Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 5, 2026

PRIVACY DETECTION BY A COMPREHENSIVE REVIEW OF MACHINE LEARNING AND DEEP LEARNING TECHNIQUES TO ENHANCE SECURE DATA SHARING IN AUTONOMOUS VEHICLES

[1]Muhammad Qasim, [2]Muhammad Asif, [3]Misbah Kanwal, [4]Farhan Hassan
[1-4]Department of Information and Communication Engineering The Islamia University of Bahawalpur, Pakistan
[1]binqasim4035@gmail.com, [2]asifbhutta7519@gmail.com, [3]raomisbah456}@gmail.com, [4]farhan.hassan@iub.edu.pk

DOI:-

Keywords
Connected Vehicles, Autonomous Vehicles, Data Privacy, Cybersecurity, Internet of Vehicles, Privacy-Preserving Machine Learning.

Article History
Received: 19 April 2026
Accepted: 19 May 2026
Published: 21 May2026

Corresponding Author: *

Muhammad Qasim
binqasim4035@gmail.com

Abstract
Autonomous and connected vehicles (ACVs) are changing the transportation of the modern world they combine sophisticated sensing, communication, and modern technologies. These vehicles will keep on gathering, processing and distributing a significant amount of data about drivers, passengers and the environment around them. Although such data is necessary in terms of safety, navigation and intelligent decision-making, it also brings major privacy and security concerns. There is a chance that sensitive information can be revealed to cyberattacks, abuse, or unwarranted monitoring such as location history, driving behavior, and personal identifiers. The paper summarizes the key privacy and security issues in autonomous and connected vehicles, discusses current protection methods that include feder-ated learning, homomorphic encryption, and differential privacy, and also outlines the gaps in research. It tries to give a general overview of current issues and solutions to the problems at the undergraduate level and stresses the need of privacy-sensitive design in the next generation of intelligent transport systems.

I. Introduction

In this modern era the use of autonomous and connected vehicles (ACVs) as one of the key technological advancements in the field of intelligent transportation systems so it receives a lot of media attention. The artificial intelligence and sensor technologies and wireless communication have enabled cars to detect the environment around them, handle more complex driving scenarios and make decisions in real time with a minimal amount of human intervention[1]. They can also be used to access and communicate with the other vehicles, roadside infrastructure and cloud based systems to have the smart coordinated transportation networks. These abilities will likely lower human error-related traffic accidents, improve traffic flow efficiency, cut down on fuel waste, and increase the mobility of the elderly and disabled persons[2][3]. As a result, governments, automakers, and tech companies are spending a lot of money developing and implementing autonomous vehicle technologies. In contrast to other vehicles, autonomous and connected vehicles are linked to serious privacy and security concerns despite these potential advantages.

The traditional cars are largely viewed as a mechanical system with very limited data processing capacity, whereas the autonomous cars are complicated cyber-physical systems that constantly collect, process, store and transmit significant volumes of data[4][5]. Such information implies precise geo- graphic location, speed, acceleration, deceleration, camera and LiDAR sensor images, and data about drivers and passengers. Even though such form of data collection is required to have safe and efficient vehicle operation, it is also linked to threat of unauthorized access, abuse, and surveillance. Data privacy is one of the most serious problems of autonomous vehicle systems. Information of location and movement collected by these vehicles may reveal some of the most personal information about the individual such as routine, home, place of work, their traveling habits and contacts with others[3].

This information can be profiled, be analyzed in terms of behavior or even be sold commercially whenever they are stored over a long period or when they are revealed to third party organizations such as manufacturers, insurance companies or even service providers. It is difficult to imagine everyday life without vehicles as opposed to online services, mobile applications, and this is why such violations of privacy in autonomous vehicles are more invasive but, at the same time, can be even more detrimental. Security weaknesses also enhance privacy[6][7]. The autopilot cars can barely manage without continuous connectivity to guide, arrange the real time traffic, software applications and emergency services. This reliance on connectivity exposes vehicles to all types of cyber attacks including unauthorized access, data interception, spoofing, and control of communication channel.

Successful cyberattacks may allow the opponents to track the vehicles or embezzle confidential personal data or have control over the work of the vehicles. In the worst-case scenarios such attacks may undermine physical safety leading to traffic jam or accidents. Therefore, privacy and security in autonomous vehicles possess a good interconnection and are to be considered together[8]. Besides individual problematic aspects on privacy, autonomous vehicles also have more prob- lems with privacy on a larger scale and to the society and the population. The data of vehicles running simultaneously may deliver the information on the detailed state of the traffic, utilization of urban facilities and movement of people. Even though such data will help in planning a smart city and ensuring traffic is optimized, hacking or misuse of such data can result in the exposure of sensitive data in the city and critical infrastructure and hence the ethics and security concern[9] [1].

Another major problem is the absence of transparency and access of automotive data practices to the end user. Not every user is aware of what his or her cars are recording, how long the storage time is and who can actually gain access to such information. Data consent is complicated or rather provided only at the initial stage of establishing a vehicle but never provides people with an opportunity to control their privacy settings[10]. It has been found out that the privacy concerns of the users depend on context, based on the perceived benefits, and trust they have with the manufacturers and that there should be clear and simple models of data governance. Machine learning technology in autonomous vehicles presents more privacy and security risks. Large datasets including sensitive personal or environmental information are trained to provide perception, prediction and decision making of machine learning models[11]. The privacy information may be threatened without even the actual sharing of raw data using trained models that are susceptible to various attacks such as membership inference or model inversion. There is a need, therefore, to secure training data and learned models[12].

The purpose of this paper is to provide a comprehensive view on the problem of privacy and security with regard to autonomous and connected vehicles. It takes recourse to the lit- erature, analyzes the severe threat models and types of attacks, remarks on privacy-saving machine learning techniques, and leave the problem and future outlook with the goal to develop secure and privacy-conscious autonomous car systems[13].

II. Background and Related Work

A. Unmanned Aircraft Vehicles and Connected Autopilot Vehicles Data Collection.

The self driving cars and the internet driven cars require a lot of information to work. Examples of sensors that measure continuous streams of environmental and positional information include cameras, LiDAR, radar and GPS. Besides, vehicles will gather in-car data related to speeding, braking, steering and system troubleshooting. Along with user profiles and infotainment systems, this information can be linked to the individual drivers and passengers[6][8]. It is known that such information may reveal

sensitive aspects, i.e., work and home destinations, habits every day, and personal habits. The use of vehicle data also may uncover population level data, such as traffic flows or road network plans, in smart cities, which can be both economically and security-based in nature. The abundance of these data sets when pooled on large scale does hold the threat of abuse unless security is offered[14].

