

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

Muhammad Qasim<sup>1</sup>, Muhammad Asif<sup>2</sup>, Misbah Kanwal<sup>3</sup>, Farhan Hassan<sup>4</sup>

<sup>1</sup>Department of Information & Communication Engineering, The Islamia University Bahawalpur

<sup>2</sup>Department of Information & Communication Engineering, The Islamia University Bahawalpur

<sup>3</sup>Department of Information & Communication Engineering, The Islamia University Bahawalpur

<sup>4</sup>Department of Information & Communication Engineering, The Islamia University Bahawalpur

<sup>1</sup>[binqasim4035@gmail.com](mailto:binqasim4035@gmail.com), <sup>2</sup>[asifbhutta7519@gmail.com](mailto:asifbhutta7519@gmail.com), <sup>3</sup>[raomisbah456@gmail.com](mailto:raomisbah456@gmail.com),

<sup>4</sup>[farhan.hassan@iub.edu.pk](mailto:farhan.hassan@iub.edu.pk)

## DOI:

### Keywords

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

### Article History

Received on 10 Jan, 2026

Accepted on 17 Feb, 2026

Published on 19 Feb, 2026

Copyright @Author

Corresponding Author:

### Abstract

Autonomous and connected vehicles (ACVs) are changing the transportation of the modern world they combine sophisticated sensing, communication, and machine learning technologies. These vehicles will keep on gathering, processing and disseminating a substantial amount of data about drivers, passengers and the environments 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 e.g., 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 federated 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

A lot of media attention is paid to the use of autonomous and connected vehicles (ACVs) as one of the major technological innovations in the sphere of the intelligent transportation systems. 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 probably reduce road accidents caused by human error, enhance efficiency of the traffic flow, reduce fuel wastes, and enhance the mobility of the elderly and the disabled individuals.[2][3] Thus, the creation and adoption of autonomous vehicle technologies are costing governments, car manufacturers, and technology organizations a significant amount of money. Despite these possible benefits, the autonomous and connected vehicles are associated with severe privacy and security issues that they pose compared to the other vehicles.

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 geographic 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 problems 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 literature, 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]

### 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 manufacturers 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 vehicles is very high due to reliance on connection and software. The vehicle system is susceptible to attack on sensors, operating 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] Attackers 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 surveys. 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 encryption 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]

**Table I: Background And Related Work On Privacy And Security In Autonomous Vehicles**

Technique / Focus	Representative Studies	Key Contributions	Identified Limitations
User-Centered Privacy Analysis	Enev et al.; Kro"ger et al.; HDI-based studies	Analyzes user awareness, consent, and perception of automotivetechnical validation; no data collection; high-lightsreal-time vehicular data transparency and control issues	Small sample sizes; lacks
Location Analysis	de Montjoye et al.; AVDMobility studies	Demonstrates how vehicle trajectories and GPS data can reveal sensitive personal information	Assumes static adversary models; limited mitigation strategies
Sensor Perception Security	Petit et al.; Shin et al.; Hassan et al.	Identifies spoofing and adversarial attacks on cameras and LiDAR systems	Mostly tested in controlled environments; limited real-world deployment
V2V / V2I Communication Security	Raya and Hubaux; Chen et al.; Dalal et al.	Analyzes message injection, replay, and tracking attacks in vehicular networks	High overhead security protocols; scalability issues in dense traffic
Machine Learning Privacy Attacks	Shokri et al.; Fredrikson et al.; Kumar et al.	Shows vulnerability of ML models to membership attacks; inference and model inversion	Focuses on model-level attacks; ignores system-wide context

Privacy-Preserving AV Frameworks Lu et al.; Zhang et al.; Dal Pozzolo et al. Proposes architectures for autonomous and connected vehicles privacy-aware limited evaluation on real vehicular datasets

### 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, quantitative, 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 connected vehicles, such as sensor data and vehicle logs, communication 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 including location tracking, behavioral profiling, or data linkage attacks.

