


## Review Article

# Real-Time Intrusion Detection in Controller Area Networks: An Evaluation of Current Methods and Future Directions

Sreelekshmi M. S.<sup>1\*</sup> , Aji S.<sup>2</sup> 

<sup>1</sup>Department of Computer Science, University of Kerala, Trivandrum, Kerala, India

<sup>2</sup>Department of Computer Science, University of Kerala, Trivandrum, Kerala, India

\*Corresponding Author: 

Received: 10/Mar/2024, Accepted: 02/Apr/2025, Published: 30/Apr/2025 | DOI: <https://doi.org/10.26438/ijsrnsc.v13i2.266>



Copyright © 2025 by author(s). This is an Open Access article distributed under the terms of the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/) which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited & its authors credited.

**Abstract**— Controller Area Networks (CANs) are critical components of modern vehicles and industrial systems, facilitating communication between various electronic control units. However, the widespread connectivity and lack of inherent security measures make CANs vulnerable to cyber-attacks. Intrusion detection systems (IDS) safeguard CANs by detecting and mitigating potential attacks. This paper presents a comprehensive analysis of current methods for the real-time detection of attacks in CANs. The IDSs based on different input data modalities are evaluated based on their effectiveness, accuracy, and efficiency. The analysis highlights the strengths and limitations of each method, providing valuable insights for researchers and practitioners in developing robust and reliable intrusion detection systems for CANs. The findings suggest that the lightweight strategy in IDS is widely accepted for real-time application due to its computational simplicity and model structure. Furthermore, the paper identifies future directions to enhance the security of CANs and ensure their resilience against evolving threats.

**Keywords**— Intrusion detection system, Controller Area Network, Electronic Control Unit Communication, Real Time Intrusion Detection, CAN Bus Attacks

## 1. Introduction

Nowadays, modern vehicles are coming up with several embedded Electronic Control Units (ECU) that are integrated internally to automate the driving experience. Most of the ECUs converse with each other using the broadcast communication protocol known as Controller Area Network (CAN). The security threats in CAN networks are increasing along with the rapid growth in the number of connected vehicles on the road, and the trail in the efficient methods for encryption and authentication makes it highly vulnerable. A robust and intelligent Intrusion Detection System (IDS) has an inevitable role in the design of digitally controlled vehicles. ECU integrated vehicles are in the early stages of development, and the strategies employed in the IDS must be effectively tuned together with the changes in attack behaviour to ensure sound security. In the automotive industry, the ECUs are resource-constrained, and the computation time of any application must be adequate for real-time scenarios. Practical intrusion detection algorithms are mainly machine learning-based, and it has to be with low latency, consume few resources and are highly accurate in

the case of vehicular networks [1]. This work aims to conduct an intensive study on the real-time intrusion detection systems on the CAN bus. Among the intensive studies on intrusion detection in CAN buses, Hussain et al. [2] looks into false information attacks on the road side unit's ongoing federated learning operation. Another set of works, [3], [4], [5], and [6], present artificial intelligence and machine learning techniques for intrusion detection in in-vehicle networks.

We have comprehensively studied a bunch of works in real-time IDS in CAN, where a significant number of the latest publications were on the list. Our preliminary studies noted that the research in the problem domain could be categorized according to the input data models. CAN ID (ID), CAN Payload (Payload), and CAN frame are the leading data models in most publications [7]. Important attacks like DoS and spoofing rely on message ID sequences to operate. The ID-based detection methods have been using the 11-bit identifier and are found effective in hitting up on those attacks [8]. Here, the incoming messages' IDs are compared against a

pre-configured list of authorized IDs, and the messages with unauthorized IDs will be treated as intrusion attempts [9]. In the payload-based detection, the 64-bit CAN data is used for the detailed analysis [10]. Attacks like fuzzing create threats by manipulating the payload data, resulting in unexpected scenarios in the target system. The entire standard CAN frame or the different combinations of the CAN fields explored in the IDS in the CAN frame-based detection strategies. Multiple attack detection is found easier with CAN frame than ID-based and payload-based methods. While analysing the

performance of IDS, it is seen that the published methods can be categorized into two - lightweight and strategies with computationally expensive deep learning architectures. The inline computational simplicity and model structure of the lightweight strategy is widely accepted for real-time applications [11]. It can strongly comply with such applications' prime requirement-responsible response time.

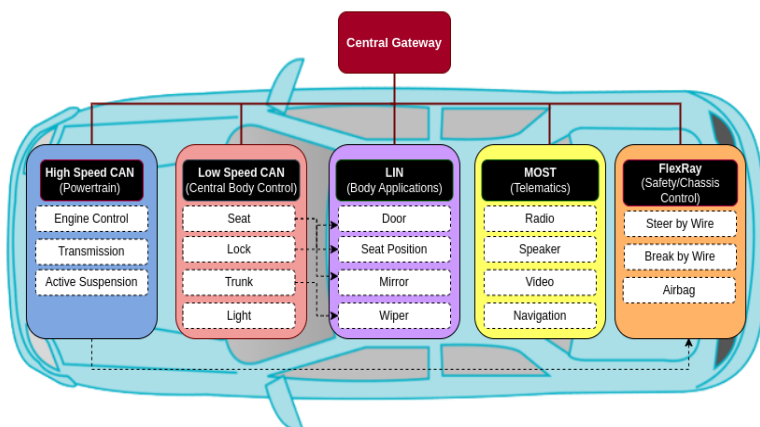


Figure 1: Basic Protocols for ECU Communications

The organization of this work is as follows: Section II describes the background of the CAN frame and possible attacks. Recent research works are introduced in Section III. The performance analysis of these techniques is covered in Section IV. We provide our insights from these studies and future directions in Section V. The conclusions are given in Section VI.

## 2. Background

The most significant concern in automobiles, especially autonomous vehicles, is the high-speed data processing and communication between the ECUs at low cost. As shown in figure 1, there are various protocols, including CAN, LIN, Flex Ray, MOST, and Ethernet [7], that make communication easier in vehicles. Among these, the CAN protocol designed by the Bosch Corporation is widely utilized because of its cost efficiency and flexibility. The CAN-FD (Flexible Data Rate), one of the CAN variants, provides more bandwidth. The switches and motors that roll windows and operate seats use the Local Interconnected Network or LIN. The Flex ray is generally used in safety-critical functions like a brake by wire, in general 'x-by wire' [12]. The MOST (Media Oriented Serial Transport) supports infotainment devices. It is observed that the Automotive Ethernet is used less frequently, and many more studies and innovations need to be done to improve the existing communication strategies in autonomous vehicles.

