Systematic Literature Review: Anomaly Detection in Connected and Autonomous Vehicles

John Roar Ventura Solaas, Enrico Mariconti, Nilufer Tuptuk

***Abstract*—This systematic literature review provides a structured and detailed overview of research on anomaly detection for connected and autonomous vehicles, focusing on the Artificial Intelligence methods employed, training approaches, and testing and evaluation techniques. The initial database search identified 2,160 articles, of which 203 were included in this review after rigorous screening and assessment.**

This study revealed that the most commonly used anomaly detection techniques employed are deep learning networks such as LSTM, CNN, and autoencoders, alongside one-class SVM. Most detection models were trained using real-world operational vehicle data, although anomalies, such as attacks and faults, were often injected artificially into the datasets. The models were evaluated primarily using five key evaluation metrics: recall, accuracy, precision, F1-score, and false positive rate. The most frequently used set of evaluation metrics for detection models were accuracy, precision, recall, and F1-score.

The review makes several recommendations to improve future work related to anomaly detection models. It recommends providing comprehensive assessment of the anomaly detection models and emphasise the importance to share models publicly to facilitate collaboration within the research community and enable further validation. Recommendations also include the need for benchmarking datasets with predefined anomalies or cyberattacks (with comprehensive threat modelling) to test and improve the effectiveness of the proposed anomaly detection models. Future research should focus on the deployment of anomaly based detection in vehicles to evaluate their performance in real-world driving conditions, and explore systems using communication protocols beyond CAN, such as Ethernet and FlexRay.

***Index Terms*—Connected and Autonomous Vehicles, Anomaly Detection, Intrusion Detection System, Artificial Intelligence.**

I. Introduction

THE last decade have seen unprecedented growth in the technology of Connected and Autonomous Vehicles (CAVs), which is driven by improvements and innovations in Artificial Intelligence (AI) [1] and enabling technology related to sensors and communication systems. CAVs include a variety of internal and external sensors, including cameras, LiDar (Light Detection and Ranging), radar, GNSS/GPS, and infrared sensors, to help them gather data about their surroundings and make important judgments. These vehicles are expected to be connected to other vehicles through Vehicle-to-Vehicle (V2V) communication and to the infrastructure using the Vehicle-to-Infrastructure (V2I) communication network. By using in-vehicle communication, the vehicle connects the components of the vehicle and enables the exchange of information between different modules and sensors within the vehicle. Machine Learning (ML) including Deep Learning (DL) techniques are used to process large sets of data and enable CAVs to operate safely and independently without a human driver. Examples of such techniques include real-time sensor anomaly detection [2], detecting faults in the vehicle parts such as battery [3] and detecting driver behaviour anomalies [4].

The different levels of vehicle autonomy have been classified into six levels where level 0 is a normal human driver without any assistance, and level 5 is a self-driving vehicle without any human supervision [5]. Several companies, such as Waymo (formerly known as the Google Self-Driving Car Project), Cruise, TuSimple, and Aurora, are working actively towards developing level 5 autonomous vehicles. Technological advancements, particularly in deep learning, are enabling the development of fully autonomous vehicles. This is done through advanced data analytics that allows vehicles with the capability to process and understand a large volume of complex data from multiple sources, essential for their operation. Deep learning models can analyse sensor data in real time, identify objects, pedestrians and road infrastructure, improving the vehicle's ability to navigate safely. Recent developments in deep learning have demonstrated performance that is superior to that of humans [6], and it is expected that autonomous vehicles will significantly reduce the risk of road users and other vehicles compared to vehicles operated by human drivers [7]. Other predicted benefits of connected and autonomous vehicles include reducing isolation for people with disabilities or elderly people; improving access to education, work and leisure; and helping deliver essential goods and groceries [8]. In April 2023, Wayve [9] teamed up with the supermarket Asda in the UK, launching a year-long trial delivering groceries to 72,000 households in London using autonomous vehicles. Industry efforts like these show that CAVs are becoming a fast reality and they are expected to grow both in popularity and advance in their technology.

Although CAVs have become a promising technology for the future of transportation, ensuring their safety and security remains a significant challenge. Anomaly detection, which is the ability to identify abnormal behaviour or events, plays an important role in maintaining the safety and security of CAVs. Anomaly detection can be an effective way to secure CAVs [10]. It could be used to detect faults in the vehicle's hardware and software, dangerous road conditions, cyber and physical attacks targeting the vehicle, or unusual driver behaviour. Furthermore, anomaly detection techniques have already been proposed to address the complex task of ensuring both the security and safety of CAVs. ML and DL have emerged as one of the most promising methods for detecting anomalies in CAVs due to their ability to efficiently process vast amounts

TABLE I
OVERVIEW OF REVIEWS AND SURVEYS ON ANOMALY DETECTION FOR CONNECTED AND AUTONOMOUS VEHICLES

	[10]	[12]	[13]	[14]	This review
Type	Survey	Survey	Survey	Survey	Systematic review
Years	Early 2000's–2018	2016–2020	2015–2022	2019–2023	2013–2023
Attack surface	X	X			X
Data source	X			X	X
Application targeted	X	X	X	X	X
Dataset used			X	X	X
Dataset characteristics					X
Simulation method (data generation)			X	X	X
Detection technique	X	X	X	X	X
Security or safety-focused					X
Model availability					X
Anomaly generation					X
Evaluation metrics				X	X
Anomaly types detected		X			
Scientific method	X	X	X	X	X

of data and detect patterns that indicate anomalies [11]. By using ML algorithms, anomaly detection models can learn from historical data on normal vehicle operation to recognise abnormal behaviour, such as zero-day attacks.

Table I presents related surveys and reviews relevant to CAVs. These earlier studies lacked a systematic literature review and did not cover the following aspects: information on model availability, generation of anomalies, dataset characteristics, and evaluation metrics. Taking into consideration these gaps, a systematic review is carried out to examine the current state of the literature on anomaly detection for CAVs in a systematic and structured way. This review does not explore types of anomalies detected, as the focus of this paper is on the broader objectives of identifying AI methods used, training processes, and evaluation metrics for anomaly detection in CAVs, leaving analysis of anomaly types beyond the scope of this research.

Conducting a systematic literature review of anomaly detection for CAVs is important for several reasons. First, the field is rapidly evolving, with advancements and new research being published regularly. A systematic review will ensure that the latest findings are included, thereby providing a comprehensive and contemporary overview of the literature. Moreover, the systematic approach enables us to critically evaluate and synthesise the existing research rigorously to minimise bias [15]. By employing inclusion and exclusion criteria, it is possible to systematically identify and select relevant studies from diverse sources. Lastly, a systematic review allows for the identification of trends, patterns, and gaps in the current literature [16]. By analysing the various methods used for anomaly detection, the training procedures employed, and the evaluation methodologies utilised, it is possible to gain a comprehensive understanding of the strengths and limitations of existing approaches. This knowledge can serve as a foundation for future research directions and inform the development of more transparent and robust anomaly detection techniques.

This systematic review aims to analyse the existing literature on anomaly detection for CAVs focusing on exploring the various methods employed for anomaly detection, the training procedures for detection models, and the evaluation methodologies. This review aims to provide a comprehensive understanding of the current state of anomaly detection for CAVs by answering the following research questions:

- RQ1: What AI methods have been developed to detect anomalies in CAVs?
- RQ2: How are anomaly detection models for CAVs trained?
- RQ3: How are anomaly detection models for CAVs tested and evaluated?

Addressing these research questions include gaining an understanding of the types of algorithms used in anomaly detection models, the application domain of each model, and whether the method is focused on safety or security.

The remainder of the paper is organised as follows. Section II provides an overview of the background, covering CAVs, attack surfaces, Artificial Intelligence, and anomaly detection. Section III outlines the methodology for the systematic literature review, detailing the review protocol. Section IV presents the results, followed by Section V, which discusses the findings and provides recommendations. Finally, Section VI concludes the paper.

II. BACKGROUND

A. Connected and Autonomous Vehicles

CAVs have emerged as a transformative technology, gradually replacing human drivers to varying extents in the operation of vehicles [17]. The advent of automated driving systems can be traced back to the early 20th century when initial technological functionalities, such as autonomous speed, brake, lane control, and basic cruise control capabilities, were introduced [18]–[21]. Furthermore, over the past decade, there has been an unprecedented surge in technological advancements, leading to the testing of numerous prototype CAVs on public roads [22]. Consequently, CAVs are widely regarded as the epitome of future automotive engineering [23].

CAVs are different from traditional vehicles in several aspects. CAVs are equipped with sensors to create a perception of the vehicle's surroundings. Cameras, radar, LiDAR, and GPS sensors on the CAV are responsible for perceiving the vehicle's dynamics (such as location and speed) as well as its immediate environment (such as distances to other vehicles,

traffic conditions, and traffic signals) [24], [25]. This data is processed by the onboard computer, which then issues commands to the Electronic Control Units (ECUs). The ECUs, smaller controllers that control specific functions within the vehicle, in turn, control the relevant actuators to adjust the vehicle's speed and direction as required. Communication systems within the vehicle, such as the Controller Area Network (CAN) bus, enables the communication between the in-vehicle network's actuators, external sensors, ECUs, and the onboard computer. CAVs also frequently employ the Global Navigation Satellite System (GNSS) such as Global Positioning System (GPS) to provide precise location data.

According to the Society of Automotive Engineers (SAE), vehicles are categorised into six levels of autonomy [26]. The six levels, which range from 0 (no autonomous feature) to 5 (completely self-driving vehicle), can be thought of as a progression of self-driving features [27]. Level 0 has no automation and completely puts the driver in charge. At Level 1, the vehicle may notify the driver of problems and circumstances using smart sensors. Level 2 automation allows the vehicle to carry out some assistance tasks, but the driver retains control. Nominal autonomy is Level 3, where the majority of safety-critical operations can be carried out by the vehicle under recognised circumstances, but the driver must be prepared to take over. At level 4, also known as high automation, the vehicle is capable of performing all safety-critical driving tasks in constrained spaces without human intervention. Level 5 is the ultimate step of autonomy. At this point, the vehicle is capable of moving under any conditions without a human driver, and the vehicle no longer requires a steering wheel or a brake pedal.

The new generation of information and communication technologies that connect vehicles to everything is known as Vehicle-to-Everything (V2X) communication [28]. V2X communication encapsulates diverse communication modalities, including communication with infrastructure, denominated as Vehicle-to-Infrastructure (V2I); communication with peer vehicles, designated as Vehicle-to-Vehicle (V2V); communication with pedestrians, termed Vehicle-to-Pedestrian (V2P); connections with network systems or cloud-based services, recognised as Vehicle-to-Network (V2N) and Vehicle-to-Cloud (V2C), respectively. Furthermore, internal communication within the vehicular framework is subsumed within the V2X paradigm, encompassing all intra-vehicular components such as sensors, LiDAR systems, cameras, peripheral devices, and the onboard computational unit. Specifically, the rubric of Vehicle-to-Grid (V2G) communication pertains to the communication occurring between Electric Vehicles (EVs) and the electric grid infrastructure, facilitating not only energy consumption for EV charging but also enabling surplus energy discharge into the grid. Also, the domain of Vehicle-to-Device (V2D) communication encompasses the interaction between vehicles and an array of external devices or cloud-hosted services. Essentially, V2X is the communication that occurs external to the vehicle as well as in-vehicle communication. This communication is essential for the proper operation of CAVs, however, reliance on these communication channels also exposes the vehicle to security attacks.

B. Attack Surfaces

The expanding network communication infrastructure surrounding CAVs increases their vulnerability to security threats, as each connection point represents a potential entry point for attackers [27]. Potential attackers could exploit vulnerabilities within the V2X network through various connection points, including links within the controller network connecting the CAN bus with ECUs, interconnections among ECUs, connections from ECUs to actuators, and even targeting internal sensors and actuators themselves, highlighting the vulnerabilities in in-vehicle communication. In contemporary vehicles, the proliferation of ECUs, ranging from 70 to 100 [29], in contrast to only two ECUs in the 1980s [30], has significantly escalated the attack surface. Furthermore, CAVs are exposed to heightened risk due to their diverse onboard computer connections, encompassing both wireless interfaces like WiFi for external devices and physical connections like Ethernet and USB, extending to sensors, dashboards, and externally introduced devices. These extended connection points lack robust security measures, rendering CAVs susceptible to various forms of cyberattacks, thereby attracting potential malevolent actors seeking to exploit these vulnerabilities to steal personal data, inflict damage to the property and environment, or cause bodily injury [31].

To address the expanded attack surface in CAVs, several authors have attempted to address security requirements, which are, in essence, an expansion and modification of the Confidentiality, Integrity, and Availability (CIA) triangle. Confidentiality is a principle concerned about the secrecy of information and inaccessibility to unauthorised actors; integrity ensures that data remains trustworthy and accurate; and availability ensures that information is accessible when needed. The CIA triangle is a fundamental framework for designing and evaluating information security measures. The security requirements of CAVs; vehicular ad hoc networks (VANETs), which are wireless networks formed by vehicles and roadside infrastructure for improved road safety and traffic management through V2V and V2I communication; and Intelligent Transportation Systems (ITS), which are communication systems used to enhance the safety, efficiency, and sustainability of transportation networks by improving traffic management, providing real-time information to travellers, and optimising infrastructure utilisation, can be categorised into four subcategories [32]–[35]:

1) Authenticity/identification: It is necessary to guarantee the identity of the vehicle driver, the data source, and the vehicle's position. To stop attacks involving fabricated entities, user authentication is first required. Second, data source authenticity is crucial to determining whether a valid company produced the data. Third, location authenticity is employed to guarantee the accuracy of location information collected through GPS sensors and other vehicles.
2) Availability: Information sent or shared, services, and functionality must be processed and made readily available in real-time.
3) Data integrity: Data must be received in the correct

form without being tampered with, altered, or deleted inadvertently or maliciously during transmission.
4) Confidentiality: Exchanged data should not be accessible to harmful or unauthorised users and should only be exposed to authorised and legitimate users.

