technologies

Review

Connected and Automated Vehicles: Infrastructure, Applications, Security, Critical Challenges, and Future Aspects

Memoona Sadaf [1], Zafar Iqbal [1], Abdul Rehman Javed [1,2,*], Irum Saba [3], Moez Krichen [4,5,*], Sajid Majeed [1] and Arooj Raza [1]

[1] Department of Cyber Security, Air University, Islamabad 44000, Pakistan; 220380@students.au.edu.pk (S.M.); 222488@students.au.edu.pk (A.R.)
[2] Department of Electrical and Computer Engineering, Lebanese American University, Byblos 36/S-12, Lebanon
[3] Department of Electrical Engineering, National University of Computer & Emerging Sciences, Islamabad 44000, Pakistan
[4] Faculty of Computer Science and Information Technology, Al-Baha University, Al-Baha 65528, Saudi Arabia
[5] ReDCAD Laboratory, National School of Engineers of Sfax, University of Sfax, Sfax 3029, Tunisia
* Correspondence: abdulrehman.cs@au.edu.pk (A.R.J.); prof.moez.krichen@gmail.com (M.K.)

Abstract: Autonomous vehicles (AV) are game-changing innovations that promise a safer, more convenient, and environmentally friendly mode of transportation than traditional vehicles. Therefore, understanding AV technologies and their impact on society is critical as we continue this revolutionary journey. Generally, there needs to be a detailed study available to assist a researcher in understanding AV and its challenges. This research presents a comprehensive survey encompassing various aspects of AVs, such as public adoption, driverless city planning, traffic management, environmental impact, public health, social implications, international standards, safety, and security. Furthermore, it presents emerging technologies such as artificial intelligence (AI), integration of cloud computing, and solar power usage in automated vehicles. It also presents forensics approaches, tools used, standards involved, and challenges associated with conducting digital forensics in the context of autonomous vehicles. Moreover, this research provides an overview of cyber attacks affecting autonomous vehicles, attack management, traditional security devices, threat modeling, authentication schemes, over-the-air updates, zero-trust architectures, data privacy, and the corresponding defensive strategies to mitigate such risks. It also presents international standards, guidelines, and best practices for AVs. Finally, it outlines the future directions of AVs and the challenges that must be addressed to achieve widespread adoption.

Keywords: survey; autonomous vehicles; vehicular technology; security; challenges; sensors; artificial intelligence; federated learning; deep learning; machine learning; cloud computing; protocols; in-vehicle systems; communication networks; cyber security risks; smart cities; automotive industry

Citation: Sadaf, M.; Iqbal, Z.; Javed, A.R.; Saba, I.; Krichen, M.; Majeed, S.; Raza, A. Connected and Automated Vehicles: Infrastructure, Applications, Security, Critical Challenges, and Future Aspects. *Technologies* **2023**, *11*, 117. https://doi.org/10.3390/technologies11050117

Academic Editor: George F. Fragulis

Received: 5 August 2023
Revised: 26 August 2023
Accepted: 29 August 2023
Published: 4 September 2023

1. Introduction

An autonomous vehicle is a self-driving vehicle that can operate independently without human intervention [1]. According to a report by Allied Market Research, the global autonomous vehicle market size was valued at $54.23 billion in 2019 and is projected to reach $556.67 billion by 2026, with a Compound Annual Growth Rate (CAGR) of 39.47% from 2019 to 2026 [2]. Fifty-seven percent of the global population are familiar with self-driving cars and willing to ride inside them [3]. Currently, the market of autonomous vehicles sits at $54 billion. By 2023, Audi, the German brand, plans on spending $16 billion. According to a report, there will be 33 million AVs in use by 2040 [4]. All over the world, approximately 80 companies are currently testing more than 1400 self-driving vehicles [5].

The development and deployment of autonomous vehicles (AVs) have captured the attention of researchers, policymakers, and the public alike. AVs promise to transform how

we travel and interact with the world. Their advanced sensors, machine-learning algorithms, and sophisticated control systems offer a safer, more efficient, and more convenient mode of transportation than traditional vehicles. AVs are expected to profoundly impact society, with potential benefits including enhanced safety, increased efficiency, reduced traffic congestion, and improved mobility. Driver automation provides only one automatic feature. For instance, with the help of cruise control, speed is monitored. In partial automation, the vehicle has the feature of steering and acceleration. Conditional automation can detect the environment, and all tasks are performed automatically, but still, human efforts are required. In high automation, human efforts are optional but are preferable. In high automation, zero human intervention is required [6,7].

Since the 1920s, when the radio-based vehicle-to-vehicle (V2V) communication system was developed, researchers have been interested in automated cars. Later, in the 1930s and 1940s, electromagnetic vehicle guidance was developed, and in the 1950s and 1960s, magnets were added to vehicles to test smart motorways [8]. Autonomous vehicles can view the world in a 360° range, thanks to high-precision technology, which is twice as much as humans, who can only see 180° horizontally [4]. Vehicle-to-Everything (V2X) communication is an essential technology for enabling the full potential of autonomous vehicles. It enables communication between vehicles and other road users, including pedestrians, bicyclists, and infrastructure, such as traffic signals and road signs. V2X technology allows AVs to exchange data with other vehicles and infrastructure in real-time, improving safety, efficiency, and environmental impact, as shown in Figure 1.

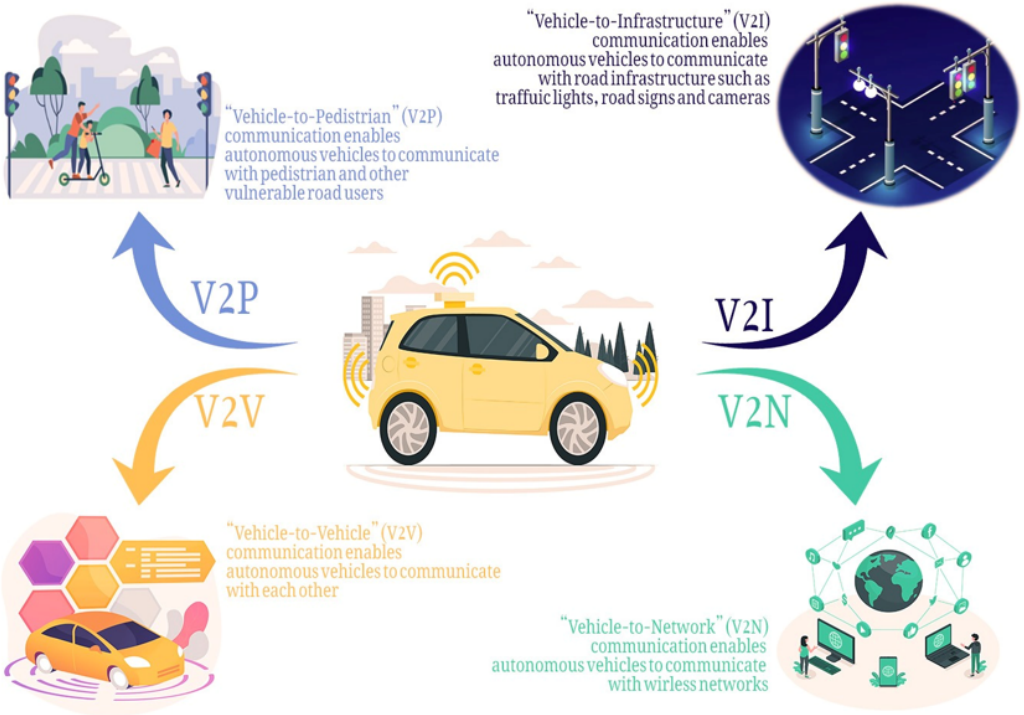

Figure 1. AVs Communication Scenarios.

Due to the autonomous nature of the vehicle and the fact that it would function with little to no human input, even those with visual or hearing impairments can own one, making them inclusive. The first issue is because of constant connectivity with the outside world; data protection might develop into a cyber issue. Autonomous driving has advanced gradually and is becoming more sophisticated in perceiving environments in everyday life properly and quickly analyzing sensor information; thanks to the growth of the Internet of Things and artificial intelligence technologies, it can now make complex decisions by itself.

1.1. Motivation

The rapid advancement of AV technology has generated significant interest from both the public and private sectors. The potential benefits of AVs are vast, ranging from enhanced safety to increased mobility and efficiency. However, significant challenges must be addressed before AVs can fully integrate into society. These challenges include technical issues such as cybersecurity, machine-learning algorithms, cloud employment, and legal and ethical concerns regarding liability and data privacy. In addition, AVs can impact public health and the environment significantly. Given the far-reaching implications of AV technology, there is a pressing need for research to understand better the opportunities and challenges associated with its adoption. This paper aims to provide a comprehensive overview of AVs, highlighting their potential benefits and challenges and offering recommendations for future research and development in this critical area. Some survey papers exist on the selected research topic, the details of which are provided in the following paragraphs.

Authors in [9] discussed the environmental impact, data dissemination, and defensive approaches for autonomous vehicles. Ref. [10] presented traffic management, Artificial Intelligence approaches, and environmental impact. In the work [11], the researcher shared standards and guidelines. Authors in [12] also provided the international standards and guidelines for autonomous vehicles. In ref. [13], authors discussed public adoption, traffic management, and international standards and guidelines. Authors in [14] discussed the public adoption of AVs. Authors in [15] presented a survey on artificial intelligence techniques in developing autonomous vehicles. Ref. [16] discussed security attacks and their defensive approaches. In Ref. [17], authors discussed security attacks, defensive techniques, and artificial intelligence techniques. Authors in [18] presented artificial intelligence techniques for AVs. This survey aims to provide a 360-degree study of infrastructure and ad hoc autonomous vehicles, including the planning and development of driverless cities and emerging technologies such as artificial intelligence and cloud management techniques. Moreover, it discusses cyber attacks and management, focusing on the limitations of traditional security devices. Furthermore, this survey also covers forensics approaches, including tools, standards, and challenges. Simulators and international standards are also addressed. Table 1 compares the important existing surveys and highlights their limitations.

Table 1. Comparison of survey articles on autonomous vehicles. Key: IILAV-Infrastructure and Infrastructure less Autonomous Vehicle, Rou-Routing, DD-Data Dissemination, SPEV-Solar Power Electric Vehicles, CE-Cloud Employment, PA-Public Adoption of Autonomous Vehicles, PDC-Planning The Driverless City, TM-Traffic Management, EI-Environmental Impact, PH-Public Health, SA-Security Attacks, DA-Defensive Approaches, TSD-Traditional Security Devices, TMA-Threat Modeling Approaches, AI-Artificial Intelligence Techniques, FA-Forensics Approaches, SIM-Simulators, AS-Authentication Schemes, ISG-International Standards, and Guidelines ZT-Zero Trust Architecture.

Surveys	IILAV	ROU	DD	SPEV	CE	PA	PDC	TM	EI	PH	SA	DA	TSD	TMA	AI	FA	SIM	AS	ISG	ZT
Parekh et al., 2022 [9]	X	X	X	X	X	X	X	X	✓	X	✓	✓	X	X	X	X	X	X	X	X
Aradi 2020 [10]	X	X	X	X	X	X	X	✓	✓	X	X	X	X	X	✓	X	✓	X	X	X
Faisal et al., 2019 [11]	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	✓	X
Ahangar et al., 2021 [12]	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	✓	X
Duarte et al., 2018 [13]	X	X	X	X	X	✓	X	✓	X	X	X	X	X	X	X	X	X	X	✓	X
Gkartzonikas et al., 2019 [14]	X	X	X	X	X	✓	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Ma et al., 2020 [15]	X	X	X	X	X	X	X	X	X	X	X	X	X	X	✓	X	X	X	X	X
Pham et al., 2020 [16]	X	X	X	X	X	X	X	X	X	X	✓	✓	X	X	X	X	X	X	X	X
Kim et al., 2021 [17]	X	X	X	X	X	X	X	X	X	X	✓	✓	X	X	✓	X	X	X	X	X
Janai et al., 2020 [18]	X	X	X	X	X	X	X	X	X	X	X	X	X	X	✓	X	X	X	X	X
This Survey	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

1.2. Contributions

This study aims to provide a comprehensive view of the challenges and opportunities associated with AVs. It examines the current state of AV technology. It explores various aspects of AVs, including their public adoption, cloud employment, standards, cybersecurity, threat modeling approaches, artificial intelligence techniques, forensics, and public health implications. The paper analyzes the technical, legal, ethical, and societal aspects of AVs and identifies the key factors shaping the future of autonomous driving. Key contributions of the paper are:

1. Presents a comprehensive survey on the current state-of-the-art of AVs and provides an in-depth discussion of the various aspects of AVs and their impact on society.
2. Presents the infrastructure and Ad Hoc autonomous vehicles, focusing on their respective technologies, routing methodologies, and data dissemination mechanisms.
3. Presents various aspects of AVs in smart cities, such as public adoption, driverless city planning, traffic management, environmental impact, and public health, and discusses key associated challenges.
4. Presents emerging technologies such as artificial intelligence (AI), cloud computing integration, and solar power use in automated vehicles.
5. Presents cyber attacks that can affect autonomous vehicles, attack management, traditional security devices, threat modeling, authentication schemes, over-the-air updates, zero trust architectures, data privacy, and the corresponding defensive strategies to mitigate such risks.
6. Provides forensics approaches, tools used, standards involved, and challenges associated with conducting digital forensics in the context of autonomous vehicles.
7. Provides various simulators used in developing and testing autonomous vehicles. Further, it presents international standards, guidelines, and best practices available for autonomous vehicles (AVs).
8. The core contribution of this paper is to discuss open research problems, challenges, and future directions.

1.3. Organisation

Figure 2 summarizes the structure of this research paper, while Table 2 provides the list of abbreviations. The subsequent sections of the paper are organized as follows. Section 2 provides the infrastructure and Ad Hoc autonomous vehicles. Section 3 explains Autonomous Vehicles in cities. After that, Section 4 identifies the emerging technologies. Then, Section 5 discusses Cyber Attacks and Management. Section 6 presents forensics approaches for AVs. Afterward, Section 7 presents simulators. Section 8 presents International Standards and Guidelines. Then, Section 9 presents research challenges, open issues, and future directions. Finally, Section 10 concludes this paper.

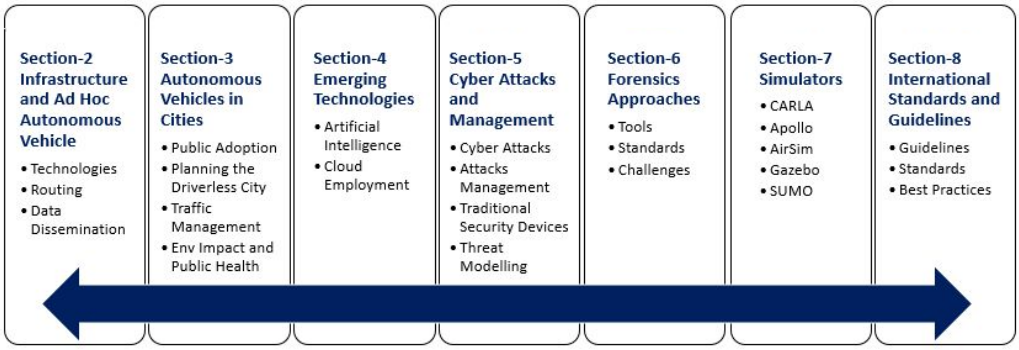

Figure 2. Paper Flow Diagram.

Table 2. List of Abbreviations.