The initial CAN 2.0A, the Bosch CAN, has undergone several enhancements and is now an ISO standard multicast protocol for the interconnection of distributed embedded modules to execute shared tasks. In Fig. 2, we can see that a standard CAN bus frame is 47 to 111-bit long, and a total of 8-bit is used for synchronization. Among them, 1 bit represents the SOF, the beginning of the message, and the remaining 7-bit, known as EOF, indicates the end. The 7-bit EOF will disable bit stuffing, showing a stuffing error when dominant. An 11-bit identifier (standard format) allows different messages for a total of 211 (= 2048). The identifier is used for identifying the messages and also for prioritizing them. The message with a lower id will have a higher chance of being transmitted. In the arbitration field, the first bit is MSB. The RTR in the arbitration field indicates transmission of a data frame (RTR=0) or a Remote Request Frame (RTR=1). Data frame has higher priority than a remote frame. The 6-bit control field includes IDE, r0, and DLC. DLC contains the number of bytes in the data field, and IDE indicates either standard 11-bit or 29-bit format. The car's control commands, which means signal information is available in the data field. The CAN data payload is maintained confidentially by every car manufacturer in the form of a DBC file. In the Data field, the first bit is MSB. The 15-bit CRC segment has the frame check sequence, control, and data fields. The CRC delimiter bit and acknowledgement are the other parts of the protocol. CAN 2.0B, an enhanced version of CAN, is

evolved to support lower device IDs. Compared with the CAN 2.0A message, the CAN 2.0B message allows IDs of 11-bit (standard) and 29-bit (extended) lengths. [13].

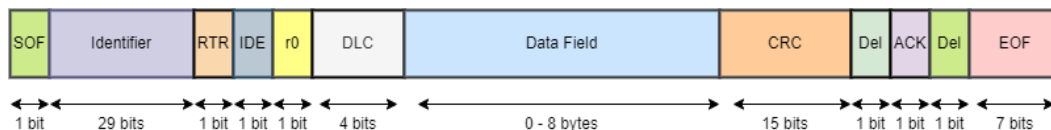


Figure 2: Structure of a standard CAN Data Frame

## 2.1 Prominent CAN Attacks

The CAN bus packets do not have any knowledge about the sender and receiver. Generally, the nodes will broadcast the packets on demand according to the arbitration identifier. So, it is difficult for the receiver node to identify whether it comes from a legitimate sender [14]. The lag in the security features like encryption and authentication techniques also makes the CAN bus vulnerable to several security threats [15]. The studies [16], [17], [18], [19] reveal some of the attacks that happened through the CAN bus and the malicious activities explored to gain control of windows, break, and lights. Attackers can generally access the CAN bus through physical interfaces like the OBD-II and USB ports. The attacks are also possible when a car is connected to Bluetooth, GPS, and other wireless networks [20]. This section gives abstract information on the general categories of intrusion on CAN buses, and Figure 3 picturizes some of the standard scenarios of those attacks.

**Denial of Service(DoS):** Here, the attacker floods the CAN bus with high priority messages. Since the CAN protocol prioritizes messages based on their identifier, these high priority messages can dominate the bus and prevent other critical messages from being transmitted. It is noted that both of the attack's prime intention is to prevent legitimate message transmission [21] and mess up the communication network. It is clear in Figure 3 that the attacker in this category inserts messages with IDs 000, which may result in the prior legal message being rejected and the subsequent genuine message being delayed.

**Fuzzing:** In this category, the attacker will send messages with randomly generated Arbitration Identifier, Data Length Code (DLC), and Data payloads to cause the vehicle to act in an unexpected way. The Fuzzing attacks can create a set of unanticipated actions like turning on/off signal lights, changing gear shifts and shaking the steering wheel. Identifying such a type of attack is possible by monitoring the message sequences and comparing the actual IDs to their original ones [22].

**Replay:** In a replay attack, the attacker records legitimate in-vehicle messages and rebroadcasts them in the future to trigger unexpected behaviours. Replay is the most difficult attack to identify since it completely duplicates the genuine message. The replay attack in Figure 3 demonstrates how an attacker keeps sending messages that are duplicates of earlier normal ones [23].

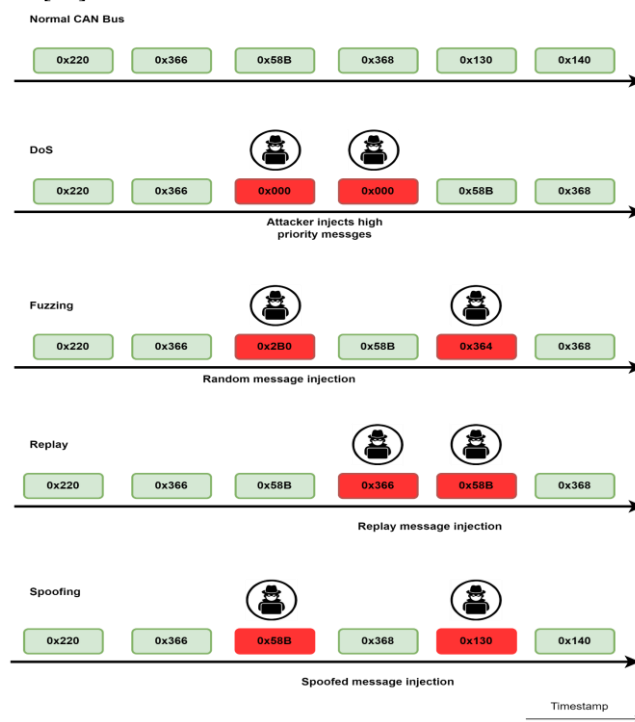


Figure 3: Common CAN Bus Attacks

**Spoofing:** In the beginning, the spoofing attack will try to sniff some ECUs connected to the CAN bus system. It will next attempt to impersonate those infected ECUs. Figure 3 illustrates a spoofing attack that targets ID 0x58B and injects spoofed messages. The occurrence of the targeted ID and ID sequences may fluctuate because of this attack [22].

## 3. Input Data Modalities in Intrusion Detection Methods

The target of each CAN bus attack is different according to the objective of the intruder, and it can be CAN IDs, message

payloads, and the entire CAN frame. Our study considers the various targets as input modalities in the proposed taxonomy to effectively classify the intrusion detection systems. Table 1 comprehensively summarizes the ID-based, payload-based, and CAN frame-based strategies.

### 3.1 ID Based Detection Methods

Some recent and advanced IDS methods are selected here to investigate their performances in real-time scenarios. There is a Graph based Gaussian Naive Bayes (GGNB)[24] that combines characteristics of PageRank (PR) with a GNB algorithm. The Gaussian Naive Bayes classifier used the PR features to distinguish the attacks in a given set of samples. A feature reduction method with correlation matrices is also incorporated in the exercises. Denial of service (DoS), fuzzy, spoofing, replay, and mixed attacks are considered in the investigations. The experimental results report that the algorithm performed well at identifying various attacks, but there is still room for improvement while dealing with replay attacks.

A voltage-based, light-weight intrusion detection (VALID) model was demonstrated in a work by Leg Schell and Marcel Kneib [25], which was focused on the resource availability of vehicle networks. VALID extracts voltages from the differential CAN signals. They go through a pre-processing step called drift mitigation to reduce fluctuations in voltage. A quasi-linear model is created for each ECU, and any observed slope deviation of the associated linear model during attack detection denotes an unauthorized transfer. Heng Sun et al. [26] developed a novel similarity-based intrusion detection technique called SIDuDTW, which uses the Dynamic Time Warping (DTW) distance between CAN ID sequences to identify malicious messages inside the Controller Area Network. SIDuDTW works in phases; first, they read the CAN messages and extract the IDs. The extracted ID values are then reconstructed, and the DTW distance between new and prior IDs is calculated to identify anomalies. They validated the model using public datasets and also gathered data from a vehicle to show the performance of SIDuDTW in a real-world scenario.