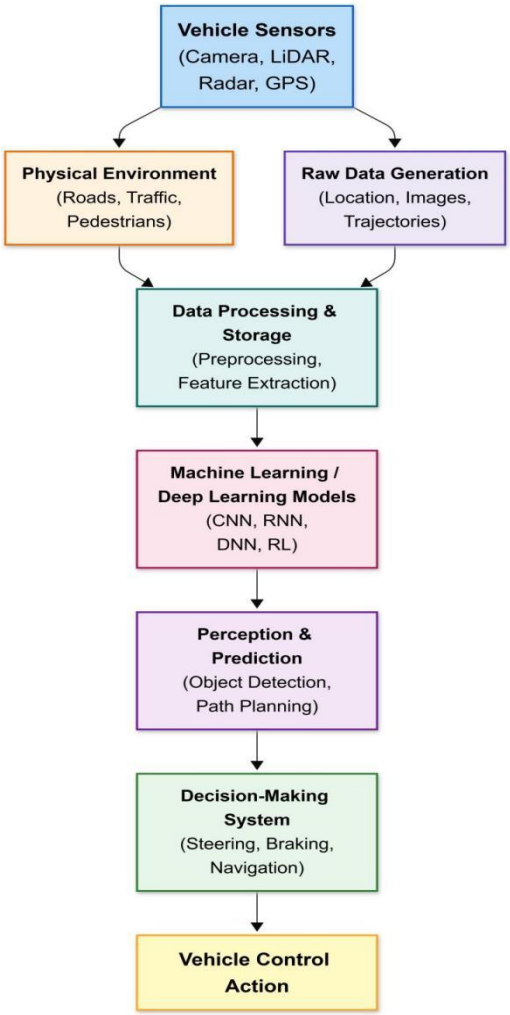

Fig. 1. Generalized Workflow of Reviewed Autonomous Vehicle Systems

TABLE I: Literature Review on Security and Privacy in Autonomous Vehicles and AI

Technique / Focus	Representative Studies	Key Contributions	Identified Limitations
Privacy-Preserving ML	[1], [13], [21], [23], [29], [33]	Secure model training using Fully Homo- morphic Encryption (FHE) and Federated Learning (FL); protects raw user data dur- ing training.	High computational overhead in FHE; communication bottlenecks in FL; tradeoff between privacy and model utility.
Sensor Fusion & Perception	[4], [9], [12], [30]	Enables high-performance 3D object de- tection using LiDAR-camera fusion and secure V2X data sharing.	Limited bandwidth in dense environments; latency challenges; vulnerability to false data injection attacks.
Adversarial Security	[25], [31], [34]	Identifies vulnerabilities in AV perception systems and surveys physical/digital ad- versarial defenses mechanisms.	Heavy reliance on simulation-based evaluations; real-time defense intro- duces processing overhead.
Edge & Blockchain Data	[7], [8], [14], [20], [24], [27]	Supports decentralized and secure AV data sharing through edge computing, blockchain, and IPFS integration.	Scalability limitations in blockchain consensus; resource constraints at edge devices; difficult legacy integration.
Trustworthy AI & Ethics	[2], [3], [22], [26], [36]	Promotes Explainable AI (XAI), certified safety mechanisms, and ethical AI gover- nance frameworks.	Tradeoff between explainability and ac- curacy; absence of globally accepted regulations and standards.
Trajectory Privacy	[5], [6], [11], [28], [32], [35]	Provides trajectory anonymization and privacy-preserving data publishing for au- tonomous vehicle systems.	Assumes static adversary models; ex- cessive anonymization decreases data usefulness and analytical quality.

B. Threats to data privacy in self-driving vehicles

The autonomous car privacy risks can be categorized under the following broad categories namely, individual, population and proprietary privacy. The problem of the individual privacy is a question that also appears in case one gets to know about personal data such as the history of their location or biometrical identifiers. Population level risks comprise of inferential privacy of the communities or cities, such as traffic volume or infrastructure vulnerability[15].Protecting machine learning models and intellectual property used by manufactur- ers is connected to proprietary privacy. In the user studies, it was revealed that many drivers do not feel comfortable with the idea of the continuous collection and utilization of secondary data and constant collection of data without their knowledge or adequate control of how their information is being disseminated. These concerns indicate the applicability of privacy models and consent systems on a user-building viewpoint[16][17].

C. Security Threat and Surface of attack

The range of threats to cybersecurity of autonomous vehi- cles is very high due to reliance on connection and software. The vehicle system is susceptible to attack on sensors, operat- ing systems, communication networks and cloud services. The most typical of the attacks include data spoofing, man-in-the- middle, model inversion and vehicle tracking[10][15]. Attack- ers are capable of using car-car and car-infrastructure (V2V and V2I) communication vulnerabilities to inject a malicious data or steal sensitive knowledge according to layer-based sur- veys. Such attacks may lead to inappropriate decisions during the driving process, traffic jam or even privacy violations. The threat to training data or inference processes is not less critical because vehicles become increasingly dependent upon machine learning models[18].

D. Privacy-Saving Methods

To minimize such risks, some machine learning techniques that preserve privacy have been developed. Federated learning also enables vehicles to learn models collaboratively with each other without accessing raw data to minimize the exposure of sensitive information. Differential privacy introduces certain controlled noise to the model outputs or data so as to decrease the chances of subject identification[19]. Homomorphic en- cryption allows computing the data on the encrypted data and the privacy is preserved during the calculation. Though these are promising methods, trade-offs between privacy, accuracy and computational efficiency are likely to emerge. These trade- offs are critical in the comprehension that can be employed in the actual systems in cars[16].

III. Review Methodology

In the studies used in the paper, various methodologies are applied to explore the problem of privacy and security in autonomous and connected cars. The complexity of the problem has caused

researchers to embrace qualitative, quanti- tative, experimental, and survey-based methods basing on the objectives of the research[20].

A. Data Collection and Data Analysis Methodologies

A significant portion of the reviewed literature is concerned with the analysis of data produced by autonomous and con- nected vehicles, such as sensor data and vehicle logs, commu- nication messages and mobility traces. Such studies are usually carried out to understand the sensitivities of such data in exposing the information about drivers or passengers or other living environments[21]. Certain papers examine actual car data sets as measured by test fleets or simulation environments, whereas others use artificial data sets which are generated with traffic simulators to study large-scale automotive behavior. A set of data is then processed to determine privacy threats in- cluding location tracking, behavioral profiling, or data linkage attacks.