Abbreviations	Description
AV	Autonomous Vehicle
CAGR	Compound Annual Growth Rate
CAN	Controller Area Network
VCC	Vehicular Cloud Computing
DFIRP	Digital Forensics Investigation Readiness Procedures
DRL	Deep Reinforcement Learning
ECU	Electronic Control Unit
FANET	Flying Ad Hoc Network
FL	Fuzzy Logic
GPS	Global Positioning System
GA	Genetic Algorithm
LiDAR	Light detection and Ranging
ML	Machine Learning
MBRL	Model-based RL
NLP	Natural Language Processing
OTA	Over-the-Air
P2P	Peer to Peer Network
PKI	Public Key Infrastructure
RL	Reinforcement Learning
SDN	Software Defined Networking
SUMO	Simulation of Urban Mobility
SLAM	Simultaneous Localization and Mapping
TDM	Time Division Multiple Access
VANETs	Vehicle Ad Hoc Network
V2X	Vehicle to Everything
V2I	Vehicle to Infrastructure
V2N	Vehicle to Network
V2P	Vehicle to Pedestrian

2. Infrastructure and Ad Hoc Autonomous Vehicle

This section comprehensively presents the topics of infrastructure and ad hoc autonomous vehicles, focusing on their respective technologies, routing methodologies, and data dissemination mechanisms. A detailed analysis and discussion will be provided for these key components. Autonomous vehicles can be classified into two categories based on the usage of infrastructure they use infrastructure-based autonomous vehicles and Ad hoc (infrastructure-less) autonomous vehicles. Infrastructure-based autonomous vehicles rely on physical infrastructure such as roads, traffic signals, and mapping systems. They use Global Positioning System (GPS), LiDAR, RADAR, cameras, and other sensors to navigate, but also require a well-maintained network of roads, signs, and signals to ensure safe and efficient operation [19]. Infrastructure-based autonomous vehicles are autonomous vehicles that rely on physical infrastructure such as roads, traffic signals, and mapping systems to operate. These vehicles use GPS, LiDAR, RADAR, cameras, and other sensors to navigate and make decisions. Still, they also require a well-maintained network of roads, signs, and signals to ensure safe and efficient operation. Some key features and benefits of infrastructure-based autonomous vehicles include [20]:

1. **Improved Safety:** By relying on physical infrastructure, infrastructure-based autonomous vehicles can use safety features such as traffic signals, road markings, and signs to make driving decisions and reduce the risk of accidents.
2. **Increased Efficiency:** Infrastructure-based autonomous vehicles can optimize their routes based on real-time traffic data and use dedicated autonomous vehicle lanes to reduce congestion and improve overall traffic flow.
3. **Improved User Experience:** Infrastructure-based autonomous vehicles can provide a more comfortable and convenient riding experience, using amenities such as rest

stops, charging stations, and service facilities along the way. However, there are also some limitations to infrastructure-based autonomous vehicles [21], such as:

- **Cost:** Implementing the necessary physical infrastructure can be expensive, and maintaining it can also be a high ongoing cost.
- **Limited Operating Environments:** Infrastructure-based autonomous vehicles are limited to operating in areas with well-defined roads and traffic signals and may not be suitable for rural or off-road environments.
- **Dependence on Human Intervention:** While infrastructure-based autonomous vehicles can use physical infrastructure to make driving decisions, they may still require human intervention in certain scenarios, such as system failure or road closure.

On the other hand, infrastructure-less autonomous vehicles do not rely on any physical infrastructure to operate. Instead, they use advanced sensors and algorithms to perceive their environment, make decisions, and navigate [22]. This allows them to operate in environments without well-defined roads or traffic signals. However, the lack of physical infrastructure can also pose challenges regarding safety, reliability, and scalability [23].

2.1. Technologies

Autonomous vehicles utilize several important technologies that are as follows:

- **Sensors:** To observe and comprehend their environment, autonomous cars use a range of sensors, including cameras, LiDAR, radar, and ultrasonic sensors. These sensors give the vehicle information about its surroundings, such as the location, mobility of other cars, pedestrians, and obstacles [24].
- **Computer Vision:** Computer vision algorithms are used to process and analyze the data collected by the vehicle's sensors. These algorithms help the vehicle to identify and track objects in its environment, as well as to understand their movement and behavior.
- **Artificial Intelligence (AI) and Machine Learning:** Algorithms based on machine learning and artificial intelligence are utilized to make choices and direct the vehicle's activities. For example, they can be used to determine the vehicle's best path to follow, predict the behavior of other road users, and react to unexpected events.
- **GPS and Maps:** GPS and high-definition maps are used to provide the vehicle with information about its location and help it navigate and avoid obstacles [25].
- **Communication Systems:** Autonomous vehicles use a variety of communication systems, such as cellular networks, dedicated short-range communication (DSRC), and Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication, to exchange information with other vehicles, road infrastructure, and the cloud.
- **Actuation Systems:** Autonomous vehicles use actuation systems, such as electric motors, hydraulic actuators, and pneumatic systems, to control the vehicle's movement and perform tasks such as steering, accelerating, and braking.
- **Power and Energy Management Systems:** Autonomous vehicles use power and energy management systems, such as batteries, fuel cells, and regenerative braking, to provide the vehicle with the energy needed to operate and optimize its energy efficiency.

2.2. Routing

Routing in autonomous vehicles refers to determining the best path for the vehicle from its starting point to its destination. This is an important aspect of autonomous vehicle technology, enabling it to navigate safely and efficiently through its environment [26]. Several key factors are considered when determining the best route for an autonomous vehicle, including:

- **Traffic Conditions:** The vehicle uses real-time traffic data to avoid congested areas and to select the fastest and most efficient route.

- **Road Infrastructure:** The vehicle considers the physical layout of the road network, including the presence of intersections, toll booths, and other road features when selecting a route.
- **Obstacles:** The vehicle uses its sensors to detect and avoid obstacles, such as other vehicles, pedestrians, and road work that may be present along the route.
- **Safety:** The vehicle considers the safety of its passengers and other road users when selecting a route. For example, it may avoid routes with a high incidence of accidents or with poor road conditions.
- **Energy Efficiency:** The vehicle considers the energy consumption of different routes and selects the route that minimizes energy usage.

The routing process in autonomous vehicles is typically performed by algorithms running on the vehicle's onboard computer. These algorithms use historical data, real-time data, and predictions to determine the best route, considering the factors mentioned earlier. Once the route has been determined, the vehicle's navigation system provides the vehicle with step-by-step instructions for how to reach its destination, including information on when to turn, change lanes, or stop. The vehicle's control systems then use this information to control its movement and keep it on the track [27].

2.3. Data Dissemination

Data dissemination in autonomous vehicles refers to the process of sharing and distributing data within the vehicle and between vehicles. This data can include information about the vehicle's surroundings, such as the location of other vehicles and obstacles, traffic signals and road signs, and the road itself. It can also include information about the vehicle's state, such as its speed, acceleration, and direction [28]. In autonomous cars, data distribution aims to ensure that the appropriate information is available to the appropriate vehicle components at the appropriate moment. This enables the vehicle to make informed decisions and respond to changing conditions in real-time. Data dissemination in autonomous vehicles is a complex process that requires robust and reliable communication protocols and algorithms to ensure the data are accurate, timely, and secure. The specific methods used for data dissemination will depend on the requirements of the vehicle and the specific applications being supported [29].

There are several ways in which data can be disseminated in autonomous vehicles; autonomous vehicles use onboard networks, such as Ethernet and Controller Area Network (CAN) Bus, to share data within the vehicle. This enables different systems and components to exchange information and collaborate to make informed decisions. It uses V2V communication to share data with other vehicles. This enables the vehicles to share information about their surroundings, such as the location of other vehicles and obstacles, and to coordinate their movements to improve safety and efficiency. V2I communication shares data with road infrastructure, such as traffic signals and signs. This enables the vehicle to receive information about traffic conditions, road closures, and other relevant information that can be used to make informed decisions. Autonomous vehicles can also use cloud services to access real-time data and cloud-based resources. This includes data from remote sensors, traffic information, and weather data, which can be used to make informed decisions and improve the vehicle's performance [29].

3. Autonomous Vehicles in Smart Cities in a Nutshell

This section thoroughly presents various aspects of AVs in smart cities, such as public adoption, driverless city planning, traffic management, environmental impact, and public health. Further, it discusses key challenges associated with them.

3.1. Public Adoption

Autonomous vehicle (AV) public acceptance is a complicated subject reliant on several variables, including technology improvements, laws, infrastructure, and customer trust, as seen in Figure 3. AV technology is still under development and not yet completely

prepared for wide-scale implementation [30]. Numerous businesses and governments fund research and testing to enhance the technology and sell AVs. Many areas still develop AV regulations, which differ by nation and region [31]. Additionally, it is necessary to construct and enhance the AV infrastructure, which consists of dedicated lanes, charging stations, and communication networks. Another crucial aspect of AV adoption is consumer faith in them. According to studies, many individuals are reluctant to ride in AVs or permit them to operate on public roads because they are concerned about their reliability and safety [32]. As technology advances and is widely recognized, the general public will likely adopt AVs. However, it is challenging to foresee precisely when or how quickly this may occur.

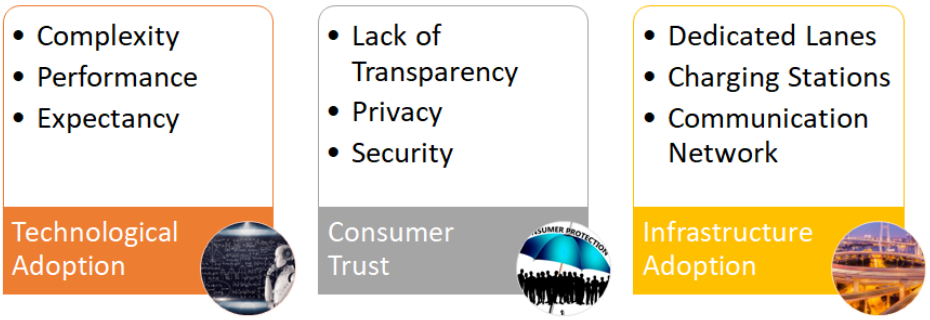

Figure 3. Public Adoption of Autonomous Vehicles.

3.1.1. Technological Adoption

The complicated technology underlying AVs includes many systems and elements, including sensors, perception algorithms, decision-making systems, etc. In concert, the seamless and reliable operation of any of these systems poses a significant challenge. It is expensive to develop and incorporate AV technology into automobiles [33]. As a result, AVs might become more expensive, reducing their accessibility for the typical user. People can have inflated expectations of what AVs are capable of, which could lead to disappointment and mistrust when the technology falls short.

3.1.2. Consumer Trust

As it is essential for successfully adopting the technology, consumer trust is a significant issue with autonomous vehicles (AVs). If consumers believe AVs to be risky, they might be reluctant to trust them. This can result from previous AV-related mishaps, a lack of knowledge about the technology, or doubts regarding the dependability of the systems. Suppose customers are unsure of how AVs operate or believe that the businesses creating and marketing the technology need to be more honest about its capabilities and restrictions. In that case, customers can be reluctant to trust AVs [34]. Customers could worry about the security of AVs since they could be exposed to hacking or other online risks. Due to the possibility that the device may capture and send sensitive data, consumers may worry about how AVs would affect their privacy. If consumers think AVs cannot handle certain scenarios and need human involvement, they might be less likely to trust them, which could make them feel less safe. In general, AV consumer trust must be established for the technology to be successfully adopted. It necessitates open dialogue regarding technological possibilities and constraints and emphasizes security, privacy, and safety [35]. Additionally, AVs must establish a solid track record for dependability, safety, and performance to earn consumers' trust.

3.1.3. Infrastructure Adoption

The minimal AV infrastructure now available is one of the key issues. This includes the absence of the AVs' necessary communication networks, charging stations, and dedicated lanes. Standardization and interoperability are necessary for AV infrastructure to interact with the vehicles smoothly and communicate with them to assure flawless operation [36]. As AVs have the potential to alter how we move across space and utilize it, new urban

design methods will be necessary. When creating new infrastructure, this will need to be considered. The required infrastructure must be created and integrated in a way that is economical, interoperable, and responsive to the changing requirements of the transportation system to support the safe and effective operation of AVs.

Autonomous vehicle (AV) deployment has been modest in developed nations thus far but is anticipated to pick up. Several businesses, like Waymo and Tesla, have started to deploy AVs in small numbers, primarily for research and development. For instance, Tesla has been utilizing its Autopilot technology on its electric cars, while Waymo has been testing its autonomous vehicles on public highways in California and Arizona [37]. In some cities, businesses like Uber have also started offering ride-hailing services utilizing AVs. Autonomous vehicle deployment in underdeveloped nations will likely encounter several difficulties, such as a lack of infrastructure, insufficient legislation, and restricted technological capabilities [38]. Furthermore, many developing nations might need more financial means to invest in the infrastructure and technology needed for autonomous vehicles. Nevertheless, autonomous vehicles may help these nations with some of their transportation issues, such as lowering traffic congestion, enhancing safety, and expanding access to transportation for those who do not currently have it [39]. Making autonomous vehicles possible in developing nations will require major investment in technology, infrastructure, and laws [40].

Critical Analysis: Consumer confidence and trust pose a significant barrier to adoption on a large scale. High-profile events and mishaps involving the technology have impacted how the public views AVs and generated concerns about their dependability and safety. It will need a persistent investment in research and development and open and consistent communication from manufacturers and authorities about the technology's potential and constraints to win over the public's faith in AVs.

3.2. Planning the Driverless City

The process of preparing cities for integrating autonomous cars and its effects on urban life is called "Planning the Driverless City". This considers variables including transportation networks, urban planning, and public policy [41]. The goal is to minimize negative effects while ensuring that cities are fully prepared to benefit from driverless technology. Governmental organizations, transportation businesses, IT firms, and other stakeholders might work together during the planning phase. Designing a driverless city necessitates considering several considerations, such as infrastructure, communication and coordination, Data and Privacy, regulations, integration with public transportation, and social and cultural impacts, as shown in Figure 4.

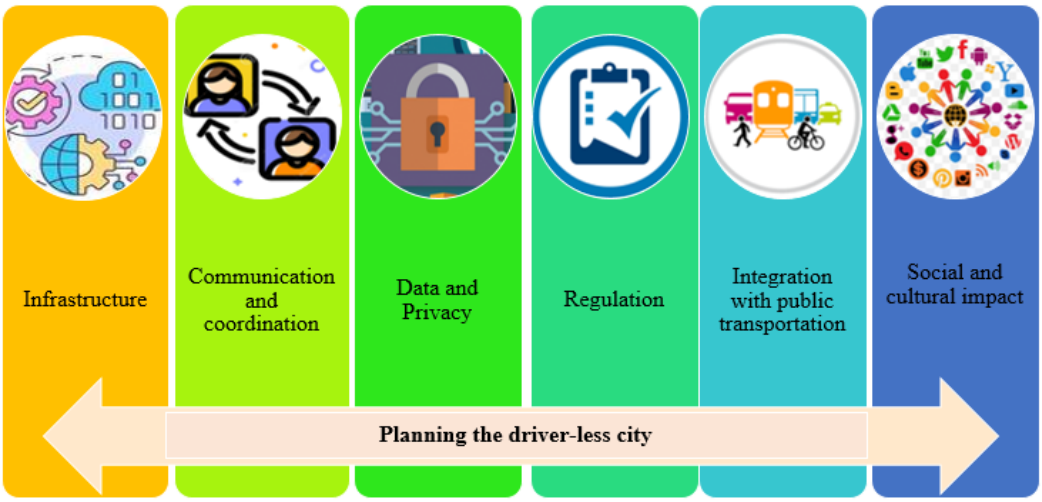

Figure 4. Key Pillars of a Sustainable and Resilient Smart City Ecosystem.