Araya et al.'s work [27] is the first to use recurrent plots to generate images from CAN traffic, which are subsequently used in CNN for intrusion detection. They could detect the attacks - DoS, fuzzy, spoofing gear, and spoofing RPM - with an accuracy of 0.999. They have compared the proposed method with other methods and established their upper hand while considering latency and accuracy. One of the significant drawbacks of this study is that the model may not perform

well with the impersonation attacks because the sequence of CAN IDs is the primary concern.

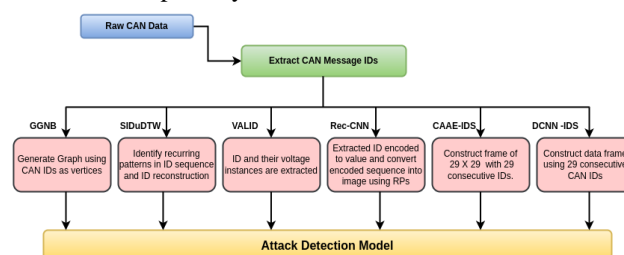


Figure 4: Role of CAN Message IDs in ID Based Detection Models

In [28], a deep convolutional neural network-based IDS with two stages is proposed. The first stage is the training phase, where the CAN IDs are extracted from CAN traffic data, and a set of frames will be generated using 29 sequential IDs. This rendered frame is further applied to the DCNN model, which employed the Inception-Resnet structure at the detection phase. Because the model is based on a supervised learning technique, detecting the unknown attacks here is problematic.

Studies by Thein-Nu et al.[29] have led to a more profound understanding of semi-supervised learning techniques used for IDS in CAN. Two popular deep learning models, auto encoders and generative adversarial networks are used here to obtain better real-time detection. This model can detect message injection attacks, such as DoS, fuzzy, spoofing, and unknown attacks. The researchers also plan to extend the detection of attacks in inter-vehicle networks, which now deal with in-vehicle only.

### 3.2 Payload Based Detection Methods

Linxi Zhang et al. [30] explore how an IDS can execute with reduced memory and energy consumption using Binarized Neural Network architecture. This is the first work that used BNN for intrusion detection in in-vehicle networks. During the training phase, a frame of consecutive CAN bus payloads was

constructed, with labels assigned to the frames. These named input frames are then used to train the BNN model. The trained BNN is used for prediction during the detection phase. Additionally, the suggested model used FGPA to accelerate its performance.

In H-IDFS, Derhab et al. [31] outline a histogram-based intrusion detection system for CAN buses. Here, the CAN packet is put together into a window, and its histograms are calculated. These windows are then input into a novel one class SVM. Their model has two parts- intrusion detection and filtering, where the intrusion detection module will find the malicious window. The normal messages are extracted from the malicious window in the filtering phase. DoS, fuzzy, and

spoofing attacks are the kinds of attacks covered in this research. Results of experiments are gathered from the OTIDS and Car-Hacking CAN datasets.

Wei Leo et al. [32] explored the extraction of spatiotemporal features from in-vehicle network traffic for intrusion

detection. They have used CNN and LSTM for detection purposes. Here, some questions regarding the updating of available datasets and the use of unsupervised models still need to be addressed.

**Table 1 An abstract view of the recent works considered for the study. The works are arranged according to the Data Input Model and the kind of strategy followed in it.**

Data Input Model	Strategy	Work	Key Technique	Datasets
ID-Based	Light Weight	GGNB [2]	Graph-Based Model with Naive Bayes Algorithm	1) raw CAN 2) Opel Astra
		VALID [3]	Voltage Deviation Analysis	Privately captured dataset from Fiat 500 and Porsche Panama S E-Hybrid
		SIDuDTW [4]	DTW Distance between waves	1) Car Hacking Dataset 2) Privately captured real CAN data
	Deep Learning	Rec-CNN [5]	Ensemble of RP and CNN	1) Car Hacking Dataset 2) Privately captured real CAN data
		DCNN-IDS [6]	Reduced Inception-ResNet and LSTM	Privately captured CAN data
		CAAE-IDS [7]	Ensemble of AE and GAN	Car Hacking Dataset
	Payload-Based	Light Weight	BNN-IDS [8]	Binarized Neural Network
H-IDFS [9]			One-Class SVM	1) OTIDS 2) Car Hacking Dataset
Deep Learning		HyDL-IDS [10]	Combination of CNN and LSTM	Car Hacking Dataset
		CANDito [11]	LSTM-Based Auto encoder	ReCAN Dataset
		TSP [12]	LSTM with two input data formats	Privately captured CAN data
CAN Frame-Based	Light Weight	ASSASSIN [13]	Clock-Skew and Gaussian Naive Bayes	Real-time Data
		QMLP-IDS [14]	Quantized MLP	Car Hacking Dataset
		MTH-IDS [15]	Cluster Labelling and BO	1) CAN Intrusion Dataset 2) CICIDS2017
	Deep Learning	CAN-ADF [16]	Ensemble of Rule-based and RNN-based detection	CAN Intrusion Dataset
		NovelADS [17]	CNN and LSTM	Car Hacking Dataset
		CANintelliIDS [18]	Combination of CNN and Attention-Based GRU	Privately captured CAN data

In [33], authors have improved the RNN-based state of art intrusion detection system called CANnolo [41]. The underlying concept of this work is to identify abnormalities by reconstructing the signal (packet payload) using LSTM-based auto encoders. The experiments make use of real-world datasets augmented with synthetic threats generated through CANTack. The major drawback of the suggested system is its inefficiency in detecting flow-based attacks like replay and injection since they use payload-based detection and need to consider the changes in frequency patterns.

Hongmao et al. [34] developed a deep learning technique based on time series prediction for anomaly detection. The present article describes the detection of three different attack scenario forms. Five loss functions and a multi-format data input were also suggested based on the study of threat data. The offered loss functions are experimental loss, weighted experimental loss, negative logarithmic loss, average loss, and root mean square loss. The two input data formats used are 64-bit binary and 16-bit hexadecimal data formats.

### 3.3 CAN Frame Based Detection Methods

Oleg Schell et al. [35] explored the characteristic timestamp of CAN bus messages and built an IDS on top of them. In the initial stage of the algorithm, the time characteristics, or timestamps, were taken from the data for calculating the average clock skew during the data pre-processing step. These time skews are used in the Gaussian Naive Bayes classifier of the proposed model. Also, ASSASSIN (Asymmetric Symbol and Skew Sender Identification) performs sender identification and intrusion detection after creating the model. The experimental results show that it has an average attack detection rate of 99.02% with minimal resource usage and low latency. The major limitation of this work is that it can only see malicious messages using a time stamp, so data tampering attacks, which change the payload field, are challenging to detect. Shashwat et al. [36] proposed an IDS architecture that can detect DoS, fuzzy and spoofing attacks using two lightweight quantized Multi-Layer Perceptron's. The architectures are deployed using Xilinx's DPU



accelerator [42]. The suggested model was compared with different state-of-the-art techniques, and it has significantly improved detection accuracy, latency, and power consumption. [37] Addressing the challenges of IDSs due to the high volume of traffic data, numerous network features, and various cyber-attack patterns. Here, signature- and anomaly-based IDS are proposed to detect known and unknown attacks. For intra-vehicle intrusion detection, the CAN Intrusion detection dataset is used, and for inter-vehicle intrusion detection, the CICIDS2017 dataset is used. A novel clustering k-means algorithm for intrusion detection is also presented here. For known attacks, it gets 99.99% and 99.88% accuracies for both datasets, respectively. In the case of unknown attacks, the accuracies are reduced to 96.3% and 80%.