C. Artificial Intelligence

AI can play an important role in enhancing the protection of CAVs [36]. It can aid in improving the decision-making process of CAVs, enabling them to make real-time, informed choices based on multiple diverse data inputs and evolving road conditions, ultimately increasing the safety and reliability of autonomous driving systems. With the complexity and variability of real-world driving scenarios, AI, like deep learning algorithms can analyse large and multimodal datasets collected by sensors, cameras, and other sources in CAVs to identify patterns and detect potential risks or anomalies [13]. By using AI techniques, CAVs can learn from historical data and adapt their behaviour to different situations, improving their ability to anticipate and respond to potential hazards. AI algorithms can also help develop robust anomaly detection systems to identify and mitigate malicious attacks or unauthorised access attempts, ensuring the security and integrity of the vehicle's operation [37]. Two of the subsets of AI that are used to build anomaly detection models in CAVs are ML and DL.

Machine Learning (ML) has become a widely employed method for building models that can learn complex relationships within datasets [38]. ML can be broadly classified into three branches: supervised learning, unsupervised learning, and reinforcement learning. Supervised learning is particularly effective when working with labelled data points, allowing for predictive modelling. On the other hand, unsupervised learning techniques are employed to analyse and group datasets without labels, uncovering underlying patterns and structures. Lastly, reinforcement learning focuses on planning and environment control, emphasising the selection of actions that maximise rewards in specific situations. CAVs leverage these algorithms to make predictions and informed decisions regarding driving actions.

Deep Learning (DL) models use artificial neural networks with multiple layers, referred to as deep neural networks, to process and interpret complex sensor data. In the context of CAVs, DL is instrumental in several critical aspects. Firstly, it facilitates perception, allowing CAVs to accurately detect and identify objects, pedestrians, road signs, and lane boundaries from data collected by cameras, LiDAR, radar, and other sensors [39]. Secondly, DL enables sophisticated decision-making by incorporating reinforcement learning techniques, which enable CAVs to navigate complex traffic scenarios, make safe lane changes, and respond to dynamic road conditions [40]. Additionally, DL is important in mapping and localisation, enabling CAVs to create high-definition maps of their environment and precisely determine their position on the road [41]. The adaptability and scalability of deep learning models are of paramount importance in the evolution of CAVs, as they can be continuously improved and updated to handle evolving real-world driving scenarios.

D. Anomaly Detection

Anomaly detection in the form of monitoring for faults and cyber-physical attacks is important to maintain a high level of security and safety for CAVs. Anomaly detection is not exclusively used to identify cyberattacks—it can also be used for predictive maintenance and identify components that become defective over time or to identify anomalies resulting from human error. However, the term Intrusion Detection System (IDS) is commonly used to refer to anomaly detection used to detect cyberattacks [42]. As the attack surface of CAVs expands due to increased interconnectedness with other vehicles and infrastructure, improving their security becomes more necessary than ever to cover the potential points of vulnerabilities. IDSs utilise various techniques, such as signature-based detection, and prediction-based anomaly detection, to identify patterns that indicate potential intrusion attempts or malicious behaviour.

Signature-based IDS is one of the simplest systems for this purpose and is designed to compare the incoming data traffic to a database with known attacks. In this system, an alert will occur when incoming data matches the already stored known attacks. This approach uses the method of blacklisting. Another alternative is a system using a signature-based IDS with a whitelist method. This method only accepts information that corresponds to known benign examples [43]. However, the use of signature-based IDS has the drawback of being inflexible—and not capable of detecting unknown attacks, zero-day attacks. An attacker can bypass the blacklist by making a modest tweak to an attack, but whitelist modes are only useful for smaller systems with specific behaviour requirements.

A prediction-based anomaly detection system could be an alternative to signature-based IDS. In this approach, signatures will not be created, but a model of data dynamics gathered from a system could be generated. Subsequently, by using statistical techniques, it is possible to find unexpected deviations in the data. More specifically, a future prediction of the system value is computed and compared to the actual observed data. An indicator of whether the system is in an abnormal state is the difference between these two values. This approach, which uses prediction-based methods to monitor features like sensor input and control commands, is used in several papers [42], [44]–[46].

To evaluate an ML/DL-based anomaly detection models, several evaluation metrics can be used [47]. A confusion matrix is a table that provides a comprehensive view of the performance of a classification model. In the matrix, four classes are highlighted: true positive (TP), false negative (FN), false positive (FP), and true negative (TN). Based on the information provided in the confusion metrics, widely used evaluation or performance metrics include accuracy, recall, precision, and F1-score can be computed.

III. Methodology

This systematic literature review was conducted using the PRISMA protocol [48].

A. Search Terms

In September 2023, an exhaustive literature search was conducted across multiple scholarly databases, including Web of Science, ProQuest, Scopus, IEEE Xplore Digital Library, and ACM Digital Library. The search was restricted to articles published between January 2013 and September 2023 to capture the latest decade of research on the topic. To achieve a balance between sensitivity and specificity in the literature review process, various search terms were piloted and refined. Multiple iterations were carried out, with 100 articles assessed for each search iteration to determine the relevance rate of each search. Ultimately, the search term that yielded the highest number of relevant articles was identified using a keyword search with the following keywords:

”vehicle*” AND ”anomaly detection”

B. Inclusion/exclusion Criteria

To answer the research questions introduced in the introduction, and ensure a comprehensive and reliable review, criteria were set to guide the identification and selection of relevant academic literature. The search was restricted to peer-reviewed international conference papers and journal articles. Conversely, articles that were published in magazines or newspapers or those that were behind a paywall that our institution did not have access to were excluded from the review. The exclusion criteria proposed in Edanz-Learning-Team [49] and Meline [50] were employed to eliminate any articles that did not meet the criteria for inclusion:

- Issues with methodological quality
- Review articles with no original data
- Works which are not relevant to the research question and outcomes
- Sources in languages other than English

Furthermore, specific criteria have been established to narrow the relevance of the articles. These exclusion criteria are:

- Published before 2013
- The main subject is unmanned aerial vehicles (UAV), military/naval systems, air vehicles, rail vehicles or non-ground vehicles.
- The anomaly detection model is built on supervised models.

C. Filtering Stages

Following the initial literature search, a process of removing duplication was conducted using the Zotero software, which identified and eliminated duplicate entries. The remaining articles were then screened using Rayyan, a tool for systematic reviews, to assess conformity with the basic inclusion and exclusion criteria. This tool was also used to remove duplicated articles that were previously not identified using Zotero.

1) Inter-rater Reliability: In the screening stage, identified citations and abstracts were imported to Rayyan, and duplicates were removed. Two researchers have separately read the titles and abstracts of 100 random samples of the identified papers to assess whether they meet the inclusion criteria and to assess inter-rater reliability (IRR) and mitigate coder drift [51]. IRR was assessed using the prevalence- and bias-adjusted kappa (PABAK) statistic, which controls for chance agreement [52]. As a result of the screening and the calculation, the PABAK score of 0.89 indicated high inter-rater agreement (see [53]).

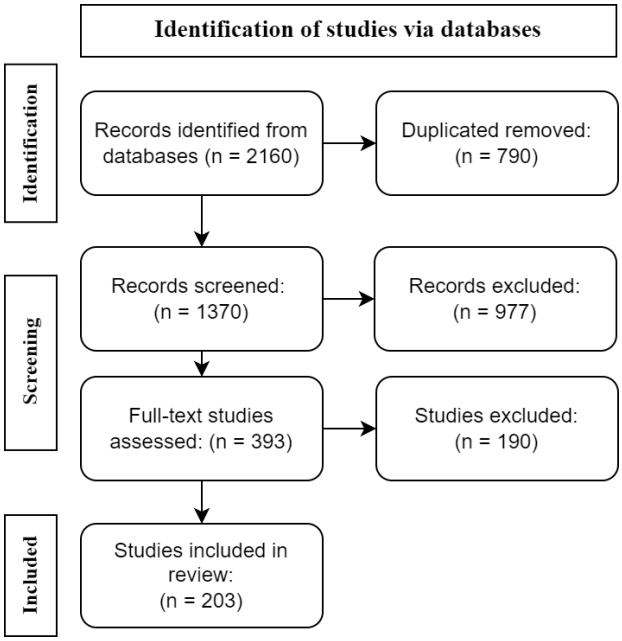

Fig. 1. PRISMA flow diagram of the identification, screening, and inclusion of studies in the review

2) Data Extraction and Management: A pro forma was created to extract information from each study, ensuring that relevant information was captured [53]. The pro forma was piloted on a sample of articles to validate the span of captured data. The pro forma captured the following information categorised to each of the research questions:

1) What AI methods have been developed to detect anomalies in CAVs?
   - Algorithm used in anomaly detection model
   - Application domain of the model
   - Is the method safety or security focused
   - Open source or not
2) How are anomaly detection for CAVs trained?
   - Data used in training anomaly detection models
   - Generation of anomalies in the data
   - Size and date of collection
   - Is the data collected for specific levels of autonomy
3) How are anomaly detection models for CAVs tested and evaluated?
   - Metrics used to test and evaluate the models
   - Detection latency

IV. Results

A. Summary of Search Results

The initial database search yielded 2160 articles (see Fig. 1). In the first stage, 790 duplicates were identified and removed.

In the screening stage, 1370 articles were screened based on titles and articles. Of these, 977 articles were removed. These articles were excluded from the full-text assessment because they focused on unmanned aerial vehicles, naval systems, traffic surveillance, spacecraft, railway systems, launch vehicles, or charging stations. In addition, articles were removed because of no relevance to CAVs. After the screening of titles and abstracts, 393 articles remained for full-text assessment. Of these, 190 articles were excluded due to the same reasons as the previous step, such as lack of access, non-English language, or irrelevance to the study topic. In the end, 203 articles were included in this review. [1]

B. AI Methods used in Anomaly Detection for CAVs

This section will address the first research question: What AI methods have been developed to detect anomalies in CAVs?

1) Algorithms: The analysis revealed the prevalence of several prominent algorithms across the selected articles. Figure 2 provides an overview of the 20 most frequently used methods in the reviewed studies. An overview of datasets commonly used in anomaly detection models, including details on the algorithms implemented and the best-performing models for each dataset, can be found in Table II. All datasets listed in this overview are public. Furthermore, this section highlights the top five AI algorithms most frequently employed, excluding traditional statistics-based methods:

- Long Short-Term Memory (LSTM): LSTM is a type of Recurrent Neural Network (RNN) that is particularly effective in modelling sequential data [54], which was used in 41 papers. LSTM's distinguishing feature lies in its ability to capture intricate, long-range dependencies and to preserve contextual information, rendering it robust for detecting anomalies within the dynamic, time-series data typically emanating from autonomous vehicles. In practical application, LSTM constructs predictive models that are trained to learn the anticipated data patterns. Outliers from these learned patterns are subsequently identified and flagged as anomalies.
- Convolutional Neural Network (CNN): The second most commonly employed algorithm in the reviewed articles, with a count of 21. CNNs are primarily known for their performance in computer vision tasks, as they effectively extract features from images [55]. In CAVs, CNNs are deployed to analyse visual data, notably images derived from onboard cameras. These networks, underpinned by convolutional layers, are adept at identifying abnormal visual patterns or objects that may signify potential anomalies.
- Autoencoder: The third most prevalent algorithm in the reviewed studies, which was used in 13 articles. Autoencoders, representing unsupervised neural networks, are designed to reconstruct input data by learning a compressed representation of the input data. By training an autoencoder on normal operating conditions, any deviations from the learned representation can be interpreted as anomalies [56]. The core principle underpinning their operation is the capacity to encode data into a compact latent representation and subsequently decode it back to its original form. Anomalies come to light when the reconstructed data exhibits disparities from the expected input.
- Deep Learning: The fourth most used algorithm. This category includes models rooted in deep learning principles [57] without specifying a particular algorithm. Deep learning constitutes a subset of machine learning algorithms employing multi-layered neural networks, known as deep neural networks. These networks process data by incorporating data features and utilising multiple layers of processing to represent the data. Deep learning was used in 10 papers.
- One-class Support Vector Machine (one-class SVM): Used in 9 papers. This algorithm is designed to identify a decision boundary that effectively segregates normal data instances from anomalies [58]. One-class SVMs, primarily trained on normal data, possess the ability to establish a hypersphere or hyperplane encapsulating typical data points. Any data instances that deviate beyond this designated hypersphere are categorised as anomalies. These algorithms prove especially efficient when anomalies within the dataset are sparse in proportion.