3.2.1. Infrastructure

Infrastructure plays a crucial role in deploying and operating autonomous cars since it impacts how well they can function. To understand their surroundings and abide by traffic laws, autonomous cars need delineated roads and traffic lights [42]. The car needs accurate GPS and mapping data to locate and decide its course. To ensure they can run continually and effectively, they also need facilities for charging and maintenance. A lot of data is produced and needed by AVs, and this data needs to be processed and stored in secure data centers. Autonomous cars rely on various sensors, including cameras, LiDAR, and radar, to learn more about their environment. For optimum functioning, the sensors need to be set up and maintained. AVs need high-bandwidth, low-latency communication networks to share data with other vehicles and the infrastructure and receive real-time updates.

3.2.2. Communication and Coordination

The deployment and operation of autonomous vehicles depend heavily on collaboration and communication. To coordinate their movements, exchange data about their location, speed, and trajectory, and prevent crashes while maximizing traffic flow, autonomous vehicles must be able to communicate with one another [43]. Being able to interface with the infrastructure, such as traffic lights and road signs, to receive real-time updates on the state of the roads and traffic patterns. For efficient decision-making and coordination, AVs must be able to generate and consume massive amounts of data that must be shared and analyzed in real time. Autonomous vehicle operations must be coordinated and managed in real-time to ensure safe and effective transportation and address unforeseen issues.

3.2.3. Data and Privacy

Autonomous vehicles must have access to real-time data and traffic information while maintaining individual privacy to assure safety and effectiveness. The creation and use of autonomous cars depend heavily on data and privacy. Safety, public trust, legal compliance, and maintaining a competitive edge depend on safeguarding data gathered by AVs [44]. For decision-making and safe operation, AVs rely on enormous volumes of data. For the safety of passengers and other road users, it is essential to ensure that these data are accurate and secure. To protect citizens' personal information, governments all around the world are putting in place privacy legislation. To ensure that their technology is consistent with the law, AV developers must abide by these rules.

3.2.4. Regulation

Regulations aid in making sure that AVs are built, tested, and used in a way that protects passengers and other road users and that they comply with safety requirements. It can ensure that AVs are created and used consistently across numerous areas and legal systems. This can make deploying AVs on a large scale easier and ensure system compatibility. By defining standards for AV design, operation, and maintenance, as well as specific rules for protecting the personal data gathered by AVs, regulations can aid in the protection of consumers. Governments must establish rules to guarantee autonomous vehicles' security and moral use in urban settings [45].

3.2.5. Integration with Public Transportation

Autonomous vehicles can enhance the current public transit networks, giving passengers more options and easing congestion. Integrating AVs with public transportation can increase accessibility for those who cannot drive, such as the elderly, disabled, and children. It can also make it simpler for people to access public transportation services, thereby lowering the demand for private vehicles and easing traffic congestion [45]. Lowering wait times and streamlining scheduling can also increase the effectiveness of public transit networks.

3.2.6. Social and Cultural Impact

It is necessary to consider how these changes will be handled and disseminated to the general public because the advent of autonomous vehicles will have a big social and cultural influence. Many occupations in the transportation industry, including those of truck and taxi drivers, could be replaced by AVs, which could substantially affect the labor market. It affects various groups of people differently, such as low-income neighborhoods; thus, it is crucial to consider these consequences and deal with any inequalities that may emerge [46].

Critical Analysis: One key challenge in planning the driverless city is the Integration of AVs into existing urban infrastructure. This requires a significant investment in developing new technologies and systems, such as digital mapping and real-time communication networks, as well as upgrading existing transportation infrastructure, such as roads, bridges, and traffic control systems.

3.3. Traffic Management

The coordination of self-driving automobiles is referred to as traffic management in autonomous vehicles, and it aims to improve traffic flow, lessen congestion, and boost road safety. Numerous methods can accomplish this, including real-time traffic monitoring, vehicle communication, traffic prediction, and routing algorithms. The infrastructure of smart cities can also be combined with traffic management systems to create a connected network that can react to shifting road conditions. The objective is to develop a transportation system that is safer, more effective, and more sustainable. The subject of traffic management and control in a transportation system with autonomous cars is the focus of ref. [47]. The author analyzes the difficulties and constraints that must be solved to fully exploit autonomous vehicle advantages, including increased safety, effectiveness, and sustainability. The essay also highlights the necessity for a fresh strategy for managing and controlling traffic in an environment with autonomous vehicles, including the application of cutting-edge tools like real-time traffic monitoring and vehicle communication. Even if there is still much to be accomplished in this area, the author concludes that incorporating autonomous vehicles into the transportation system has great potential.

The main focus of [47] is developing a simulation-based traffic management system for connected and autonomous cars. The author describes a traffic management system that uses sophisticated routing algorithms, vehicle-to-traffic control center communication, and improved traffic flow to lessen congestion. The system's flexibility and adaptability enable it to react quickly to shifting traffic conditions. The author also explains the outcomes of simulations performed with the system, showing how well it works to improve traffic flow and lessen congestion. The article's conclusion highlights the potential of simulation-based traffic management systems to be crucial in creating a secure and effective transportation network for autonomous cars.

Critical Analysis: The Integration of AVs into existing traffic management systems, such as traffic control centers, road signs, and traffic lights, is a major concern. This requires the development of new algorithms and systems that can effectively manage the flow of AVs and the upgrading of existing infrastructure to accommodate the new technology.

3.4. Environmental Impact and Public Health

The design and use of the vehicles, the charging and power infrastructure for electric vehicles, and the broader transportation system in which they are incorporated are just a few of the variables that affect how environmentally friendly autonomous vehicles are [48,49]. Autonomous cars can potentially increase overall sustainability in the transportation industry by lowering emissions and energy use. The design of the vehicles, the charging and power systems for electric vehicles, and the overall transportation system in which they are integrated are just a few of the variables that will determine whether or not autonomous vehicles can reduce emissions and energy consumption in the transportation sector, according to research [47]. The authors also point out that there are still a lot of unanswered

questions regarding how autonomous vehicles will affect the environment and that more research is required to comprehend these effects and create workable solutions completely. The link between automated vehicles and the environment is the subject of ref. [50,51], emphasizing on-demand mobility services. The writers explore both the possible advantages of autonomous vehicles, such as decreased energy use, emissions, and traffic, and the disadvantages, such as increased travel demand and a decline in the use of public transit.

Several variables, such as the decline in traffic accidents, noise pollution, and changes in physical activity, will affect how autonomous vehicles affect public health. Policy choices, technological developments, and changes in transportation behavior and habits likely influence these variables. To ensure that the development of autonomous vehicles benefits society, it will be crucial to monitor and evaluate their influence on public health closely. Increased sedentary behavior and decreased physical activity could result from autonomous vehicles, exacerbating obesity and other health issues. The need for travel may rise due to autonomous vehicles, resulting in more clogged roads and less physical exercise [52,53].

An analysis of how autonomous vehicles affect public health can be found in article [54]. The authors examine self-driving cars' potential advantages and disadvantages, such as increased safety, physical activity, lower pollution, and screen time. To make sure that the development of autonomous vehicles has a good impact on public health, there is a need for technological advancements as well as regulatory interventions. The authors conclude that interdisciplinary research, stakeholder involvement, and evidence-based policymaking are necessary to address the health effects of autonomous vehicles.

The significance of taking other developing technologies and transportation trends, such as the sharing economy, electrification, and urbanization, into account when evaluating the health effects of autonomous vehicles. They point out that a variety of factors, such as the design of the vehicles, the charging and power systems for electric vehicles, and the entire transportation system in which they are incorporated, will affect how these trends will affect public health [48].

The loss of jobs in the transportation industry exacerbates poverty and social problems. Decreased amounts of physical activity as people become more dependent on driverless vehicles. Obesity and an increase in sedentary behavior as a result of extended driving. Autonomous vehicle data gathering and use raises privacy and security concerns. This necessitates the creation of fresh systems and algorithms for managing the flow of AVs, as well as the modernization of current infrastructure to support the new technology.

4. Emerging Technologies

This section presents emerging technologies in autonomous vehicles (AVs). Specifically, it delves into the intricacies of artificial intelligence (AI) techniques, the integration of cloud computing, and the use of solar power in electric vehicles.

4.1. Artificial Intelligence Techniques

The development of autonomous cars depends heavily on artificial intelligence (AI). It allows the vehicle to perceive, comprehend, and act in its environment. To enhance different areas such as communication, safety, and traffic efficiency in vehicle ad hoc networks (VANETs), artificial intelligence approaches have been extensively investigated [55]. The following are some typical AI methods applied in Autonomous Vehicles:

- Machine learning (ML) is utilized for anomaly detection, route optimization, and traffic prediction [56].
- Reinforcement learning (RL) is a technique for dynamic route planning and adaptive traffic control.
- Artificial neural networks (ANN) are used to identify, classify, and communicate about vehicles.
- Fuzzy logic is used to make safety-critical decisions like emergency braking.

- The use of genetic algorithms (GA) to improve network communication and energy efficiency.
- Swarm intelligence—utilized in platooning of vehicles for cooperative communication.
- Natural language processing (NLP)—utilized for hands-free operation and other human-vehicle interactions. Figure 5 shows the graphical representation of AI techniques.

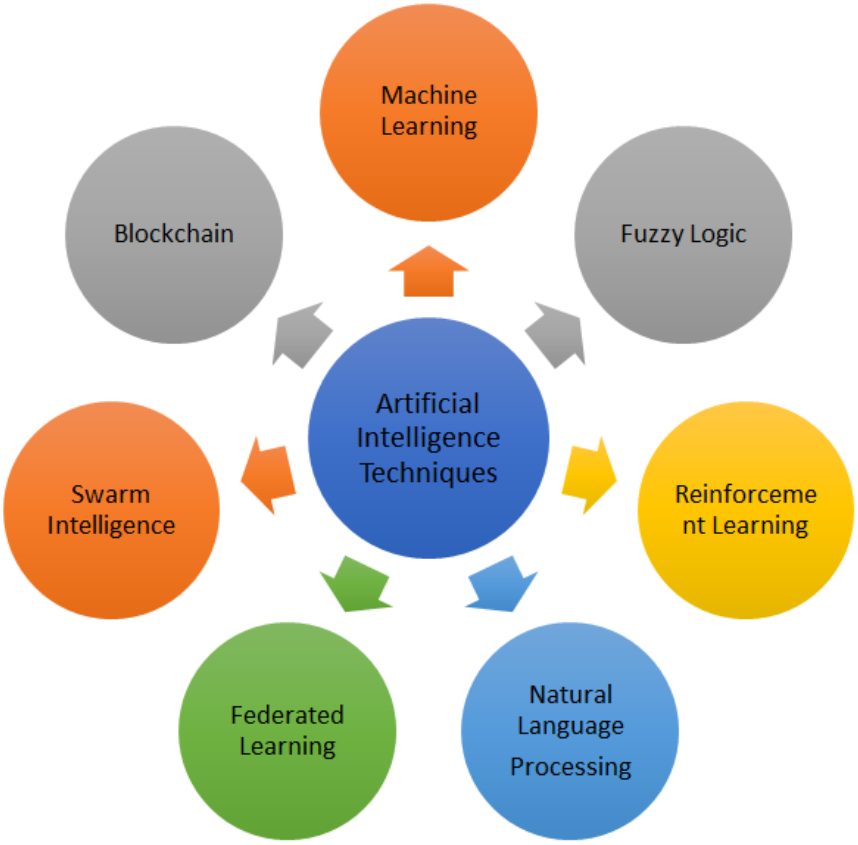

Figure 5. The Evolving Landscape of Artificial Intelligence Techniques.

4.1.1. Machine Learning

Artificial intelligence (AI) is the simulation of human intelligence by machines taught to think and learn like people. Machine learning, a subfield of artificial intelligence, uses statistical models and algorithms to enable computers to learn from data and improve without explicit programming. In other words, whereas AI is a broader concept, machine learning is a specific method for obtaining AI [57].

Machine learning is a critical component in developing and operating autonomous vehicles (AVs). It enables AVs to perceive and interpret their surroundings, make decisions, and interact with their environment in real-time. Table 3 summarizes the machine learning literature. Various machine learning techniques are used in AVs, including supervised learning, unsupervised learning, and reinforcement learning [58]. Supervised learning trains AVs to recognize objects in their environment, such as other vehicles and pedestrians. This is performed by providing labeled data to the AV's machine learning algorithms, which then learn to identify objects based on their features. Unsupervised learning is used to identify patterns in the AV's environment, such as traffic flow patterns or pedestrian behavior [59]. This is performed by clustering data points based on their similarities. Reinforcement learning trains AVs to make decisions based on rewards and penalties. For example, an AV can be trained to avoid collisions by being penalized for collisions and rewarded for successfully avoiding them. The development of autonomous vehicles depends heavily on machine learning. It enables these vehicles to operate autonomously,

making judgments and navigating their surroundings [60]. Machine learning is employed extensively in autonomous cars, particularly in the following areas:

- **Sensor Fusion:** Autonomous vehicles use a variety of sensors, such as cameras, LiDAR, radar, and ultrasonic sensors, to learn about their surroundings [61]. Machine learning algorithms combine and interpret data from various sensors to create a more accurate and complete image of the area around the vehicle.
- **Perception:** Sensor data are analyzed by machine learning algorithms to identify environmental items like other cars, people, and traffic lights [62]. As a result, the autonomous car can comprehend its surroundings and decide what to do depending on them.
- **Prediction:** The behavior of other road users, such as pedestrians and automobiles, can be predicted using machine learning techniques. The vehicle's path and any judgments regarding how to deal with other road users can be made using this knowledge [61].
- **Control:** Machine learning algorithms regulate the car's movement, including steering, stopping, and acceleration. Combining supervised and reinforcement learning approaches can achieve this [63].
- **Adaptive Cruise Control:** Using sensor data to identify the speed and proximity of other vehicles and modify speed cyber accordingly, adaptive cruise control uses machine learning algorithms to adapt the vehicle's speed. The creation of autonomous vehicles depends on machine learning. It makes it possible for these vehicles to navigate their surroundings safely and effectively. The development of autonomous vehicles uses various technologies, including machine learning. However, it is vital to remember that several obstacles must be overcome before they can be completely implemented on public roads.

Critical Analysis: Overall, while machine learning is a powerful tool for developing autonomous vehicles, several challenges still must be overcome before they can be fully deployed on the roads. These include the need for high-quality data, robust and reliable algorithms, explainable models, and the ability to handle uncertainty and imperfect information.

Table 3. Key Findings from Machine Learning Literature.

Ref.	Contribution Area	Evaluation Approach	Main Contribution	Evaluation Metrics	Findings
[64]	Object Detection	CNN-based Object Detection and Classification	Accuracy, Speed, Computational Complexity	Accuracy, Speed, Computational Complexity	Successful real-time object detection for autonomous vehicles
[65]	Collision Avoidance	Fuzzy Logic-based Risk Assessment	Safety, Reliability, Real-time Performance	Safety, Reliability, Real-time Performance	Effective collision avoidance system for autonomous vehicles
[66]	Decision-making	Reinforcement Learning for Driving Policies	Efficiency, Adaptability, Safety	Efficiency, Adaptability, Safety	Effective decision-making system for autonomous vehicles
[67]	Trajectory Planning	Genetic Algorithm for Optimal Trajectories	Feasibility, Optimality, Scalability	Feasibility, Optimality, Scalability	Optimal trajectory planning for autonomous vehicles
[68]	Voice Control	Natural Language Processing for Voice Commands	Accuracy, Usability, Robustness	Accuracy, Usability, Robustness	Successful voice-activated control for IoT

4.1.2. Federated Learning

Federated learning is an AI approach that enables training models across multiple decentralized devices or nodes while keeping data localized. This is particularly relevant in

scenarios like autonomous vehicles, where data privacy, network bandwidth, and real-time decision-making are crucial. Table 4 summarizes the federated learning literature. In the context of autonomous vehicles, federated learning offers several benefits:

- **Privacy and Data Security:** Autonomous vehicles collect massive amounts of data, including sensor readings, images, and location information. These data are sensitive and subject to privacy regulations. Federated learning allows models to be trained locally on individual vehicles without transmitting raw data to a central server, thus preserving user privacy.
- **Low Latency:** Real-time decision-making is crucial for autonomous vehicles to navigate safely. Traditional methods of sending data to a central server for training and receiving updated models can introduce latency. With Federated Learning, models can be updated on the vehicle or within a localized network, reducing communication delays.
- **Bandwidth Efficiency**: Transmitting large amounts of data to a central server for training can be resource-intensive, especially in scenarios with limited network bandwidth [69]. Federated learning mitigates this issue by sending model updates instead of raw data, saving bandwidth and reducing the strain on communication networks.
- **Adaptability**: Autonomous vehicles operate in diverse environments and encounter many scenarios. Federated learning enables models to be trained on specific scenarios that individual vehicles encounter, leading to more accurate and robust models tailored to real-world conditions.
- **Decentralization**: Autonomous vehicles often operate independently or in groups. Federated learning fits well with this decentralized structure, allowing vehicles within a fleet to collaborate on model training without relying on a central authority.