**Table 2 Input Features used for CAN Frame Based Detection**

Model	Input Feature Used
QMLP-IDS [14]	CAN-ID + Data Field
MTH-IDS [15]	CAN-ID + Data Field
CAN-ADF [16]	Time Interval + CAN-ID + DLC + Data Field
NovelADS [17]	CAN-ID + Data Field
CANintelliIDS [18]	Time Interval + CAN-ID + DLC + Data Field

The CAN-ADF [38] is an ensemble rule-based attack detection system that proposes a CAN bus attack detection framework that performs anomaly generation, detection, and evaluation.

**Table 3 Summary of Data Pre-processing Techniques**

Input Data Model	Works	Pre-processing Techniques
CAN ID	[2], [3], [5], [6]	Quantile Transformation, Signal Alignment Approach, Frame Building
CAN Payload	[8], [10], [11], [12]	Number Conversion, Conversion to Signals, Encoding, Normalization
CAN Frame	[13], [14], [15], [16], [17], [18]	Average Asymmetry Calculation, K-Means Clustering, Zero-padding, Conversion to Vector Sequence

They have used the traffic data collected from real cars, KIA Soul and Hyundai Sonata, for evaluation. The Recurrent Neural Network (RNN) is employed here to detect common attacks like DoS, fuzzy, and replay.

Agarwal et al. introduce NovelADS [39], a novel intrusion detection model based on deep learning which employs thresholding and error reconstruction techniques. This work tests the system on attacks like DoS, fuzzy, RPM Spoofing and Gear Spoofing. They have conducted experiments with four different architectures in deep learning - single-layer LSTM, CNN followed by single-layer LSTM, two-layer stacked LSTM, and CNN followed by two-layer stacked LSTM.

A CNN model with attention-based GRU is used in CANintelliIDS [40] for intrusion detection in in-vehicle networks. The attack types used here are DoS, fuzzy, and impersonations. The performance of CANintelliIDS is compared with conventional approaches like Random Forest, Logistic Regression, SVM, DNN, and CNN. Also, state-of-the-art methods like OCSVM, IF OTIDS, CANTransfer, and DCNN are used for the performance comparison. They recorded a performance matrix of F1-Score, Precision and Recall with 93.79%, 93.69%, and 93.91%, respectively. A summary of data pre-processing techniques used in reviewed articles is presented in Table 3.

#### 4. Performance Analysis

This study investigates real-time IDS for controller area networks, considering the various input methods. This section includes a performance study of each model, outlining its benefits, drawbacks, and ways in which it varies from other models. The detection time of the model is considered in this analysis since the latency is crucial in real-time detection.

There are various measures for assessing detection methods on intelligent vehicles. The major detection criteria are accuracy, precision, recall, FPR, F1-score, and ROC curves [43]. The number of samples that a detection method accurately identified as abnormal is known as True Positive (TP). The number of samples that a detection method accurately identified as normal is known as True Negative (TN). False-positive (FP) samples are those where a detection technique mistakenly classifies them as abnormal. The False-negative is the quantity of samples that a detection technique incorrectly classifies as normal [43].

Accuracy refers to a classifier's efficiency in correctly identifying messages as invasive or normal [44]. Precision is defined as the ratio of TPs to all expected positive class values. A low precision score indicates a large percentage of false

positives, in which normal occurrences are mistakenly classified as attack occurrences [45]. Recall, also known as the True Positive Rate or Detection Rate, is defined as the ratio of detected intrusions to total intrusions [46]. The precision and recall rates are added together to create the F-score.

#### 4.1 Analysis of Model performances

Table 4 highlights a performance analysis of ID-based detection methods. While comparing the results in terms of the core strategies, it is noted that the works with deep learning techniques outperform lightweight. Among lightweight detection techniques, VALID shows better accuracy than GGNB and SIDuDTW. Because it is unable to distinguish attacks that involve a single malicious message, SIDuDTW performs less well in the lightweight category.

**Table 4 : Performance analysis of ID Based Detection**

Strategy	Work	Precision	Recall	F1-Score	Accuracy
Light Weight	GGNB	0.9886	0.966	0.9762	0.962
	VALID	-	-	-	0.9954
	SIDuDTW	-	0.983	0.932	0.9565
Deep Learning	Rec-CNN	0.9097	0.974	0.9408	0.9803
	DCNN	0.9999	0.9984	0.9991	-
	CAAE	0.9996	0.982	0.9907	-

Regarding deep learning-based techniques of ID based detection, DCNN surpasses others with its precision, recall, and F1 score. Also, a similar pattern of results was obtained in DCNN and CAAE, contrary to Rec-CNN.

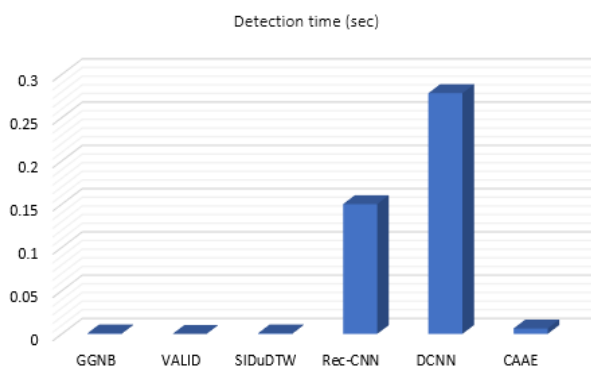


Figure 5: Detection Time of ID Based Techniques

A comparison in time consumption of different ID-based detection methods is given in Figure 5. It is clear that the deep

learning methods Rec- CNN and DCNN have the largest time consumption for detection- 0.15 sec and 0.2783 sec. Lightweight approaches GGNB, SIDuDTW and VALID take only 0.00064 sec, 0.00069 sec, and 0.0005 sec, respectively, much less than other strategies. GGNB, Graph-based IDS, shows low detection time because graph structures always allow input data to be compressed as users define an abstraction of the scene [47]. So, while considering the evaluation matrices and latency together, VALID performs better because it can give an accuracy of 99% in a reduced detection time.

**Table 5 Performance analysis of Payload Based Detection**

Strategy	Work	Precision	Recall	F1-Score	Accuracy
Light Weight	BNN-IDS	-	0.9467	-	0.9315
	H-IDSFS	0.9998	0.9778	0.9881	0.9811
Deep Learning	HyDL-IDS	0.9999	0.9999	0.9998	0.9999
	CANdito	-	-	0.901	0.8509
	TSP	0.911	0.97	0.94	0.8624

The performance evaluation of payload-based detection techniques is illustrated in Table 5, and as in the previous case, the deep learning-based HyDL - IDS produces the best results among all models. It is noted in the results that the lightweight models have an accuracy range between 0.93 to 0.98, and it was about 0.85 to 0.999 in the deep learning models. The accuracy of CANdito and TSP, which rely on LSTM for their attack detection, is comparable.