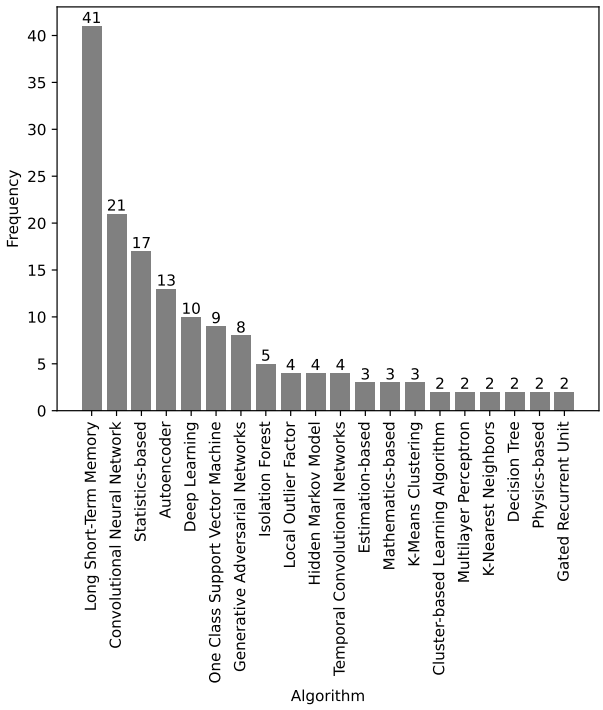

Fig. 2. Algorithms used in anomaly detection for vehicles

2) Application Domain: In terms of the application domain, the analysis revealed the prevalence of several prominent domains in which anomaly detection techniques were applied. Figure 3 provides an overview of the 20 most researched domains covered in the reviewed studies. In this subsection, the focus is on presenting the top five domains that garnered

[1]The collected data can be found at: https://github.com/JRoarVS/ADSCAVs

the most attention:

- CAN (Controller Area Network) bus: The most frequently studied domain for anomaly detection, with a significant focus observed in 78 articles. The CAN bus network serves as a vital communication backbone within vehicles, enabling ECUs to exchange data necessary for controlling various vehicle systems such as brakes, steering, lighting, and more. [59]. Anomaly detection in the CAN bus network involves monitoring and analysing the communication traffic, detecting abnormal traffic patterns, and identifying potential security threats or malfunctions.
- Vehicle sensors: The second most frequently studied field for anomaly detection, with 27 papers. This category encompasses sensor readings from the vehicle's internal components in the form of time series data. Automotive vehicles contain many different types of sensors installed on a vehicle, such as sensors measuring temperature, Revolutions Per Minute (RPM), speed, acceleration, air quality, and fuel level. Vehicle sensors differs from what is recorded as environment sensors (see Fig. 3), which was the application domain for 5 papers. The category environment sensors encompass models that use data from sensors that relate to the vehicle's perception of its environmental surroundings.
- Image: Involves the utilisation of visual data from onboard cameras and other sensors to understand the vehicle's surroundings, contributing to tasks like object detection. Anomaly detection using this type of data allows CAVs to identify irregular or unexpected patterns, objects, or events within the visual systems of the vehicle [60]. 26 articles focused on this domain.
- Internet of Vehicles (IoV): The fifth most prevalent domain in the reviewed studies, with a count of 11 articles. Anomaly detection in this domain is concerned with identifying abnormal behaviours or events in the interconnected vehicular network to ensure the safety, security, and efficiency of the transportation system [61].
- Lane Detection: Encompasses anomaly detection models that focus on detecting anomalous lane driving behaviour through the camera. This category uses the image domain to detect anomalies, but specifically focuses on lane detection. 7 papers focused on anomaly detection for lane abnormalities.

3) Safety and Security: The analysis of the selected articles revealed that out of the total 203 articles, 102 articles specifically emphasised security, 64 articles focused on safety, and 36 articles addressed both safety and security aspects. Data for this section was recorded based on the paper's primary focus. Safety and security are two critical dimensions that require attention in the context of CAVs. Although there may be some overlap between the two, it is important to distinguish between safety and security concerns in this domain. In an information technology context, safety can be described as system's inability to cause harm or undesired effects in its environment while security can be defined as the environment's (e.g. external threats) inability to affect the system [62]:

This review treats safety as ensuring the physical well-being of occupants, pedestrians, other road users, and vehicles. Safety measures aim to minimise the risk of accidents, injuries, and fatalities caused by the operation of CAVs. Anomaly detection techniques focused on safety aim to identify deviations, malfunctions, or abnormal behaviours that may compromise the vehicle's ability to navigate, respond to hazards, or adhere to traffic rules.

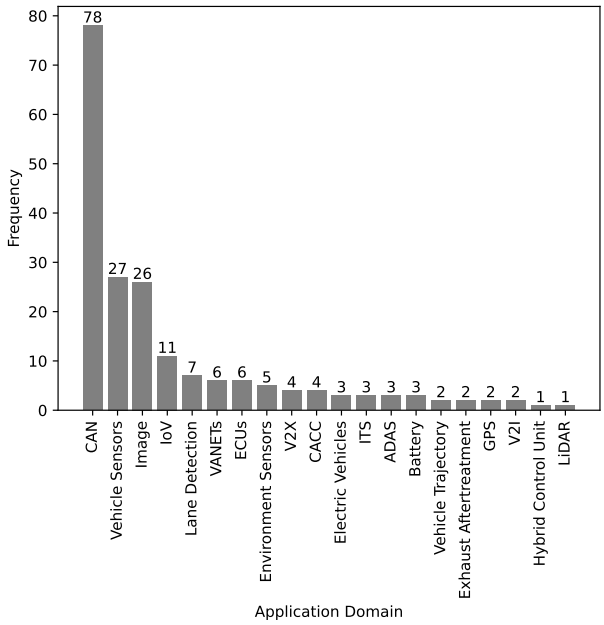

Fig. 3. Top 20 applications domains in anomaly detection models for CAVs

Security, on the other hand, focusses on protecting CAVs and their associated infrastructure from malicious attacks such as unauthorised access and data breaches. Anomaly detection techniques focused on security aim to identify abnormal network behaviours, intrusions, cyber threats, and privacy breaches that may compromise the integrity, availability, or confidentiality of the vehicle's systems or the data it generates. Ensuring security in CAVs involves implementing measures such as authentication, encryption, access control, intrusion detection, and secure communication protocols.

4) Open-source: In the analysis of the reviewed articles, only nine studies made their models publicly available on online accessible platforms, such as on GitHub (see [63]–[71]). Most studies collected their data to construct datasets through simulation or real vehicles.

C. Training of Anomaly Detection Models

This section will address the second research question: How are anomaly detection models for CAVs trained?

1) Data used in Training Anomaly Detection Models: The analysis revealed that out of the analysed articles, 136 studies trained their models using real-world data (that is, data collected from a real vehicle), while 50 studies utilised simulation-based training. 15 articles incorporated a combination of both real-world and simulation data. By utilising real-world data, researchers aim to capture the intricacies and complexities of actual driving conditions, including various

TABLE II
OVERVIEW OF DATASETS USED IN ANOMALY DETECTION MODELS

Dataset	Algorithm used	Models with highest F1-score
Car-Hacking dataset [72] — CAN dataset	1) Long Short-Term Memory [68], [73]–[76] 2) Genetic Algorithm [77], [78] 3) Spiking Neural Network [79] 4) Graph Neural Network [80] 5) Statistics-based [81] 6) Convolutional Neural Network [82] 7) Logarithmic Ratio (Over-sampling strategy) [83] 8) Temporal Convolutional Networks [84] 9) K-Nearest Neighbor [85] 10) Autoencoder [86]	1) DoS attack: [76], [81], [85] achieved 100% precision, accuracy, recall and F1-score. 2) Fuzzy attack: [81] achieved 100% precision, accuracy, recall and F1-score. 3) RPM attack: [76] achieved 100% precision, accuracy, recall and F1-score. 4) Gear attack: [76] achieved 100% precision, accuracy, recall and F1-score.
SPMD [87] — Basic safety messages dataset	1) Convolutional Neural Network [37], [88]–[90] 2) One-Class Support Vector Machine [91], [92] 3) Long Short-Term Memory [89] 4) Estimation-based [93] 5) Wavelet Kernel Network [94] 6) Temporal Neural Networks [95]	[94] achieved 99.9% accuracy, 99.8% recall, 99.9% precision, and 99.9% F1-score.
OTIDS [96] — CAN dataset	1) Maximum Likelihood Estimator with N-grams [97] 2) One-Class Support Vector Machine [98] 3) Artificial Neural Network [99] 4) Convolutional Neural Network [100] 5) Logarithmic Ratio (Over-sampling strategy) [83] 6) Autoencoder [86]	1) DoS attack: [99] achieved 99.98% accuracy, precision, recall, and F1-score. 2) Fuzzy attack: [99] achieved 100% accuracy, precision, recall, and F1-score. 3) RPM attack: [97] achieved 100% accuracy. 4) Gear attack: [97] achieved 100% accuracy.
SynCAN [101] — CAN dataset	1) Deep Learning [102] 2) Convolutional Neural Network [103] 3) One-Class Support Vector Machine [104] 4) Long Short-Term Memory [104] 5) Temporal Convolutional Networks [105]	[102] achieved 99.7% F1-score, 99.8% recall, and 99.5% precision.
Open Sourcing 223 GB of Driving Data by Udacity [106] — Image dataset	1) Edge Computing-Based [107] 2) Continuous Wavelet Transform [92] 3) Convolutional Neural Network [92], [108]	[108] achieved 99.7% accuracy, 98,7% recall, 99.43% precision, and 99.06% F1-score.
KITTI [109] — Image dataset	1) Generative Adversarial Networks [110] 2) Regularized Diffusion Process [111] 3) Unsupervised Discriminative Feature Learning [112]	[111] did not report F1, but had the highest AUC score. The model achieved 80% AUC, 31% MAE, and 61% OvR.
UNSW-NB15 [113] — Attack dataset	1) Explainable Neural Network [114] 2) Genetic Algorithm [77]	[114] achieved 99.7% accuracy, 99.3% precision, 98.7% recall, and 98.7% F1-score.
VeReMi [115] — Image dataset	1) Deep Neural Network [116] 2) Convolutional Neural Network [117] 3) Long Short-Term Memory [117], [118]	[116] achieved 98% accuracy, 95.6% recall, 99.6% precision, and 97.6% F1-score.
Cityscapes [119] — Image dataset	1) Generative Adversarial Networks [110] 2) Regularized Diffusion Process [111]	[111] achieved 80% AUC, 18% MAE, and 71% overlapping ratio (OvR).
BDD100k [120] — Image dataset	1) Convolutional Neural Network [39] 2) Unsupervised Discriminative Feature Learning [112]	[39] did not report F1-score, but achieved 79% AUROC.
UAH-Driveset [121] — Image dataset	1) Kalman Variational Autoencoder [56] 2) Generalized Markov Jump Particle Filter [122]	[122] did not report F1-score, but achieved 73.3% accuracy.
ROAD [123] — Image dataset	1) Gated Recurrent Unit [124] 2) Logarithmic Ratio (Over-sampling strategy) [83]	[83] did not report F1-score, but achieved 99.8 precision, 99.8 recall, 99,8 FMeasure, 99.9 accuracy, and 99.9 AUC.

road surfaces, traffic scenarios, and environmental factors. It is important to note that, the data collected for this section only looks at whether the training data is simulated or collected from a real-world scenario. If the training data is based on real-world data and attacks are later simulated, it is categorised as real-world data.

Simulation environments offer researchers precise control over the parameters, scenarios, and ground truth labels, providing a controlled and repeatable setting for training and evaluation. They allow for the generation of diverse scenarios, including rare or dangerous events that may be difficult to encounter in real-world data [125]. Training models on simulated data can facilitate rapid experimentation, scalability, and the exploration of extreme or edge cases that are otherwise hard to obtain in real-world scenarios. In addition to the above approaches, 15 articles adopted a hybrid approach, combining both real-world and simulation data for training their anomaly detection models. The most frequently used methods for generating simulated data were: simulating vehicle components through a test bed, Simulation of Urban MObility (SUMO), and OMNET++ (a framework used for simulating communication networks).

2) Generation of Anomalies in the Data: The analysis revealed a range of approaches used by researchers, with different degrees of explanation. It is worth noting that in some cases, there were no explanations provided related to how anomalies were introduced. The results are as follows:

- Random Injections: In 48 articles, anomalies were generated through random data injections into the dataset. This approach involved modifying existing data within the dataset to represent outliers or injecting outliers randomly. By randomly introducing anomalies, researchers aimed to simulate abnormal scenarios and evaluate the effectiveness of their anomaly detection models in identifying these anomalies.
- Attacks Performed While Recording the Log: 41 articles employed attacks performed while recording the CAN log through the Onboard Diagnostic (OBD-II) port. In these cases, real-world attacks were executed in a controlled environment by the research team or in a lab. The attacks were recorded in real-time, capturing the dynamics of the anomalies introduced during the attack.
- Simulated Attacks: 28 articles simulated attacks to generate anomalies within the dataset. Simulated attacks provided researchers with precise control over the anomaly characteristics, enabling the evaluation of the detection models' performance against specific attack types or patterns.
- Anomalies Generated: 24 articles used algorithms or models to generate anomalies within the dataset. Researchers employed data generation techniques, such as Generative Adversarial Networks (GANs) (such as [126], [127]), to synthesise anomalies that resemble real-world anomalies.
- Real-World Anomalies: 11 articles used real-world anomalies—of these, with the majority focusing on road surface detection. These anomalies were derived from actual obstacles encountered in real-world scenarios. Researchers incorporated data captured from real-world road surfaces with irregularities, such as potholes, bumps, cracks, or other physical disturbances.
- No Explanation: 50 articles lacked clear explanations regarding the anomalies generated within the dataset.