However, there are also a few challenges and considerations regarding federated learning, such as:

- **Heterogeneity**: Vehicles in a fleet may have varying hardware capabilities, sensor configurations, and data distributions. Ensuring that models are effectively trained and generalized across this Heterogeneity can be challenging.
- **Communication Overhead**: Although federated learning reduces data transmission, communication is still required during model aggregation and synchronization. Managing this communication overhead efficiently is important.
- **Data Drift**: Over time, the data distribution that individual vehicles encounter may change due to varying driving conditions, road layouts, and more. Models need to adapt to this data drift to remain accurate and reliable.
- **Model Aggregation**: Combining the updates from various vehicles into a cohesive model while accounting for potential biases and anomalies is a complex task that requires careful algorithm design.
- **Security**: Federated learning introduces new security considerations, such as potential model poisoning attacks or malicious nodes. Ensuring the integrity of the model and the participants' privacy is crucial.
- **Promise**, Despite these challenges, federated learning holds significant promise for improving the efficiency, privacy, and adaptability of machine learning models in autonomous vehicles. It is an area of active research and development, and its successful implementation could contribute to safer and more capable autonomous driving systems.

Authors in [70] explores the integration of Federated learning and the Blockchain for autonomous vehicles (AVs). It addresses the challenges and design considerations of combining these technologies. The authors discuss how federated learning can enhance AVs' performance while maintaining data privacy and how the Blockchain can provide secure and transparent data sharing. The paper highlights the potential benefits of this combination and offers insights into the challenges related to communication overhead, data privacy, and Blockchain scalability [71]. Overall, the paper contributes to the understanding

of leveraging Federated learning and the Blockchain for AVs. Authors in [72] focused on the design of a federated learning-based autonomous controller for connected and autonomous vehicles (CAVs). It presented a controller design that collaboratively improves over-the-road performance using data from multiple vehicles. The authors discuss the benefits of federated learning in enhancing CAV control while considering communication constraints. Authors in [73] introduced "Bift", a Blockchain-based federated learning system tailored for connected and autonomous vehicles. The authors addressed data privacy and Security challenges in federated learning by integrating Blockchain technology. They presented a system architecture that facilitates data sharing and model aggregation while preserving privacy.

Table 4. Key Findings from Federated Learning Literature.

Paper	Contribution Area	Evaluation Approach	Main Contribution	Evaluation Metrics & Findings
Federated Learning with Blockchain (2020)	Federated learning Blockchain for AVs	Challenges analysis	Merge federated learning and Blockchain	Communication, privacy, scalability issues AV performance, security benefits
Federated Learning Controller Design (2022)	CAV controller design Federated learning	Not specified	Cooperative controller with federated learning	Over-the-road performance, cooperation
Bift: Blockchain-Based Federated Learning (2021)	Blockchain for CAVs Federated learning	Not specified	AV model training with federated learning	Data sharing, privacy, efficiency
WITHDRAWN: Efficient FL with Blockchain (2020)	Federated learning Blockchain for AVs	Not available	Withdrawn paper	Paper withdrawn
Privacy-Preserved FL for Autonomous Driving (2021)	Privacy-preserving FL AV collaborative improvement	Not specified	Privacy-enhanced AV model improvement	Privacy preservation shared knowledge

4.1.3. Blockchain

Blockchain technology has the potential to revolutionize various industries, and the automotive sector, including autonomous vehicles, is no exception. Table 5 summarizes Blockchain in the literature. Blockchain offers several potential benefits and applications in the context of autonomous vehicles:

- **Data Integrity and Security:** Autonomous vehicles generate massive amounts of data from various sensors and systems. Blockchain's decentralized and tamper-resistant nature can help ensure the integrity and Security of this data. It can prevent unauthorized access, tampering, or falsification of vehicle data, which is crucial for safety and reliability. Authors in [74] proposed a Blockchain-based framework to enhance the Security of connected and autonomous vehicles (CAVs). As CAVs become increasingly prevalent, ensuring their security and data integrity is paramount to preventing malicious attacks and accidents. A comprehensive framework has been proposed that demonstrates how Blockchain technology can be integrated into connected and autonomous vehicles to enhance Security, data integrity, and trust. The proposed framework can potentially address critical security concerns associated with CAVs, contributing to the safe deployment of these advanced vehicles on the roads.
- **Supply Chain Management:** Authors in [75] proposed that the Blockchain can track the entire supply chain of automotive components, ensuring transparency and authenticity. In the case of autonomous vehicles, which rely on advanced sensors and

hardware, maintaining the integrity of components is essential for safety and performance.

- **Vehicle Identity and Authentication:** Blockchain can provide a secure and tamper-proof identity for each autonomous vehicle. This can help prevent vehicle identity theft, unauthorized modifications, and fraudulent activities related to vehicle registration and ownership.
- **Smart Contracts for Mobility Services:** Smart contracts, which are self-executing contracts with the terms directly written into code, can automate transactions and agreements between autonomous vehicles and other parties. For instance, vehicles could automatically pay for tolls, charging, or parking without human intervention.
- **Decentralized Traffic Management:** Blockchain can create a decentralized and secure traffic management system for autonomous vehicles. It could facilitate communication and coordination between vehicles, traffic infrastructure, and other stakeholders, optimizing traffic flow and safety. Authors in [76] presented an innovative approach to addressing data integrity and security challenges in autonomous vehicles through a Blockchain-inspired event recording system. By leveraging decentralized data organization, hashing, and time-stamping, the system aims to provide a trustworthy and tamper-resistant record of events for post-analysis, accountability, and overall system reliability.
- **Data Sharing and Monetization:** Autonomous vehicles generate valuable data that can be shared with other vehicles, infrastructure providers, and third-party applications. Blockchain can enable secure and controlled data sharing, allowing vehicle owners to monetize their data while retaining control over who accesses it.
- **Insurance and Claims Processing:** Blockchain's transparency and traceability can simplify the insurance process for autonomous vehicles. Smart contracts could automatically trigger claims processing when predefined conditions (such as an accident) are met, speeding up the resolution process.
- **Decentralized Car-Sharing and Rentals:** Blockchain can support peer-to-peer car-sharing and rental platforms for autonomous vehicles. Smart contracts could manage reservations, payments, and access control without relying on intermediaries.
- **V2X Communication:** Vehicles-to-everything (V2X) communication is crucial for autonomous vehicles to interact with other vehicles and infrastructure. Blockchain can enhance the Security and privacy of these communications, preventing malicious attacks and unauthorized access.

Table 5. Key Findings from Blockchain Literature.

Paper	Contribution Area	Evaluation Approach	Main Contribution	Evaluation Metrics & Findings
[74]	Security CAVs	Simulation	Blockchain framework	Data integrity, security transparency, trust
[75]	Resilience Industry 4.0	Literature review	AV security schemes	Attack analysis, categorization, gaps
[76]	Event AVs	Not mentioned	Event recording system	Data integrity, tamper resistance

4.1.4. Fuzzy Logic

Fuzzy logic is a mathematical tool that can be used in autonomous vehicles to handle uncertainty and vagueness in the decision-making process. In autonomous vehicles, fuzzy logic can help model the human-like decision-making process by considering various factors that may affect the driving situation, such as weather, traffic conditions, road conditions, and pedestrian behavior [77]. Fuzzy logic assigns membership functions to various

input variables and rules that map the inputs to output variables. These membership functions and rules can be derived from expert knowledge or learned from data using machine learning techniques. The output of the fuzzy logic system is a degree of membership to a specific category, such as a speed limit or a safe distance to another vehicle.

Fuzzy logic can be used in AI to simulate the ambiguous and imprecise information frequently present in sensor data, natural language, and other sources. Allowing the AI system to make conclusions based on approximate rather than precise knowledge can produce more human-like reasoning [78]. Fuzzy logic is utilized in autonomous vehicles to assist the vehicle in making judgments based on incomplete or ambiguous information [79]. An autonomous vehicle may use fuzzy logic to decide the best course of action when navigating a road with plenty of other vehicles. The car may consider variables including road conditions, traffic signals, and other vehicles' speeds and distances from it. It can then utilize this knowledge to decide whether to brake, accelerate, or turn [80]. The vision system of autonomous vehicles can also use fuzzy logic. In this instance, the vehicle uses cameras and LiDAR as sensors to learn more about its surroundings [80]. The control system of autonomous vehicles uses fuzzy logic as well. The vehicle's steering, accelerating, and braking are all under the control of the control system [81]. The vehicle can employ fuzzy logic to identify the optimal action based on the circumstances and the desired result. Because it enables autonomous vehicles to manage imprecise and uncertain information and make judgments based on it, fuzzy logic is a useful tool. This can make it easier for the car to maneuver through challenging and changing circumstances, such as congested highways or shifting weather conditions [82].

The fuzzy logic system must be carefully designed to ensure that it can effectively handle the specific types of uncertainty and imprecision in the vehicle's environment. Additionally, the system must be properly calibrated and fine-tuned to ensure that it produces accurate and reliable results. Fuzzy logic systems are sensitive to input data, and it is essential to validate the data to ensure it is accurate and reliable. Even small errors in the input data can lead to significant errors in the output of the fuzzy logic system. Table 6 summarizes fuzzy logic in autonomous vehicles.

Table 6. Fuzzy Logic in Autonomous Vehicles.

Paper	Contribution Area	Evaluation Approach	Main Contribution	Evaluation Metrics	Findings
[83]	Path Following	Fuzzy Controller	Commands	Steering Speed	Successful
[84]	Lane Change	Fuzzy System	Commands	Steering Acceleration	Effective
[85]	Obstacle Avoidance	Fuzzy System	Commands	Steering Speed	Promising
[86]	Collision Avoidance	Fuzzy System	Safe Path	-	Efficient
[87]	Adaptive Cruise	Fuzzy System	Optimal Speed	Following Distance	Improved

4.1.5. Reinforcement Learning

A subset of machine learning known as reinforcement learning (RL) is concerned with teaching agents—such as software or robots—how to make decisions in a given environment. The agent learns how to make better judgments in the future by using the rewards it receives or incurs as a result of its activities [88]. To build more complex and effective systems, reinforcement learning can be combined with other forms of AI, such as supervised learning and unsupervised learning. For instance, an RL agent can be taught to recognize objects in an image using a combination of supervised learning and unsupervised learning techniques and then utilize that information to decide how to navigate in its surroundings [10].

One of the important uses of RL is in autonomous vehicles, where the RL agent may adapt its driving style over time while considering traffic, road conditions, and other variables. Robotics also uses RL to teach its agents how to carry out challenging tasks like grabbing things or exploring uncharted territory [89]. The recent research on RL for automobiles has focused on developing and enhancing RL algorithms to help autonomous vehicles make prudent driving judgments. The summary of Reinforcement Learning in Autonomous Vehicles is shown in Table 7.

Table 7. Reinforcement Learning in Autonomous Vehicles.

Paper	Contribution Area	Evaluation Approach	Main Contribution	Findings
[90]	Navigation	RL Controller	Optimal Decisions	Successful
[91]	Cooperative Driving	Centralized RL	Traffic Flow	Improved
[92]	Adverse Weather	RL Controller	Driving Decisions	Adaptive
[93]	Learning from Humans	RL Framework	Driving Skills	Mimicry
[94]	Vehicle Platooning	Decentralized RL	Fuel Efficiency	Enhanced

4.1.6. Deep Reinforcement Learning

Autonomous vehicles are trained using this technique. Deep neural networks are used in Deep Reinforcement learning (DRL), a kind of reinforcement learning, to allow RL agents to learn from highly dimensional, non-linear situations. According to studies, DRL can teach autonomous vehicles to change lanes in traffic properly, navigate through uncharted terrain, and make other driving decisions [89].

- Multi-Agent RL: This technique teaches autonomous vehicles how to communicate with other cars and pedestrians in a shared space. Multiple agents (like autonomous vehicles) can learn from one another and enhance their decision-making using this kind of RL. Multi-agent RL can teach autonomous vehicles to properly negotiate challenging traffic situations, such as roundabouts and intersections, according to research articles [95].
- Model-based RL (MBRL): Model-based RL techniques create better judgments for the RL agent by predicting the effects of various actions using a model of the environment. According to studies, MBRL can be used to increase the sample efficiency of RL algorithms, enabling the training of autonomous vehicles to happen more quickly and with fewer data [96]. The development and enhancement of RL algorithms that can help autonomous vehicles make prudent driving judgments has been the focus of recent research in RL for automobiles. This encompasses the application of model-based, multi-agent, and deep reinforcement learning approaches and the fusion of RL with other AI methodologies [97].

RL algorithms can require a large amount of data to train effectively. Autonomous vehicles must be able to make decisions in various conditions and environments, and it cannot be easy to collect enough data to train the RL algorithm to handle all possible scenarios. Ensuring that the vehicle is making safe decisions in RL can be difficult. RL algorithms are not inherently safe, unlike traditional control systems designed to guarantee certain safety properties. Ensuring the vehicle will not make decisions that could lead to accidents or other dangerous situations is challenging. The summary of Deep Reinforcement Learning in Autonomous Vehicles is shown in Table 8.

Table 8. Deep Reinforcement Learning in Autonomous Vehicles.

Reference	Contribution Area	Evaluation Approach	Main Contribution	Findings
[98]	Navigation	Deep RL Controller	Optimal Decisions	Improved
[99]	Vehicle Platooning	Deep RL-based System	Fuel Efficiency	Enhanced
[100]	Challenging Scenarios	Deep RL Controller	Driving Decisions	Effective
[101]	Learning from Humans	Deep RL Framework	Driving Skills	Adaptive
[102]	High-Speed Obstacle Avoidance	Deep RL-based System	Rapid Decisions	Accurate

4.1.7. Genetic Algorithm

Genetic algorithm (GA) is a powerful optimization technique used in autonomous vehicles to find optimal solutions for various problems, such as route planning, trajectory planning, and vehicle control. The GA is based on the principles of natural selection and evolution, and it works by creating a population of candidate solutions and evolving them through selection, crossover, and mutation [103]. A class of optimization methods called genetic algorithms (GAs) is motivated by the ideas of natural selection and evolution. Genetic operators like selection, crossover, and mutation evolve a population of solutions in GAs over several generations. Various domains, including optimization, machine learning, and control systems, have extensively used GAs. A summary of the genetic algorithm used in autonomous vehicles is shown in Table 9.

Table 9. Genetic Algorithm in Autonomous Vehicles.

