of training Instability: due to generator and discriminator imbalance.	F1-score, Precision, Accuracy.	Python IDE and Programming Language	NSL-KDD Dataset.
Wei et al., (2024). Research on the Intrusion Detection Methods of Automotive Networks Based on GAN	Complication of interactions between vehicle's interior and external network.	GAN Algorithm	Optimized detection of malicious intrusive attacks.	Difficulty in learning discrete data.	Accuracy, Recall, F1-score	Python IDE and Programming Language	NSL-KDD Dataset.

Table 2: Comparative Performance of Deep Reinforcement Learning for Intrusion Detection in Vehicular Networks

References	Problem	Techniques	Achievement	Weakness	Metrics	Tools	Benchmark
Shitong et al., 2024. A DRL-based intelligent QoS optimization algorithm for efficient routing in VN	Intricacy of inter-vehicle communication mgt and improvement of network efficiency.	Deep Reinforcement Learning-Based Intelligent QoS (DRLIQ) Algorithm.	High-speed efficient mgt of vehicular movements and changing network topologies.	Criticality of Interpretability challenges and computational constraints.	BER, Network Delay, Error Rate, Transmission Rate.		CSE-CIC-IDS2018 Datase
Yoon et al., (2024). Intrusion response system for in-vehicle networks: uncertainty-aware DRL-based approach.	Lacking authentication, authorization & crypto- graphic protection mechanisms.	Deep Reinforcement Learning (DRL) Algorithm.	Optimal defense strategic response, maximizing defense utility.	DRL stationary environments assumption, leading to localized performance outcomes.	F1-score, Precision, Accuracy.	Python IDE and Programming Language	UNSW-NB15 Dataset.
Roshan et al., (2024). DRL-Based Adversarial Defense in Vehicular Communication Systems.	Complexity of adversarial attacks, causing trained models to exhibit undesirable behaviors.	Deep Reinforcement Learning (DRL) Algorithm.	Label-flipping and policy induction best defenses.	Limited training VANETs data, as success of DRL models depends on large amounts of labeled data.	False Positive Rate (FPR), Precision, F1-score.		NSL-KDD Dataset.
Rukhsar et al., (2024). Intelligent defense strategies: Comprehensive attack detection in VANET with DRL.	Messages sent between cars are susceptible to a number of security risks.	DRL Algorithm	Efficient security solutions, protecting network from various security threats across different VANET contexts	High computational overhead and training complexity.	Accuracy, Precision, F1-score.	Python IDE and Programming Language	VeReMi Dataset.
Pratima et al., (2023). An improved deep reinforcement learning routing technique for collision-free VANET.	Convolution of excessive control overhead and routing complexity in VANETs.	Improved DRL (IDRL) Algorithm.	Decreased latency, increased packet delivery ratio, and improvement in data reliability.	Crucial need to include anonymity, mutual authentication, and intractability, to reduce complexities.	Packet Delivery Ratio (PDR), velocity of vehicles, density of vehicles, range of transmission, and delay in network	Python IDE and Programming Language	Network Simulator (NS-2.35)
Boshra et al., (2024). A Micro Reinforcement Learning architecture for Intrusion Detection System.	Criticality of biinary and multiclass intrusion classi-fications.	DRL Algorithm	Fine-grained enhanced performance of binary and multiclass intrusion classi-fication.	Applied only on local scope of minimal search space.	Precision, F1-score, Recall	Python IDE and Programming Language	NSL-KDD, CIC-IDS2018, and UNSW-NB15 Datasets

Table 3: Comparative Performance of Feed Forward Neural Networks (FFNN) for Intrusion Detection in Vehicular Networks