TABLE II: Methodological Stages in Autonomous Vehicle Security and Privacy Research

Ref. No	Methodological Stage	Approach Used	Purpose	Limitations
[4], [5], [9], [11], [12], [30]	Data Acquisition	GPS traces, sensor datasets, and simulated environments	Analyze location privacy and mobility au- tonomous driving behavior	Limited access to real-world and large-scale AV datasets
[3], [10], [22], [36]	System Modeling	Cyber-physical systems and lay- ered AV architectures	Study interactions between sen- sors, machine learning, and vehi- cle control systems	Simplistic assumptions and lim- ited consideration of hardware con- straints
[6], [25], [28], [32]	Threat Modeling	Adversary models and attack sur- face analysis	Classify spoofing, tracking, and inference-based attacks	Mostly theoretical analysis with limited real-world diversity
[2], [4], [10], [12], [24], [26]	ML/DL Evaluation	CNN, RNN, DNN, SVM, and clus- tering techniques	Evaluate detection accuracy, anomaly recognition, and privacy leakage	High computational cost and risk of dataset overfitting
[25], [31], [34]	Attack Simulation	Membership inference, model in- version, and poisoning attacks	Measure information leakage and vulnerabilities in ML models	Primarily offline evaluation without continuous learning support
[1], [7], [8], [13], [14], [20], [21], [23], [27],	Privacy Techniques	Federated learning, differential pri- vacy, and encryption mechanisms	Protect sensitive data and mini- mize direct data sharing	Reduced accuracy and increased latency/communication overhead
[1], [21], [24], [27]	Performance Analysis	Accuracy, latency, computa- tional overhead metrics	Evaluate feasibility for real-time autonomous vehicle deployment	Tradeoff between privacy preserva- tion and real-time safety require- ments
[2], [6], [13], [25], [30], [36]	Result Interpretation	Comparative studies and qualitative analysis	Identify research gaps, trends, and future research directions	Lack of standardized benchmarks and evaluation criteria

B. Qualitative and User-Centered Studies

A number of papers use qualitative research methods to learn how users perceive privacy with autonomous cars. Such studies typically employ surveys, interviews or focus group among drivers and vehicle owners[22].Respondents will be requested to respond to issues regarding their knowledge of automotive data gathering, their privacy and their readiness to share information under various circumstances. The thematic or framework-based analysis is applied to the responses in order to detect the main factors that can drive the privacy preferences, which include benefits perceived, trust into man- ufacturers, and situational factors, like the location or time. This method allows the researcher to see privacy as a technical problem and a human concern.

C. Security Analysis and Threat Modelling

Formal threat modeling techniques are employed in a large number of papers in order to study security risks. Adversarial models define the capabilities, access level and the goals a set of attackers can achieve. According to these threat models, research classifies attacks as sensor spoofing, communication- based attacks, and machine learning inference attacks[23]. Security evaluation may involve theoretical analysis, protocol analysis or simulation to show how the attack can be per- formed and what the consequences of such an attack could be on vehicle safety and data privacy[8][24].

D. Attack Experimental Evaluation

Other studies that have been examined carry out experi- mental assessments to prove attack scenarios proposed. Such experiments could be simulated vehicular networks, controlled testbeds, or prototyped. As an example, communication attacks are analyzed

by introducing fake messages into simulated vehicle to vehicle networks, and machine learning attacks are analyzed by counting how sensitive information to be inferred by trained models[25]. The severity of the threat is usually measured by the use of performance measures like the attack success rate, accuracy loss, and leakage of information.

E.Assessment of Privatizing Techs

Articles to which privacy preserving machine learning meth- ods are proposed, have the common style of an experimental methodology. It can be federated learning, differential privacy, or homomorphic encryption, and scholars apply these methods and assess them with the help of benchmark datasets or vehicles[26]. These studies quantify the trade-offs among the following: privacy, accuracy, computational overhead and communication cost. Comparative analysis is commonly done to demonstrate how the proposed methods would enhance privacy without impacting on the acceptable performance of the system.

F.Comparison and Survey-Based Reviews

A number of the papers choose survey-based methodologies to review the literature on the privacy and security issues in autonomous vehicles in a systematic manner[27]. The studies classify the previous work on the basis of type of attack, the level of privacy, and the layer of the system or the technique of protection. Survey papers in such a way as to compare the strengths, limitations, and assumptions of the works give a systematized view of the available research environment and define gaps that have to be filled by additional studies[28].

IV.Databases of Autonomous vehicles privacy and security research

The articles used in this paper argue on the basis of real- life, simulated, and benchmark data to explore the problem of privacy and security of autonomous and connected vehi- cles. The data on large scale proprietary automotive systems is usually not accessible, so scholars have been utilizing openly accessible data and data simulated through simulations, to validate threats, attacks, and different privacy preserving solutions[29].

A.Physical Vehicular and Mobility Data-set

Some of the studies are based on pragmatic data concerning computers, information sets that are monitored on test fleets on intelligent cities or mobility experiments. These types of data sets include: GPS routes, speed, accelerator, time-stamps and map. Such type of data has generally been used in the analysis of location privacy threats, tracking attacks, and behavioral profiling[30]. Based on the example of real mobility traces, the researchers demonstrate that the data concerning the home locations, daily routine, and traveling habits is sensitive personal information that can be inferred by the data on vehicles. Some of the studies rely also on the datasets collected on related car pilot programs, where cars communicate basic safety messages or telemetry data. The communication-based attack and privacy leakage of vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) networks can be analyzed on the datasets[31].

B.Sensors and Perception Data Sets

Many of the papers use publicly available sensor data that was initially generated as autonomous driving research in the context of perception-based security analysis. Such data include camera images, LiDAR point clouds, radar data and identified objects. Researchers use such datasets to test sensor spoofing attacks, adversarial examples, and perception model robustness[17][10]. Experiments can be used to establish the degree to which perception systems can be deceived and the privacy implications of sensor data leakage by modifying sensor-readings, or simply adding noise to such data.