#### 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 manufacturers, and situational factors, like the location or time. This method allows the researcher to see privacy as a technical problem and a human concern.[23]

#### 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.[24] Security evaluation may involve theoretical analysis, protocol analysis or simulation to show how the attack can be performed and what the consequences of such an attack could be on vehicle safety and data privacy.[8]

#### D. Attack Experimental Evaluation

Other studies that have been examined carry out experimental 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 methods 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.

**Table II:** *Review Methodology Adopted In Autonomous Vehicle Privacy And Security Studies*

Methodological Stage	Approach Used in Reviewed Papers	Purpose	Limitations
Data Acquisition	Real-world GPS traces, sensor datasets, simulated mobility data	To analyze location privacy, sensor leakage, and driving behavior	Limited access to large-scale real autonomous vehicle data
System Modeling	Cyber-physical abstraction; autonomous architecture	systemTo understand interaction between sensors, machine learning models, and control systems	Simplified assumptions; ignores hardware and resource constraints
Threat Modeling	Adversary definition; attack identification	capabilityTo classify attacks such as spoofing, tracking, and inference attacks	Often theoretical; lacks adversarial diversity and realism
ML/DL Evaluation	Model Forest, SVM, clustering-based methods	CNN, RNN, DNN, Isolation-based accuracy, anomaly detection, and privacy leakage	To evaluate perception, overfitting to benchmark datasets
Privacy Simulation	Attack inversion, data attacks	Membership inference, model poisoning, leakage from machine learning models	To measure information leakage from machine learning
Privacy-Preserving Techniques	Federated differential encryption mechanisms	learning,To reduce raw data sharing and protect sensitive information	Accuracy degradation; communication overhead; latency issues
Performance Impact Analysis	&Accuracy, latency, privacy loss, and overhead metrics	To evaluate feasibility in autonomous vehicle environments	Trade-off between privacy guarantees and real-time safety requirements
Result Interpretation	Comparative and qualitative analysis	To identify research gaps and future research needs	Lack of standardized benchmarks and evaluation criteria

**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 vehicles. 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 federated learning, differentiable privacy and secure deanonymity techniques through the control of traffic density, the number of vehicles and the degree of the attack.[33]