References	Problem	Technique	Achievement	Weakness	Metrics	Tools	Benchmark
Anyanwu et al., (2023). RBF-SVM kernel-based model for detecting DDoS attacks in SDN integrated vehicular network.	Because of its centralized design, VANETs are vulnerable to attacks, creating risky situations.	RBF Algorithm. SVM Algorithm.	Approximation of difficult functions and relationships	Limited ability to handle nonlinearities, compared to more advanced techniques like DNN	Accuracy, Mean Absolute Error (MAE), Precision.	Python IDE and Programming Language	NSL-KDD Dataset.
Saranya et al., (2024). Efficient Development of Intrusion Detection Using Multilayer Perceptron Using Deep Learning Approaches.	Criticality of intrusive network activities by illegitimate users.	R-SVM Algorithm, Adaptive Boosting Algorithm and MLP Algorithm	Complex layered data structure resolution	Inaccurate intrusion detection due to susceptibility to noisy or data	Precision, Accuracy, F-Measure, Recall	Jupiter Notebook, Python	NSL-KDD Dataset
Prashant et al., (2024). Advanced Intrusion Detection in VN: Empowering Security through Hybrid Off-loading Techniques and Enhanced RBNN.	Complexity of Intrusion detection in vehicular networks.	Hybrid Offloading Algorithm. Radial Basis Neural Network (RBNN) Algorithm.	Detection of DDoS and Replay attacks, Intrusions and other assaults.	Training difficulty in selecting right parameters which is computationaly expensive.	Specificity, Recall, F1-score, Accuracy, Precision.	Python IDE and Programming Language	UNSW-NB15 Dataset
Rohit et al., (2024). Feature Selection Using COA with Modified FFNN for Prediction of Attacks in Cyber-Security.	Complication of network intrusion detection, prediction, and mitigation systems.	Crayfish Optimization Algorithm (COA), FFNN Algorithm	Introduced COA for features selection from cybersecurity datasets.	Limited generalization due to shallow architecture.	Precision, Accuracy,	MATLAB IDE and Programming Language	NSL-KDD Dataset
Arnaud et al., (2021). Multi-layer perceptron for network intrusion detection.	Intricacy of Intrusion attacks in the network system.	MLP Algorithm.	Critical layered resolution of data structures	Require large datasets: a lot of labeled data needed to train effectively.	Accuracy, False Positive Rate (FPR), Précision.	Python IDE and Programming Language	CSE-CIC-IDS2018, CIC-IDS2017.
Ahmed et al., (2022). Improved DDoS Detection Utilizing DNN and FFNN as Autoencoder.	Under-coverage of attack diversity and classification aspects.	DNN Algorithm. FFNN Algorithm.	Hybrid IDS model for detecting DDoS attacks SDN environments.	Scalability Issues, as VANETs generate massive amounts of data	F1-score, Precision, Accuracy, Recall.	Not specified	ISCX-IDS-2012, UNSW2018

Table 4: Comparative Performance of Convolutional Neural Network (CNN) for Intrusion Detection in Vehicular Networks

Authors	Problems	Techniques	Achievements	Weakness	Metrics	Tools	Benchmarks
Alsaleh et al., (2024). A Novel Intrusion Detection Model of Unknown Attacks Using CNN	Increasing network intrusions and need for advanced security models.	CNN Algorithm.	Higher detection accuracy compared to traditional detection methods.	Prone to overfitting with small dataset or that which lacks diversity.	Accuracy, F-Measure, Recall	Python IDE and Programming Language.	AWID datasets.
Hyungchul et al., (2024). TinyML-Based Intrusion Detection System for In-Vehicle Network Using CNN on Embedded Devices.	Existing models' high computing requirements make them unsuitable for deployment on low-power embedded devices.	CNN Algorithm	Requires considerably less computational load, provides superior detection performance.	Intricacy of handling sequential or time-series data or temporal patterns of network traffic.	F1-score, Precision, Accuracy.	Python IDE and Programming Language	NSL-KDD Dataset
Saima et al., (2025). Enhancing network security: an IDS using residual network-based CNN.	Scalability, manual feature extraction complexities and IDS attack types intricacy.	ResNet-CNN Algorithm.	Enhanced feature extraction and detection of evolving and diverse IDSs attack types.	Optimal classification features complexity.	Accuracy, Recall, Precision.	Python IDE and Programming Language	NSL-KDD Dataset.
Wu et al., (2025). ResNet-Swin Transformer based intrusion detection system for in-vehicle network	Convolution of diverse complex attack types in in-vehicle network (IVN)	Swim Transformer (SR) Algorithm, ResNet Algorithm.	Enhanced detection capability for diverse attack types.	Complex ResNet architectures, requiring careful design to prevent vanishing or gradients issues	True Positive Rate (TPR), Accuracy,	Python IDE and Programming Language	HCRL Survival Analysis Dataset.
Amit et al., (2024). Attention-CNN-LSTM based intrusion detection system (ACL-IDS) for in-vehicle networks.	Intricacy of inadequate extraction of network traffic features' dependencies in a time-series context by existing IDSs.	CNN Algorithm.	Collects network traffic's short- and long-term dependencies in an efficient manner.	Prone to overfitting, especially when trained on limited or imbalanced datasets	Accuracy, False Positive Rate (FPR), Precision.	Python IDE and Programming Language	NSL-KDD Dataset.
Luo et al., (2025). An anomaly detection model for in-vehicle networks based on lightweight convolution with spectral residuals.	Intricacy of embedded device resources and model complexity.	Spectral Residuals (SR) Algorithm, Depth-Separable CNN (DSCNN)	Reduced congestion in the computation pipeline and optimized resource usage	Criticality of attaining balance between accuracy and complexity.	True Positive Rate (TPR), Accuracy, Precision.		SynCAN Dataset, ROAD Dataset.