3) Characteristics of the Datasets: The description of the dataset used for training varied throughout the reviewed articles. The different ways to describe the data size include the length of data in time, byte size of data, number of car signals, number of data points, number of data samples, number of messages, number of nodes, and number of packets. Only 47 out of 203 articles contained a description of data size. Furthermore, in terms of the temporal date of collection, only 14 of the articles indicated the time frame of data collection. Moreover, the different datasets used across the publicly available papers can be found in Table II.

4) Levels of Autonomy: None of the papers mentioned whether the data collected or the anomaly detection was developed for a specific level of autonomous vehicles. However, one paper noted that their model was built for highly automated vehicles (HAD) [128]. This does not indicate a specific level as defined by the Society of Automotive Engineers [26].

D. Testing and evaluation of anomaly detection models

This section will address the third research question: How are anomaly detection models for CAVs tested and evaluated?

1) Testing and Evaluation Metrics: The analysis revealed that the top five evaluation metrics, in terms of frequency, were: recall, accuracy, precision, F1-score, and false positive rate (see Fig. 4):

- Recall: Used 106 times, measures the proportion of correctly identified anomalies (true positives) out of the actual anomalies (true positives and false negatives). It focuses the model's ability to identify all relevant anomalies.
- Accuracy: Used 86 times, measures the overall correctness of the anomaly detection model by calculating the ratio of correctly classified instances to the total number of instances.
- Precision: Used 73 times, measures the proportion of correctly identified anomalies (true positives) out of the total instances identified as anomalies (true positives and false positives).
- F1-score: Used 62 times, is the harmonic mean of precision and recall. It provides a balance between precision and recall, capturing the trade-off between correctly identifying anomalies and minimising false positives and false negatives.
- False Positive Rate: Used 33 times, measures the proportion of normal instances incorrectly labelled as anomalies (false positives) out of the total number of actual normal instances. It focuses on the model's ability to avoid misclassifying normal instances.

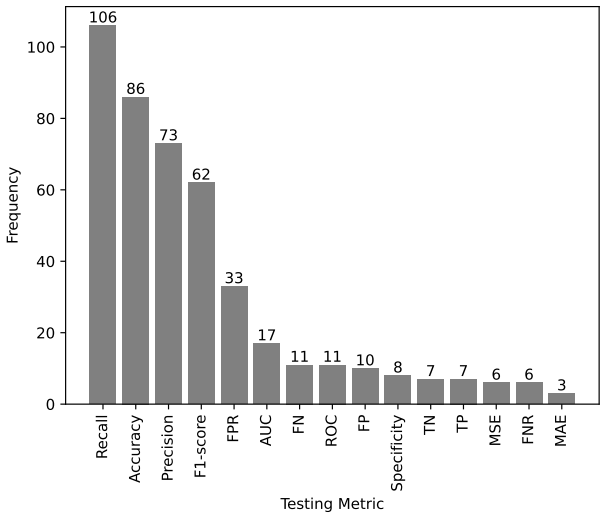

Fig. 4. Frequency of metrics used to test and evaluate anomaly detection models

The set of evaluation metrics used collectively in the papers is presented here, to illustrate the commonly chosen evaluation metrics used in the reviewed papers. Figure 5 provides an overview of the 10 most frequently used evaluation metric

combinations in the reviewed studies. Here, the focus is on presenting the top five most commonly used selection of metrics:

- F1-score, Precision, Recall, and Accuracy: The most common selection of evaluation metrics, allowed for an evaluation that considers overall correctness, a balance between precision and recall, and a trade-off between correctly identifying anomalies and minimising false positives and false negatives. This combination was used 22 times.
- Accuracy: Used in 21 papers. Researchers relied solely on accuracy to evaluate the overall correctness of the anomaly detection model, without considering additional metrics.
- F1-score, Precision, and Recall: This combination was the second most frequent combination, appearing 19 times. These metrics were employed together to evaluate the model's ability to strike a balance between correctly identifying anomalies and avoiding false positives.
- False Positive Rate (FPR) and Recall: Used 10 times. FPR and recall, often employed in receiver operating characteristic (ROC) analysis, provide insights into the model's ability to avoid misclassifying normal instances (FPR) and correctly detect anomalies (recall).
- Accuracy, FPR, and Recall: Used 8 times. Accuracy represents the overall correctness of predictions, capturing the ratio of correctly classified instances to the total number of instances. FPR, on the other hand, focuses on the rate of falsely predicted positive instances out of all negative instances. It helps evaluate the model's ability to avoid false alarms and misclassifications. Recall, also known as sensitivity, measures the proportion of true positive instances that are correctly identified as positive.

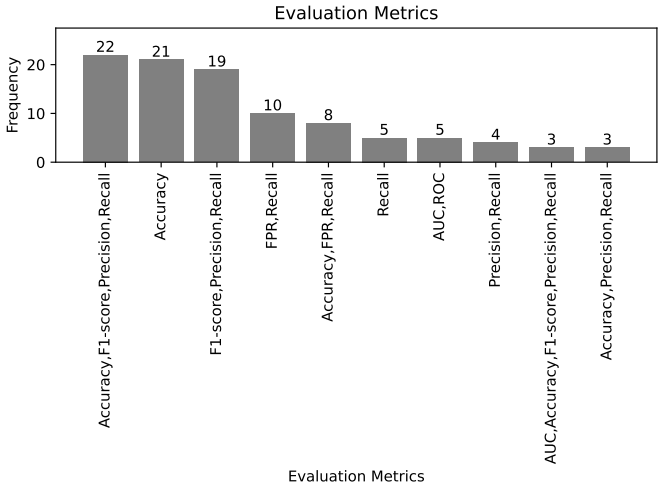

Fig. 5. 10 most frequently used combinations of metrics to test and evaluate anomaly detection models

2) Detection Latency: Among the reviewed articles, 18 papers provided data on the detection latency in anomaly detection for CAVs. The detection latency, which represents the time taken to detect anomalies, varied across these studies. The reported detection latency ranged from 0.06 ms to 6,000 ms. The best model in terms of detection latency [76] used long short-term memory on the car hacking dataset [72] and achieved 0.06 ms. Detection latency plays an important role in real-time anomaly response and is an important consideration in ensuring the effectiveness and timeliness of anomaly detection mechanisms for CAVs.

3) Case studies: This section presents two case studies showcasing a successful implementation of anomaly detection. The first study uses a CAN dataset and develops a prediction-based IDS. The study described below [76], presents a novel framework for detecting anomalies and attacks on the CAN bus. The model is trained using the most frequently used dataset (the Car-Hacking Dataset by HCRL) and is one of the highest-scoring models in terms of F1-score. The dataset comes with four attacks: DoS, Fuzzy, RPM spoofing, and gear spoofing. The IDS utilises a prediction-based approach, leveraging the temporal correlation of message contents to detect anomalies and attacks. Two prediction modules are introduced: a Long Short-Term Memory (LSTM) network and a Convolutional LSTM (ConvLSTM) network. An attack is classified based on prediction errors using a Gaussian Naïve Bayes classifier. Evaluation against state-of-the-art one-class classifiers and existing works demonstrate superior accuracy, with 100% F1-score, accuracy, precision, and recall on the RPM and gear spoofing datasets. This study highlights the effectiveness of the proposed IDS framework in enhancing CAV cybersecurity.

The second study uses an image dataset and proposes an innovative intrusion detection system that integrates Space Dimension and Time Dimension Models based on sensor data fusion to detect simultaneous attacks on multiple sensors [108]. In the Space Dimension Model, correlations among multivariate in-vehicle sensor data are leveraged using an optimised CNN to detect independent and confederate attacks. Vehicle state matrices are constructed to capture the underlying data correlations between sensors, facilitating classification. The Time Dimension Model, on the other hand, utilises the Mahalanobis distance metric to capture abrupt deviations caused by anomalous sensor data over time. The paper utilises the Open Sourcing 223 GB of Driving Data by Udacity [106] image dataset and achieved 99.7% accuracy, 98.7% recall, 99.43% precision, and 99.06% F1-score, which is the highest F1-score for this dataset.

V. Discussion

A. AI Methods used in Anomaly Detection for CAVs

In answering the first research question, LSTM, CNN, autoencoders, other deep learning, and one-class SVM represent the most commonly employed methods for detecting anomalies in CAVs. These five algorithms together are used in 91 of the 203 articles in the review. In the most frequently used CAN dataset, Car-Hacking Dataset [72], the highest performing algorithm was LSTM which achieved 100% precision, accuracy, recall, and F1-score on the DoS, fuzzy attacks, and gear spoofing attacks [76]. In the most frequently used

image dataset, which was from Udacity Inc [106], the best-performing model used CNN and achieved 99.7% accuracy, 98.7% recall, 99.43% precision, and 99.06% F1-score [108].

While the existing detection models demonstrate strong results within single case study contexts, such as CAN bus anomaly detection, the usability and effectiveness of these models in a real-world context remain uncertain. CAVs are complex systems of systems, where anomalies may stem from a range of sources across internal vehicles subsystems and external infrastructures. The need to manage various anomaly types (e.g., faults and attacks) across multiple systems adds a layer of complexity that current models may not be equipped to handle, highlighting an area for further research and development.

When it comes to the application domain, the majority of the articles were focused on the CAN bus network, vehicle sensors, the image domain, IoV, and lane detection. The papers that focused on the CAN bus network extracted data from either a simulated environment or through a real vehicle using the OBD-II port. This port is available on most vehicles and enables access to the in-vehicle network traffic. Connected to the in-vehicle network, the vehicle sensors measure the performance of the vehicle's components, such as sensor data from acceleration, engine RPM, vehicle speed, and GPS. This differs from environment sensors, encompassing sensors that perceive the vehicle's surroundings. The next most frequently studied area is the image domain. This category predominantly focuses on road anomaly detection, such as potholes or other obstacles that the camera can detect. Furthermore, the next most studied field is IoV, which primarily applies to traffic management, emergency message delivery, traffic, and temperature monitoring [129]. As opposed to the aforementioned categories, IoV entails external communication. Next, the field of lane detection was the fifth most frequently studied domain. In this domain, the authors proposed methods for detecting sudden lane changes. This also used the image domain but is specifically focused on detecting anomalous events such as sudden lane changing that could be dangerous. The findings of this review show that most research is concerned with CAN (78 out of 203 papers).

The review has highlighted a focus on both security and safety in anomaly detection research for CAVs and shows the recognition of their intertwined importance. While there is a higher number of papers focusing on security, there is a significant high focus on safety too. This is similar to the findings of Rajbahadur et al. [10]. By taking into account both security and safety dimensions, researchers can contribute to the development of more resilient, secure, and safe connected and autonomous vehicles.

The low number of open-source models in the review highlights the need for increased emphasis on open collaboration and transparency within the security research community. As outlined in ITU-T X.1382 [130], the International Telecommunication Union has proposed a guideline for sharing security threat information pertaining to connected vehicles. This recommendation emphasises the need to establish a dedicated platform for exchanging data related to the information security of CAVs. Such a platform would foster collaboration between academic institutions and industry stakeholders, enabling them to work together in addressing and mitigating cyber threats. UNECE WP.29 mandates consideration for monitoring, detecting, and responding to cyber threats to CAVs for all new vehicle types, which will be enforced July 2024 [131]. It also includes a mandate for establishing a management system to take accountability for the response and processing of this information. By encouraging researchers to share their models and datasets openly, the security community can benefit from the collective expertise, shared knowledge, reproduce and validate the models, and compare and validate the reliability of the studies, ultimately driving improvements in anomaly detection for CAVs and contributing to safer and more secure autonomous systems.

B. Training of Anomaly Detection Models

In addressing the second research question of how anomaly detection models are trained, the majority of the reviewed papers used real-world data over simulated data. Only a few models used real-world attacks or faults during the training process. Instead, popular methods included randomly injecting anomalies into the dataset and performing attacks through the OBD-II port while recording the vehicle's log. These findings align with Rajbahadur et al. [10], who found that most datasets are used with simulated attacks. Incorporating real-world attacks that accurately reflect the threat model or faults can expose detection models to realistic adversarial situations, allowing them to better tested against real-world anomalies and threats. None of the reviewed studies included a dataset featuring real-world attacks. As aforementioned, the recommendation [130] to create a community where data is shared openly with relevant cybersecurity for CAV actors is necessary to share real anomaly data. Currently, the most realistic attack scenario is to attack a vehicle in a secure environment while recording the log.

Current threat modelling for anomaly detection in CAVs tends to be oversimplified, often focusing on a narrow range of attack scenarios that may not fully reflect the diversity of real-world threats. Effective deployment of these models will require more comprehensive threat modelling that captures a broader spectrum of attack vectors and scenarios. Without this, the detection models may struggle to generalise to new, evolving threats across different contexts and sources, highlighting the need for further research into more sophisticated threat modelling techniques.