Here, we found that the payload-based detection technique BNN performs well in terms of time and memory consumption among the selected models, using only 512 kb memory and 0.0004 sec detection time. FPGAs [48],[49] are used by the BNN to speed up efficiency in terms of time, memory, and energy. In Table 6, the analysis of CAN frame-based techniques is presented. Among these methods, MTH-IDS excels in the lightweight category, whereas NovelADS performs well in the deep learning category. CANintelliIDS performed the least in the list in terms of precision, recall, and F1-Score. The lightweight model MTH-IDS, which can detect diverse attacks with an accuracy of 99.85 % and a detection time of 0.0005 sec, is the best-performing model in CAN frame-based detection.

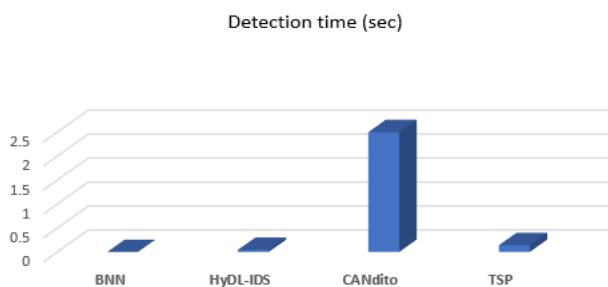


Figure 6: Detection Time of Payload Based Techniques

The deep learning techniques CAN-ADF and HyDL-IDS detect the fuzzy and RPM Spoofing attack with similar performance. The reason is that both extract spatiotemporal characteristics, and CAN - ADF has a combined heuristics algorithm [43]. Among different input data modalities, most works have used CAN Data frame. Lightweight intrusion detection systems often leverage physical characteristics of the CAN bus, such as voltage and clock-skew, to detect intrusions. Additionally, machine learning techniques like Naive Bayes and Bayesian optimization are commonly employed in this particular field of IDS. In the case of deep learning IDS, unsupervised techniques like OCSVM and auto encoders are commonly used. Because of the significant role of timestamps in CAN messages, supervised techniques like LSTM, GRU, and an ensemble of those methods are also widely used for intrusion detection. The methods that use the physical characteristics of CAN bus, VALID, and ASSASSIN show better latency. While considering all selected works, we see that the deep learning-based models use more time to detect the attacks, so they lack their performance in real-time responsiveness.

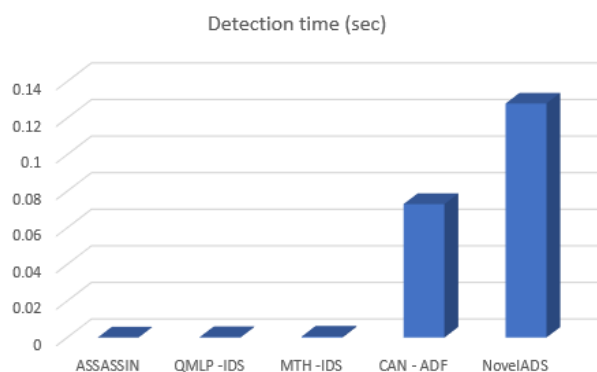


Figure 7: Detection Time of CAN Frame Based Techniques

Table 6 Performance analysis of CAN Frame Based Detection

Strategy	Work	Precision	Recall	F1-Score	Accuracy
Light Weight	ASSASSIN	-	-	-	0.9902
	QMLP-IDS	0.992	0.9991	0.9991	-
	MTH-IDS	-	-	0.9999	0.9985
Deep Learning	CAN-ADF	-	-	0.9999	0.9945
	NovelADS	0.9995	0.9991	0.9993	-
	CANintelli IDS	0.9369	0.9391	0.9373	-

This study found that prior research generally used the Car Hacking Dataset [57] of Hacking and Countermeasure Research Lab (HCRL) for their experiments. Additionally, recent studies have promoted the use of privately captured CAN traffic. Figure 8 depicts the attack- wise detection capabilities of algorithms with the Car Hacking Dataset. The commonly available datasets for intrusion detection in controller area networks are shown in Table 7.

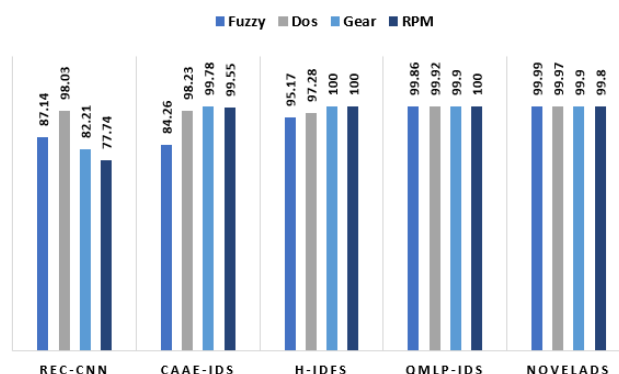


Figure 8: Accuracy of different models using Car Hacking Dataset

Table 7: Commonly Available Datasets for CAN Intrusion Detection

Ref	Dataset	Organization	Vehicle Used	Attacks
[31]	Car-Hacking dataset	HCRL	Real vehicle	DoS, Fuzzing, RPM Spoofing, Gear Spoofing
[35]	CAN Dataset (OTIDS)	HCRL	KIA Soul	DoS, Fuzzing, Impersonation Attack



[36]	Survival Analysis	HCRL	HYUNDAI YF Sonata, KIA Soul, CHEVROLET Spark	DoS, Fuzzing, Malfunction (Spoofing)
[37]	Car Hacking Attack and Defense Challenge	HCRL	Hyundai Avante CN7	DoS, Fuzzing, Spoofing, Replay
[38]	SynCAN dataset	BOSCH	-	Plateau, Continuous, Playback, Suppress, Loading
[39]	TU Eindhoven CAN Bus Intrusion Dataset	Eindhoven University of Technology	Opel Astra, Renault Clio	DoS, Fuzzing, Diagnostic, Replay, Suspension
[40]	CrySyS Lab Dataset and CAN Log Infector	Budapest University of Technology and Economics	-	DoS, Fuzzing, Replay
[41]	Real ORNL Automotive Dynamometer (ROAD)	ORNL	-	Fuzzing, Targeted ID Attacks, Accelerator Attacks

Table 8 Attack wise performances

Fuzzy	HyDL - IDS	Deep Learning, Payload	100	Car Hacking Dataset
Replay	CAN - ADF	Deep Learning, CAN Frame	97	CAN Intrusion Dataset
Spoofing	HyDL - IDS	Deep Learning, Payload	100	Car Hacking Dataset

## 5. Inferences and Future Directions

The analysis of IDS using differing different input modalities leads to the conclusion that CAN frame- based techniques consistently improve their performances compared to other model input modalities leads to the conclusion that CAN frame- based techniques consistently improve their performances compared to other modalities. The highest-performing strategy and modality for each attack are shown in Table 8. According to the results presented in the table, the CAN frame-based detection technique is better than others for DoS and replay attacks. In CAN frame-based techniques, the input data consists of either the complete CAN frame or a combination of various fields within the frame. It is worth noting that when it comes to detecting replay attacks, CAN frame- based detection proves to be more effective compared to other approaches. It is noted in the table that the best results were reported for the CAN Intrusion and Car Hacking datasets. These datasets could support the models to perform well through their characteristics like availability, the large volume of labelled data, real traces, diversity of attacks, and network configurations. Both CAN frame and Payload modalities are found important in the experiments, where the payload could claim the maximum output in the two attacks. The CAN frame is a reliable modality for detecting reply attacks, and its accuracy was just 3% away from the maximum. The prior studies already found that a strong replay attack cannot be predicted with arbitration ID or data alone [58]. In the case of strategy wise performances, it is essential to highlight the fact that deep learning based techniques give better accuracies compared to lightweight.