Reference	Contribution Area	Evaluation Approach	Main Contribution	Findings
[104]	Fuel Efficiency	GA-based Approach	Speed, Gear Optimization	Savings
[105]	Traffic Flow	GA-based Approach	Speed, Headway Optimization	Improvement
[106]	Obstacle Avoidance	GA-based Approach	Control Parameters	Success Rate
[107]	Vehicle Routing	GA-based Approach	Routing, Charging Optimization	Efficiency
[108]	Traffic Flow	GA-based Approach	Lane-Changing Optimization	Reduced Time

GAs can be used to improve a number of the decision-making and control systems in autonomous vehicles [109]. The vehicle's course planning, control settings, and sensor fusion algorithms can all be improved with GAs. The advantage of GAs for autonomous vehicles is their ability to tackle difficult, high-dimensional, and non-linear optimization issues. In addition, GAs can withstand environmental noise and uncertainty, which is a prevalent feature of real-world driving situations. They can also optimize the trade-off between various performance measures, including comfort, safety, and fuel efficiency.

The creation and advancement of GA-based optimization algorithms have been the main research topics in [110]. One area of research is using multi-objective GAs to optimize different performance indicators simultaneously. The usage of hybrid GAs, which combines GAs with other optimization algorithms like particle swarm optimization and simulated annealing, is another field of research. Ref. [111] presents a genetic strategy for adaptive navigation of a robot-like simulation vehicle [112]. The recommended algorithm creates practical paths by conducting an adaptive search on populations of plausible courses of action. The program's performance is demonstrated on problems involving cars driving in two-dimensional grids and contrasted with that of a simple greedy algorithm and a random search technique [113].

Since GAs need a lot of computing, they may not be suitable for real-time applications like autonomous vehicles. Additionally, GAs are sensitive to halting criteria, genetic operators, and initial population selection. It can be challenging to select an acceptable initial population, genetic operators, and stopping criteria, and even minor mistakes in these decisions can result in large behavioral problems.

4.1.8. Natural Language Processing

A branch of AI called "natural language processing" (NLP) studies how computers and human languages interact. NLP enables computers to naturally comprehend and respond to human language by processing and analyzing human language data, such as speech, text, and written language. NLP can be employed in autonomous vehicles to help them comprehend and communicate with their human passengers. Additionally, it can help the car comprehend and comply with oral instructions, like "Take me to the closest gas station" or "What is the weather like today?" NLP can also help the car comprehend and react to written content like emails or text messages. According to [114], NLP can let autonomous vehicles communicate with their human passengers naturally and intuitively. In addition, NLP can increase passenger comfort and safety by allowing cars to comprehend and comply with verbal commands like "Take me to the closest gas station" or "What is the weather like today?"

The topic of ref. [115] has been the creation and enhancement of NLP algorithms. They use deep learning methods to enhance the precision and fluidity of the NLP system, such as recurrent neural networks and transformer networks. The use of multimodal NLP, which integrates speech, text, and additional modalities like images and videos to increase the vehicle's comprehension of the passenger's intent, is another field of research [116]. NLP, however, may have significant drawbacks and difficulties. One of its key drawbacks is that NLP can be sensitive to differences in the human voice, and language might be an issue in real-world settings. Background noise and other environmental elements can also be a concern in real-world settings because NLP can be sensitive to them [117]. NLP can be sensitive to human voice and language variations, which can be problematic in real-world environments like Autonomous Vehicles. Additionally, NLP can be sensitive to background noise and other environmental factors. A summary of NLP is discussed in Table 10.

Table 10. Natural Language Processing in Autonomous Vehicles.

Reference	Contribution Area	Evaluation Approach	Main Contribution	Findings
[118]	Voice Assistant	DNN and Rules	Meaning Extraction	Accuracy, Robustness
[119]	Safety	NLU Integration	Situational Awareness	Enhanced
[120]	Intelligent Transportation	NLP Framework	User Understanding	Natural Interaction
[121]	Entertainment Control	Speech Recognition	User Intents	Personalized Control
[107]	Dialogue Management	RL and Hierarchical Structure	Multi-turn Conversations	Natural Communication

4.1.9. Swarm Intelligence

The study of decentralized systems' behavior, such as the behavior of ants, bees, or birds, as well as the collective intelligence that develops through interactions among the individual agents, is known as swarm intelligence. In swarm intelligence, a collection of straightforward agents known as "swarm agents" cooperate to accomplish a single objective. Table 11 summarizes swarm intelligence in autonomous vehicles. Swarm intelligence can be utilized in autonomous cars to enable a collection of vehicles to collaborate to accomplish a common objective, such as traffic flow optimization, cooperative navigation, and emergency response. By altering the speed and spacing of the cars, a group of vehicles can cooperate to improve traffic flow on a roadway using swarm intelligence [122]. Swarm intelligence can allow a collection of vehicles to cooperate to accomplish a common goal, which is one of its main benefits for autonomous cars [114]. Swarm intelligence also enables vehicles to share information and coordinate activities, enhancing the decision-making process's safety and effectiveness. Developing and enhancing swarm intelligence algorithms have been the focus of recent swarm intelligence research for autonomous vehicles. The use of particle swarm optimization (PSO) and ant colony optimization (ACO) methods to improve the behavior of the swarm agents is one field of research. Using swarm intelligence to enable a collection of vehicles to cooperate and work toward a common objective, such as traffic flow optimization, cooperative navigation, and emergency response, is another area of research [123]. Swarm intelligence can be sensitive to variations in the behavior

of the individual agents, which can also be a problem in Autonomous Vehicles. Careful design, implementation, and validation are essential to ensure that the swarm intelligence algorithm performs effectively and safely in the real-world environment.

Table 11. Swarm Intelligence in Autonomous Vehicles.

Reference	Contribution Area	Evaluation Approach	Main Contribution	Findings
[58]	Vehicle Routing	PSO Algorithm	Route Optimization	Efficiency
[124]	Cooperative Perception	Swarm-based Algorithm	Sensing, Perception	Enhanced
[125]	Path Planning	PSO Algorithm	Cooperative Planning	Efficiency
[120]	Adaptive Cruise Control	Swarm-based Algorithm	Traffic Flow, Fuel Consumption	Improved
[126]	Vehicle Platooning	PSO Algorithm	Formation, Movement Optimization	Efficiency

4.2. Cloud Computing

The technology behind autonomous cars aims to lessen our reliance on fossil fuels, reduce traffic jams, and make it easier for the disabled and the elderly to travel. The employment of technology in autonomous vehicles allows for a 60% reduction in pollutants and a 90% reduction in road accidents. Automobiles employ AI methods for data management and analysis to make sense of the vast volumes of information generated by sensors and other onboard equipment. Voice recognition, picture identification, and decision-making are just some of the many uses for machine learning algorithms, deep learning, reinforcement learning, and simultaneous localization and mapping (SLAM) in autonomous vehicles. Edge computing, vehicular cloud computing (VCC), software-defined networking (SDN), network function virtualization (NFV), and named data networking are all promising new developments in the field of autonomous vehicles (NDN). While NFV emphasizes computational power, NDN facilitates efficient data transfer, edge computing enables real-time data processing, SDN enables interoperability between different data sources, virtualized compute infrastructure improves traffic management and road safety, and VCC focuses on data center consolidation. These advancements in technology are crucial to ensuring that autonomous vehicles can be used safely and effectively [127].

The hardest part of securing autonomous automobiles is designing an edge computing infrastructure. Autonomous automobiles need enough computing power, redundancy, and security to prevent accidents. Dealing with massive amounts of real-time data is tough. Due to their mobility, edge computing systems have strict energy consumption constraints, and sensor data are usually quite varied. High-speed autonomous automobile safety demands plenty of computing power with low energy use. Vehicle-to-everything (V2X) communications can improve peripheral performance and energy. Studying how V2X-enabled automobiles interact with one other and infrastructure is needed. Autonomous driving requires safeguarding edge computing systems from attacks across the sensor and computing stack [128]. Edge YOLO is a method for detecting movable objects proposed in the study and is adapted specifically for edge computing technology. The Edge YOLO, based on the latest object detection network in the YOLO series, YOLOV4, is superior for edge computing circumstances based on 5G for traffic safety monitoring and driving assistance. The cloud manages timed training and automatically updates weights depending on new data, while the edge handles model reasoning and data uploads when conditions are idle [129].

Vehicular cloud computing (VCC), which advances cloud computing, enables intelligent transportation, autonomous driving, vehicle control, Internet surfing, online documentation, and infotainment applications. The authors' survey examined privacy and safety issues in VCC research. The authors examine security, privacy, VCC design, feature analysis, and application scenarios. To address VCC security and privacy challenges, the authors first evaluate the various attack surfaces of linked VCC, including the in-vehicle network, V2X network, and vehicular cloud [130]. A smart autonomous vehicle parking (SAVP) system is created to help AVs find parking places indoors and outside.

Various techniques have been explored for object detection and tracking in the literature. One common approach is using LiDAR-based object detection, where LiDAR sensors measure the distance and position of objects in the vehicle's vicinity. Research works, such as [131,132], have focused on using LiDAR data for accurate object detection and tracking. The research work of [131] proposes a comprehensive data acquisition and analytics platform specifically designed for automated driving systems. The platform integrates various data sources, including LiDAR data, from connected vehicles to provide real-time and post-processing analytics. The study focuses on leveraging LiDAR-based object detection to identify and track objects in the vehicle's surroundings accurately. By utilizing LiDAR sensors' ability to measure the distance and position of objects in 3D space, the platform aims to improve object detection and tracking accuracy, enabling more robust and safe autonomous driving [133,134]. Additionally, datasets like "V2V4REAL: A Real-World Large-Scale Dataset for Vehicle-to-Vehicle Cooperative Perception" have been developed to facilitate research in cooperative perception, where multiple vehicles share their perception data to enhance the accuracy of object detection and tracking.

The SAVP system uses Fog-computing and Blockchain technologies to improve the collaborative IoT-cloud platform for building and administering AV SP systems. Fog nodes connect edge devices that support the Internet of Things to parking-related services [135]. A lightweight, integrated Blockchain and cryptography (LIBC) module at each fog node authorizes and grants AV access in every parking phase to meet privacy and security concerns. A proof-of-concept implementation of the proposed SAVP system showed that its average response time, efficiency, privacy, and security were very good, opening the way for a proven system [136,137]. The authors in [138] proposed a cross-domain solution for the Cognitive Internet of Vehicles to achieve ultra-flow delay and ultra-high dependability in autonomous driving. This study's two most important innovations were the global AI fog-computing paradigm and the IoT AI service architecture.

Cloud Challenges in Autonomous Vehicles

Cyberattacks, ransomware, and vehicle theft can affect autonomous automobiles [139–143]. Radar Interference Management: Thousands of connected cars using radar technology can cause dangerous radar blindings. Integrating disparate vehicular networks raises new obstacles Scalability issues: A deluge of data from many connected devices can make it difficult for the edge node to do analytics while achieving autonomous car latency constraints [128]. Autonomous vehicles are expensive because they need sophisticated sensors and computer systems to ensure their reliability and safety. Hence, Vehicle-to-Everything (V2X) connectivity technology can cut autonomous car prices. Cooperative sensing's main challenge is sharing real-time infrastructure sensor data with autonomous vehicles and balancing infrastructure sensor and on-vehicle sensor costs. Edge computing could solve the challenge of real-time data sharing between infrastructure sensors and autonomous vehicles by processing and compressing at both the edge node (car) and edge server (infrastructure) [127].

4.3. Solar Power Electric Vehicles

Ad hoc networks provide an environment of cooperation and coordination among self-operated nodes, which allows communication to occur typically through several hops. Nodes sometimes refuse to work with one another because of their social likeness and mobility. This study examines the primary causes of selfish behavior adaptation in nodes and management strategies for such nodes. It is possible to control the selfish nodes by restricting or encouraging their network participation. In recent literature, credit-based incentive programs are thought to be more effective and efficient for dealing with misbehaving or uncooperative nodes in ad hoc networks. Additionally, incentive-based methods are designed and implemented using game theory. This study concludes that incentive-based or evolutionary-based approaches can control a node's selfishness [5].

A thorough analysis of the design challenges, communication strategies, and routing protocols of UAVs with unresolved research questions. In UAV communication, preserving data links' integrity is an ongoing research topic. The data-centric routing algorithm opens up new research possibilities. The topic of UAV communication while addressing nodes in 3D is still substantially unexplored. The distribution of audio-video data severely constrains the FANET application scenario's requirement for bandwidth. Noise is added to the transmission as data transfer bandwidth is increased. Network latency reduction in dense ad hoc network deployment remains a crucial research area. The non-Line-of-Sight communication FANET architecture is still substantially unexplored. One of the biggest obstacles facing FANETs is still communication. The multi-level routing protocols and data-centric routing algorithms are promising new routing techniques. FANET communicates using a variety of bands. FANET needs standards and a strong algorithm to maintain stability in a hostile environment like that seen in flight. Strong algorithm design is a popular area of research for the global scientific community [144].

Researchers have paid more attention to VANET due to its greater mobility, dynamic connection, and decentralized administration. Security is the main issue preventing the VANET from disseminating data effectively. Effective security frameworks are necessary for the VANET's secure message processing & sharing. There are several network security issues that VANET faces that are also present in traditional wireless networks. However, because of the unbounded network's size, high mobility, frequent information sharing, and regular topology changes, security issues in VANET are both inherent and unique. In addition to these problems, privacy considerations and concerns about authentication and non-repudiation are difficult to reconcile. This study presents a thorough literature evaluation of the current data dissemination approaches and data-related traits and applications for safety and infotainment in VANET [145].

Solar-powered electric vehicle (EV) charging in vehicular ad hoc networks (VANETs) refers to a system for charging electric vehicles using solar energy and wireless communication technology in a decentralized manner. In this system, EVs act as mobile nodes in a VANET and are equipped with photovoltaic panels to generate sun electricity. The generated electricity is stored in a battery to power the vehicle. When an EV needs to be charged, it searches for other nearby EVs with excess energy stored in their batteries and requests to be charged wirelessly. If a neighboring EV agrees to the request, it transfers some of its stored energy to the requesting EV. This process is known as "vehicle-to-vehicle (V2V) charging" or "peer-to-peer (P2P) charging" [146] Solar-powered EV charging in VANETs provides several benefits over traditional centralized charging systems, including [147]:

- Decentralization: With VANETs, there is no need for a centralized charging station, which can reduce the cost of infrastructure and increase accessibility for EVs.
- Increased efficiency: By allowing EVs to charge from each other, the system can better use the available energy and reduce the need for additional energy generation.
- Reduced dependence on the grid: Solar-powered VANETs reduce the dependence on the grid, which can be beneficial in areas with unreliable or absent grid infrastructure.
- Increased energy security: Having multiple energy sources available in the VANET makes the system more resilient to failures and less susceptible to energy blackouts.

5. Cyber Attacks and Management

This section will provide an overview of cyber attacks affecting autonomous vehicles and the corresponding defensive strategies to mitigate such risks. The following discussion will focus on the different types of traditional security devices, threat modeling approaches, authentication schemes, and zero trust architecture.

5.1. Cyber Attacks

Over the past few years, autonomous automobile excitement has increased quickly as numerous major technology companies support the idea. Google established the Waymo subsidiary to create and sell consumer-ready autonomous cars worldwide. The organiza-

tion wagers that driverless cars will soon fundamentally alter how we travel, along with numerous other players in the tech and automotive sectors. Safer roads, less reliance on fossil fuels, and more affordable transportation will all be dramatic improvements. Figure 6 shows the potential attacks on sensors, protocols, and in-vehicle systems.