C.Simulation-Based Datasets

The significant portion of research that is sampled with is the use of simulation-generated data due to the safety, cost, and scalability factors. Traffic simulators and autonomous driving simulators produce synthetic vehicular data under a controlled environment[32]. These datasets can permit the researcher to simulate the large scale traffic conditions, communication networks and attack conditions which would be workable or unsafe to test in the real world. Testing of the communication attacks, data injection and privacy-preserving protocols are greatly familiar with the use of simulation-based datasets. They also enable the experimental implementation of feder- ated learning, differentiable privacy and secure deanonymity techniques through the control of traffic density, the number of vehicles and the degree of the attack[33].

D.Machine Learning Benchmark Datasets

When testing machine learning privacy attack and defense methods, researchers have the habit of using the conven- tional benchmark datasets adapted to autonomous vehicle tasks. These are image classification datasets, object detection datasets and trajectory prediction datasets[11]. Though the sets of data are not directly accesses in cars, it is required to demonstrate the danger of privacy, e.g. membership inference and model inversion attacks in the learning models which are similar to the systems of autonomous driving. Machine learn- ing In preserving privacy machine learning, a tradeoff between model accuracy, model privacy and model computation has been studied using benchmark data. This helps the researcher to compare different techniques under similar conditions of the experiment[34].

E.Federated Learning and Distributed Data sets

The studies of federated learning used in the context of vehicle networks tend to operate with the simulation of distributed dataset between several vehicles. Each simulated vehicle contains a local subset of data i.e. onboard sensor data or driving data[35]. These databases are either division of public datasets or artificial data which is developed to reflect realistic driving heterogeneity. These configurations are taken to evaluate the safety of uncoded

information and the functionality of the model by federated learning[36].

F.Weaknesses of current Data

The papers that are reviewed also include inadequacies in the existing datasets. Most of the real world autonomous vehicle datasets are not annotated with privacy information in detail and privacy leakage is not directly measurable. Moreover, the majority of data is seen under controlled con- ditions and cannot be sufficient to characterize the variety of reality in driving behaviour or users demographics[19]. Because of this fact, researchers observe that the privacy- sensitive dataset architecture and privacy- and security-testing standard benchmarks are required in autonomous cars[37].

V.Techniques of Machine Learning and Deep Learning Applied in Reviewed Papers

The literature review on privacy and security in autonomous and connected vehicles uses a variety of machine learning (ML) and deep learning (DL) algorithms.

Its applications are mainly perception, decision-making, at- tack modelling, leakage privacy analysis, and privacy preserv- ing mechanism implementation. Classical ML models as well as high-end deep learning architectures are used depending on the goal of the research[38] .

TABLE III: ML and Privacy Techniques in Autonomous Vehicle Systems

Ref. No	*Technique*	*Learning Type*	*Application in AV Systems*	*Identified Limitations*
[2], [6], [32]	*Support Vector Machine (SVM)*	*Supervised*	*Intrusion and anomaly detection in ve- hicular communication networks*	*Sensitive to parameter tuning and af- fected by concept drift*
[6], [22]	*Random Forest*	*Supervised*	*Detection of abnormal communication patterns and malicious behaviors*	*High computational complexity and limited interpretability*
[6], [26]	*Isolation Forest*	*Unsupervised*	*Detection of rare or previously unseen attacks without labeled datasets*	*Sensitive to contamination parameter and prone to false positives*
[11], [24]	*Clustering-Based Methods*	*Unsupervised*	*Identification of unusual driving behav- iors and communication anomalies*	*Requires frequent re-clustering and un- stable under dynamic traffic conditions*
[6], [10]	*One-Class SVM*	*Semi-Supervised*	*Modeling normal vehicle behavior for intrusion and anomaly detection*	*Kernel sensitivity and scalability chal- lenges in real-time environments*
[4], [12], [23], [25], [31]	*Convolutional Neural Net- works (CNN)*	*Deep Learning*	*Object detection, LiDAR-camera fu- sion, and autonomous vehicle percep- tion*	*Vulnerable to adversarial attacks and computationally expensive*
[5], [10], [28]	*Recurrent Neural Networks (RNN/LSTM)*	*Deep Learning*	*Trajectory prediction and driver behav- ior modeling*	*Long training duration and possible pri- vacy leakage from sequential data*
[13], [21], [23], [29], [33]	*Federated Learning*	*Distributed*	*Privacy-preserving collaborative model training across distributed vehicles*	*Communication overhead and vulnera- bility to inference/model inversion at- tacks*
[1], [7], [8], [9], [14]	*Differential Privacy /Privacy-Preserving ML FHE*		*Prevents data leakage during model training and secure raw data sharing*	*Reduced model accuracy and complex privacy parameter configuration*

A.Supervised Techniques in Machine Learning

In a number of research studies, supervised machine learn- ing methods are applied in the analysis of car data and identification of security threats. Examples of algorithms used are Support Vector Machines (SVM), Decision Trees, Random Forests and k-Nearest Neighbors (k-NN)[39]. Normal and malicious vehicular behavior is normally performed on labeled datasets to train these models. As an example, intrusion detection systems employ supervised classifiers that detect the presence of abnormal communication patterns, spoofed messages or unauthorized access in vehicle networks[28]. Supervised learning can also be used to forecast driving behavior or identify mobility behavior, to illustrate the extent to which sensitive personal data may be deduced using vehicle data. These methods have been preferred because they can be interpreted and have low cost of computation as compared to deep learning models.

B.Perception Tasks Deep Learning

Deep learning is core in the autonomous vehicle perception systems. A large number of reviewed articles utilize Convo- lutional Neural Networks (CNNs) to perform image-related tasks including object detection, lane detection, traffic sign recognition, and pedestrian identification[40][1]. The CNN- based models are trained using data of cameras and sensors to model real-life autonomous driving scenarios. These per- ception models are frequently utilized in research of privacy and security to measure adversarial attack. The scholars tweak the input images or sensor data to investigate the ability of tiny distortions to induce misclassification, which are the weaknesses of perception systems. These studies prove that deep learning models can be manipulated, and this can result in safety and privacy risks[39].

C.Recurrent and Sequence-Based Model

A variety of papers use Recurrent Neural Networks (RNNs), such as Long Short-Term Memory (LSTM), Gated Recurrent Unit (GRU), models, in order to perform trajectory prediction, driver behavior analysis, and time-series data processing. Such models also work well in temporal dependencies in sequential information like vehicle speed, acceleration, and location history[41]. In terms of privacy, sequence-based models have been applied to demonstrate how driving trends over a long period of time could be learned and used to deduce sensitive data on a person. They are also applicable in attack situations to determine their future positions of vehicles so that it is possible to track and profile attacks.