Table 5: Comparative Performance of Recurrent Neural Networks (RNN) for Intrusion Detection in Vehicular Networks

Authors	Problems	Techniques	Achievements	Weakness	Metrics	Tools	Benchmarks
Njud et al., (2024). Hybrid RNN-LSTM Networks for Enhanced Intrusion Detection in Vehicle CAN Systems	Convolution of DoS, Fuzzy, and Impersonation attacks in CAN.	RNN Algorithm, LSTM Algorithm	Improved electric vehicle cyber security setup against DoS, fuzzy, and impersonation attacks.	Intricate need secure vehicles with a safe, reliable, and resilient automotive future.	F1-score, Recall, Precision.	Python IDE and Programming Language	CAN Dataset (OTIDS)
Kishore et al., (2024). Intelligent Intrusion Detection Framework for Anomaly-Based CAN Bus Network Using Bidirectional LSTM.	Vulnerability due to DoS, Fuzzing, spoofing attacks due to lacking authentication/ authorization protocols.	Bidirectional LSTM (Bi-LSTM) Algorithm.	Intrusion detection with improved accuracy, outperforming traditional approaches.	Prone to overfitting, especially when trained on limited or imbalanced datasets.	Precision, Accuracy, F-Measure.		NSL-KDD Dataset.
Zhao et al., (2024). CAN Intrusion Detection System Based on Data Augmentation and Improved Bi-LSTM.	Susceptibility of CAN protocol to various cyber attacks due to its openness and lack of security measures.	ADASYN Algorithm, Bi-LSTM Algorithm.	Self-attention mechanism capturing CAN critical information, enhanced detection	Not enough generalization on novel or zero-day attacks if not trained on diverse enough data, limiting their real-world effectiveness.	Recall, F1-score, Precision, Accuracy.	Python IDE and Programming Language	
Hongyun et al., (2024). Intrusion Detection System for Vehicle Network based on Embedded Convolutional LSTM.	Complexity of unattended CAN message-to-message's time sequence and data frames continuity.	CNN Algorithms, LSTM Algorithm.	Increased evaluation metrics performance.	Prone to overfitting, especially when trained on limited or imbalanced datasets.	Recall, F1-score, Accuracy, Precision.		In-vehicle CAN Datasets.
Ying et al., (2025). UGL: A comprehensive hybrid model integrating GCN and LSTM for enhanced intrusion detection in UAV controller area networks.	Significant obstacles face UAV networks, such as low information density and fewer electronic components.	Graph Neural Network (GNN) Algorithm, LSTM Algorithm.	improves detection performance and information density in UAV internal CAN networks in an efficient manner.	Intrusion detection latency, which is critical in safety-centric vehicular applications.	Precision, F1-score, Accuracy, Recall.	Python IDE and Programming Language	Car-Hacking Dataset.
Li et al., (2024) HP-LSTM: Hawkes Process–LSTM-Based Detection of DDoS Attack for In-Vehicle Network	DDoS assaults on in-car networks are critical, causing driving assistance systems to malfunction and impairing vehicle control features.	Hawkes Process Algorithm, LSTM Algorithm.	Surpass the original LSTM model in detection accuracy, thereby evidencing enhanced performance	Critical need to expand scope to include DoS and man-in-the middle attacks, for wider range of attack detection scenarios.	Precision, F1-score, Recall, Accuracy.		Simulated Datasets.