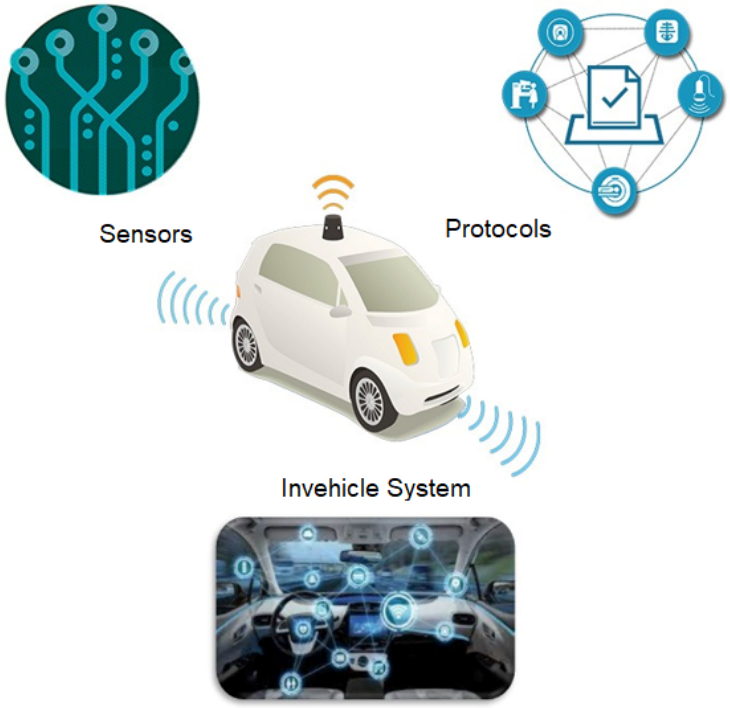

Figure 6. Autonomous Vehicles Attack Surface.

5.1.1. Various Sensor Attacks

The safety of autonomous vehicles is strongly dependent on the accuracy of the sensors they use to assess the state of the road and make driving judgments. Sensor-related heterogeneous and multi-modal features are included in the collected data, and these characteristics are further combined to provide useful decision rules. As a result, sensors are crucial to how AVs make decisions. Figure 7 shows different types of sensors, and Table 12 shows the use of those types [148]. Most AV sensors can be accessed internally; these programs ensure the car keeps going and functioning.

Just a few particular kinds of applications are associated with the perception of the environment. The method of transforming the physical world into digital information for further processing is called sensor perception, like calculating distances or forces. Attackers are interested in using sensor networks to their advantage [149]. Although only focused on intrusions through vulnerable channels for input and output, such as ports for wireless maintenance, Bluetooth, and systems for keyless entry, the research of [63] examines external threats.

5.1.2. Ultrasonic Sensor Attacks

The ultrasound sensor transmits and receives waves of ultrasound, which are high-frequency sound waves humans cannot hear. Typically, sounds with frequencies greater than 18 kHz are invisible to most individuals. It uses the propagation time of reflected ultrasonic pulses to determine the distance to the closest barriers. This capacity makes ultrasonic sensors suitable for automatic or partially automatic parking in Autonomous Vehicles [150]. Similar to other attacks, jamming and spoofing threaten the ultrasonic sensor. Spoofing attack attempts to use the expertly designed ultrasound to fabricate a barrier [151]. When no real obstacles are within the detecting range, the spoofing assault can produce fake ones.

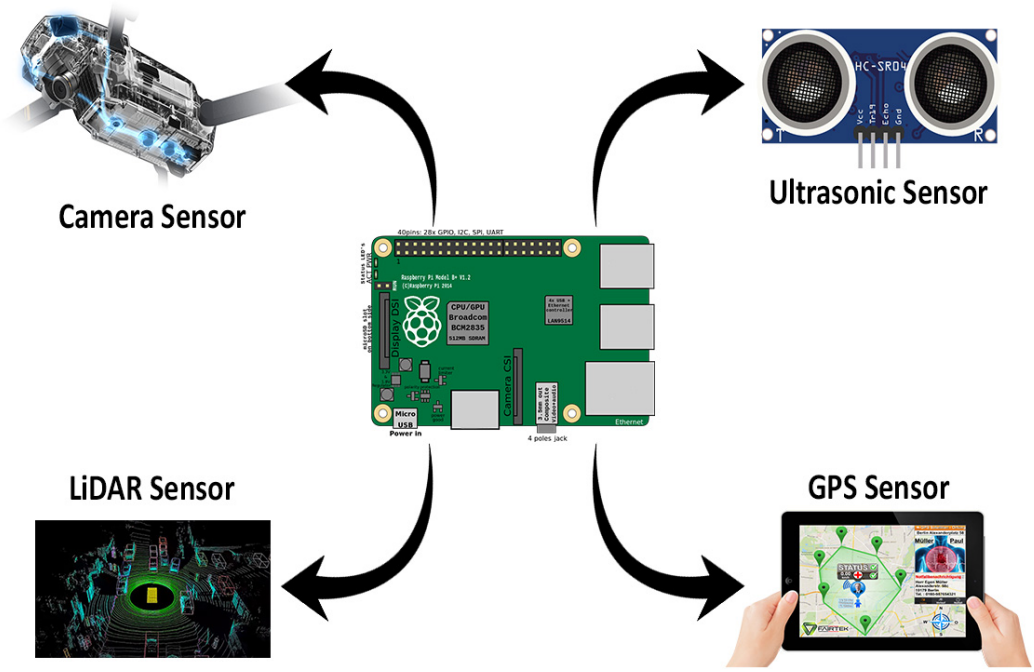

Figure 7. Types of Sensors.

Table 12. Usage of Sensors.

Sensor	Use of Sensor
Ultrasound	Parking assistance
Camera	Traffic sign recognition, Lane detection, Obstacle detection
LiDAR	Collision Avoidance
MMW Radar	Adaptive Cursive Control
GPS	Navigation

On the other hand, if there are additional barriers, this attack might quickly lead to confusion when Autonomous Vehicles are making decisions. Beyond this study, Authors in [152] further illustrates the efficacy of the adaptive spoofing assaults by putting up virtual barriers against both commercially available sensors built into Autonomous Vehicles. Jamming attacks are less complex but dangerous because they seek to lower the ultrasonic sensor's Sound to Noise Ratio by continuously producing ultrasound. Tests on Volkswagen, Audi, Ford, and Tesla revealed that jammer attacks could cause vehicles to become confused when the driver is not given any advance notice of potential difficulties [153]. Another investigation by [152] demonstrates that jammer attacks are successful against Tesla vehicles operating in both the summons and self-parking modes. Both times, an automobile that is stuck may run to avoid objects. Ultrasonic sensor attacks can also use acoustic quieting techniques like cloaking and sound cancellation. In ref. [152], authors proved the viability of attacks on ultrasonic sensors, including jamming attacks, adaptive spoofing, and random spoofing. They demonstrated how they could lead to poor autonomous driving decisions for moving vehicles.

5.1.3. Light Detection and Ranging (LiDAR) Attacks

LiDAR uses a particular type of sensor for range detection of target [154]. It operates by emitting a light pulse and measuring the time required for light to be reflected off by a faraway surface. As LiDAR is the primary method employed by speed measurement devices on the (underground) market, jammers are readily confused. LiDAR, on the other

hand, can detect objects that reflect the signal [155]. If the signal is absent, the system concludes there is no object. Absorbing light, rain, and snow can drastically lower the remission frequency. By relaying the initial signal from the LiDAR system of a target vehicle from a different location, the assault, a development of a replay attack, aims to produce phony echoes.

Perception is critical in self-driving systems, so onboard cameras and LiDARs are examples of sensors that scan the environment. Ref. [156] has demonstrated how spoofing assaults, in which attackers trick a self-driving car into thinking it is another vehicle by carefully sending laser beams to the LiDAR of the victim sensor, can impair LiDAR-based perception. However, the effectiveness and generality of existing assaults are constrained. The vulnerability of today's Light detection and ranging perception systems was examined by [156], who discovered that Autonomous vehicles are prone to spoofing attacks because occlusion patterns are ignored in LiDAR point clouds. Ref. [156] developed work based on their recognized weakness and launched the first black box spoofing attack, which regularly achieves a mean success rate of more than 80% on every target model. They conducted the initial defense analysis and recommended CARLO to decrease the dangers of LiDAR spoofing. When CARLO recognizes falsified data by interpreting occlusion patterns ignored as invariant physical characteristics, the average attack rate of success has dropped to 5.5 percent. At the same time, they proposed SVF as the initial step in researching a general framework for reliable LiDAR-based perception. SVF includes the hitherto disregarded physical factors in end-to-end learning. SVF lowers the mean attack rate of success to around 2.3 percent.

In ref. [157], the authors examined camera–LiDAR fusion in the context of AV defense against LiDAR spoofing attacks. According to recent research, LiDAR-only perception is susceptible to LiDAR spoofing assaults, but they also showed that camera-LiDAR fusion is unaffected by these attacks. They devised a brand-new, context-aware technique called the "frustum attack" and demonstrated how all eight of the most popular perception algorithms have been developed for three LiDAR-only designs as well as three camera-LiDAR designs (Light Detection and Ranging) fusion architectures are notably vulnerable to it [158]. Additionally, they showed that the frustum attack respects consistency between camera and LiDAR semantics, making it undetectable to conventional defenses against LiDAR spoofing. Last but not least, they demonstrated how the frustum attack might be used repeatedly over time to create covert longitudinal attack sequences that would compromise the tracking module and negatively affect end-to-end autonomous vehicle control.

One area of extensive exploration involves estimating the sideslip angle of autonomous vehicles using a consensus Kalman filter. By synthesizing the kinematics and dynamics of the vehicle, this approach aims to collaboratively refine localization estimates from different sensors, leading to a more robust and accurate determination of the sideslip angle. Additionally, researchers have delved into considering signal measurement characteristics in automated vehicle sideslip angle estimation. This involves accounting for the idiosyncrasies and limitations of individual sensors to achieve more accurate fusion and localization outcomes. Integrating inertial measurement units (IMUs) and global navigation satellite systems (GNSS) with heading alignment has garnered significant attention. This fusion enhances sideslip angle estimation by combining high-frequency data from IMUs with the global positioning data from GNSS. At the same time, careful heading alignment ensures precise localization even in challenging environments. Parallel adaptive Kalman filters have been proposed to aid IMU-based sideslip angle and attitude estimation. This allows the system to dynamically adjust filtering parameters for optimal accuracy in varying conditions. Moreover, research efforts have been directed toward mitigating IMU yaw misalignment by fusing information from various sensors within the vehicle, enhancing the overall accuracy of sideslip angle estimation. An intriguing avenue explored involves single antenna GNSS/IMU fusion with observability analysis. This approach combines data from a single GNSS antenna and an IMU while assessing the system's observability, ensuring that the fused estimates reflect the vehicle's true state.

5.1.4. Attacks against Cameras

Cameras are used for lane departure warnings, traffic sign recognition, and backward cameras for parking assistance [159]. Short-range radars (SRR) detect blind spots and provide Cross-traffic cautions [154,160]. Given its role in visual perception and translation of video into digital signals for the vehicles' computer systems, the camera is an important component of the AV operational systems. The cameras have a variety of functions in the AV systems' operations. First, they are helpful for vehicle object tracking and traffic light detection. It is also obvious that the numerous applications and uses of AV systems directly reflect the various types of system threats. For instance, to ensure that the vehicles read and identify the incorrect information, adversaries can intercept the data and light patterns for traffic signals [148,161,162].

The cameras locate obstacles, headlights, and traffic signs, among other things. They could also be applied. Cameras will be partially blocked by high-beam headlights or by the headlamps of automobiles in the opposite direction. Security issues like false or object detection may result from this [163]. The camera contains additional oxide-based (CMOS) sensors that blow up due to the intense beams. According to an article in the MIT Technology Review, the Google Autonomous Car is vulnerable to this issue, in which low light causes the camera to become blind. Recent terrible events at Tesla demonstrate that neither the car nor the driver noticed a white bottle against a well-lit sky. This is a serious issue. This raises the question of whether a CAV's powerful, brilliant lights will raise concerns about the vehicle's safety. Furthermore, a natural occurrence that disturbs the lighting conditions for camera systems due to environmental instability may occur.

Ref. [164] demonstrates the effectiveness of using multiple light sources to blind a commercially available camera system, the MobilEye C2-270. It demonstrates that using a laser or LED matrix may cause the camera to go blind. Authors in [164] demonstrated that an attacker may repeatedly turn the light ON and OFF in a lab setting to trick the camera. Infrared light aspects were studied by [153] in 2021, who also developed the ICSL Attack. This novel security risk can affect how an autonomous vehicle perceives its environment and result in SLAM errors. They discovered that invisible IR lights could properly trigger the sensor compared to human sight. In addition, the infrared light in the camera appears magenta, which activates several visible light-sensitive pixels and can be used to identify crucial locations for the autonomous vehicle's SLAM process.

They investigated how to generate invisible traffic lights by utilizing these properties and made fictitious invisible objects. The in-car user experience was ruined, and SLAM faults were added to the AV. They carried out the ICSL Attack using readily available IR light sources, and under various conditions, the Tesla Model 3 and an enterprise-level self-driving platform were tested. They verified the performance of the ICSL Attack and the fact that the self-driving vehicle industry has not yet been considered, creating significant security risks [165]. By analyzing the unique characteristics of the IR light, they offered a detection module based on software to protect the autonomous vehicle from the ICSL Attack.

5.1.5. Attacks against GPS

The primary purpose of satellite systems is to give cars access to time and location recognition. Different software and techniques have been created to improve the ability of gadgets to know their location and time. The global positioning system is a typical example of such a system (GPS). Coded data and signals transmit GPS data and information from the device to the satellites. The data being shared are frequently not encrypted. To safeguard communications, the GPS systems utilize their codes [166]. The ability to decode and comprehend the data communicated in the devices is only available to authorized entities. The performance of the transmission systems has been improved in the present satellite systems, but enhancements have also been made to the security measures used throughout the communication channels. Several strategies are now in use to properly supply the location and time codes for the devices, in this case, the vehicles, and to supplement and

manage the GPS data. These systems frequently employ three fundamental strategies and methods. First, satellite-based technology is frequently employed in aircraft, namely in the landing procedures and processes [167].

A few satellites and additional ground-based stations are used in the techniques. These satellite-based methods only work in select places and regions. The earth's satellites that control these communications circle the planet, typically located about 20,000 km above its surface. Because of their placement at such great altitudes, satellites are susceptible to various impacts and influences [168]. The contact of the satellites with the powerful radiation and rays of the sun, which affect the satellites' ability to transmit signals, is one of the natural ways they are impacted. Precise timing is necessary for the satellites to function properly and assign positions and times. When a signal transmission is compromised, the AVs' ability to calculate time and distance also be negatively impacted. The GPS gives absolute position data with an accuracy of one meter. This is difficult, though, because there are so many recognized problems with GPS and ways that the technology is hampered [169]. These shortcomings are frequently overcome by using more satellites to provide wider coverage. Although GPS is a widely used standard, military devices employ encrypted communications. GPS is common, yet rogue signals are simple because of the system's clear deception and blocking mechanisms.

The broadcast of false GPS messages, even though they are true and legitimate, to deceive GPS recipients is a very intricate part of the GPS spoofing mechanism. For instance, a spoofing attack starts by delivering signals consistent with the signals the target recipient sees. Then, the faked signals' strength is increased while their direction is gradually altered. In a perfect world, GPS devices would always be programmed to use the strongest signal, making them significantly more dependable. Theoretically, this method is rather simple due to the hardware constraints needed to generate realistic signals. The secondary satellite navigation network can withstand jamming attempts only if the invaders do not talk at different frequencies. Their transfer techniques are the same, and they regularly employ different frequencies. Since an attacker must spoof numerous systems, making the attack more challenging, various measurement mechanisms are even more crucial.