Furthermore, only one article explicitly mentioned the level of autonomy at which the data was collected or for which anomaly detection was conducted [128]. The level of autonomy is a critical factor that influences the complexity of the data and the specific challenges associated with anomaly detection. Understanding the level of autonomy allows for a better interpretation of the results and their relevance to different autonomous driving scenarios. As vehicles transition from conventional to semi-autonomous and fully autonomous modes, the complexity of anomaly detection methodologies may need to undergo a significant evolution. At lower autonomy levels, where human drivers are actively engaged

in vehicle operation, anomaly detection may primarily focus on identifying deviations from expected driver behaviour or vehicle performance metrics. Contrarily, as vehicles progress towards higher autonomy levels, where human intervention becomes less frequent or non-existent, anomaly detection must adapt to account for the increased reliance on onboard sensor suites, decision-making algorithms, and communication networks. For instance, integrating Advanced Driver Assistance Systems (ADAS) adds complexity to anomaly detection in CAVs. As CAVs incorporate more sophisticated ADAS functionalities, anomaly detection becomes increasingly challenging, emphasising the importance of robust and adaptable detection systems for ensuring vehicle safety and reliability. Moreover, the dynamic nature of operational contexts across different autonomy levels may require the development of adaptive anomaly detection systems capable of discerning anomalies amidst evolving environmental conditions, traffic scenarios, and system configurations.

1) Creation, maintenance, and standardisation of benchmarking datasets: The creation of benchmarking datasets faces several challenges. First, the creators have to decide whether to use real or simulated data. Most models identified in this paper used real-world data: image classification models have trained their models mostly on real images, and time series anomaly detection models have trained on log data from the vehicle's OBD-II port or recorded sensor data. Next, the authors have to decide on a method for introducing anomalies into the dataset. The scenario that is most similar to a real attack or fault scenario is injecting attacks on the vehicle while it is operating in a controlled environment. A problem identified with some of the datasets is a lack of attack data, which leads to researchers having to generate their anomalies. This restricts the comparability between models using the same dataset. For a dataset to be used for benchmarking, it is most effective to have a dataset with pre-injected or pre-performed attacks. Another limitation of attack data is the lack of variation. The most commonly employed dataset was the car-hacking dataset [72] which includes DoS, fuzzy (randomly injected values), gear spoofing, and RPM spoofing, which is restricted to only four different attacks.

In terms of maintaining datasets for anomaly detection models, they will have to be updated relating to new attack types. For instance, a more recent dataset [132] addresses this by including more attack types. The authors introduce nine different attack types on the CAN bus: DoS, fuzzing, systematic, gear spoofing, RPM spoofing, speed spoofing, combined spoofing, standstill, and interval. To advance the field of anomaly detection for CAVs, benchmarking datasets will have to add new attack types as they are discovered either in the field of academics or in the industry.

2) Testing and Evaluation of Anomaly Detection Models: In addressing the second research question, recall was the most frequently used evaluation metric across all papers. The most frequently used set of metrics were accuracy, F1-score, precision, and recall. Looking at the most frequently used metric, the use of recall highlights a significance in capturing the ability of a model to identify true positive instances. Given the criticality of detecting anomalies in autonomous vehicles to ensure safe and efficient operation, a high recall value is essential to minimise the chances of false negatives and the potential risks associated with undetected anomalies. Maximising true positives and minimising false negatives should be the highest priority when evaluating anomaly detection models [133], [134].

Out of the 203 reviewed articles, only 18 studies provided data on detection latency. This metric measures the time from the anomaly first occurs until it is detected. Detection latency is an important metric in anomaly detection models [133], [134]. This metric should be included when evaluating anomaly detection models for CAVs since a timely response can potentially avoid a dangerous on-road situation for CAVs. This limited inclusion of detection latency information suggests a gap in reporting and analysing this crucial aspect of anomaly detection.

C. Limitations

This review identified two limitations in the reporting practices across the reviewed papers, which restricts comparisons between the proposed models:

1) Data on the detection latency was generally missing from the reviewed papers. The limited availability of such data inhibits a comprehensive analysis of detection latency trends across the reviewed studies, hindering the ability to draw conclusive insights.
2) The wide variation in the description of datasets used for training anomaly detection models poses a challenge to standardisation and comparability. The lack of a uniform framework for describing data sets complicates efforts to understand their characteristics and assess their applicability to different scenarios.

These limitations underscore the need for improved data quality and standardised reporting practices in future studies, ensuring greater transparency, comparability, and depth of analysis in the field of anomaly detection for CAVs. Furthermore, these limitations exacerbate the already existing challenges associated with the lack of baseline evaluations and benchmarking observed in anomaly detection studies, as highlighted by Rajbahadur et al. [10] in their study.

D. Recommendations

Based on the findings and limitations identified in this systematic review, several recommendations are proposed to guide future research developing anomaly detection for CAVs:

1) Incorporate multiple evaluation metrics: To provide a comprehensive assessment of anomaly detection models, it is recommended to include multiple evaluation metrics in future research [135]. Utilising a diverse set of evaluation metrics allows for a better understanding of the strengths and weaknesses of the models, better trade-off analysis, and improved transparency in reporting the effectiveness of the anomaly detection approaches. There should also be a consensus on what set of evaluation metrics should be used for anomaly detection.
2) Open-source anomaly detection models, threat models, and datasets: Future studies should consider making

their models, threat models, and datasets open-source to foster collaboration, transparency, and reproducibility within the field [135]. Currently, existing threat models are often oversimplified and focus on a narrow set of attack scenarios. Sharing a wider range of comprehensive threat models would allow for more realistic and varied attack scenarios beyond current cases, aligning with ITU's recommendation to establish a community for sharing security-related information on CAVs [130].

3) Enhanced benchmarking to handle diverse anomaly types in complex CAV systems: Current datasets lack predefined, varied anomalies and attacks. Many studies rely on normal traffic data, requiring researchers to generate their own anomalies. This lack of standard benchmarking makes it challenging to compare the performance of different algorithms consistently. To address this, future research should develop standardised datasets featuring a range of predefined attacks, as CAVs will require models capable of detecting multiple types of anomalies across various systems. These datasets should accommodate the multi-system nature of CAVs, which are complex systems of systems, to assess model efficacy in diverse scenarios.
4) Lack of data on the deployment of anomaly detection models: The anomaly detection models reviewed have not been tested in real-world settings, and therefore, their performance remains uncertain. It is challenging to draw conclusions about the usability and effectiveness of these models, given the absence of real-world deployment data. It will be useful for future research to investigate the deployment and maintenance of these models to understand how they will perform in real settings and vehicles over time.
5) Lack of anomaly detection models for Ethernet, FlexRay, and LIN: As CAVs progress to include more automated functions and ultimately progress to a fully automated vehicle, more components will be connected to the in-vehicle network. This has posed challenges to the traditional CAN, leading Bosch to develop new CAN protocols, CAN FD and CAN XL [136], that have increased bandwidth to adapt to this change. Ethernet is used to accommodate the need for bigger bandwidth for technologies, such as LiDAR, radar, and cameras. In this review, only one paper [137] investigates anomaly detection for traffic in the Ethernet. Companies such as Garrett Motion and ETAS have already developed IDS for Ethernet network traffic. This is an area that could benefit from more research to establish effective IDS. Furthermore, there were no papers investigating anomaly detection models for FlexRay and LIN.

Implementing these recommendations in future research could improve the transparency, reproducibility, and effectiveness of anomaly detection models designed for CAVs. By promoting open collaboration, specifying relevant details, improving data reporting, ensuring uniformity, and utilising a comprehensive set of evaluation metrics, the field can advance more rapidly and foster the development of more reliable, robust, and applicable anomaly detection solutions for CAVs.

VI. Conclusion

This systematic literature review examined the landscape of AI-based anomaly detection for CAVs, covering a broad spectrum of articles and incorporating a total of 203 research papers in the final review. The review was structured around three principal research inquiries: AI algorithms employed for anomaly detection; the training processes of these models; and the strategies for their testing and evaluation.

The findings indicate that LSTM is the most frequently used AI method in anomaly detection for CAVs, followed by CNN, Autoencoder, other deep learning algorithms, and one-class SVM. The CAV component that has received the most research interest is the CAN bus, with a significant focus on security, although safety also constitutes a substantial portion of the research. Overall, only a small fraction (9 out of 203) of the articles reviewed provided open access to their models.

The review also aimed to understand the training processes of the anomaly detection models proposed for CAVs. The data reveals that real-world data is the preferred choice for training datasets, utilised nearly three times as often as simulated data. Anomalies were introduced into these datasets through various methods, with the most prevalent approach being the random data injection of anomalies into an existing dataset. However, the use of real-world attacks and faults was less common.

The final research question addressed the evaluation of anomaly detection models. The review identified that accuracy, F1-score, precision, and recall were the most frequently selected set of metrics used to evaluate anomaly detection models. Throughout all papers, recall was the most frequently used metric. Detection latency ranged from 0.06 milliseconds to 6,000 milliseconds but was used as a metric in 18 papers.

This systematic review provides a comprehensive overview of the current state of anomaly detection for CAVs, highlighting key methodologies, training processes, evaluation strategies, and the current state-of-the-art models for the most frequently used datasets. It emphasises the need for further research to incorporate multiple evaluation metrics; include detection latency as an evaluation metric; open source their models for transparency and reproducibility, and create a community where the vehicle industry and researchers can benefit from the research; and keep benchmarking datasets up to date with known attacks. The recommendation for future research includes assessing the performance of the anomaly detection models when deployed in a vehicle on the road, as well as exploring their application to emerging communication protocols such as Ethernet and FlexRay.

While anomaly-based detection is the initial stage of detecting faults and cyber-physical attacks, what follows next, addressing anomalies and response, requires further research and attention, an area that is currently lacking attention.

VII. Acknowledgement

This work was supported by the Engineering and Physical Sciences Research Council [EP/S022503/1]. For the purpose

REFERENCES

[1] S. Grigorescu, B. Trasnea, T. Cocias, and G. Macesanu, "A survey of deep learning techniques for autonomous driving," *Journal of Field Robotics*, vol. 37, no. 3, pp. 362–386, 2020, ISBN: 1556-4959 Publisher: Wiley Online Library.

[2] J. Wang, L. Zhang, Y. Huang, J. Zhao, and F. Bella, "Safety of autonomous vehicles," *Journal of advanced transportation*, vol. 2020, pp. 1–13, 2020, ISBN: 2042-3195 Publisher: Hindawi Limited.

[3] X. Li, J. Li, A. Abdollahi, and T. Jones, "Data-driven thermal anomaly detection for batteries using unsupervised shape clustering," in *2021 IEEE 30th International Symposium on Industrial Electronics (ISIE)*, IEEE, 2021, pp. 1–6, ISBN: 1-72819-023-1.

[4] F. Quader and V. Janeja, "Anomaly detection: Under the [data] hood in smart cars," in *2019 IEEE International Conference on Smart Computing (SMARTCOMP)*, Journal Abbreviation: 2019 IEEE International Conference on Smart Computing (SMARTCOMP), Jun. 12, 2019, pp. 126–131. DOI: 10.1109/SMARTCOMP.2019.00041.

[5] A. D. Spratlin Jr Jr, "Autonomous and electric cars and" trucks: Old they survive COVIDP," *The Brief*, vol. 50, no. 2, pp. 50–59, 2021, ISBN: 0273-0995 Publisher: American Bar Association.

[6] A. Chakraborty, M. Alam, V. Dey, A. Chattopadhyay, and D. Mukhopadhyay, "Adversarial attacks and defences: A survey," *arXiv preprint arXiv:1810.00069*, 2018.

[7] R. Sparrow and M. Howard, "When human beings are like drunk robots: Driverless vehicles, ethics, and the future of transport," *Transportation Research Part C: Emerging Technologies*, vol. 80, pp. 206–215, 2017, ISBN: 0968-090X Publisher: Elsevier.

[8] G. Shapps and K. Kwarteng, *Connected & automated mobility 2025: Realising the benefits of self-driving vehicles in the UK*. 2022.

[9] Wayve, *Asda and wayve launch UK's largest self-driving grocery home delivery trial*. 2023. [Online]. Available: https://wayve.ai/press/asda-and-wayve-launch-grocery-delivery-trial/.

[10] G. K. Rajbahadur, A. J. Malton, A. Walenstein, and A. E. Hassan, "A survey of anomaly detection for connected vehicle cybersecurity and safety," in *2018 IEEE Intelligent Vehicles Symposium (IV)*, IEEE, 2018, pp. 421–426, ISBN: 1-5386-4452-5.

[11] S. Omar, A. Ngadi, and H. H. Jebur, "Machine learning techniques for anomaly detection: An overview," *International Journal of Computer Applications*, vol. 79, no. 2, pp. 33–41, Oct. 18, 2013, ISSN: 09758887. DOI: 10.5120/13715-1478. [Online]. Available: http://research.ijcaonline.org/volume79/number2/pxc3891478.pdf (visited on 04/10/2024).

[12] P. Dixit, P. Bhattacharya, S. Tanwar, and R. Gupta, "Anomaly detection in autonomous electric vehicles using AI techniques: A comprehensive survey," *Expert Systems*, vol. 39, no. 5, 2022. DOI: 10.1111/exsy.12754. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85107761290&doi=10.1111%2fexsy.12754&partnerID=40&md5=76a09eb72630bef9924b1d8a38f49701.

[13] D. Bogdoll, M. Nitsche, and J. M. Zöllner, "Anomaly detection in autonomous driving: A survey," in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, 2022, pp. 4488–4499.