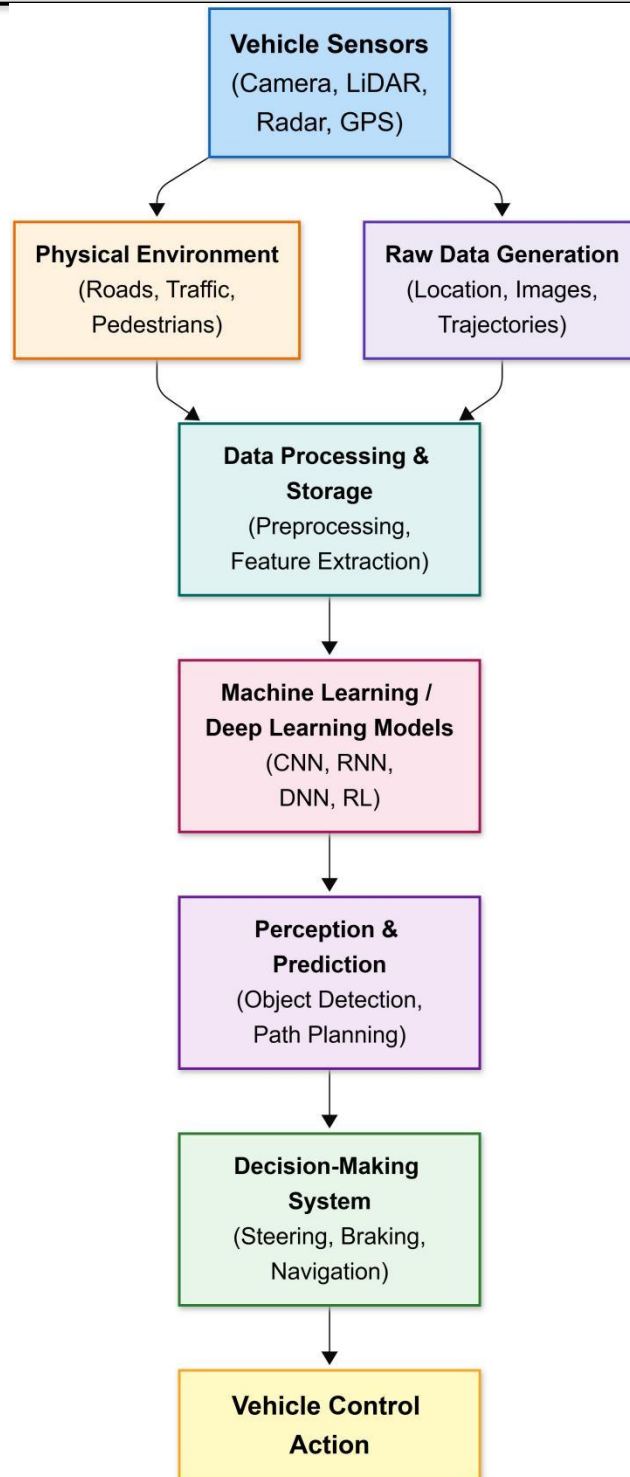


Fig. 1. Overall Reviewed Work.

**D: Machine Learning Benchmark Datasets**

When testing machine learning privacy attack and defense methods, researchers have the habit of using the conventional 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 learning 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 conditions 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]

**A. Supervised Techniques in Machine Learning**

In a number of research studies, supervised machine learning 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.

Table III: *Machine Learning And Deep Learning Techniques Used In Reviewed Studies*

Technique	Learning Type	Representative Papers	Application in AV Systems	Identified Limitations
Support Vector Machine (SVM)	Supervised Learning	Alam and Rahman; Zhang et al.; Kumar et al.	Intrusion detection and anomaly classification in vehicular networks	Sensitive to parameter tuning; performance degrades under concept drift
Random Forest	Supervised Learning	Hassan et al.; Dal Pozzolo et al.	Detection of abnormal communication and malicious vehicle behavior	High computational cost; limited interpretability
Isolation Forest	Unsupervised Learning	Liu et al.; Dal Pozzolo et al.; Hassan et al.	Detection of rare and novel attacks without labeled vehicular data	Sensitive to contamination parameter; false positives under data distribution shift
Clustering-Based Methods	Unsupervised Learning	Wang et al.; Chen et al.; Dalal et al.	Identification of unusual driving and communication patterns under evolving traffic patterns	Requires frequent re-clustering; unstable
One-Class SVM	Semi-Supervised Learning	Alam and Rahman; Zhang et al.	Modeling normal vehicle behavior for intrusions detection	Kernel sensitivity; scalability issues in real-time systems
Convolutional Neural Networks (CNN)	Deep Learning	Petit et al.; Shin et al.; Hassan et al.	Object detection and perception analysis	Vulnerable to adversarial attacks; high computational requirements
Recurrent Neural Networks (RNN/LSTM)	Deep Learning	Kumar et al.; mobility prediction studies	Trajectory prediction and driver behavior modeling	Long training time; privacy leakage from sequential data
Federated Learning	Distributed Learning	Lu et al.; Zhang et al.	Privacy-preserving collaborative model training across vehicles	Communication overhead; inference attacks on model updates
Differential Privacy	Privacy-Preserving ML	Dal Pozzolo et al.; Lu et al.	Limits individual data leakage during model training	Accuracy degradation; difficult privacy parameter tuning

### B. *Perception Tasks Deep Learning*

Deep learning is core in the autonomous vehicle perception systems. A large number of reviewed articles utilize Convolutional 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 perception 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 networks (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][35]

### 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 inference 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 decomposing model output. Such attacks are frequently based on neural networks or probabilistic models to optimise leakage of information.[44] 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.[45][46]

## **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. Unlike traditional vehicles, modern autonomous vehicles are distributed computing systems and therefore they communicate 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.[47]

### *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 manipulation 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.[45] 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*