Table 6: Gated Recurrent Unit and Hybrid Models for Intrusion Detection in Vehicular Networks

Authors	Resolved Gaps	Methodology	Contribution	Evaluation Paramters	Programming Paradigm	Benchmark
Almahadin et al., (2023). VANETs Network Traffic Anomaly Detection Using GRU Based DL Model	Crucial need to detect DoS floods and cyber assaults with the rise of Vehicular Ad-hoc Networks (VANETs).	SMOTE Algorithm, Multi-year Bidirectionnel GRU (MLB-GRU) Algorithm.	Outperforms existing methods in detecting network anomalies with low false positive rates.	False Alarm Rate (FPR), Accuracy, F1-score, Precision, Recall.		NSL-KDD Dataset.
Haoyu et al., (2022). A GRU-Based Lightweight System for CAN Intrusion Detection in Real Time.	Criticality of security risks in vehicular networks, potentially catastrophic, due to communication loopholes	GRU Algorithm.	Successfully deployed the IDS in embedded computing in-vehicle devices.	Precision, F1-score, Recall	Python IDE and Programming Language	Publicly Available Datasets
Wang et al., (2025) ConvGRU: A Lightweight Intrusion Detection System for Vehicle Networks Based on Shallow CNN and GRU	Complication of ensuring real-time detection and efficient deployment in vehicular networks.	Shallow CNN-GRU Algorithm	ConvGRU shows significant advantages in terms of model lightweighting, making it especially suitable for real-time monitoring of VANETs	F1-score, Accuracy, Precision, Recall.	Python IDE and Programming Language	HCRL-OTIDS, CIC-IDS2018, Car Hacking Datasets.
Islam et al., (2024). CF-AIDS: Comprehensive Frequency-Agnostic Intrusion Detection System on In-VN	Critical significat need of different intensive packet injection techniques as existing IDSs are vulnerable or failing to detect real-world attacks.	GRU Algorithm	IDS detects high-frequency intrusions effectively, with exceptional performance in Gabor high-resolution feature extraction	ROC-AUC, Accuracy, Precision, F1-score, Recall		HCRL Dataset, BMW, Kia, Tesla Datasets
Shobana et al., (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	VANET security threats including Sybil, black hole, and wormhole attacks, where malicious nodes manipulate network communication.	GRU, Bi-LSTM, PSO Algorithms.	Signifcant efectiveness in detecting blackhole attacks, outperforming conventional deep learning models, such as CNN, LSTM, and GRU.	False Alarm Rate (FAR), Precision, Accuracy.	Python IDE and Programming Language.	SUMO, NS-3 Synthetic Datasets
Zhao et al., (2024). CAN IDS Based on Data Augmentation and Improved Bi-LSTM.	Inability for time series applications to meet real-time requirements with large resources.	GRU Algorithm, Dynamic Label Watermark (DLW) Algorithm.	Performs better when compared with traditional techniques.	F1-score, Accuracy, Recall, Precision.	Python IDE and Programming Language	NSL-KDD Dataset.
Kothai et al., (2024). A hybrid CNN-GRU-based intrusion detection system for secure communication in vehicular adhoc network.	Convolution of overfitting and low-velocity problems in VANETs and data transmission disruption.	Convolutional Neural Network (CNN)/ Gated Recurrent Unit (GRU) -- Algorithms.	Overfitting and low-velocity problems resolution.	Precision, Recall, F1-score, Accuracy.	MATLAB IDE and Programming Language.	Unspecified.

Discussion

Discussion on RQ1: One kind of RNN that falls under the DL distribution category is the GRU. CNN, FFNN, DRL, and Generative Models are other DL divisions. Vehicle networks have employed these techniques for intrusion detection. We discovered that among the chosen publications, the following were suggested: generative model approaches; DRL techniques; FFNN methods; CNNs; and RNN methodologies. As needed by the specific problem being tackled, several of the DL techniques were hybrids, combining various DL algorithms for increased efficiency. In automotive network systems, GRU tackles issues with memory efficiency, real-time processing, dynamic network topology, multi-dimensional feature learning, and sequential pattern recognition.

Discussion on RQ2: The review highlights a number of accomplishments made possible by the use of DL models, such as the following: the ability to capture and analyze broadcast vehicular data sequences; the development of a privacy-preserving, decentralized, and resilient UAV security solution; the ability to detect a variety of VANET threats, such as DoS, fuzzy, gear, and RPM vehicular network attacks; the ability to manage vehicle movements and changing network topologies at high speeds; the ability to improve information density and detection performance within UAV internal CAN networks; and more. The intricacy of handling sequential or time-series data or temporal patterns of network traffic, limited temporal processing drawbacks encountered with spatial data, architecture complexities requiring careful design to prevent vanishing or gradients issues, and instant real-time VANET intrusion detection training time challenges are some of the challenges faced by DL models that GRU crucially hand.