[14] S. Baccari, M. Hadded, H. Ghazzai, H. Touati, and M. Elhadef, "Anomaly detection in connected and autonomous vehicles: A survey, analysis, and research challenges," *IEEE Access*, 2024, ISBN: 2169-3536 Publisher: IEEE.

[15] M. Delgado-Rodríguez and M. Sillero-Arenas, "Systematic review and meta-analysis," *Medicina Intensiva (English Edition)*, vol. 42, no. 7, pp. 444–453, 2018, ISBN: 2173-5727 Publisher: Elsevier.

[16] S. Götz, "Supporting systematic literature reviews in computer science: The systematic literature review toolkit," in *Proceedings of the 21st ACM/IEEE International Conference on Model Driven Engineering Languages and Systems: Companion Proceedings*, 2018, pp. 22–26.

[17] S. E. Shladover, "Connected and automated vehicle systems: Introduction and overview," *Journal of Intelligent Transportation Systems*, vol. 22, no. 3, pp. 190–200, 2018, ISBN: 1547-2450 Publisher: Taylor & Francis.

[18] S. E. Shladover, D. Su, and X.-Y. Lu, "Impacts of cooperative adaptive cruise control on freeway traffic flow," *Transportation Research Record*, vol. 2324, no. 1, pp. 63–70, 2012, ISBN: 0361-1981 Publisher: SAGE Publications Sage CA: Los Angeles, CA.

[19] J. M. Anderson, K. Nidhi, K. D. Stanley, P. Sorensen, C. Samaras, and O. A. Oluwatola, *Autonomous vehicle technology: A guide for policymakers*. Rand Corporation, 2014, ISBN: 0-8330-8437-2.

[20] G. M. Arnaout and J.-P. Arnaout, "Exploring the effects of cooperative adaptive cruise control on highway traffic flow using microscopic traffic simulation," *Transportation Planning and Technology*, vol. 37, no. 2, pp. 186–199, 2014, ISBN: 0308-1060 Publisher: Taylor & Francis.

[21] S. D. Pendleton, H. Andersen, X. Du, *et al.*, "Perception, planning, control, and coordination for autonomous vehicles," *Machines*, vol. 5, no. 1, p. 6, 2017, ISBN: 2075-1702 Publisher: MDPI.

[22] D. Christie, A. Koymans, T. Chanard, J.-M. Lasgouttes, and V. Kaufmann, "Pioneering driverless electric vehicles in europe: The city automated transport system (CATS)," *Transportation Research Procedia*, vol. 13, pp. 30–39, 2016, ISBN: 2352-1465 Publisher: Elsevier.

[23] Z. Wang, G. Zhang, B. Hu, and X. Feng, "Real time detection and identification of UAV abnormal trajectory," presented at the ACM International Conference Proceeding Series, 2020, pp. 51–56. DOI: 10.1145/3430199.3430212. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85099336353&doi=10.1145%2f3430199.3430212&partnerID=40&md5=379beadf139a88a3f5931fbd692e96c4.

[24] F. Zhang, D. Clarke, and A. Knoll, "Vehicle detection based on LiDAR and camera fusion," in *17th International IEEE Conference on Intelligent Transportation Systems (ITSC)*, IEEE, 2014, pp. 1620–1625, ISBN: 1-4799-6078-0.

[25] M. Zhao, A. Mammeri, and A. Boukerche, "Distance measurement system for smart vehicles," in *2015 7th International Conference on New Technologies, Mobility and Security (NTMS)*, IEEE, 2015, pp. 1–5, ISBN: 1-4799-8784-0.

[26] S. International, *Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles*.

[27] J. Cui, L. S. Liew, G. Sabaliauskaite, and F. Zhou, "A review on safety failures, security attacks, and available countermeasures for autonomous vehicles," *Ad Hoc Networks*, vol. 90, p. 101 823, 2019, ISBN: 1570-8705 Publisher: Elsevier.

[28] J. Wang, Y. Shao, Y. Ge, and R. Yu, "A survey of vehicle to everything (v2x) testing," *Sensors*, vol. 19, no. 2, p. 334, 2019, ISBN: 1424-8220 Publisher: MDPI.

[29] S. Jadhav and D. Kshirsagar, "A survey on security in automotive networks," in *2018 Fourth international conference on computing communication control and automation (ICCUBEA)*, IEEE, 2018, pp. 1–6, ISBN: 1-5386-5257-9.

[30] R. Schmidgall, "Automotive embedded systems software reprogramming," Ph.D. dissertation, Brunel University, 2012.

[31] M. Pham and K. Xiong, "A survey on security attacks and defense techniques for connected and autonomous vehicles," *Computers & Security*, vol. 109, p. 102 269, 2021, ISBN: 0167-4048 Publisher: Elsevier.

[32] A. M. Malla and R. K. Sahu, "Security attacks with an effective solution for dos attacks in VANET," *International Journal of Computer Applications*, vol. 66, no. 22, 2013, ISBN: 0975-8887 Publisher: Foundation of Computer Science.

[33] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," *Computer Communications*, vol. 44, pp. 1–13, 2014, ISBN: 0140-3664 Publisher: Elsevier.

[34] S. S. Manvi and S. Tangade, "A survey on authentication schemes in VANETs for secured communication," *Vehicular Communications*, vol. 9, pp. 19–30, 2017, ISBN: 2214-2096 Publisher: Elsevier.

[35] L. B. Othmane, H. Weffers, M. M. Mohamad, and M. Wolf, "A survey of security and privacy in connected vehicles," *Wireless sensor and mobile ad-hoc networks: vehicular and space applications*, pp. 217–247, 2015, ISBN: 1493924672 Publisher: Springer.

[36] P. Koopman and M. Wagner, "Autonomous vehicle safety: An interdisciplinary challenge," *IEEE Intelligent Transportation Systems Magazine*, vol. 9, no. 1, pp. 90–96, 2017, ISBN: 1939-1390 Publisher: IEEE.

[37] F. van Wyk, Y. Wang, A. Khojandi, and N. Masoud, "Real-time sensor anomaly detection and identification in automated vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 3, pp. 1264–1276, Mar. 2020, ISSN: 1558-0016. DOI: 10.1109/TITS.2019.2906038.

[38] E. F. Morales and H. J. Escalante, "A brief introduction to supervised, unsupervised, and reinforcement learning," in *Biosignal processing and classification using computational learning and intelligence*, Elsevier, 2022, pp. 111–129.

[39] A. Ranjbar, S. Hornauer, J. Fredriksson, S. X. Yu, and C. -Y. Chan, "Safety monitoring of neural networks using unsupervised feature learning and novelty estimation," *IEEE Transactions on Intelligent Vehicles*, vol. 7, no. 3, pp. 711–721, Sep. 2022, ISSN: 2379-8904. DOI: 10.1109/TIV.2022.3152084.

[40] G. Basile, A. Petrillo, and S. Santini, "DDPG based end-to-end driving enhanced with safe anomaly detection functionality for autonomous vehicles," in *2022 IEEE International Conference on Metrology for Extended Reality, Artificial Intelligence and Neural Engineering (MetroXRAINE)*, Journal Abbreviation: 2022 IEEE International Conference on Metrology for Extended Reality, Artificial Intelligence and Neural Engineering (MetroXRAINE), Oct. 26, 2022, pp. 248–253. DOI: 10.1109/MetroXRAINE54828.2022.9967647.

[41] T. He, L. Zhang, F. Kong, and A. Salekin, "Exploring inherent sensor redundancy for automotive anomaly detection," in *Proceedings of the 57th ACM/EDAC/IEEE Design Automation Conference*, ser. DAC '20, Place: Virtual Event, USA, IEEE Press, 2020, ISBN: 978-1-4503-6725-7.

[42] G. Zizzo, "Machine learning for security and security for machine learning," 2021, Publisher: Imperial College London.

[43] V. Kumar and O. P. Sangwan, "Signature based intrusion detection system using SNORT," *International Journal of Computer Applications & Information Technology*, vol. 1, no. 3, pp. 35–41, 2012.

[44] M. Kravchik and A. Shabtai, "Detecting cyber attacks in industrial control systems using convolutional neural networks," in *Proceedings of the 2018 workshop on cyber-physical systems security and privacy*, 2018, pp. 72–83.

[45] M. Kravchik and A. Shabtai, "Efficient cyber attack detection in industrial control systems using lightweight neural networks and pca," *IEEE transac-*

tions on dependable and secure computing, vol. 19, no. 4, pp. 2179–2197, 2021, ISBN: 1545-5971 Publisher: IEEE.

[46] S. Sapkota, A. N. Mehdy, S. Reese, and H. Mehrpouyan, "Falcon: Framework for anomaly detection in industrial control systems," *Electronics*, vol. 9, no. 8, p. 1192, 2020, ISBN: 2079-9292 Publisher: MDPI.

[47] G. S. Handelman, H. K. Kok, R. V. Chandra, *et al.*, "Peering into the black box of artificial intelligence: Evaluation metrics of machine learning methods.," *AJR. American journal of roentgenology*, vol. 212, no. 1, pp. 38–43, 2018, ISBN: 0361-803X.

[48] D. Moher, L. Shamseer, M. Clarke, *et al.*, "Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-p) 2015 statement," *Systematic reviews*, vol. 4, pp. 1–9, 2015, Publisher: Springer.

[49] Edanz-Learning-Team, *Understanding a PRISMA flow diagram*, 2022. [Online]. Available: https://learning.edanz.com/prisma-flow-diagram/.

[50] T. Meline, "Selecting studies for systemic review: Inclusion and exclusion criteria," *Contemporary issues in communication science and disorders*, vol. 33, pp. 21–27, Spring 2006, ISBN: 1092-5171 Publisher: ASHA.

[51] E. Ratajczyk, U. Brady, J. A. Baggio, *et al.*, "Challenges and opportunities in coding the commons: Problems, procedures, and potential solutions in large-n comparative case studies," *International Journal of the Commons*, vol. 10, no. 2, pp. 440–466, 2016, ISBN: 1875-0281 Publisher: JSTOR.

[52] T. Byrt, J. Bishop, and J. B. Carlin, "Bias, prevalence and kappa," *Journal of clinical epidemiology*, vol. 46, no. 5, pp. 423–429, 1993, ISBN: 0895-4356 Publisher: Elsevier.

[53] M. Cumpston, T. Li, M. J. Page, *et al.*, "Updated guidance for trusted systematic reviews: A new edition of the cochrane handbook for systematic reviews of interventions," *The Cochrane database of systematic reviews*, vol. 2019, no. 10, 2019, Publisher: John Wiley and Sons, Inc. and the Cochrane Library.

[54] A. Graves and A. Graves, *Supervised sequence labelling*. Springer, 2012, ISBN: 3-642-24796-2.

[55] K. O'Shea and R. Nash, "An introduction to convolutional neural networks," *arXiv preprint arXiv:1511.08458*, 2015.

[56] G. Slavic, A. S. Alemaw, L. Marcenaro, D. Martín Gómez, and C. Regazzoni, "A kalman variational autoencoder model assisted by odometric clustering for video frame prediction and anomaly detection," *IEEE Transactions on Image Processing*, vol. 32, pp. 415–429, 2023, ISSN: 1941-0042. DOI: 10.1109/TIP.2022.3229620.

[57] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *nature*, vol. 521, no. 7553, pp. 436–444, 2015, ISBN: 0028-0836 Publisher: Nature Publishing Group UK London.

[58] S. Yin, X. Zhu, and C. Jing, "Fault detection based on a robust one class support vector machine," *Neurocomputing*, vol. 145, pp. 263–268, 2014, ISBN: 0925-2312 Publisher: Elsevier.

[59] S. C. HPL, "Introduction to the controller area network (CAN)," *Application Report SLOA101*, pp. 1–17, 2002, Publisher: Texas instruments.

[60] T. P. Kapusi, L. Kovács, and A. Hajdu, "Deep learning-based anomaly detection for imaging in autonomous vehicles," in *2022 IEEE 2nd Conference on Information Technology and Data Science (CITDS)*, Journal Abbreviation: 2022 IEEE 2nd Conference on Information Technology and Data Science (CITDS), May 16, 2022, pp. 142–147. DOI: 10.1109/CITDS54976.2022.9914092.

[61] F. Yang, S. Wang, J. Li, Z. Liu, and Q. Sun, "An overview of internet of vehicles," *China communications*, vol. 11, no. 10, pp. 1–15, 2014, ISBN: 1673-5447 Publisher: IEEE.

[62] M. B. Line, O. Nordland, L. Røstad, and I. A. Tøndel, "Safety vs security?" In *PSAM Conference, New Orleans, USA*, sn, 2006.

[63] A. Stocco, M. Weiss, M. Calzana, and P. Tonella, "Misbehaviour prediction for autonomous driving systems," presented at the Proceedings - International Conference on Software Engineering, 2020, pp. 359–371. DOI: 10.1145/3377811.3380353. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85094321490&doi=10.1145%2f3377811.3380353&partnerID=40&md5=83d7e79824348d1270a21fe3a7fc4989.

[64] L. Yang, A. Moubayed, and A. Shami, "MTH-IDS: A multitiered hybrid intrusion detection system for internet of vehicles," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 616–632, Jan. 1, 2022, ISSN: 2327-4662. DOI: 10.1109/JIOT.2021.3084796.