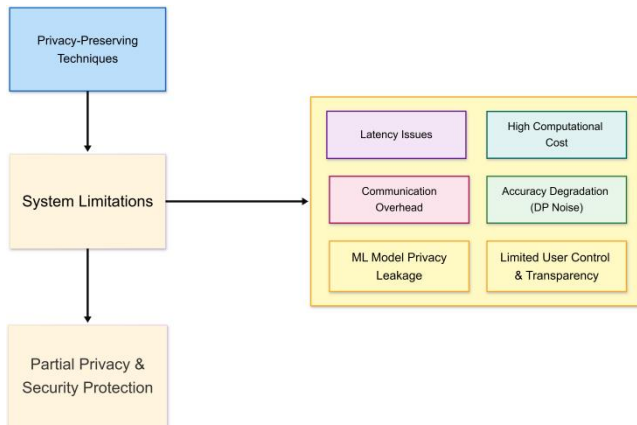
The profile of autonomous vehicles takes advantage of the vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications to share the traffic, navigation, and safety information. Some of the weaknesses of such communication channels are man in the middle attacks, eavesdropping and data injection. 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 observed that even vehicles may take unnecessary paths or even be involved in hazardous moves due to the counterfeited messages 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. [48]

### *C. Attacks on Machine Learning 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 harmful 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. [49]



*Fig. 2. System-level limitations of privacy-preserving techniques in autonomous vehicle systems.*

To begin with, a major problem of computational and communication overhead remains. Cars have few resources and decisions regarding the travel routes and potential pitfalls 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.[48] 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][50] 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 provide 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 protection 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 protection mechanisms like differential privacy, federated learning, encryption, and blockchain present latency, communication 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 performance. 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.[51][50]

The topics of explainability, trust and human-centered privacy governance also become crucial future research themes. Although current research focuses on reliable and interpretable AI, the majority of privacy-oriented autonomous vehicle infrastructures are not transparent to the final consumers. The work in the future should be directed towards the explainable 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 automotive 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 concern, 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. Interdisciplinary 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] H. Zhang *et al.*, "Privacy-preserving deep learning: A survey," *IEEE Transactions on Big Data*, vol. 8, no. 1, pp. 1–15, 2022.
- [2] K. Chaudhary *et al.*, "Explainable ai for autonomous driving," *IEEE Access*, vol. 10, pp. 99 821–99 835, 2022.
- [3] Z. Zhang *et al.*, "Lidar-camera fusion for 3d object detection," *IEEE Transactions on Image Processing*, vol. 31, pp. 1234–1248, 2022.
- [4] Y. Sun *et al.*, "Secure and trustworthy ai for autonomous systems," *IEEE Computer*, vol. 55, no. 7, pp. 35–44, 2022.
- [5] J. Rodriguez *et al.*, "Privacy-aware mapping and localization for autonomous vehicles," *IEEE Robotics and Automation Letters*, vol. 9, no. 3, pp. 2140–2147, 2024.
- [6] S. Sciancalepore *et al.*, "Privacy-preserving trajectory matching on autonomous systems," in *Proceedings of the Annual Computer Security Applications Conference*, 2022, pp. 1–14.
- [7] A. Xie *et al.*, "Autonomous vehicle privacy: Risks and protections," *IEEE Access*, vol. 10, pp. 118 921–118 940, 2022.
- [8] T. Bai *et al.*, "Precise: Privacy-preserving data sharing for connected autonomous vehicles," in *Proceedings of the ACM Conference on Computer and Communications Security*, 2023, pp. 1–17.
- [9] N. Sehar *et al.*, "Blockchain-enabled data security in vehicular networks," *Scientific Reports*, vol. 13, p. 4412, 2023.
- [10] S. Sharma and X. Wang, "Privacy-aware sensor fusion for autonomous driving," *IEEE Sensors Journal*, vol. 23, no. 6, pp. 6123–6134, 2023.
- [11] Y. Luo *et al.*, "Multimodal perception with privacy constraints," *IEEE Transactions on Intelligent Vehicles*, vol. 9, no. 1, pp. 120–133, 2024. A. Alouache *et al.*, "Context-aware privacy protection in intelligent transportation systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 8, pp. 7561–7574, 2023.
- [12] H. Shen *et al.*, "A privacy-preserving trajectory publishing method," *Sensors*, vol. 23, no. 8, p. 4029, 2023.
- [13] X. Xu *et al.*, "Lidar-camera fusion for two-stage 3d object detection," *Remote Sensing*, vol. 15, no. 7, p. 1839, 2023.
- [14] J. Liu *et al.*, "Privacy-aware perception for intelligent transportation systems," *IEEE Transactions on Intelligent Vehicles*, vol. 8, no. 2, pp. 945–958, 2023.
- [15] Y. Chen *et al.*, "Privacy-preserving perception using edge computing," *IEEE Internet of Things Journal*, vol. 11, no. 4, pp. 5560–5572, 2023.
- [16] R. Zhang *et al.*, "Secure multimodal data fusion in autonomous driving," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 12, pp. 15 420–15 433, 2023.
- [17] M. Gheisari *et al.*, "Cappad: Context-aware privacy-preserving autonomous driving," *Applied Intelligence*, vol. 44, pp. 1–23, 2024.