Table 8 Attack wise performances

Attack	Work	Strategy & Input Modality	Accuracy (%)	Dataset
DoS	MTH - IDS	Light Weight, CAN Frame	100	CAN Intrusion Dataset

Table 8 shows that deep learning strategies can detect attacks like fuzzy, replay, and spoofing effectively. Among these three attacks, the deep learning strategy could claim a reliable prediction in two by hitting the maximum performances in the evaluation. Even though the attacking methodology of Replay makes the deep learning process complicated, it could manage a reasonable performance with an accuracy of 97%. The inclined working principle of deep learning models used the available attack data effectively to train their models [59]; as a result, making the process more time and resource-consuming.

One of the keen aspects of high-profile real-time applications is its capability to produce outcomes in faster and better ways [60]. Because the CAN bus is time-constrained, in- vehicle IDSs should identify the threats and enforce necessary defences in real-time or near real-time. There must be more resource constrained developments to enjoy the performance of heavy-weight deep architectures in autonomous vehicles. The research and industry community is eagerly watching the developments in deep models like the pruning of neural networks [61] that could support edge computing more effectively.

The intelligent use of cloud infrastructure will also help the future IDSs. Figure 10 gives an interesting study between the lightweight and Deep learning based learning models in intrusion detection in autonomous vehicles. The performance of these two strategies with different datasets is compiled in the figure. The lightweight models performed well in both

CAN Frame and ID based input modalities, and the deep learning model could perform well only in the payload. The lightweight model achieved a maximum performance of 99.85 %, which is only 0.14% lower than that of the deep learning model. In the lightweight model, the lowest performance was 98.11 %, which surpasses the deep learning model's performance using the ID input modality. Specifically, in ID-based detection, the lightweight model exhibited superior performance with a margin of 1.51%. The capabilities of a deep learning model to explore the payload are exciting and could attain the maximum accuracy. While considering the light weight model, the CAN Frame of CAN Intrusion Dataset (HCRL) performed well, while the Payload and ID modalities worked well with Car Hacking Dataset and Privately captured dataset from Fiat 500 and Porsche Panama S E-Hybrid datasets, respectively. In the case of deep learning models, the CAN Frame worked well with CAN Intrusion Dataset and Car Hacking Dataset was found suitable for both payload and ID modalities.

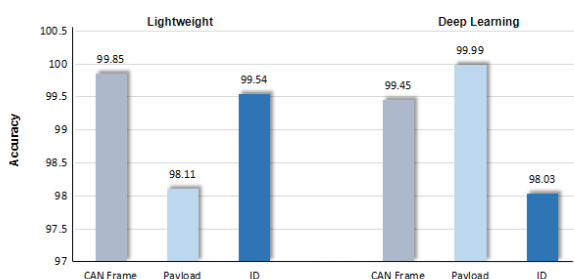


Figure 9: Comparison of various input modalities considering overall accuracy with all the attack classes

The CAN bus's reliable and consistent data makes unsupervised learning (OCSVM, auto encoders) a good fit for it [62]. The major constraint was the need for an extensive dataset that accurately reflects the general scenario. Algorithms like transfer learning [63], one-shot learning [64], and zero-shot learning [65] have been applied to other fields, including image recognition and NLP applications can be employed for accommodating the CAN stream data. The Deep Packet Inspection (DPI) [66] is also effective in CAN bus analysis. Future IDS in CANs may focus on behaviour-based detection rather than relying solely on signature-based approaches. Creating a reliable vehicular dataset with a sufficient and labelled dataset [67] is challenging since capturing the capture message variations in CAN is hard. Such unbalanced data will restrict the learning capability of supervised learning-based models [68] and may badly affect the research progress of the domain. Synthetic datasets created through statistical methods or simulation tools like SUMO [69], MOVE [70], and NS-3 [71] are used to evaluate the security models.

## 6. Conclusion

The CAN bus is highly vulnerable to security threats due to the lack of appropriate encryption and authentication mechanisms. With the technological evolution of Intelligent Transportation Systems (ITS), there is a growing scope for research and innovation in intrusion detection. This study reviewed seventeen recent approaches for real-time intrusion detection in CAN, categorizing them based on input modalities and analyzing the strategies employed—ranging from deep learning to lightweight techniques. Our analysis revealed that while lightweight models tend to underperform with payload-based inputs, they can still deliver competitive results in other modalities compared to deep models. Conversely, deep learning techniques show significant promise in real-time ITS environments, offering high detection capabilities even with constrained computational resources.

Looking ahead, the consistent and reliable structure of CAN bus data makes it a suitable candidate for unsupervised learning methods such as One-Class SVMs and autoencoders. However, a major limitation is the scarcity of comprehensive datasets that represent real-world driving scenarios. To overcome this, advanced learning paradigms such as transfer learning, one-shot learning, and zero-shot learning—successfully applied in domains like image recognition and NLP—could be adapted for CAN data analysis. Additionally, Deep Packet Inspection (DPI) shows potential for enhancing CAN bus security analysis.

Future IDS solutions for CAN should move towards behavior-based detection rather than relying solely on signature-based methods. A persistent challenge in this field is the creation of robust and well-labeled vehicular datasets, as capturing diverse message variations within the CAN is inherently difficult. This imbalance can hinder the performance of supervised learning models and slow the progress of research. To address this, synthetic datasets generated through statistical approaches or simulation tools such as SUMO, MOVE, and NS-3 can be instrumental in evaluating and training IDS models effectively.

## Author's statements

**Acknowledgements-** This work was supported by the Department of Science and Technology, Govt. of India INSPIRE Program.