[65] D. Bogdoll, E. Eisen, M. Nitsche, C. Scheib, and J. M. Zöllner, "Multimodal detection of unknown objects on roads for autonomous driving," in *2022 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, Journal Abbreviation: 2022 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Oct. 9, 2022, pp. 325–332, ISBN: 2577-1655. DOI: 10.1109/SMC53654.2022.9945211.

[66] A. K. Desta, S. Ohira, I. Arai, and K. Fujikawa, "MLIDS: Handling raw high-dimensional CAN bus data using long short-term memory networks for intrusion detection in in-vehicle networks," in *2020 30th International Telecommunication Networks and Applications Conference (ITNAC)*, Journal Abbreviation: 2020 30th International Telecommunication Networks and Applications Conference (ITNAC), Nov. 25, 2020, pp. 1–7, ISBN: 2474-154X. DOI: 10.1109/ITNAC50341.2020.9315024.

[67] D. Stabili, L. Ferretti, M. Andreolini, and M. Marchetti, "DAGA: Detecting attacks to in-vehicle networks via n-gram analysis," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 11, pp. 11 540–11 554, Nov. 2022, ISSN: 1939-9359. DOI: 10.1109/TVT.2022.3190721.

[68] K. Agrawal, Tejasvi Alladi, A. Agrawal, V. Chamola, and A. Benslimane, "NovelADS: A novel anomaly detection system for intra-vehicular networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 11, pp. 22 596–22 606, 2022, Place: New York Publisher: The Institute of Electrical and Electronics Engineers, Inc. (IEEE), ISSN: 15249050. DOI: 10.1109/TITS.2022.3146024. [Online]. Available: https://www.proquest.com/scholarly-journals/novelads-novel-anomaly-detection-system-intra/docview/2734387311/se-2?accountid=14511.

[69] B. Peralta, R. Soria, O. Nicolis, F. Ruggeri, L. Caro, and A. Bronfman, "Outlier vehicle trajectory detection using deep autoencoders in santiago, chile," *Sensors*, vol. 23, no. 3, 2023. DOI: 10.3390/s23031440. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85147843135&doi=10.3390%2fs23031440&partnerID=40&md5=972b9b995514f8c3b515d5a46879faef.

[70] G. Di Biase, H. Blum, R. Siegwart, and C. Cadena, "Pixel-wise anomaly detection in complex driving scenes," presented at the Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2021, pp. 16 913–16 922. DOI: 10.1109/CVPR46437.2021.01664. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85114857150&doi=10.1109%2fCVPR46437.2021.01664&partnerID=40&md5=d08f9c72c1d819197c1adfaa4a1c9b65.

[71] G. Zhang, Q. Liu, C. Cao, J. Li, and Y. Li, "Bit scanner: Anomaly detection for in-vehicle CAN bus using binary sequence whitelisting," *Computers and Security*, vol. 134, 2023. DOI: 10.1016/j.cose.2023.103436. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85169029560&doi=10.1016%2fj.cose.2023.103436&partnerID=40&md5=f9c2902f66d3c28b8c4f1fb289e23836.

[72] H. M. Song, J. Woo, and H. K. Kim, "In-vehicle network intrusion detection using deep convolutional neural network," *Vehicular Communications*, vol. 21, p. 100 198, 2020, Publisher: Elsevier.

[73] P. Balaji, M. Ghaderi, and H. Zhang, "CANLite: Anomaly detection in controller area networks with multitask learning," in *2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring)*, Journal Abbreviation: 2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring), Jun. 19, 2022, pp. 1–5, ISBN: 2577-2465. DOI: 10.1109/VTC2022-Spring54318.2022.9860358.

[74] H. M. Song and Huy Kang Kim, "Self-supervised anomaly detection for in-vehicle network using noised pseudo normal data," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 2, pp. 1098–1108, 2021, Place: New York Publisher: The Institute of Electrical and Electronics Engineers, Inc. (IEEE), ISSN: 00189545. DOI: 10.1109/TVT.2021.3051026. [Online]. Available: https://www.proquest.com/scholarly-journals/self-supervised-anomaly-detection-vehicle-network/docview/2501323760/se-2?accountid=14511.

[75] P. Balaji and M. Ghaderi, "NeuroCAN: Contextual anomaly detection in controller area networks," presented at the 2021 IEEE International Smart Cities Conference, ISC2 2021, 2021. DOI: 10.1109/ISC253183.2021.9562830. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85118158390&doi=10.1109%2fISC253183.2021.9562830&partnerID=40&md5=d9843119d900afdeb3226528eefe997f.

[76] P. Mansourian, N. Zhang, A. Jaekel, and M. Kneppers, "Deep learning-based anomaly detection for connected autonomous vehicles using spatiotemporal information," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–12, 2023, ISSN: 1558-0016. DOI: 10.1109/TITS.2023.3286611.

[77] D. Aksu and M. Aydin, "MGA-IDS: Optimal feature subset selection for anomaly detection framework on in-vehicle networks-CAN bus based on genetic algorithm and intrusion detection approach," *Computers and Security*, vol. 118, 2022. DOI: 10.1016/j.cose.2022.102717. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85129550859&doi=10.1016%2fj.cose.2022.102717&partnerID=40&md5=1d8a09b7fd51d70589912d042af9d820.

[78] F. Fenzl, R. Rieke, and A. Dominik, "In-vehicle detection of targeted CAN bus attacks," presented at the ACM International Conference Proceeding Series, 2021. DOI: 10.1145/3465481.3465755. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85113196129&doi=10.1145%2f3465481.3465755&partnerID=40&md5=2c2726ab2381f39df7bad91900b48e6d.

[79] Y. Jaoudi, C. Yakopcic, and T. Taha, "Conversion of an unsupervised anomaly detection system to spiking neural network for car hacking identification," in *2020 11th International Green and Sustainable Computing Workshops (IGSC)*, Journal Abbreviation: 2020 11th International Green and Sustainable Computing Workshops (IGSC), Oct. 19, 2020, pp. 1–4. DOI: 10.1109/IGSC51522.2020.9291232.

[80] J. Xiao, L. Yang, F. Zhong, H. Chen, and X. Li, "Robust anomaly-based intrusion detection system for in-vehicle network by graph neural network framework," *Applied Intelligence*, vol. 53, no. 3, pp. 3183–3206, Feb. 2023, Place: Boston Publisher: Springer Nature B.V., ISSN: 0924669X. DOI: 10.1007/s10489-022-03412-8. [Online]. Available: https://www.proquest.com/scholarly-journals/robust-anomaly-based-intrusion-detection-system/docview/2763975957/se-2?accountid=14511.

[81] J. Khan, Dae-Woon Lim, and K. Young-Sik, "Intrusion detection system CAN-bus in-vehicle networks based on the statistical characteristics of attacks," *Sensors*, vol. 23, no. 7, p. 3554, 2023, Place: Basel Publisher: MDPI AG. DOI: 10.3390/s23073554. [Online]. Available: https://www.proquest.com/scholarly-journals/intrusion-detection-system-can-bus-vehicle/docview/2799783522/se-2.

[82] P. Hade and K. Waghmare, "Detection and classification of anomalies in internet of vehicles using convolutional neural networks," presented at the 2022 1st International Conference on Computational Science and Technology,

ICCST 2022 - Proceedings, 2022, pp. 512–517. DOI: 10.1109/ICCST55948.2022.10040446. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85149377507&doi=10.1109%2fICCST55948.2022.10040446&partnerID=40&md5=a16a4880002d6efad35ee0d5528a6676.

[83] F. Jin, M. Chen, W. Zhang, Y. Yuan, and S. Wang, "Intrusion detection on internet of vehicles via combining log-ratio oversampling, outlier detection and metric learning," *Information Sciences*, vol. 579, pp. 814–831, 2021. DOI: 10.1016/j.ins.2021.08.010. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85113605573&doi=10.1016%2fj.ins.2021.08.010&partnerID=40&md5=3c664ab908043274dd37611538fc0652.

[84] D. Shi, M. Xu, T. Wu, and L. Kou, "Intrusion detecting system based on temporal convolutional network for in-vehicle CAN networks," *Mobile Information Systems*, vol. 2021, 2021. DOI: 10.1155/2021/1440259. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85116668173&doi=10.1155%2f2021%2f1440259&partnerID=40&md5=17496596358db827b272db4d40d8e584.

[85] G. D'Angelo, M. Ficco, and A. Robustelli, "An association rules-based approach for anomaly detection on CAN-bus," presented at the Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 14105 LNCS, 2023, pp. 174–190. DOI: 10.1007/978-3-031-37108-0_12. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85168773608&doi=10.1007%2f978-3-031-37108-0_12&partnerID=40&md5=f8fc08e0697f579f060868894667d54d.

[86] C. S. Wickramasinghe, D. L. Marino, H. S. Mavikumbure, *et al.*, "RX-ADS: Interpretable anomaly detection using adversarial ML for electric vehicle CAN data," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–13, 2023, ISSN: 1558-0016. DOI: 10.1109/TITS.2023.3294349.

[87] U. D. of Transportation, *Safety pilot model deployment data*, 2022. [Online]. Available: https://catalog.data.gov/dataset/safety-pilot-model-deployment-data.

[88] J. Watts, F. Van Wyk, S. Rezaei, Y. Wang, N. Masoud, and A. Khojandi, "A dynamic deep reinforcement learning-bayesian framework for anomaly detection," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 12, pp. 22 884–22 894, Dec. 2022, ISSN: 1558-0016. DOI: 10.1109/TITS.2022.3200906.

[89] A. R. Javed, M. Usman, S. U. Rehman, M. U. Khan, and M. S. Haghighi, "Anomaly detection in automated vehicles using multistage attention-based convolutional neural network," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4291–4300, Jul. 2021, ISSN: 1558-0016. DOI: 10.1109/TITS.2020.3025875.

[90] S. Rajendar and V. Kaliappan, "Sensor data based anomaly detection in autonomous vehicles using modified convolutional neural network," *INTELLIGENT AUTOMATION AND SOFT COMPUTING*, vol. 32, no. 2, pp. 859–875, 2022, ISSN: 1079-8587. DOI: 10.32604/iasc.2022.020936.

[91] Y. Wang, N. Masoud, and A. Khojandi, "Real-time sensor anomaly detection and recovery in connected automated vehicle sensors," *IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS*, vol. 22, no. 3, pp. 1411–1421, Mar. 2021, ISSN: 1524-9050. DOI: 10.1109/TITS.2020.2970295.

[92] Y. Wang, R. Zhang, N. Masoud, and H. Liu, "Anomaly detection and string stability analysis in connected automated vehicular platoons," *Transportation Research Part C: Emerging Technologies*, vol. 151, 2023. DOI: 10.1016/j.trc.2023.104114. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85151795511&doi=10.1016%2fj.trc.2023.104114&partnerID=40&md5=f8fff55b29a6ae0bbc059ee760f80ee7.

[93] Y. Wang, N. Masoud, and A. Khojandi, "Anomaly detection in connected and automated vehicles using an augmented state formulation," in *2020 Forum on Integrated and Sustainable Transportation Systems (FISTS)*, Journal Abbreviation: 2020 Forum on Integrated and Sustainable Transportation Systems (FISTS), Nov. 3, 2020, pp. 156–161. DOI: 10.1109/FISTS46898.2020.9264885.

[94] Z. He, Y. Chen, and H. Zhang, "WKN-OC: A new deep learning method for anomaly detection in intelligent vehicles," *IEEE Transactions on Intelligent Vehicles*, pp. 1–12, 2023. DOI: 10.1109/TIV.2023.3243356. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85149408876&doi=10.1109%2fTIV.2023.3243356&partnerID=40&md5=58d70a1f2cb684011d7fc4d75c710841.

[95] Z. He, Y. Chen, D. Zhang, and M. Abdulaal, "Vehicle anomaly detection by attention-enhanced temporal convolutional network," in *2023 IEEE 6th International Conference on Industrial Cyber-Physical Systems (ICPS)*, Journal Abbreviation: 2023 IEEE 6th International Conference on Industrial Cyber-Physical Systems (ICPS), May 8, 2023, pp. 1–6, ISBN: 2769-3899. DOI: 10.1109/ICPS58381.2023.10128090.

[96] H. Lee, S. H. Jeong, and H. K. Kim, "OTIDS: A novel intrusion detection system for in-vehicle network by using remote frame," in *2017 15th Annual Conference on Privacy, Security and Trust (PST)*, vol. 00, Aug. 2017, pp. 57–5709. DOI: 10.1109/PST.2017.00017. [Online]. Available: doi.ieeecomputersociety.org/10.1109/PST.2017.00017.

[97] H. K. Kalutarage, M. O. Al-Kadri, M. Cheah, and G. Madzudzo, "Context-aware anomaly detector for monitoring cyber attacks on automotive CAN bus," in *Proceedings of the 3rd ACM Computer Science in Cars Symposium*, ser. CSCS '19, event-place: Kaiserslautern, Germany, New York, NY, USA: Association for Computing Machinery, 2019, ISBN: 978-1-4503-7004-2. DOI: 10.1145/3359999.3360496. [Online]. Available: https://doi.org/10.1145/3359999.3360496.

[98] O. Avatefipour, A. S. Al-Sumaiti, A. M. El-Sherbeeny, *et al.*, "An intelligent secured framework for cyberattack detection in electric vehicles' CAN bus using machine learning," *IEEE Access*, vol. 7, pp. 127 580–127 592, 2019, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2019.2937576.