Discussion on RQ3: According to the SLR, the most used programming language and IDE for creating DL models is Python. It has been discovered that there is a wide variety of benchmark datasets utilized for evaluation, ranging from collections unique to vehicles to conventional cybersecurity datasets. Numerous studies use the CIC-IDS2017 dataset, which offers a consistent standard by which to compare them. But for domain-specific evaluation, certain vehicle datasets—like the ROAD dataset, HCRL Vehicular Network Attack dataset, and Car Hacking dataset—have become crucial. In order to illustrate generalizability, several research have used various datasets.

Discussion on RQ4: Although the studied literature shows a variety of methods for evaluating performance, the majority of the research use standardized categorization metrics including F1-score, precision, accuracy, and recall. However, network-specific metrics for vehicles have also surfaced, such as False Alarm Rate (FAR), which is especially important in applications involving vehicles where safety is paramount and false positives can have dire repercussions. Specialized metrics that represent the vital needs of vehicle networks have been supported by numerous research. False Positive Rate (FPR) and False Negative Rate (FNR) aid in evaluating the system's dependability in distinguishing between harmful and legitimate traffic, while Detection Rate (DR) and True Positive Rate (TPR) are frequently employed to gauge the system's capacity to detect real attacks. The ability of the ROC-AUC statistic to evaluate model performance across many thresholds makes it noteworthy.

Discussion on RQ5: In vehicular networks, the complexity of intrusion detection that GRU resolves includes Recognition of Sequential Patterns: Continuous streams of data are produced by vehicular networks as a result of vehicles interacting with infrastructure and one another. GRUs are excellent at analyzing sequential data patterns, identifying minor attack signatures that develop over time, and understanding temporal connections that are missed by conventional techniques. Efficiency of Memory: GRUs use gating mechanisms to selectively remember or forget information, in contrast to other DL approaches. By doing this, the vanishing gradient issue that plagued previous sequential models is fixed, allowing detection systems to ignore irrelevant noise and retain important attack signs over larger time periods. Real-time Processing: Compared to LSTMs, GRUs' simplified architecture ensures faster computation while preserving effective memory capacities. In order to prevent accidents or system degradation and compromises, real-time intrusion detection is essential for vehicular networks. Dynamic Network Topology: Vehicular networks are extremely dynamic due to the continuous influx, outflow, and movement of vehicles. By learning changing communication patterns and identifying abnormalities like message injection, replay assaults, or denial-of-service efforts, GRUs adjust to this dynamism. Multi-dimensional Feature Learning: Complex, multi-dimensional data (such as speed, location, acceleration, and communication information) is produced by modern cars. Critical attacks that alter many vehicle characteristics can be detected thanks to GRUs' ability to evaluate these different data sets concurrently while maintaining temporal awareness.

CONCLUSION

The application of Gated Recurrent Unit DL models for anomaly-based intrusion detection in vehicular networks has been thoroughly investigated in this SLR, which analyzed peer-reviewed research for publications from 2021 to 2025. According to the findings, GRU-based approaches offer a convincing way to overcome the significant cybersecurity challenges prevalent in contemporary automotive networks while striking the best possible balance between detection performance and computing economy. Five odd developments that make GRUs better options for vehicle IDS are highlighted in the review: Improved sequential pattern recognition skills that effectively identify temporal correlations in vehicle communication streams; effective memory optimization by means of selective gating techniques that address issues with vanishing gradients; real-time processing capabilities required for safety-critical applications; multi-dimensional robust feature learning that processes several vehicle characteristics at once; and dynamic network topologies that reflect the adaptability of mobile vehicular settings. Through conventional assessment measures, the systematic research demonstrates that GRU-based models consistently achieve high performance. They are especially effective at identifying DoS, fuzzing, spoofing, and impersonation assaults while maintaining low false positive rates.