Ref. [170] demonstrated how to safeguard the platooning of autonomous cars in the event of an attack on an unidentified vehicle in the presence of bounded system uncertainties. A malicious attacker could freely modify the position and speed of the targeted vehicle's GPS data. First, two detectors are suggested to identify which car is being attacked using relative measures (camera or radar) and the data-driven local innovation by neighboring automobiles. Then, utilizing the saturation method and the detector data, the measurement innovation was used to produce that each vehicle has an observer from the local state [170]. Based on the observer's estimates of the neighboring cars' states, a distributed controller is also recommended to accomplish agreement on automotive speed and maintain the predetermined desired separation between them. In some cases, the observer's estimate error and the controller's platooning error were demonstrated to be exponential upper bounding.

5.1.6. In-Vehicle Protocol Attacks

The in-vehicle protocols, such as "CAN, LIN, and FlexRay", have aroused much interest from attackers. Particularly, the CAN bus security study has drawn a lot of interest. Recent research works have shown that numerous assaults, including spoofing and denial-of-service (DoS) attacks, have been created in opposition to in-vehicle protocols. We thoroughly examine and present these attacks against the CAN, LIN, and FlexRay protocols.

5.1.7. Controller Area Network (CAN) Protocol Attack

When onboard electronic gadgets proliferated, when did CAN protocol become the standard form of communication for cars? The benefits of the CAN bus, including its many masters, low cost, and high transmit rate, are well known. However, the CAN protocol was not created with security in mind initially, making it susceptible to attacks, like inserting

bogus messages into the CAN bus. Any implementation of the CAN protocol will have a variety of intrinsic flaws [171]. These are the top five security risks that the CAN protocol poses: Because CAN packets logically and physically send messages to every node, a suspicious network component can easily eavesdrop on all conversations or send data to any node. CARSHARK uses this trait to enable us to watch, reverse-engineer, and inject new packets to cause different actions. Denial-of-service attacks can be very damaging to the CAN protocol. CAN's method of priority-based arbitration permits a node to establish a "dominant" position indefinitely on the bus and force every other CAN node to retreat, in addition to direct packet flooding assaults [172]. While most controllers incorporate logic to prevent unintentionally disrupting the network in this manner, adversarial-controlled hardware would not be required to take such safety measures.

Because CAN packets lack source identity fields and authenticator fields, any component can transmit a packet to another without being able to tell it apart. Because the elements themselves do not offer defences, any vulnerable element can be used to control all of the bus's other components [172].

5.1.8. Local Interconnect Network Protocol (LIN) Attack

The LIN bus is a serial communications technology inexpensively designed to work with the CAN bus. The LIN bus, such as doors and seats, is frequently used for vehicle body control. High-speed cars are in great danger of security breaches due to the LIN bus attack, even if it is not as serious as the CAN bus assault. Authors in [173] focused on the LIN bus, a cheap data bus created to connect the growing number of auxiliary devices and sensors that are not needed for safety. Given the need to make cars safer, the sensors will most likely impact the vehicle's decision to adopt automatic safety changes. This analysis shows that, in line with the LIN bus's cost-effective design objectives, it costs less and is less protected than existing vehicular data buses. Certain compromised LIN systems may cause the driver to become extremely irritated or affect the vehicle's capacity to help the driver (e.g., radar sensors). Even though the LIN bus and CAN bus are quite similar, the LIN bus has a lower entry barrier for low-level LIN communications interruption. The LIN bus can be used as a low-cost solution for low-impact systems in a secure vehicle bus infrastructure if properly integrated.

The LIN bus consists of master-slave nodes and is broadcast. The specified identification is only responded to by one agent node once the controller node initiates a header with the identifier (ID). Implementing a collision detection system is unnecessary because the master starts all communication. To attack the LIN bus, a flawed error-handling system is employed. The regular sender node in the LIN error-handling system halts the packet transport when the collision is discovered. It allows malicious nodes to send a fake message instead of a genuine one [174].

5.1.9. Attacks against FlexRay

Although FlexRay is known for its innovative automotive communications technologies, CAN and LIN buses are still used. All requirements for data communication, including low prices and high data rates, high levels of stability, and adaptability, are met. FlexRay is a time-triggered protocol [171]. It uses TDMA (time-division multiple access) to accomplish real-time redundant communication and prevent bus congestion. Like the CAN bus, confidentiality and authentication measures are lacking on the FlexRay bus. As a result, the attacker's read and spoof operations are simple.

5.1.10. Voice Controllable Systems (VCS) Attack

According to [175], controllable voice systems have matured and developed more quickly due to AV developments. Until completely automated driving automobiles are available, intelligent speech interfaces will remain the preferred means of human-vehicle contact. According to recent research, intelligent systems of this type are susceptible to covert voice commands that are hard for people to interpret or go unnoticed. In particular,

an adversary can take control of autonomous vehicles using covert oral orders. For instance, hostile voice commands cloaked in the sound of online shared videos can covertly control the vehicle when viewed in a car. Authors in [175] examined the possible harm covert voice commands could do to the VCS of autonomous vehicles before discussing workable defense tactics. They ultimately suggested a general defense method based on pop noise that may withstand varied attacks.

The working of VCS can be seen in Figure 8. It consists of 3 phases: voice capture, speech recognition, and command execution. Attacks using hidden voice commands employ various methods. Still, they all aim to combine acoustic signals to cause a VCS to silently carry out malicious speech commands while ensuring the user cannot hear or recognize them. The three primary stages of a traditional VCS are voice capture, command execution, and speech recognition. Speech recognition pre-processes the unprocessed digital speech signals and recognizes commands using machine learning techniques. Voice capture records a human voice using a microphone and converts it to digital speech signals (e.g., the neural network). Depending on the target stages, the current audio adversarial situations and commands that are not audible are two types of attacks (attacking the voice capture stage) (and attacking the speech recognition stage).

The authors of [174] presented the Dolphin Attack in 2019, which takes advantage of the hardware characteristics of the audio circuitry to introduce covert speech commands that are invisible to humans. A UHF carrier, commonly called an ultrasonic carrier, is used in Dolphin Attack to modulate the ordinary speech signal, which is frequently in the low-frequency region. By doing this, the voice commands are guaranteed to be undetectable. As a result, amplitude modulation is used to take advantage of the MEMS microphones' nonlinear ability to down-convert high-frequency signals to lower-frequency signals. Thus, the nonlinear microphone can recover the desired voice control signal with a correctly prepared input signal. Although it works on most major voice recognition systems, Dolphin Attack must be close to the target devices; for example, it can be launched up to 5 feet away from an Amazon Echo. This is so that the higher frequencies may be played while the speaker's non-linearity can also generate lower audio frequencies. As a result, Dolphin Attack must be used at low power, which limits the attack's range. Authors in [176], developed LipRead, an inaudible assault system, to increase the scope of a successful breach. The authors employ several speakers to address the paradox of inaudibility and extended range. A single speaker can only "leak" a small portion of low-frequency information. By addressing the min-max optimization problem, the aggregate data leakage could be kept below the curve of human auditory response. The maximum attack distance is increased to 8m using this methodology.

The researchers also suggest viable defense measures against such attacks by locating non-linearity traces, a characteristic frequently preserved in signals with disguised voice commands [177]. Despite its effectiveness and inventiveness, both Dolphin Attacks demand that the attack devices transmit ultrasonic signals; therefore, the foe must carry an especially made device. The intended victim may still see the transmitter that emits unique signals as the inaudible voice command attack range is still limited. This constraint hampers the viability of concealed voice command attacks.

5.1.11. Immobilizer Attack

The vulnerability of a vehicle immobilizer (key) predominantly employed by original equipment and car manufacturers was described by [178]. They first extracted encryption keys and methods from the immobilizer. Next, a remote control signal from a VW Group car was sent using the found key, and the signal was intercepted to grant unauthorized access to the vehicle. With four to eight rolling codes and a quick calculation time, this attack can replicate the remote control key and extract the encryption key. This study's findings impacted Millions of vehicles worldwide, today regarded as a crucial element of physical vehicle security. The typical anti-theft device is known as an electronic auto immobilizer. Electronic security prevents the automobile engine from starting to the key

fob, also referred to as a transponder or a physical security token. In recent years, it has been shown that several regularly used transponders in the automotive immobilizer industry are vulnerable. The strengths and limitations of several strategies are shown in Table 13.

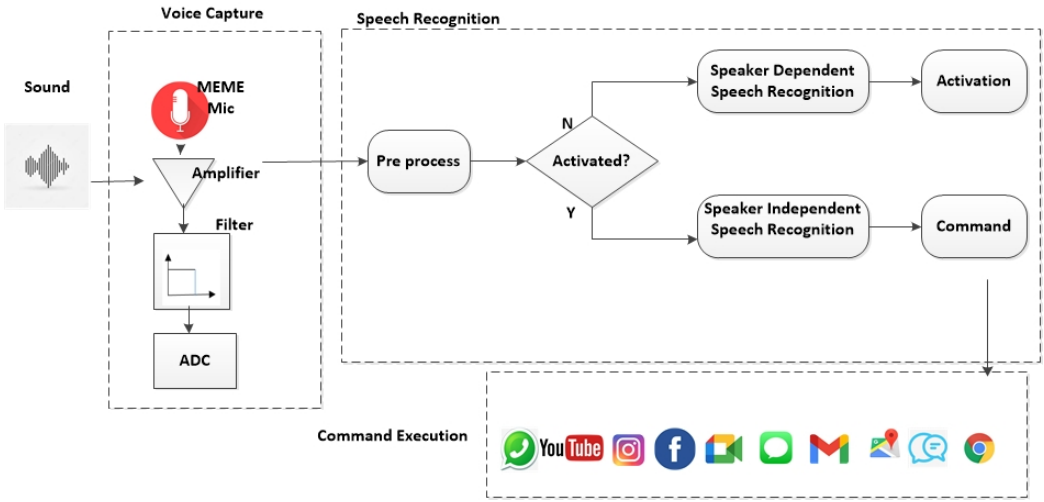

Figure 8. Voice Controllable system.

In Table 13, targets have been discussed with their vulnerabilities and security schemes. Starting the system by passive keyless entry is the first target that can be performed passively and in fake proximity, but the LF RFID Tag scheme can eradicate it. The attack that the aforesaid vulnerability can cause is the Replay attack [179]. Among these, Hitag2 and Megamos are broken due to flaws in the cipher designs, such as the absence of a PRG and the cipher's internal states being too brief with the private key. The Hitag2 cryptographic method has flaws, and three crypt-analytic techniques are suggested to recover the private keying information. The first attack is successful in reading the identification of the transponder and recovering the keystream by taking advantage of the cipher's malleability and the absence of a high-quality PRG. The second, more general attack can defeat the general-purpose encryption designed by LFSRs. Despite being used to surpass the security token's read protection mechanism, the private keying materials can be retrieved quickly and effectively. Utilizing the crucial discovery that there is interdependence between several authentication sessions with the car's immobilizer, the final assault attempt is made. These dependencies can be utilized to obtain the materials for private keying similarly to the second method, albeit much more slowly (of the order of minutes).

Table 13. Target and their Vulnerabilities.

Target	Vulnerability in Target	Security Scheme	Consequences
Starting system by passive key-less entry	Passive, fake proximity	LF RFID Tag	Relay attack
Hitag2	Lack of pseudorandom number generators	48bit linear feedback shift registers and non-linear filter	Key recovery attack
Security Protocol Stack	Key storage	Advanced Encryption Standard	Fault injection attack
Megamos	Invertabilty, Lack of pseudo-random number generators	PIN code and a 96-bit secret key	Key recovery attack
Digital Signature System	secret key is too short	Challenge response protocol	Relay attack

Starting the system with the Digital Signature System is the last target that can be performed when the secret key is too short, but the challenge-response protocol can eradicate it. The attack that can be caused by the vulnerability above is the Relay attack [180].

The first attack uses two brand-new observations in addition to the previously known vulnerabilities to access the materials for private keying: (1) The successor cipher state may be invertible, and (2) The multi-factor authentication procedure's latter stages reveal some plaintext. The private keying materials are only extracted in the second attack, which takes place in a half-hour, using the default PIN code, which is well known. In addition, the retrieval time of secret keys is reduced from days to hours to minutes to seconds by using a time-memory trade-off (TMTO) in both assaults. An open protocol stack was advised for the car immobilizer system's security. It manages the authentication process and employs pre-configured AES encryption. Each of the three duplicates of the secret key is used for key fob authentication, Boosting the availability and reliability of the immobilizer system. All three secret keys are utilized one at a time for key fob authentication, increasing the reliability and availability of the immobilizer system. However, the attacker can test the remaining secret key component while changing some data at the first secret key's physical address through fault injections.

However, fault injections allow the attacker to experiment with the remaining secret key while altering some data at the first secret key's physical address. By regularly executing fault injection and making educated guesses, the adversary can acquire the whole secret key by diligently searching using the other two private keys [178].

5.1.12. Key-Less Entry Systems Attack

While the vehicle immobilizer system concentrates more on starting the motor, attacks on keyless entry systems primarily aim to break inside the car. The entrance method guarantees the safety of the contents inside the car [181]. Thanks to technical development, there are presently three car keys: Options include conventional physical keys, remote active key-less entry, and remote passive key-less entry and start (PKES). The only functions of the original physical keys were to unlock a door and start an engine manually. The key must be inserted into the lock hole because there is no electrical connection between it and the car. The remote active keyless entry system is housed in a key fob. Interactions between the key fob user and the entry system are referred to as "active". Figure 9 shows the attacks against the keyless entry system. Details of the attacks are provided in the ensuing paragraphs.

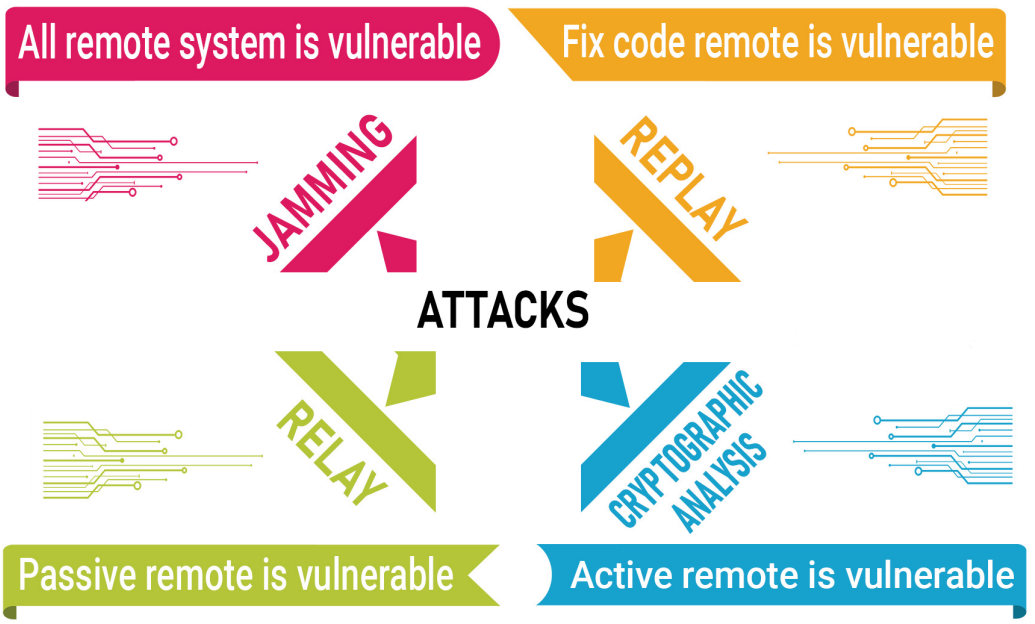

Figure 9. Attacks Against Key-less Entry System.