[99] A. Paul and M. R. Islam, "An artificial neural network based anomaly detection method in CAN bus messages in vehicles," in *2021 International Conference on Automation, Control and Mechatronics for Industry 4.0 (ACMI)*, Journal Abbreviation: 2021 International Conference on Automation, Control and Mechatronics for Industry 4.0 (ACMI), Jul. 8, 2021, pp. 1–5. DOI: 10.1109/ACMI53878.2021.9528201.

[100] S. -F. Lokman, A. T. Bin Othman, and M. -H. Abu-Bakar, "Optimised structure of convolutional neural networks for controller area network classification," in *2018 14th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD)*, Journal Abbreviation: 2018 14th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD), Jul. 28, 2018, pp. 475–481. DOI: 10.1109/FSKD.2018.8687274.

[101] M. Hanselmann, T. Strauss, K. Dormann, and H. Ulmer, "CANet: An unsupervised intrusion detection system for high dimensional CAN bus data," *Ieee Access*, vol. 8, pp. 58 194–58 205, 2020, ISBN: 2169-3536 Publisher: IEEE.

[102] E. Gherbi, B. Hanczar, J. -C. Janodet, and W. Klaudel, "DAD: A distributed anomaly detection framework for future in-vehicle network," in *2022 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, Journal Abbreviation: 2022 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), Nov. 16, 2022, pp. 1–6. DOI: 10.1109/ICECCME55909.2022.9988392.

[103] S. V. Thiruloga, V. K. Kukkala, and S. Pasricha, "TENET: Temporal CNN with attention for anomaly detection in automotive cyber-physical systems," in *2022 27th Asia and South Pacific Design Automation Conference (ASP-DAC)*, Journal Abbreviation: 2022 27th Asia and South Pacific Design Automation Conference (ASP-DAC), Jan. 17, 2022, pp. 326–331, ISBN: 2153-697X. DOI: 10.1109/ASP-DAC52403.2022.9712524.

[104] V. Kukkala, S. Thiruloga, and S. Pasricha, "LATTE: LSTM self-attention based anomaly detection in embedded automotive platforms," *ACM Transactions on Embedded Computing Systems*, vol. 20, no. 5, 2021. DOI: 10.1145/3476998. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85115852058&doi=10.1145%2f3476998&partnerID=40&md5=8bf6c5f8a6323f12f6e39b6cfbff0970.

[105] E. Gherbi, B. Hanczar, J.-C. Janodet, and W. Klaudel, *Deep Learning for In-Vehicle Intrusion Detection System* (Communications in Computer and Information Science). 2020, vol. 1332, 50 pp., Pages: 58. DOI: 10.1007/978-3-030-63820-7_6. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85097272273&doi=10.1007%2f978-3-030-63820-7_6&partnerID=40&md5=b68dcd6ca2b0a609884f452c37b384e0.

[106] Udacity Inc, *Open sourcing 223gb of driving data*, May 10, 2016. [Online]. Available: https://medium.com/udacity/open-sourcing-223gb-of-mountain-view-driving-data-f6b5593fbfa5#:~:text=What's%20Included,log%20included%20in%20the%20dataset..

[107] F. Guo, Z. Wang, S. Du, *et al.*, "Detecting vehicle anomaly in the edge via sensor consistency and frequency characteristic," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 6, pp. 5618–5628, Jun. 2019, ISSN: 1939-9359. DOI: 10.1109/TVT.2019.2907692.

[108] L. Wang, X. Zhang, D. Li, and H. Liu, "Multi-sensors space and time dimension based intrusion detection system in automated vehicles," *IEEE Transactions on Vehicular Technology*, pp. 1–16, 2023, ISSN: 1939-9359. DOI: 10.1109/TVT.2023.3306345.

[109] A. Geiger, P. Lenz, and R. Urtasun, "Are we ready for autonomous driving? the kitti vision benchmark suite," in *2012 IEEE conference on computer vision and pattern recognition*, IEEE, 2012, pp. 3354–3361, ISBN: 1-4673-1228-2.

[110] D. Bogdoll, M. Zhang, M. Nitsche, and J. M. Zöllner, "Experiments on anomaly detection in autonomous driving by forward-backward style transfers," in *2022 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, Journal Abbreviation: 2022 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), Nov. 16, 2022, pp. 1–7. DOI: 10.1109/ICECCME55909.2022.9988287.

[111] B. Ganguly, D. Dey, and S. Munshi, "An unsupervised learning approach for road anomaly segmentation using RGB-d sensor for advanced driver assistance system," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 10, pp. 19 042–19 053, Oct. 2022, ISSN: 1558-0016. DOI: 10.1109/TITS.2022.3164847.

[112] A. Ranjbar, C. -H. Yeh, S. Hornauer, S. X. Yu, and C. -Y. Chan, "Scene novelty prediction from unsupervised discriminative feature learning," in *2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC)*, Journal Abbreviation: 2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC), Sep. 20, 2020, pp. 1–7. DOI: 10.1109/ITSC45102.2020.9294451.

[113] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *2015 military communications and information systems conference (MilCIS)*, IEEE, 2015, pp. 1–6, ISBN: 1-4673-7008-8.

[114] S. Aziz, Muhammad Talib Faiz, A. M. Adeniyi, *et al.*, "Anomaly detection in the internet of vehicular networks using explainable neural networks (xNN)," *Mathematics*, vol. 10, no. 8, p. 1267, 2022, Place: Basel Publisher: MDPI AG.

DOI: 10.3390/math10081267. [Online]. Available: https://www.proquest.com/scholarly-journals/anomaly-detection-internet-vehicular-networks/docview/2652999045/se-2.

[115] J. Kamel, M. Wolf, R. W. Van Der Hei, A. Kaiser, P. Urien, and F. Kargl, "Veremi extension: A dataset for comparable evaluation of misbehavior detection in vanets," in *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, IEEE, 2020, pp. 1–6, ISBN: 1-72815-089-2.

[116] T. Alladi, B. Gera, A. Agrawal, V. Chamola, and F. R. Yu, "DeepADV: A deep neural network framework for anomaly detection in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 11, pp. 12 013–12 023, Nov. 2021, ISSN: 1939-9359. DOI: 10.1109/TVT.2021.3113807.

[117] T. Alladi, A. Agrawal, B. Gera, V. Chamola, B. Sikdar, and M. Guizani, "Deep neural networks for securing IoT enabled vehicular ad-hoc networks," in *ICC 2021 - IEEE International Conference on Communications*, Journal Abbreviation: ICC 2021 - IEEE International Conference on Communications, Jun. 14, 2021, pp. 1–6, ISBN: 1938-1883. DOI: 10.1109/ICC42927.2021.9500823.

[118] X. Liu, "Misbehavior detection based on deep learning for VANETs," in *2022 International Conference on Networks, Communications and Information Technology (CNCIT)*, Journal Abbreviation: 2022 International Conference on Networks, Communications and Information Technology (CNCIT), Jun. 17, 2022, pp. 122–128. DOI: 10.1109/CNCIT56797.2022.00027.

[119] M. Cordts, M. Omran, S. Ramos, *et al.*, "The cityscapes dataset," in *CVPR Workshop on the Future of Datasets in Vision*, vol. 2, sn, 2015.

[120] F. Yu, H. Chen, X. Wang, *et al.*, "Bdd100k: A diverse driving dataset for heterogeneous multitask learning," in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, 2020, pp. 2636–2645.

[121] E. Romera, L. M. Bergasa, and R. Arroyo, "Need data for driving behavior analysis? presenting the public UAH-DriveSet," in *IEEE International Conference on Intelligent Transportation Systems (ITSC)*, pp. 387–392.

[122] G. Slavic, P. Marin, D. Martin, L. Marcenaro, and C. Regazzoni, "Interpretable anomaly detection using a generalized markov jump particle filter," in *2021 IEEE International Conference on Autonomous Systems (ICAS)*, Journal Abbreviation: 2021 IEEE International Conference on Autonomous Systems (ICAS), Aug. 11, 2021, pp. 1–5. DOI: 10.1109/ICAS49788.2021.9551111.

[123] G. Singh, S. Akrigg, M. Di Maio, *et al.*, "Road: The road event awareness dataset for autonomous driving," *IEEE transactions on pattern analysis and machine intelligence*, vol. 45, no. 1, pp. 1036–1054, 2022, ISBN: 0162-8828 Publisher: IEEE.

[124] S. Rajapaksha, H. Kalutarage, M. O. Al-Kadri, G. Madzudzo, and A. V. Petrovski, "Keep the moving vehicle secure: Context-aware intrusion detection system for in-vehicle CAN bus security," in *2022 14th International Conference on Cyber Conflict: Keep Moving! (CyCon)*, Journal Abbreviation: 2022 14th International Conference on Cyber Conflict: Keep Moving! (CyCon), vol. 700, pp. 309–330, ISBN: 2325-5374. DOI: 10.23919/CyCon55549.2022.9811048.

[125] D. Birks, M. Townsley, and A. Stewart, "Emergent regularities of interpersonal victimization: An agent-based investigation," *Journal of Research in Crime and Delinquency*, vol. 51, no. 1, pp. 119–140, 2014, ISBN: 0022-4278 Publisher: Sage Publications Sage CA: Los Angeles, CA.

[126] Y. Sun, W. Yu, Y. Chen, and A. Kadam, "Time series anomaly detection based on GAN," in *2019 Sixth International Conference on Social Networks Analysis, Management and Security (SNAMS)*, Journal Abbreviation: 2019 Sixth International Conference on Social Networks Analysis, Management and Security (SNAMS), Oct. 22, 2019, pp. 375–382. DOI: 10.1109/SNAMS.2019.8931714.

[127] H. Kim, J. Park, K. Min, and K. Huh, "Anomaly monitoring framework in lane detection with a generative adversarial network," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 3, pp. 1603–1615, Mar. 2021, ISSN: 1558-0016. DOI: 10.1109/TITS.2020.2973398.

[128] J. Pfeil, J. Wieland, T. Michalke, and A. Theissler, "On why the system makes the corner case: AI-based holistic anomaly detection for autonomous driving," presented at the IEEE Intelligent Vehicles Symposium, Proceedings, vol. 2022-June, 2022, pp. 337–344. DOI: 10.1109/IV51971.2022.9827078. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85135379804&doi=10.1109%2fIV51971.2022.9827078&partnerID=40&md5=19cc3fccc2be06a8fcb2afefdd951021.

[129] S. Yaqoob, A. Hussain, F. Subhan, G. Pappalardo, and M. Awais, "Deep learning based anomaly detection for fog-assisted IoVs network," *IEEE Access*, vol. 11, pp. 19 024–19 038, 2023, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2023.3246660.

[130] International Telecommunication Union, *Recommendation ITU-t x.1382 (03/2023)*, Mar. 2023. [Online]. Available: https://www.itu.int/itu-t/recommendations/rec.aspx?id=15104.

[131] United Nations, *Addendum 154 – UN regulation no. 155*, Apr. 3, 2021. [Online]. Available: https://unece.org/sites/default/files/2023-02/R155e%20%282%29.pdf (visited on 03/15/2024).

[132] B. Lampe and W. Meng, "Can-train-and-test: A curated CAN dataset for automotive intrusion detection," *Computers & Security*, p. 103 777, 2024, ISBN: 0167-4048 Publisher: Elsevier.

[133] V. Jacob, F. Song, A. Stiegler, Y. Diao, and N. Tatbul, "Anomalybench: An open benchmark for explainable anomaly detection," *CoRR*, 2020.

[134] A. Lavin and S. Ahmad, "Evaluating real-time anomaly detection algorithms–the numenta anomaly benchmark," in *2015 IEEE 14th international conference on machine learning and applications (ICMLA)*, IEEE, 2015, pp. 38–44, ISBN: 1-5090-0287-1.

[135] M. A. Lones, "How to avoid machine learning pitfalls: A guide for academic researchers," *arXiv preprint arXiv:2108.02497*, 2021.

[136] F. Hartwich and R. Bosch, "Introducing CAN XL into CAN networks," 2020.

[137] P. Meyer, T. Häckel, F. Korf, and T. C. Schmidt, "Network anomaly detection in cars based on time-sensitive ingress control," in *2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall)*, Journal Abbreviation: 2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall), Dec. 18, 2020, pp. 1–5, ISBN: 2577-2465. DOI: 10.1109/VTC2020-Fall49728.2020.9348746.

John Roar Ventura Solaas is pursuing a PhD in cybersecurity at the Centre for Doctoral Training (CDT) at University College London. He is funded by the Engineering & Physical Sciences Research Council (EPSRC). His research interest is anomaly detection for connected and autonomous vehicles.

Dr Enrico Mariconti received his PhD degree from University College London in 2019 working on detection and prevention of automated threats such as malware using AI. He currently works as an assistant professor in the Department of Security and Crime Science at UCL and focuses on understanding and countering cyber-physical threats, from IoT devices to social media with a particular focus on hate, harassment, and safety.

Dr Nilufer Tuptuk received her PhD degree in Computer Science from the University College London in 2019. She currently works as an Assistant Professor in the Department of Security and Crime Science at the same institution. Her research interests include cyber-physical systems security, including the Internet of Things, Industrial Control Systems, and Connected and Autonomous Vehicles. Her work involves application and effectiveness of AI-based models in identifying vulnerabilities and detecting anomalous behaviours within these systems.