D.Unmonitored and Semi-Unmonitored Learning

There are also unsupervised learning methods applied in some studies to identify anomalies in vehicular net- works (e.g., clustering algorithms e.g., k-means, DBSCAN), autoencoders)[42]. These are well applicable in cases where there is no labeled attack data. Unsupervised models can also detect abnormal vehicle behavior which can be used to determine a security breach or malicious intent by learning normal vehicle behavior. Privacy The use of autoencoders in research on feature extraction and information leakage is also research in privacy. In other applications, the data that is reconstructed with the help of autoencoders is examined to estimate the extent to which the private information can be recaptured through the compressed representations[16][15].

E.Federated Learning Models

One of the most popular machine learning methods that are discussed in the reviewed articles is federated learning (FL). In FL based models, individual vehicles convert their own data into model training, and only transmit updates to a remote server[20]. This makes it less necessary to pass raw data hence enhancing privacy. Deep neural networks such as CNNs and fully connected networks are normally used by researchers with federated learning. Experimental testing is concerned with model accuracy, convergence rate, communication cost and inference attack resistance. Other works also integrate federated learning with secure aggregation or encryption in an attempt to gain more privacy assurances[43][44].

F.ML/DL Systems privacy attack models

A number of papers apply machine learning-based attack methods in order to test privacy threats[1]. Membership infer- ence attacks utilize classifiers to decide whether a particular data sample was included in the training set of a model or not. Model inversion attacks are an optimization or generative model-based method of training sensitive data by decom- posing model output. Such attacks are frequently based on neural networks or probabilistic models to optimise leakage of information[45]. These methods reveal that trained deep learning models may also expose personal information, which is why privacy-oriented training methods are relevant.

G.Differentiation privacy and noise-based models

Noise is introduced to the gradients, model updates, or outputs to train a model in the context of works on the issue of differential privacy. The techniques are typically applied together with stochastic gradient descent (SGD) in machine learning networks. Researchers examine the privacy policy and precise model accuracy trade-off, especially in autonomous driving with safety purposes[44].

VI.Hacking Networked cars and Self-Driving cars

Because of the significant rate of software and sensor use and wireless communication, autonomous and connected cars are susceptible to a wide range of security threats[46]. Unlike traditional vehicles, modern autonomous vehicles are distributed computing systems and therefore they communi- cate with the rest of the world at all times via cloud servers, roadside infrastructure, and other cars. It is this augmented attack point that makes them victims of cybercriminals[15].

A.Vulnerabilities in Sensor-Level and Perception System

Sensors are also relevant in self driving as they provide real time information with regards to the environment. Cameras, radar and LiDAR systems can have the spoofing or manip- ulation of signals. Using the example, hackers can generate images in a manner that may be construed as fake by a vehicle, or even alter LiDAR reflections to give a vehicle the impression that there is something where there is none, or nothing where there is something[44]. These attacks not only threaten privacy, but also the security of the passengers as there is a risk of risky driving behavior as a result of false perception.

B.Communication based attacks

The profile of autonomous vehicles takes advantage of the vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications to share the traffic, navigation, and safety information. Some of the weaknesses of such communication channels are man in the middle attacks, eavesdropping and data injection. The attacker has the potential to transmit information

to any vehicle under surveillance or deploy false information to cause traffic congestion[37]. It has been ob- served that even vehicles may take unnecessary paths or even be involved in hazardous moves due to the counterfeited mes- sages in vehicles networks. The vehicle tracking attacks are particularly disturbing as the long-term movement history and the personal habits of drivers can be recognized as it is possible to observe the recurring patterns of the communication[47].

C.Attacks on Machine Learin Based Model

The systems of autonomous vehicle decision making are based on the machine learning models. Privacy attacks on these models are membership inference and model inversion attacks. Membership Inference attack targets the purpose of retrieving the information on whether or not individual data point was utilized in the training stage, which may be personal information[7]. The attacks in which one attempts to reverse the output of a trained model and recover the original training data are called model inversion attacks. Such attacks are harm- ful where the personal driving information or sensor records are utilized in training the models. Because the autopilot cars become increasingly reliant on cloud-based knowledge and updates, the safety of the information and models is a point of great concern.

VII.Problems and restrictions

The privacy preserving solutions that have been developed today have good solutions that are, however, constrained by numerous factors that restrict its use in autonomous cars[48].

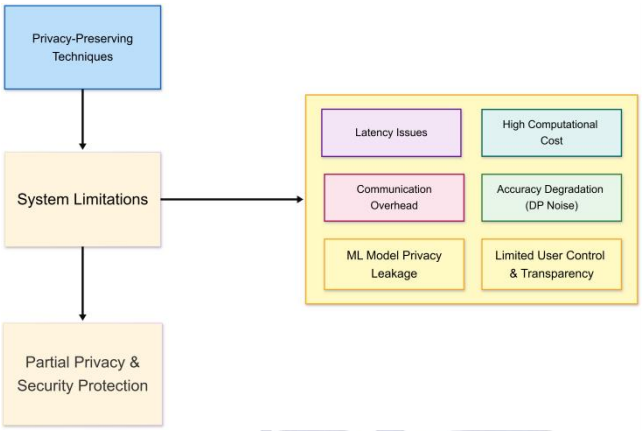

Fig. 2. System-Level Trade-offs of Privacy Preservation in AVs.

To begin with, a major problem of computational and communication overhead remains. Cars have few resources and decisions regarding the travel routes and potential pit- falls have to be made on the spot. Second, many privacy- preservation methods result in a compromise between privacy and accuracy. Small changes in the accuracy of perception can be catastrophic in the safety aspects. Third, the problem of regulatory and standardization complicates the process of deployment as the privacy rules in different locations are different, and multiple frameworks should be addressed by the manufacturer[47]. Finally, user awareness and transparency is low. A significant number of motorists do not understand that a great deal of information is gathered in the modern cars and do not possess much influence on their privacy preferences.

VIII.Future Research Directions

Although there has been a great advancement in privacy sensitive autonomous and connected cars systems, the current research has noted that the currently available solutions are still very disjointed and not comprehensive enough to implement in large scale and in a real world environment[17][49]. There is a strong future research need to create holistic and end-to- end privacy-preserving architectures that are able to integrate perception, communication, learning and decision-making into one cohesive structure. The majority of available literature addresses single elements like privacy of perception, federated learning, and sharing of secure data but does not consider cross-layers interactions. The future systems should be able to coordinate the sensor data acquisition, multimodal fusion, edge-cloud coordination, and control actions jointly and pro- vide privacy guarantees across the entire data lifecycle[36]. These architectures must also have dynamic privacy policies that change according to the driving scenario, the environment and the user preferences as opposed to using the fixed protec- tion methods.