**Funding Source-** none.

**Authors' Contributions-** Sreelekshmi M S. and Aji S. conceived of the presented idea. Sreelekshmi M S. performed

the literature search and data extraction and drafted the manuscript Sreelekshmi M S. and Aji S. reviewed and edited the manuscript. All authors approved the final version

**Conflict of Interest** - Authors declare that they do not have any conflict of interest.

**Data Availability** - None.

## References

- [1] Bi, Zixiang, et al. "Intrusion Detection Method for In-Vehicle CAN Bus Based on Message and Time Transfer Matrix." *Security and Communication Networks* 2022.1 (2022): 2554280..
- [2] Hussain, Naziya, et al. "Cyber security and privacy of connected and automated vehicles (CAVs)-based federated learning: challenges, opportunities, and open issues." *Federated learning for IoT applications* (2022): 169-183.
- [3] Mchergui, Abir, Tarek Moulahi, and Sherali Zeadally. "Survey on artificial intelligence (AI) techniques for vehicular ad-hoc networks (VANETs)." *Vehicular Communications* 34 (2022): 100403.
- [4] Bendiab, Gueltoom, et al. "Autonomous vehicles security: Challenges and solutions using blockchain and artificial intelligence." *IEEE Transactions on Intelligent Transportation Systems* 24.4 (2023): 3614-3637.
- [5] Olugbade, Samuel, et al. "A review of artificial intelligence and machine learning for incident detectors in road transport systems." *Mathematical and Computational Applications* 27.5 (2022): 77.
- [6] Refat, Rafi Ud Daula, Abdulrahman Abu Elkhail, and Hafiz Malik. "Machine learning for automotive cybersecurity: Challenges, opportunities and future directions." *AI-enabled Technologies for Autonomous and Connected Vehicles* (2022): 547-567.
- [7] Rajapaksha, Sampath, et al. "Ai-based intrusion detection systems for in-vehicle networks: A survey." *ACM Computing Surveys* 55.11 (2023): 1-40.
- [8] Wang, Qian, Zhaojun Lu, and Gang Qu. "An entropy analysis based intrusion detection system for controller area network in vehicles." *2018 31st IEEE International System-on-Chip Conference (SOCC)*. IEEE, 2018.
- [9] Ying, Xuhang, et al. "TACAN: Transmitter authentication through covert channels in controller area networks." *Proceedings of the 10th ACM/IEEE International Conference on Cyber-Physical Systems*. 2019.
- [10] Al-Jarrah, Omar Y., et al. "Intrusion detection systems for intra-vehicle networks: A review." *Ieee Access* 7 (2019): 21266-21289.
- [11] Wei, Hongqian, et al. "Real-time security warning and ECU identification for in-vehicle networks." *IEEE Sensors Journal* 23.17 (2023): 20258-20266.
- [12] Sommer, Florian, Mona Gierl, and Patrick Rebling. "Vehicle Network Platforms for Automotive Security Testing." *Reports on Energy Efficient Mobility* 3 (2023): 72-99.
- [13] Cook, J. A., and J. Sj Freudenberg. "Controller area network (can)." *EECS* 461 (2007): 1-5.
- [14] Lokman, Siti-Farhana, Abu Talib Othman, and Muhammad-Husaini Abu-Bakar. "Intrusion detection system for automotive Controller Area Network (CAN) bus system: a review." *EURASIP Journal on Wireless Communications and Networking* 2019.1 (2019): 1-17.
- [15] Rajapaksha, Sampath, et al. "Improving in-vehicle networks intrusion detection using on-device transfer learning." *Symposium on vehicles security and privacy*. Vol. 10. 2023..
- [16] Checkoway, Stephen, et al. "Comprehensive experimental analyses of automotive attack surfaces." *20th USENIX security symposium (USENIX Security 11)*. 2011.
- [17] Miller, Charlie, and Chris Valasek. "Remote exploitation of an unaltered passenger vehicle." *Black Hat USA* 2015.S 91 (2015): 1-91.
- [18] Nie, Sen, Ling Liu, and Yuefeng Du. "Free-fall: Hacking tesla from wireless to can bus." *Briefing, Black Hat USA* 25.1 (2017): 16.
- [19] Nie, Sen, et al. "Over-the-air: How we remotely compromised the gateway, BCM, and autopilot ECUs of Tesla cars." *Briefing, Black Hat USA* 91 (2018): 1-19.
- [20] Dibaei, Mahdi, et al. "Attacks and defences on intelligent connected vehicles: A survey." *Digital Communications and Networks* 6.4 (2020): 399-421.
- [21] Nichelini, Alessandro, et al. "Canova: a hybrid intrusion detection framework based on automatic signal classification for can." *Computers & Security* 128 (2023): 103166.
- [22] Hossain, Md Delwar, et al. "Long short-term memory-based intrusion detection system for in-vehicle controller area network bus." *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE, 2020.
- [23] Nguyen, Trieu Phong, Heungwoo Nam, and Daehee Kim. "Transformer-based attention network for in-vehicle intrusion detection." *IEEE Access* 11 (2023): 55389-55403.
- [24] Islam, Riadul, et al. "GGNB: Graph-based Gaussian naive Bayes intrusion detection system for CAN bus." *Vehicular Communications* 33 (2022): 100442.
- [25] Schell, Oleg, and Marcel Kneib. "VALID: Voltage-based lightweight intrusion detection for the controller area network." *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, 2020.
- [26] Sun, Heng, et al. "Analysis of ID sequences similarity using DTW in intrusion detection for CAN bus." *IEEE Transactions on Vehicular Technology* 71.10 (2022): 10426-10441.
- [27] Desta, Araya Kibrom, et al. "Rec-CNN: In-vehicle networks intrusion detection using convolutional neural networks trained on recurrence plots." *Vehicular Communications* 35 (2022): 100470.
- [28] Song, Hyun Min, Jiyoung Woo, and Huy Kang Kim. "In-vehicle network intrusion detection using deep convolutional neural network." *Vehicular Communications* 21 (2020): 100198.
- [29] Hoang, Thien-Nu, and Daehee Kim. "Detecting in-vehicle intrusion via semi-supervised learning-based