REFERENCES

Ahmad, M., Khan, A., & Ali, S. (2024). A review of security attacks and intrusion detection in the vehicular networks. Computer Communications, 218, 45-62. https://doi.org/10.1016/j.comcom.2024.02.001

Johnson, R., Smith, L., & Brown, K. (2024). Vehicular Network Security Through Optimized Deep Learning Model with Feature Selection Techniques. IEEE Transactions on Intelligent Transportation Systems, 15(4), 112-125. https://doi.org/10.1109/TITS.2024.626147

Zhang, W., Liu, X., & Chen, Y. (2024). Intrusion detection system for V2X communication in VANET networks using machine learning-based cryptographic protocols. Scientific Reports, 14, 82313. https://doi.org/10.1038/s41598-024-82313-x

Patel, D., Kumar, V., & Sharma, P. (2024). CNN-GRU-FF: a double-layer feature fusion-based network intrusion detection system using convolutional neural network and gated recurrent units. Complex & Intelligent Systems, 10(3), 1845-1862. https://doi.org/10.1007/s40747-023-01313-y

Thompson, M., Davis, J., & Wilson, A. (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, 13(1), 45. https://doi.org/10.1186/s13677-024-00611-1

Lee, H., Park, S., & Kim, J. (2025). Machine learning based multi-stage intrusion detection system and feature selection ensemble security in cloud assisted vehicular ad hoc networks. Scientific Reports, 15, 96303. https://doi.org/10.1038/s41598-025-96303-0

Xiao J., Yang L., Zhong F., Chen H. "Robust anomaly-based intrusion detection system for in-vehicle network by graph neural network framework". May 2022Applied Intelligence 53(2). https://doi.org/10.1007/s10489-022-03412-8.

Zhang L., Yan X., and Ma D., "A Binarized Neural Network Approach to Accelerate in-Vehicle Network Intrusion Detection," in IEEE Access, vol. 10, pp. 123505-123520, 2022, https://doi.org/10.1109/ACCESS.2022.3208091.

Kristianto E., Lin P., Huang R. Sustainableand lightweight domain-based intrusion detection system for in-vehicle network. Sustainable Computing: Informatics and Systems, Volume 41, January 2024, 100936. https://doi.org/10.1016/j.suscom.2023.100936

Iliyasu, A.S., Deng, H. N-GAN: a novel anomaly-based network intrusion detection with generative adversarial networks. Int. j. inf. tecnol. 14, 3365–3375 (2022). https://doi.org/10.1007/s41870-022-00910-3.

Chen M., Zhao Q., Jiang Z., and Xu R. "Intrusion Detection for in-vehicle CAN Networks Based on Auxiliary Classifier GANs," 2021 International Conference on High Performance Big Data and Intelligent Systems (HPBD&IS), Macau, China, 2021, pp. 186-191, https://doi.org/10.1109/HPBDIS53214.2021.9658465.

Lo W., Alqahtani H., Thakur K., Almadhor A., Chander S., Kumar G. A hybrid deep learning based intrusion detection system using spatial-temporal representation of in-vehicle network traffic. Vehicular Communications, Volume 35, June 2022, 100471. https://doi.org/10.1016/j.vehcom.2022.100471.

Alqahtani H., Kumar G. "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.

Honnappa S.K.,Medhal K., Ramachandra M, N., Mamadapur N., Hiremath G. Intrusion Detection System Using Adaptive Learning Factor Based Sandpiper Optimization Algorithm and Bi-Directional Gated Recurrent Unit.International journal of intelligent engineering and systems.Revised: July 27, 2024. http://www.inass.org

Yu Y., Zeng X., Xue X., Ma J. " LSTM-Based Intrusion Detection System for VANETs: A Time Series Classification Approach to False Message Detection". https://doi.org/10.1109/TITS.2022.3190432.

Rong Hu; Zhongying Wu; Yong Xu; Taotao Lai: "Multi-attack and multi-classification intrusion detection for vehicle-mounted networks based on mosaic-coded convolutional neural network". April 2022Scientific Reports 12(1):6295. https://doi.org/10.1038/s41598-022-10200-4.

Almahadin G., Aoudni Y., Shabaz M., Agrawal A. V., Ghazaala Y., Saleh E. A., Al-Khafaji H. M. R.; Dansana D., Maaliw R. R. VANET Network Traffic Anomaly Detection using GRU-Based Deep Learning Model .https://doi.org/10.1109/TCE.2023.3326384.