A different direction that is of significance is the balancing of the privacy, performance, and real-time safety constraints. Numerous sources under consideration reveal that privacy pro- tection mechanisms like differential privacy, federated learn- ing, encryption, and blockchain present latency, communica- tion overhead, and accuracy losses[26]. Especially concerning safety-critical autonomous driving processes, in which low- latency and high-reliability decisions are needed, these trade- offs are especially problematic. Future studies need to address lightweight privacy schemes, adaptive noise injection schemes, hierarchical federated learning, as well as hybrid edge-cloud intelligence to minimize

overhead but ensure acceptable per- formance. In addition, uniform benchmarking systems and real-life assessment datasets are in dire demand to measure privacy-utility trade-offs in a quantitative manner, in realistic traffic and adversarial environments[50][51].

The topics of explainability, trust and human-centered pri- vacy governance also become crucial future research themes. Although current research focuses on reliable and interpretable AI, the majority of privacy-oriented autonomous vehicle in- frastructures are not transparent to the final consumers. The work in the future should be directed towards the explain- able privacy-aware learning models, which can enable users, regulators, and system designers to comprehend the way personal data is handled, secured, and even exposed[52]. The human-in-the-loop mechanisms may be used to allow human users the opportunity to dynamically change privacy levels depending on the context and risk perception. Concurrently, there is a need to further harmonise technical privacy solutions with legal, ethical, and governance frameworks to make sure that the regulations are consistent and trusted by people. This encompasses the privacy-by-design approaches, lifecycle- driven data governance and the accountability tools that cut across the manufacturers, service providers and infrastructure operators[53].

Lastly, the future smart car environment will need to deal with threats and collaborative intelligence issues. New attack surfaces are emerging as vehicles become more and more dependent on cooperative perception, V2X communication and shared learning models through updates to their models, shared features and collective decision-making processes[54]. There is the need to conduct research on effective privacy-preserving cooperative learning, fairness-aware federated learning, and robust multimodal fusion methods that can avoid inference attacks, poisoning attacks, and leakage attacks on models. Besides, by combining adaptive risk modelling and AI-based privacy risk forecasting AI-assisted privacy risk prediction can be used to activate proactive protection systems instead of response to optimal protection. It is best to tackle these issues collectively in order to have scalable, credible, and privacy- conscious autonomous mobility systems of tomorrow[55].

IX. Conclusion

Robotic and networked vehicles are a radical change in a smart transport system in that it allows perception, decision- making, and cooperative driving through data with minimum human intervention. Nonetheless, as it is emphasized all through this review, the wide range of data being gathered and processed in the form of sensory, location, and behavioral information presents threats to privacy and security levels that cannot be dealt with through the conventional means of auto- motive security[56][57]. The present paper has summarized the available literature on the privacy threat, threat model, and attack surface in autonomous vehicle systems, especially machine learning-based perception, V2X communication, and data-sharing designs. Moreover, the state-of-the-art privacy preserving methods, such as federated learning, differential privacy, secure data fusion, blockchain based sharing, and edge intelligence were also reviewed to learn their efficiency in addressing privacy leakage[58]. Although these methods have a potential to solve these problems, they still have limitations such as computational overhead, communication latency, loss of accuracy and user unawareness.

This analysis also shows that to reach a trustful and privacy-conscious autonomous driving, one should go beyond independent technical solutions and consider human-centered system design as a whole[59]. The future autonomous vehicle ecosystems should be built on holistic privacy-by-design, covering both sensor acquisition and collaborative learning as well as the data storage over time. Simultaneously, there is a significant issue with balancing the privacy assurances at the expense of real-time safety and performance, which is a con- cern, especially in large-scale and cooperative driving[60][5]. Improving explainability, governance and adaptive privacy control will be the key to developing user trust and regulation compliance. To sum up, the two phenomena of privacy and security are not the fringe benefits but the conditions of successful implementation of autonomous vehicles. Interdis- ciplinary research and integration at the system level will be critical in deciding whether autonomous mobility will be successful and acceptable in society in the future.

References

[1]R. Podschwadt, D. Takabi, P. Hu, M. H. Rafiei, and Z. Cai, "A survey of deep learning architectures for privacy-preserving machine learning with fully homomorphic encryption," Ieee Access, vol. 10, pp. 117 477– 117 500, 2022.

[2]A. Kuznietsov, B. Gyevnar, C. Wang, S. Peters, and S. V. Albrecht, "Explainable ai for safe and trustworthy autonomous driving: A system- atic review," IEEE Transactions on Intelligent Transportation Systems, vol. 25, no. 12, pp. 19 342–19 364, 2024.

[3]J. Sifakis and D. Harel, "Trustworthy autonomous system development," ACM Transactions on Embedded Computing Systems, vol. 22, no. 3, pp. 1–24, 2023.

[4]H. Zhang, L. Liang, P. Zeng, X. Song, and Z. Wang, "Sparselif: High- performance sparse lidar-camera fusion for 3d object detection," in European conference on computer vision. Springer, 2024, pp. 109– 128.

[5]D. R. George and S. Sciancalepore, "epptm-enhanced privacy-preserving trajectory matching on autonomous vehicles," IEEE Internet of Things Journal, 2025.

[6]G. Lippi, M. Aljawarneh, Q. Al-Na'amneh, R. Hazaymih, L. D. Dhomeja et al., "Security and privacy challenges and solutions in autonomous driving systems: A comprehensive review," Journal of Cyber Security and Risk Auditing, vol. 2025, no. 3, pp. 23–41, 2025.

[7]T. Bai, Q. Yang, and S. Fu, "User-defined privacy preserving data sharing for connected autonomous vehicles utilizing edge computing," in Proceedings of the Eighth ACM/IEEE Symposium on Edge Computing, 2023, pp. 145–157.

[8]N. U. Sehar, O. Khalid, I. A. Khan, F. Rehman, M. A. Fayyaz, A. R. Ansari, and R. Nawaz, "Blockchain enabled data security in vehicular networks," Scientific Reports, vol. 13, no. 1, p. 4412, 2023.

[9]B. Liu, C. Yan, C. Jiang, S. Banerjee, and A. Prabhakara, "Privacy- aware sharing of raw spatial sensor data for cooperative perception," in Proceedings of the 27th International Workshop on Mobile Computing Systems and Applications, 2026, pp. 43–48.