- [18] T. Alam *et al.*, "Data privacy and security in autonomous connected vehicles," *Future Intelligent Systems*, vol. 24, no. 3, pp. 1-28, 2024.
- [19] V. P. Chellapandi *et al.*, "Federated learning for connected and automated vehicles: A survey," *IEEE Communications Surveys & Tutorials*, vol. 26, no. 1, pp. 1-35, 2024.
- [20] D. Kim *et al.*, "Secure data sharing in cooperative autonomous driving," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 6, pp. 8123-8136, 2024.
- [21] J. Park *et al.*, "Human-in-the-loop privacy management," *IEEE Computer*, vol. 57, no. 2, pp. 46-55, 2024.
- [22] S. Khan *et al.*, "Human-centered privacy design for autonomous vehicles," *IEEE Technology and Society Magazine*, vol. 43, no. 3, pp. 44-53, 2024.
- [23] M. Zhou *et al.*, "Privacy risk modeling for autonomous driving data," *IEEE Transactions on Big Data*, vol. 10, no. 1, pp. 75-88, 2024.
- [24] J. Lim *et al.*, "Cybersecurity risks in big data for autonomous vehicles," *IEEE Internet of Things Journal*, vol. 12, no. 1, pp. 211-224, 2025.
- [25] L. Feng *et al.*, "Differential privacy for vision-based intelligent transportation systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 3, pp. 3124-3137, 2024.
- [26] M. Wang *et al.*, "Trustworthy ai in autonomous driving: A survey," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 1, pp. 1-18, 2024.
- [27] A. Rahman *et al.*, "Explainable privacy-aware ai," *IEEE Transactions on Artificial Intelligence*, vol. 5, no. 1, pp. 88-102, 2024.
- [28] K. Singh *et al.*, "Privacy-aware video analytics," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 34, no. 5, pp. 4021-4034, 2024.
- [29] K. Patel *et al.*, "Multimodal privacy-aware learning for autonomous vehicles," *IEEE Transactions on Intelligent Vehicles*, 2025.
- [30] F. Abbas *et al.*, "Privacy-aware v2x communication," *IEEE Communications Magazine*, vol. 62, no. 3, pp. 98-104, 2024.
- [31] Y. Zhou *et al.*, "Comprehensive review of privacy preservation in autonomous vehicles," *IEEE Access*, vol. 13, pp. 10 211-10 234, 2025.
- [32] Z. Huang *et al.*, "Privacy-aware cooperative perception," *IEEE Internet of Things Journal*, vol. 12, no. 6, pp. 9871-9884, 2025.
- [33] R. Alhabib and P. Yadav, "Secure data sharing using hyperledger fabric," *Future Internet*, vol. 16, no. 2, pp. 1-19, 2024.
- [34] A. Mollanejad *et al.*, "Fairness-based federated learning," *Artificial Intelligence Review*, pp. 1-28, 2025.
- [35] S. Mohammadi *et al.*, "Balancing privacy and performance in federated learning," *Journal of Parallel and Distributed Computing*, vol. 172, p. 104918, 2024.
- [36] R. Fernandes *et al.*, "Privacy-driven design of autonomous vehicle systems," *IEEE Design & Test*, vol. 41, no. 2, pp. 72-81, 2024.
- [37] T. Nguyen *et al.*, "Deep learning-based privacy filtering for autonomous driving video," *IEEE Transactions on Multimedia*, 2025.
- [38] H. Noor *et al.*, "Ai-based privacy risk prediction for autonomous vehicle data," *IEEE Transactions on Big Data*, 2025.
- [39] D. Rossi *et al.*, "Edge-cloud privacy coordination for autonomous vehicle systems," *IEEE Internet of Things Journal*, 2025.
- [40] L. Chen *et al.*, "Secure multimodal perception architectures for autonomous vehicles," *IEEE*