- convolutional adversarial autoencoders." *Vehicular Communications* 38 (2022): 100520.
- [30] Zhang, Linxi, Xuke Yan, and Di Ma. "A binarized neural network approach to accelerate in-vehicle network intrusion detection." *IEEE Access* 10 (2022): 123505-123520..
- [31] Derhab, Abdelouahid, et al. "Histogram-based intrusion detection and filtering framework for secure and safe in-vehicle networks." *IEEE Transactions on Intelligent Transportation Systems* 23.3 (2021): 2366-2379.
- [32] Lo, Wei, et al. "A hybrid deep learning based intrusion detection system using spatial-temporal representation of in-vehicle network traffic." *Vehicular Communications* 35 (2022): 100471.
- [33] Longari, Stefano, et al. "Candito: Improving payload-based detection of attacks on controller area networks." *International Symposium on Cyber Security, Cryptology, and Machine Learning*. Cham: Springer Nature Switzerland, 2023.
- [34] Qin, Hongmao, Mengru Yan, and Haojie Ji. "Application of controller area network (CAN) bus anomaly detection based on time series prediction." *Vehicular Communications* 27 (2021): 100291.
- [35] Schell, Oleg, Claudio Oechsler, and Marcel Kneib. "Asymmetric symbol and skew sender identification for automotive networks." *IEEE Transactions on Information Forensics and Security* 17 (2022): 3959-3971.
- [36] Khandelwal, Shashwat, and Shanker Shreejith. "A lightweight FPGA-based IDS-ECU architecture for automotive CAN." *2022 international conference on field-programmable technology (ICFPT)*. IEEE, 2022.
- [37] Yang, Li, Abdallah Moubayed, and Abdallah Shami. "MTH-IDS: A multitiered hybrid intrusion detection system for internet of vehicles." *IEEE Internet of Things Journal* 9.1 (2021): 616-632.
- [38] Tariq, Shahroz, et al. "CAN-ADF: The controller area network attack detection framework." *Computers & Security* 94 (2020): 101857.
- [39] Agrawal, Kushagra, et al. "NovelADS: A novel anomaly detection system for intra-vehicular networks." *IEEE Transactions on Intelligent Transportation Systems* 23.11 (2022): 22596-22606.
- [40] Javed, Abdul Rehman, et al. "CANintelliIDS: Detecting in-vehicle intrusion attacks on a controller area network using CNN and attention-based GRU." *IEEE transactions on network science and engineering* 8.2 (2021): 1456-1466.
- [41] Longari, Stefano, et al. "CANnolo: An anomaly detection system based on LSTM autoencoders for controller area network." *IEEE Transactions on Network and Service Management* 18.2 (2020): 1913-1924.
- [42] Wang, Chao, et al. "DLAU: A scalable deep learning accelerator unit on FPGA." *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 36.3 (2016): 513-517.
- [43] Sreelekshmi, M. S., and S. Aji. "A Graph-Based Strategy for Intrusion Detection in Connected Vehicles." *International Conference on Information and Communication Technology for Competitive Strategies*. Singapore: Springer Nature Singapore, 2022.
- [44] Al-Jarrah, Omar Y., et al. "A novel detection approach of unknown cyber-attacks for intra-vehicle networks using recurrence plots and neural networks." *IEEE Open Journal of Vehicular Technology* 4 (2023): 271-280.
- [45] Syed, Naeem Firdous, Mengmeng Ge, and Zubair Baig. "Fog-cloud based intrusion detection system using Recurrent Neural Networks and feature selection for IoT networks." *Computer Networks* 225 (2023): 109662.
- [46] Nichelini, Alessandro, et al. "Canova: a hybrid intrusion detection framework based on automatic signal classification for can." *Computers & Security* 128 (2023): 103166.
- [47] Xiao, Dannier, et al. "Review of graph-based hazardous event detection methods for autonomous driving systems." *IEEE Transactions on Intelligent Transportation Systems* 24.5 (2023): 4697-4715.
- [48] Li, Zhengjie, et al. "A survey of FPGA design for AI era." *Journal of Semiconductors* 41.2 (2020): 021402.
- [49] Moss, Duncan JM, et al. "High performance binary neural networks on the Xeon+ FPGA™ platform." *2017 27th International conference on field programmable logic and applications (FPL)*. IEEE, 2017.
- [50] Lee, Hyunsung, Seong Hoon Jeong, and Huy Kang Kim. "OTIDS: A novel intrusion detection system for in-vehicle network by using remote frame." *2017 15th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, 2017.
- [51] Han, Mee Lan, Byung Il Kwak, and Huy Kang Kim. "Anomaly intrusion detection method for vehicular networks based on survival analysis." *Vehicular communications* 14 (2018): 52-63.
- [52] Kang, Hyunjae, et al. "Car hacking: Attack defense challenge 2020 dataset." (*No Title*) (2021).
- [53] Hanselmann, Markus, et al. "CANet: An unsupervised intrusion detection system for high dimensional CAN bus data." *Ieee Access* 8 (2020): 58194-58205.
- [54] Dupont, Guillaume, et al. "Evaluation framework for network intrusion detection systems for in-vehicle can." *2019 IEEE International Conference on Connected Vehicles and Expo (ICCVE)*. IEEE, 2019.
- [55] Gazdag, Andras, Levente Buttyan, and Zsolt Szalay. "FORENSICS AWARE LOSSLESS COMPRESSION OF CAN TRAFFIC LOGS." *Komunikácie* 19.4 (2017).
- [56] Verma, Miki E., et al. "A comprehensive guide to CAN IDS data & introduction of the ROAD dataset." *arXiv preprint arXiv:2012.14600* (2020).
- [57] Song, Hyun Min, Jiyoung Woo, and Huy Kang Kim. "In-vehicle network intrusion detection using deep convolutional neural network." *Vehicular Communications* 21 (2020): 100198.
- [58] Islam, Riadul, et al. "Graph-based intrusion detection system for controller area networks." *IEEE Transactions on Intelligent Transportation Systems* 23.3 (2020): 1727-1736.

- [59] Banafshehvaragh, Samira Tahajomi, and Amir Masoud Rahmani. "Intrusion, anomaly, and attack detection in smart vehicles." *Microprocessors and Microsystems* 96 (2023): 104726.
- [60] Menghani, Gaurav. "Efficient deep learning: A survey on making deep learning models smaller, faster, and better." *ACM Computing Surveys* 55.12 (2023): 1-37.
- [61] Vadera, Sunil, and Salem Ameen. "Methods for pruning deep neural networks." *IEEE Access* 10 (2022): 63280-63300.
- [62] Tomlinson, Andrew, Jeremy Bryans, and Siraj Ahmed Shaikh. "Using a one-class compound classifier to detect in-vehicle network attacks." *Proceedings of the genetic and evolutionary computation conference companion*. 2018.
- [63] Torrey, Lisa, and Jude Shavlik. "Transfer learning." *Handbook of research on machine learning applications and trends: algorithms, methods, and techniques*. IGI global, 2010. 242-264.
- [64] Vinyals, Oriol, et al. "Matching networks for one shot learning." *Advances in neural information processing systems* 29 (2016).
- [65] Xian, Yongqin, Bernt Schiele, and Zeynep Akata. "Zero-shot learning-the good, the bad and the ugly." *Proceedings of the IEEE conference on computer vision and pattern recognition*. 2017.
- [66] Sun, Miao, Qiang Zhang, and Gan Han. "Research on Deep Packet Inspection for Driving Digital Operation." *International Conference On Signal And Information Processing, Networking And Computers*. Singapore: Springer Nature Singapore, 2022.
- [67] Swessi, Dorsaf, and Hanen Idoudi. "A comparative review of security threats datasets for vehicular networks." *2021 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*. IEEE, 2021.
- [68] Cheng, Pengzhou, Mu Han, and Gongshen Liu. "DESC-IDS: Towards an efficient real-time automotive intrusion detection system based on deep evolving stream clustering." *Future Generation Computer Systems* 140 (2023): 266-281.
- [69] Krajewicz, Daniel. "Traffic simulation with SUMO—simulation of urban mobility." *Fundamentals of traffic simulation* (2010): 269-293.
- [70] Lan, Kun-Chan. "MOVE: a practical simulator for mobility model in VANET." *Telematics communication technologies and vehicular networks: wireless architectures and applications*. IGI Global Scientific Publishing, 2010. 355-368.
- [71] Carneiro, Gustavo. "NS-3: Network simulator 3." *UTM lab meeting April*. Vol. 20. No. 1. 2010.

## AUTHORS PROFILE

**Sreelekshmi M S** received the M.Sc. degree in 2020 from the Department of Computer Science, Central University of Kerala, India, where she is currently working toward the Ph.D. degree with the University of Kerala, India. Her research interests include machine learning, deep learning, intelligent transportation systems, and autonomous security.



**Aji S** received a B.Sc. degree in Physics from the University of Kerala, India in 1997, and Master of Computer Applications Degree from Cochin University of Science and Technology, India and Ph.D. in Data mining from the University of Kerala, India in 2001 and 2012 respectively. In 2001, he joined the department of Computer Science, University of Kerala. His research interests include Datamining, Cyber Security, and image and video analysis. He has published a good number of publications in internationally reputed journals. He is an active reviewer of many international journals and conferences