[10]K. H. K. Reddy, R. S. Goswami, and D. S. Roy, "A deep learning-based smart service model for context-aware intelligent transportation system: Khk reddy et al." The Journal of Supercomputing, vol. 80, no. 4, pp. 4477–4499, 2024.

[11]H. Shen, Y. Wang, and M. Zhang, "A privacy-preserving trajectory pub- lishing method based on multi-dimensional sub-trajectory similarities," Sensors, vol. 23, no. 24, p. 9652, 2023.

[12]X. Xu, S. Dong, T. Xu, L. Ding, J. Wang, P. Jiang, L. Song, and J. Li, "Fusionrcnn: Lidar-camera fusion for two-stage 3d object detection," Remote Sensing, vol. 15, no. 7, p. 1839, 2023.

[13]C. F. Akuma, P. Hewage, T. Bren, B. O. Nwozaku, and A. Eche, "Decentralized perception: A systematic review of federated learning for privacy-preserving detection of mixed road users in intelligent transportation systems (its)," International Journal of Development Mathematics (IJDM), vol. 2, no. 4, pp. 179–199, 2025.

[14]K. Sundarakantham, E. Sivasankar, S. Mercy Shalinie et al., "A hybrid deep learning framework for privacy preservation in edge computing," Computers & Security, vol. 129, p. 103209, 2023.

[15]R. Bi, J. Xiong, X. Yang, Y. Zhang, Z. Ruan, J. Tian, and X. Yi, "Privacy- preserving multi-modal object fusion for connected autonomous vehi- cles: Resilience against malicious third-party attacks," IEEE Transac- tions on Information Forensics and Security, vol. 21, pp. 3543–3558, 2026.

[16]H. A. Tahir, W. Alayed, and W. U. Hassan, "Privacy-preserving fed- erated learning with adaptive model aggregation for efficient vehicle- to-vehicle (v2v) communication in intelligent transportation systems," IEEE Access, 2025.

[17]T. Alam, "Data privacy and security in autonomous connected vehicles in smart city environment," Big Data and Cognitive Computing, vol. 8, no. 9, p. 95, 2024.

[18] V. P. Chellapandi, L. Yuan, C. G. Brinton, S. H. Ż ak, and Z. Wang, "Federated learning for connected and automated vehicles: A survey of existing approaches and challenges," IEEE Transactions on Intelligent Vehicles, vol. 9, no. 1, pp. 119–137, 2023.

[19]K. Wei, J. Li, C. Ma, M. Ding, W. Chen, J. Wu, M. Tao, and H. V. Poor, "Personalized federated learning with differential privacy and convergence guarantee," IEEE Transactions on Information Forensics and Security, vol. 18, pp. 4488–4503, 2023.

[20]F. Wen, Z. Wang, L. Qu, H. Huang, and X. Hu, "Enhancing secure multi- group data sharing through integration of ipfs and hyperledger fabric," PeerJ Computer Science, vol. 10, p. e1962, 2024.

[21]S. Mohammadi, A. Balador, S. Sinaei, and F. Flammini, "Balancing privacy and performance in federated learning: A systematic literature review on methods and metrics," Journal of Parallel and Distributed Computing, vol. 192, p. 104918, 2024.

[22]M. Song and M. Zhu, "Automotive manufacturers: Competitive land- scape and sustainable development strategies," in The Green Path of Chinese Transportation Enterprises. Springer, 2026, pp. 235–252.

[23]J. Alotaibi, "Secure and federated vision-based parking management using a hybrid deep learning and privacy-preserving framework for smart cities," Computing, vol. 108, no. 1, p. 12, 2026.

[24]Y. Lin and Q. Zhong, "Explainable and privacy-aware collaborative optimization for efficient and robust iiot clusters," Internet Technology Letters, vol. 9, no. 3, p. e70263, 2026.

[25]A. D. M. Ibrahum, M. Hussain, and J.-E. Hong, "Deep learning adversar- ial attacks and defenses in autonomous vehicles: a systematic literature review from a safety perspective," Artificial Intelligence Review, vol. 58, no. 1, p. 28, 2024.

[26]A. Banerjee, A. Maity, I. Lamrani, and S. K. Gupta, "Towards certified safe personalization in learning-enabled human-in-the-loop human-in- the-plant systems," ACM Journal on Emerging Technologies in Com- puting Systems, vol. 22, no. 1, pp. 1–27, 2025.

[27]W. Xu, S. Yang, F. Li, L. Zhu, K. Zhu, X. Chen, and Y. Wang, "Parachute: Dynamic resource-aware privacy-preserving video analytics on edge," IEEE Internet of Things Journal, 2025.

[28]X. Hui, Q. Wu, H. Qu, M. Mirmehdi, H. Rahmani, and J. Liu, "When visual privacy protection meets multimodal large language models," International Journal of Computer Vision, vol. 134, no. 4, p. 167, 2026.

[29]M. Hadded, "Centralized, federated, and privacy-preserving learning for collision risk prediction in v2x-enabled autonomous vehicles," in AINA, 2026.

[30]S. Hu, Z. Fang, Y. Deng, X. Chen, and Y. Fang, "Collaborative perception for connected and autonomous driving: Challenges, possible solutions and opportunities," IEEE Wireless Communications, 2025.

[31]A. Amirkhani, M. P. Karimi, and A. Banitalebi-Dehkordi, "A survey on adversarial attacks and defenses for object detection and their applications in autonomous vehicles," The Visual Computer, vol. 39, no. 11, pp. 5293–5307, 2023.

[32]A. Mohammed, "Cybersecurity in autonomous vehicles: Addressing risks in self-driving technology," Authorea Preprints, 2025.

[33]A. Karni, Q. Abbas, J. Ahmad, and A. K. J. Saudagar, "Skin cancer classification using novel fairness based federated learning algorithm," PeerJ Computer Science, vol. 11, p. e3171, 2025.

[34]L. Chi, M. Msahli, Q. Zhang, H. Qiu, T. Zhang, G. Memmi, and M. Qiu, "Adversarial attacks on autonomous driving systems in the physical world: a survey," IEEE Transactions on Intelligent Vehicles, 2024.

[35]F. Znidi, M. Morsy, and H. Rathore, "Future on wheels: Safeguard- ing privacy in tomorrow's connected vehicles-future-sp," IEEE Access, vol. 12, pp. 179 857–179 878, 2024.