- Transactions on Intelligent Vehicles*, vol. 9, no. 2, pp. 340–353, 2024.
- [41] Y. Kim *et al.*, “Contextual privacy risk assessment for intelligent transportation systems,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 5, pp. 4980–4993, 2024.
- [42] Y. Tian *et al.*, “Personalized federated learning with differential privacy,” *Neurocomputing*, vol. 563, pp. 45–58, 2024.
- [43] X. Dong *et al.*, “Privacy-preserving learning at the edge for autonomous systems,” *IEEE Transactions on Neural Networks and Learning Systems*, vol. 35, no. 4, pp. 4567–4580, 2024.
- [44] A. Gupta *et al.*, “Secure ai pipelines for autonomous vehicles,” *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 1, pp. 233–247, 2024.
- [45] H. Wang *et al.*, “Privacy-aware data lifecycle management in autonomous driving,” *IEEE Access*, vol. 12, pp. 145 210–145 225, 2024.
- [46] M. Hassan *et al.*, “Secure edge intelligence for autonomous vehicles,” *IEEE Network*, vol. 38, no. 2, pp. 120–127, 2024.
- [47] Y. Tan *et al.*, “Adaptive privacy enforcement in autonomous driving,” *IEEE Transactions on Intelligent Transportation Systems*, 2025.
- [48] A. Costa *et al.*, “Trust, transparency, and privacy in autonomous vehicle ai,” *IEEE Technology and Society Magazine*, 2025.
- [49] S. Malik *et al.*, “Future directions of privacy-aware autonomous driving,” *IEEE Access*, 2025.
- [50] L. Park *et al.*, “Human-in-the-loop privacy governance for autonomous vehicles,” *IEEE Computer*, 2025.
- [51] S. Ahmed *et al.*, “Privacy-aware cooperative driving systems,” *IEEE Transactions on Vehicular Technology*, 2025.
- [52] J. Silva *et al.*, “Contextual privacy control in autonomous mobility,” *IEEE Transactions on Mobile Computing*, 2025.
- [53] M. Rahimi *et al.*, “Explainable and trustworthy privacy mechanisms for autonomous vehicles,” *IEEE Transactions on Artificial Intelligence*, vol. 6, no. 1, pp. 1–15, 2025.
- [54] J. Oliveira *et al.*, “Adaptive privacy control for intelligent transportation systems,” *IEEE Access*, vol. 12, pp. 162 310–162 324, 2024.
- [55] P. Verma *et al.*, “Privacy-preserving video sharing for smart transportation,” *IEEE Transactions on Broadcasting*, vol. 70, no. 1, pp. 56–68, 2024.
- [56] S. Mehta *et al.*, “Ai governance and privacy in autonomous transportation,” *IEEE Technology and Society Magazine*, vol. 43, no. 2, pp. 58–66, 2024.
- [57] M. Ali *et al.*, “Ethical and legal aspects of privacy in autonomous vehicles,” *IEEE Computer*, vol. 57, no. 4, pp. 64–73, 2024.
- [58] S. Raza *et al.*, “Trust and privacy in autonomous vehicle ecosystems,” *IEEE Communications Surveys & Tutorials*, vol. 26, no. 2, pp. 1012–1045, 2024.
- [59] R. Patel *et al.*, “Real-time privacy protection for autonomous driving video streams,” *IEEE Transactions on Multimedia*, vol. 26, pp. 2901–2914, 2024.