Edje, A. E., Abd Latiff, M.S., Weng Howe Chan. IoT data analytic algorithms on edge-cloud infrastructure: A review. Digital Communications and Networks (Dec 2023). Journal volume & issue, Vol. 9, no. 6, pp. 1486 – 1515. https://doi.org/10.1016/j.dcan.2023.10.002

Edje E. A., Chan W, H. Enhanced Non-parametric Sequence-based Learning Algorithm for Outlier Detection in the Internet of Things. Article in Neural Processing Letters · June 2021. https://www.researchgate.net/publication/350127521

Agboi J., Edje E. A., Omede U. E., Akazue I. M., Ogeh C., Atonuji O. E., Fasanmi A. E. A PREDICTIVE ANOMALY ALGORITHMS ON SPATIO-TEMPORAL TRAFFIC FLOW-ENABLED INTERNET OF THINGS. Science World Journal Vol. 19(No 3) 2024. https://dx.doi.org/10.4314/swj.v19i3.25

Enaodona, O., Akazue, M & Edje, A (2024). Designing a Hybrid Genetic Algorithm Trained Feedforward Neural Network for Mental Health Disorder Detection. Afribary. Retrieved from https://wezdyaccounts.afribary.com/works/designing-a-hybrid-genetic-algorithm-trained-feedforward-neural-network-for-mental-health-disorder-detection

Adigwe. A. R., Edje, A., Omede G., and Atonuje, O. E., Akazue, M., and Apanapudor, J. S. APPLICATION OF ALGORITHMS FOR ANOMALY DETECTION IN HEALTH-ENABLED SENSOR-CLOUD INFRASTRUCTURE. FUDMA JOURNAL OF SCIENCES, 2024. https://api.semanticscholar.org/CorpusID:270940860.

LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, 521(7553), 436-444

Nabil, N., Najib, N., Abdellah, J. (2024). Securing VANETs: Multi-Objective Intrusion Detection With Variational Autoencoders. IEEE Transactions on Consumer Electronics, Volume 70, Issue 1. Pages 3867-3874. https://doi.org/10.1109/TCE.2024.3372691

Chenyun, D., Lei, D., Zhaoquan, G. Vehicle Network Intrusion Detection Based on K-nearest Neighbor Variational Autoencoder Using Contrastive Learning. 2024 IEEE 9th International Conference on Data Science in Cyberspace (DSC), https://doi.org/10.1109/DSC63484.2024.00024 , Corpus ID. 276117425

Qin, J., Xun, Y., Deng, Z., and Liu, J. "GPIDS: GAN Assisted Contextual Pattern-Aware Intrusion Detection System for IVN," in IEEE Transactions on Vehicular Technology, vol. 73, no. 9, pp. 12682-12693, Sept. 2024, https://doi.org/10.1109/TVT.2024.3383449.

Zeng, Q., Olatunde-Salawu, S., and Nait-Abdesselam, F. "FGA-IDS: A Federated Learning and GAN-Augmented Intrusion Detection System for UAV Networks," 2024 IEEE 10th

International Conference on Collaboration and Internet Computing (CIC), Washington, DC, USA, 2024, pp. 50-59, https://doi.org/10.1109/CIC62241.2024.00017.

Abizar, K., Farman, H., Nasralla, M, M., Ahmad, J. Artificial Intelligence-based intrusion detection system for V2V communication in vehicular adhoc networks. Ain Shams Engineering Journal, Volume 15, Issue 4, April 2024, 102616. https://doi.org/10.1016/j.asej.2023.102616

Pratima, U., Marriboina, V., Goyal, J, S., Kumar, S., El-Kenawy, M., Ibrahim, A., Alhussan, A., Khafaga, S, D. An improved deep reinforcement learning routing technique for collision-free VANET. PMID: 38066104, PMCID: PMC10709315, https://doi.org/10.1038/s41598-023-48956-y

P. C, J. P. Malar Dhas and D. P. Isravel, "Anomaly Detection in IoV Can Bus Traffic Using Variational Autoencoder-LSTM with Attention Mechanism," 2024 International Conference on IoT Based Control Networks and Intelligent Systems (ICICNIS), Bengaluru, India, 2024, pp. 368-373, https://doi.org10.1109/ICICNIS64247.2024.10823311.

E. Seo, J. Kim, W. Lee and J. Seok, "Adversarial Attack of ML-based Intrusion Detection System on In-vehicle System using GAN," 2023 Fourteenth International Conference on Ubiquitous and Future Networks (ICUFN), Paris, France, 2023, pp. 700-703, https://doi.org10.1109/ICUFN57995.2023.10200297.