[36]J. Wei and W. Li, "Challenges and countermeasures for ai ethics and privacy protection in autonomous ride-hailing platforms," Al lnnovations and Applications, vol. 2, no. 1, pp. 1–13, 2026.

[37]Z. Sarayloo, S. Lohrasbi, P. Xiong, and N. L. Azad, "A systematic review of adversarial attacks and defenses for deep reinforcement learning in autonomous vehicle applications," IEEE Transactions on Intelligent Transportation Systems, 2026.

[38]M. W. Ahmed, M. Adnan, M. Ahmed, D. Janssens, G. Wets, A. Ahmed, and W. Ectors, "Near real-time privacy protection: automated location- dependent video blurring in uav live-streams," Transportation Research Procedia, vol. 84, pp. 201–208, 2025.

[39]L. Bai, J. Cao, M. Zhang, and B. Li, "Collaborative edge intelligence for autonomous vehicles: Opportunities and challenges," IEEE Network, vol. 39, no. 2, pp. 52–60, 2025.

[40]A. Azad, "Federated learning for autonomous vehicles: Privacy- preserving edge ai," 2025.

[41]M. De Vincenzi, J. Moore, B. Smith, S. E. Sarma, and I. Matteucci, "Se- curity risks and designs in the connected vehicle ecosystem: In-vehicle and edge platforms," IEEE Open Journal of Vehicular Technology, vol. 6, pp. 442–454, 2024.

[42]A. T. Abiko, S. Chauhan, and A. Vasilakos, "Gensecure-caev: A gen- erative ai framework for proactive vulnerability discovery in connected autonomous electric vehicles," Future Generation Computer Systems, p. 108445, 2026.

[43]L. Campanile, M. Iacono, M. Mastroianni, and B. Viscardi, "Estimating performance costs of enabling privacy-awareness in data lifecycles," in International Conference on Modeling, Simulation and Computer Technology. Springer, 2024, pp. 184–195.

[44]D. Lee et al., "Privacy challenges of automated vehicles: Merging con- textual integrity and responsible innovation frameworks," Transportation Research Interdisciplinary Perspectives, vol. 32, p. 101536, 2025.

[45]Y. Xu, J. Wei, T. Mi, and Z. Chen, "Data security in autonomous driving: Multifaceted challenges of technology, law, and social ethics," World Electric Vehicle Journal, vol. 16, no. 1, p. 6, 2024.

[46]S. C. S. Pirbhulal and H. Abie, "Improving security and privacy of cognitive digital twins through dynamic consent," in HCI International 2025–Late Breaking Papers: 27th International Conference on Human- Computer Interaction, HCII 2025, Gothenburg, Sweden, June 22–27, 2025, Proceedings, Part VII. Springer Nature, 2026, p. 293.

[47]T. Bai, D. Shao, Y. He, Q. Yang, Y. Feng, and S. Fu, "Privacy-preserving driver monitoring on the edges: Transformer-based processing of secret shares from video streams," ACM Transactions on Internet of Things, vol. 7, no. 3, pp. 1–30, 2026.

[48]P. Constantinides, E. Monteiro, and L. Mathiassen, "Human-ai joint task performance: Learning from uncertainty in autonomous driving systems," Information and Organization, vol. 34, no. 2, p. 100502, 2024.

[49]Z. Lipeng, C. Minghan, W. Jiantao, L. Xiaohao, and Z. Yan, "Integrated design and parameter optimization of multi-mode coupling all-wheel drive system for plug-in hybrid electric vehicles," International Journal of Automotive Technology, pp. 1–19, 2026.

[50]S. Tekkesinoglu, A. Habibovic, and L. Kunze, "Advancing explainable autonomous vehicle systems: A comprehensive review and research roadmap," ACM Transactions on Human-Robot Interaction, vol. 14, no. 3, pp. 1–46, 2025.

[51]S. L. Burton, "Designing trustworthy futures: Research priorities for human-centered, connected, and autonomous mobility," 2026.

[52]A. Heidari, S. H. Rastegar, and A. Khonsari, "Artificial intelligence- driven privacy preservation in the internet of

vehicles: a comprehensive systematic literature review," Journal of Big Data, 2026.

[53]R. de Silva, B. D. Mach, V. Moghaddam, and A. Zaslavsky, "Adap- tive privacy-security orchestration framework in distributed contextual intelligence systems for iot," in Proceedings of the 2026 Australasian Information Security Conference, 2026, pp. 30–37.

[54]M. A. Almekhlafi, F. Alrowais, S. Alshahrani, M. Maray, M. A. AlAqil,

M. A. Alharbi, A. E. Yahya, and R. Marzouk, "Amta: An innova- tive privacy-aware adaptive transformer for real-time multimodal data fusion," Transactions on Emerging Telecommunications Technologies, vol. 37, no. 3, p. e70365, 2026.

[55]I. Croitoru, C. E. Turcu, and C. O. Turcu, "Privacy-by-design in ai- assisted systems for caregivers of children with autism: A secure multi- agent architecture," Applied Sciences, vol. 16, no. 4, p. 2157, 2026.

[56]R. Joshi, "Data-centric ai: Engineering platforms for pre-model intelli- gence," Journal Of Multidisciplinary, vol. 5, no. 6, pp. 48–54, 2025.

[57]Y. Liu, S. Liu, X. Zhu, H. Yang, J. Li, J. Guo, L. Teng, D. Yang,

Y. Wang, and J. Liu, "Privacy-preserving video anomaly detection: A survey," IEEE Transactions on Neural Networks and Learning Systems, 2025.

[58]A.-R. O. Ottun and H. Flores, "Trustworthy ai in practice: A compre- hensive review of human oversight and human-in-the-loop approaches," Authorea Preprints, 2025.

[59]D. Ferna´ndez Llorca, R. Hamon, H. Junklewitz, K. Grosse, L. Kunze,

P. Seiniger, R. Swaim, N. Reed, A. Alahi, E. Go´mez et al., "Testing autonomous vehicles and ai: perspectives and challenges from cyber- security, transparency, robustness and fairness," European Transport Research Review, vol. 17, no. 1, p. 38, 2025.

[60]T. B. Achenef, S. N. Abera, Y. A. Admas, and S. Z. Tegegne, "Latest breakthroughs, research results, and challenges in intelligent control of autonomous vehicles," Proceedings of the Institution of Mechanical Engineers, Part D: Journal of Automobile Engineering, vol. 240, no. 4, pp. 1564–1591, 2026.