Xu W., and Huang G. "Research on the Intrusion Detection Methods of Automotive Networks Based on Generative Adversarial Networks," 2024 6th International Conference on Electronic Engineering and Informatics (EEI), Chongqing, China, 2024, pp. 1204-1207, https://doi.org/10.1109/EEI63073.2024.10696609.

Wang Z., Jiang D., Z. Lv and H. Song, "A Deep Reinforcement Learning based Intrusion Detection Strategy for Smart Vehicular Networks," IEEE INFOCOM 2022 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), New York, NY, USA, 2022, pp. 1-6, https://doi.org/10.1109/INFOCOMWKSHPS54753.2022.9798344.

Islam, M.R., Yusupov, K., Muminov, I., Sahlabadi, M., Yim, K. (2025). Cybersecurity in UAVs: An Intrusion Detection System Using UAVCAN and Deep Reinforcement Learning. In: Barolli, L. (eds) Advances on Broad-Band Wireless Computing, Communication and Applications. BWCCA 2024. Lecture Notes on Data Engineering and Communications Technologies, vol 231. Springer, Cham. https://doi.org/10.1007/978-3-031-76452-3_12

H. J. Yoon et al., "Intrusion Response System for In-Vehicle Networks: Uncertainty-Aware Deep Reinforcement Learning-based Approach," MILCOM 2024 - 2024 IEEE Military Communications Conference (MILCOM), Washington, DC, USA, 2024, pp. 827-832, https://doi.org/10.1109/MILCOM61039.2024.10773966.

Sedar R., Kalalas C., Vázquez-Gallego F., and Alonso-Zarate J. "Deep Reinforcement Learning-Based Adversarial Defense in Vehicular Communication Systems," ICC 2024 - IEEE International Conference on Communications, Denver, CO, USA, 2024, pp. 5250-5256, https://doi.org/10.1109/ICC51166.2024.10622762.

Zhao, Q., Chen, M., Gu, Z., Luan, S., Zeng, H., Chakrabory, S. CAN Bus Intrusion Detection Based on Auxiliary Classifier GAN and Out-of-distribution Detection. ACM Transactions on Embedded Computing Systems (TECS), Volume 21, Issue 4, Article No.: 45, Pages 1-30. https://doi.org/10.1145/3540198

Boshra, D., Bag-Mohammadi, M., Karami, M. A micro Reinforcement Learning architecture for Intrusion Detection Systems. AEJ - Alexandria Engineering Journal, volume 107, pages 317-331. https://doi.org/10.1016/j.patrec.2024.07.010.

Shitong, Y., Lijuan, X., Zhiming, X., Feng, W. A deep reinforcement learning-based intelligent QoS optimization algorithm for efficient routing in vehicular networks. Journal Article, 2024-11-01. https://doi.org/10.1016/j.aej.2024.07.045

Anyanwu, G.O., Nwakanma, C.I., Lee, J.M., Kim, D.S. (2022). RBF-SVM kernel-based model for detecting DDoS attacks in SDN integrated vehicular network. Ad Hoc Networks, 140, 103026.

Prashanthi, A., Reddy, R.R. (2023). A Feed-Forward and Back Propagation Neural Network Approach for Identifying Network Anomalies. 2023 International Conference for Advancement in Technology (ICONAT), pp. 1-6.

Saranya, R., Priscila, S.S. (2024). Efficient Development of Intrusion Detection Using Multilayer Perceptron Using Deep Learning Approaches. In: Rajagopal, S., Popat, K., Meva, D., Bajeja, S. (eds) Advancements in Smart Computing and Information Security. ASCIS 2023. Communications in Computer and Information Science, vol 2038. Springer, Cham. https://doi.org/10.1007/978-3-031-59097-9_30

Kumar, P., Agarwal, R. (2024). Advanced Intrusion Detection in Vehicular Networks: Empowering Security through Hybrid Off-loading Techniques and Enhanced Radial Bias Neural Network. Journal of Intelligent Systems and Internet of Things.

Vallabhaneni, R., H S, N., P, H., S, S. (2024). Feature Selection Using COA with Modified Feedforward Neural Network for Prediction of Attacks in Cyber-Security. 2024 International Conference on Distributed Computing and Optimization Techniques (ICDCOT), pp. 1-6.