5.1.13. Jamming Attacks

When the user closes the door, there is a potential that the adversary will jam the signal because the wireless connection between the key and the car occurs throughout the opening or shutting procedure. The attacker can create an interference signal to jam the locking signal when the user pushes the "close" button. Unaware that the door is still unlocked, the user exits to allow the intruder to enter. The news has covered this technique. The jamming technique technically qualifies as deliberate electromagnetic interference. Authors in [182] carry out a detailed robustness study against interference through a series of experiments about systems with keyless entry. According to their experiment setting, the key fob is 2 m away from the car, and continuous-wave interference with the range from 420 up to 460 MHz is generated to test the robustness of the original signals. Results show that the two keyless systems in their experiment are sensitive to interference with a bandwidth of 5 and 4 MHz, respectively. The interference can be generated at a distance of 100 m, which provides convenience for attackers. Furthermore, the jamming attack requires no cryptographic or chip analysis, making it easy and cheap to launch.

A series of experiments involving devices with key-less entry [178], conducted a thorough robustness assessment against interference. The key fob is 2 m distant from the vehicle in their experiment setting, and continuous-wave interference with a frequency range of 420 to 460 MHz is generated to assess the resilience of the original signals. According to the results of their experiment, the two keyless systems are susceptible to interference with a bandwidth of 5 and 4 MHz, respectively. Interference can be produced at a distance of 100 m, which is convenient for attackers. Additionally, the jamming assault is simple and inexpensive to launch because it does not need any chip or cryptographic analysis.

5.1.14. Replay Attack

Replay attacks usually involve a burglar recording and listening in on the signal exchange between a common key transponder and a corresponding receiver on the car. The attacker can unlock the door using the captured signal for an unattended car. However, most contemporary car models are resistant to this kind of assault since the rolling code for the key fob has been implemented. As explained, the rolling code keeps track of a total number, and the encrypted code changes each time the button is pressed, preventing an attacker from quickly deciphering the code and replaying it [169]. However, replay attacks could be paired with other kinds of blows.

For example, the burglar might jam the system, record the proper "close" code, and then repeat it after the break-in; at this point, the car would be securely locked. Additionally, until she hears the desired signal, the attacker can keep listening in, jamming, and capturing the legal transmissions. For instance, the owner might opt to leave if she feels impatient after repeatedly attempting to unlock the door. The attacker can unlock the car by writing down the most recent valid "open" code.

5.1.15. Relay Attack

In communication networks, relay attacks are common and have drawn much attention. A relay assault can overcome the communication system's distance restriction by placing equipment between the signal transmitter and receiver and relaying the signals. About our subject, the remote PKES system enables the car owner to unlock the car without looking for a key, which is practical yet vulnerable to relay attacks. In a PKES system, remember that the door will passively open when the key is close to the vehicle, for example, within 2 m. Additionally, the vehicle's engine starts when the receiver detects the key is inside, enabling the driver to depress the accelerator and accelerate.

However, the protocol only uses communication signals and does not rely on the key. When an attacker places one antenna close to the car door and another antenna close to the car owner, the PKES system is susceptible to a relay assault. The antennae can transmit signals because of this. The challenge-response protocol can still be carried out even if there is not a close enough physical distance between the key and the door to finish it,

thanks to signals from the key sent by the antennae to the receiver in the car. According to their research, the attack can be practically effective even if the key-side antenna is up to 3000 km away from the key. It is only effective within 8 m of the key (in the best case). The authors offer a typical scenario in which, for example, the car owner leaves the parked car in the parking lot, frequently hiding it from view and leaving it unattended. While the first attacker tries to move the car-side antenna close to the door, the second attacker, who possesses the key-side antenna, can follow the owner [150]. In this way, the key fob, which is with the owner but apart from the automobile, can establish relayed communication with the parked car. It is possible that the key and the car can interact as if they were nearby. Since a relay attack does not need the interpretation or modification of signals, cryptographic authentication is useless in these circumstances.

Replay attacks, which gather measurement signals and then replay them to the system, can have severe effects since they modify messages [183]. They have only been used with linear time-invariant (LTI) systems. Dynamic watermarking techniques have begun to address the problem of identifying these attacks, which inject a private excitation into control inputs to safeguard subsequent measurement signals. LTI models may be sufficient for some applications, but other CPS, like autonomous vehicles, require more intricate models. A linear time-varying (LTV) adaptation of prior dynamic watermarking approaches was developed by [184] by including a matrix normalization component to consider temporal changes in the system. Real-world system considerations are included with the offer of implementable tests. The proposed strategy is then shown to be capable of detecting generalized replay assaults both in theory and in simulation using an LTV vehicle model. Replay attack detection in autonomous vehicles is a challenge addressed in [183].

Due to the significant presence of nonlinearities, conventional approaches based on linear dynamics approximations would not be successful. As a result, the proposed solution is based on a bank of QPV (quadratic parameter variable) observers specifically designed to resist replay attempts that target a single sensor channel. This feature permits the development of a decision algorithm whose effectiveness is assessed using simulation results. It has been shown that, with some slight approximations, the dynamics of the vehicle tracking error may be reshaped into a quadratic parameter varying (QPV) form, allowing QPV observers to be used to enforce the estimate error's convergence to zero in the attack-less scenario. On the other hand, one of the observers will demonstrate the necessary quality that only one of the components of its observed estimation error will be altered by the replay assault when the system is attacked. This feature has led to developing a mechanism for identifying the presence and localization of replay assaults. Results from simulations have validated the algorithm's effectiveness.

5.1.16. Cryptographic Analysis Attack

The attacks mentioned earlier only concentrate on communication at the physical layer and ignore signal analysis. A new attack uses cryptographic analysis to target higher-level coding and encryption methods. The remote keyless program's earlier iterative process lacked an authentication scheme. There is no use of encryption, and the code has been updated. Authentication is made possible through rolling code techniques that are useful in thwarting even the most elementary replay assault. It has been proven that attacks using side channels and cryptographic analysis can compromise cryptographic algorithms.

In addition to the fundamental defect in the cryptographic protocol, intruders may examine printed circuit boards in entry systems to steal the information in the firmware. A thorough examination of the widely used remote control systems for the VW Group is conducted, and the adversary can clone a targeted remote control and then gain access to the vehicle by analyzing the cryptography used in the schemes and listening in on the victim's signals [185]. The majority of remote control systems use a single master key, which creates a vulnerability that is exploited by the attack. The intruder could determine the codes' structures, the intricacies of the cryptographic techniques, or even the encryption key if she acquires the PCBs and thoroughly reads the firmware. The attacker can then

use the widely-used master key to intercept and decrypt the victim's signal to retrieve the counter. The authors also advise going after Hitag2. A correlation attack can quickly locate the secret key.

5.2. Attacks Management

5.2.1. Defence Approaches for Sensors

This section details various proposed countermeasures for sensor attacks, with a detailed discussion of defense strategies shared below.

- **GPS:** To prevent GPS-targeted attacks, a variety of defenses have been deployed. For instance, the false signals differ visually from those transmitted by satellites. Attacks that consider the signal's power, the time between broadcasts, and the signal clock information could be detected using this method [168]. Ref. [186] utilized the receiver's correlation function distortions to evaluate the GPS signal's accuracy. Investigate the direction of arrival (DoA), which uses an antenna array to thwart attacks because the DoA of GPS signals would disclose a different carry phase than spoofing signals. Other methods use GPS broadcasts to embed cryptographic algorithms for assault defense. Encrypt GPS L1 P(Y) code to see if a spoofing attempt is being made. Authors in [187] recommended adopting methods like navigation message authentication (NMA), which integrates a signature into the satellite broadcast, to ensure the signals are authentic. Instead, research from other areas could be combined to attain protection, as with the distance-bounding protocol. They use computer vision or cryptography tools to measure and verify the distance between entities by comparing nearby buildings and road signs.
- **LiDAR:** Changing the way LiDAR transmits and receives light is one possible technique. If the adversary intends to carry out the attack effectively, they must coordinate the false laser with the LiDAR laser. Defensive strategies for LiDAR have been shown in Figure 10. The LiDAR laser can prevent an assailant by repeatedly firing laser pulses in one direction, say three times. As LiDAR can only receive lasers from a fixed angle while rotating, limiting the impact of attacks by reducing the receiving angle is possible; however, doing so also lowers LiDAR's sensitivity. Another defense is to shorten the LiDAR receiving time, shortening the LiDAR probe's range. LiDAR determines the reception period it receives incoming lasers to ensure assurance. It is possible to invalidate lasers reflected off of additional objects while also making it difficult for attackers to begin attacks by, in particular, reducing the reception time. While using LiDAR, randomness can also be introduced. LiDAR is designed to rotate randomly and create lasers in any direction to ward off threats since it spins the transceiver to scan the area. Making the laser from a LiDAR is less predictable than producing random signals or signals with random pulse intervals, another effective defense against a hacker [154]. Last but not least, redundant or multi-sensory LiDARs allow autonomous vehicles to modify LiDAR results(s). As a result, the attacks grow more costly and sophisticated, and clients pay more to install new devices. Furthermore, there will not be any overlap when the attack is launched.
- **Camera:** Due to the camera's vulnerability brought on by its optical characteristics, it is challenging to design a completely secure camera. Redundancy, for some threats, photochromic lenses and removable near-infrared cut filters may be sufficient [4], despite any potential weaknesses or new problems they may create.
- **Ultrasonic sensors:** The first technique allows for the authentication of physical signals by utilizing the idea of changing waveform properties. The second method uses two or more sensors to identify attackers, regain the ability to recognize obstacles and identify attacks [188].

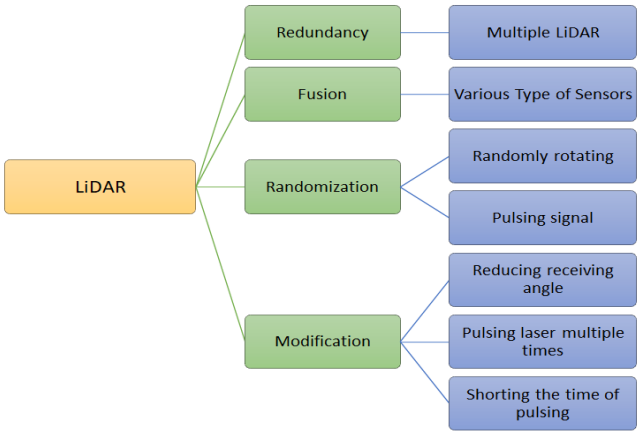

Figure 10. Defense Approaches of Attacks Against Sensors.

5.2.2. Defence Approaches for In-Vehicle Systems

The simplest method to thwart the jamming attack is to demand that the car owner double-check that the door is locked before driving away. Light or sound may be employed to verify that an automobile is correctly locked. However, the defense is only effective against assaults that use jamming alone. The remote confirmation method is useless if the intruder can replay the "unlock" signal; the door might lock properly. Therefore, the most basic form of defense is to lock the doors before exiting the vehicle. The quickest way to stop a relay assault is to shield the key when unused. The antenna on the side of the key cannot receive or transmit the signal from the key fob if the key is enclosed in a box. The passive remote keyless system's most attractive feature is disabled because using this method of entry requires the user to take their key out, which is inconvenient for them [175]. A comparable preventive measure that stops the key from sending and receiving signals is removing the battery from the key. Additionally, the functionality of PKES is impacted by this strategy.

Distance bounding can be used to defend against the Relay attack. A distance-bounding approach uses quick message exchanges to confirm the distance between the participants. The door will not automatically open until the claim is confirmed the separation between the key fob and the vehicle. Numerous keyless entry systems and car immobilizer attacks make an effort to compromise the cryptographic protocols. Enhancing the authentication process is one option. Therefore, emerging remote keyless entry (RKE) processes should employ a more protected key distribution and cryptographic algorithm scheme.

5.2.3. Defence Approaches for In-Vehicle Protocols

Encrypting data during transmission is one of the key methods for enhancing the safety of bus communications. Asymmetric and asymmetric encryption-based communication systems for automobiles should be used with cryptographic approaches to ensure excellent performance and adequate security [158]. Stop code tampering and data sniffing by using methods like encryption and obfuscation. Proper and economic protection from reverse engineering is obfuscation. To successfully encrypt the data link between both the external memory and the ECU's internal memory, additionally, on-the-fly decryption is used. Finally, encrypting and authenticating data with AES-128 combined with keyed hash MAC could decrease the bus load. To enhance bandwidth efficiency and decrease authentication delay, it is suggested that a vote-based approach be used in conjunction with time-triggered authentication. This technique reduces the probability of a per-packet counterfeit by using a unanimous vote among a group of nodes to evaluate the message's merit and validity. Instead of performing it separately for each node, use the lightweight broadcast authentication protocol, which shares the shared secret for authentication between two sets

of nodes. There is a very small percentage of compromised nodes. Thus, it makes sense to presume that [165].

Automotive Open System Architecture is a consideration for MAC. Attackers cannot send unauthorized CAN signals because they lack the authentication key. The MAC assault, however, is utilized. The error frame transmission can also be used to halt unauthorized CAN messages. The fundamental notion is that if a node discovers any unauthorized messages, it should immediately send an error frame to replace them. and prevent the receiving node from receiving them. Gateway is a well-liked and trustworthy type of defense, the system's motor bus entrance. A backbone-based architecture has now replaced the central gateway-based architecture of the in-vehicle system. The gateway handles error protection, message verification, and protocol conversion in addition to carrying the message from numerous ECUs [167]. It acts as the vehicle's communication interface. Since the gateway also includes a firewall mechanism, gaining access to the bus via attack surfaces on moving vehicles is more difficult. For instance, The OBD-II connector cannot be used to inject the attack message into the in-vehicle bus straightforwardly. Data transfer between low-speed and high-speed buses can be managed by the gateway.

5.3. Traditional Security Devices

The research on how human drivers might react to cyberattacks on autonomous vehicles carried out in a driving simulator sheds light on the difficulties and dangers that may arise from using these vehicles. The participant's ability to continue driving and regain control of the car while being attacked by cybercriminals was evaluated throughout the experiment. In addition, the participants' situational awareness during a cyberattack was assessed to demonstrate the seriousness of this kind of risk to autonomous vehicles. Similarly, the findings of prior studies on cyberattacks against autonomous vehicles were validated by this research. The participant's reactions to potential cyberattacks on the vehicle and the infrastructure were evaluated, and specific cyberattacks that could occur on currently available vehicle technology were identified. In a nutshell, the study produced knowledge that will be helpful regarding the construction of cybersecurity systems for autonomous vehicles [189].

In the context of the 5G IoV, many proposed security solutions will be the most effective remedies against the assaults that could be launched. Some strategies are successful, while others are not. Even though the suggested approaches have a high success rate, the effort required to implement them can be a significant obstacle to their widespread application. Despite this, the ecosystem for 5G IoV still requires these security solutions because of their reliability in protecting against cyberattacks [190,191].

Operations research on autonomous driving and decision support systems gains significant knowledge from this research [192]. Increasing the highly automated car market raises three significant issues. Weather, traffic, cybersecurity concerns, and the ADS' human aspect all contribute to these issues. Second, the study emphasizes the human factor when automated and human-driven cars interact. MV and ADS drivers' skills and preferences affect transportation network efficiency. The ADS needs cognition to handle driving modes and interact with all relevant parties. Finally, this research acknowledges ADS technology's revolutionary nature and role in addressing ethical issues. This research emphasizes the significance of fast regulatory policy decisions by key authorities to manage autonomous vehicle certification, insurance, and liability issues, which are complex by technology, regulation, law, and society [193].

This research increases in-vehicle communication cyber security in several ways. Second, it provides an in-car communication network infrastructure for all elements and interfaces [194]. Second, the study categorizes in-vehicle communication protocols by features and applications. Lastly, the study evaluates port-centric and machine learning-based in-vehicle communication security solutions [195]. This article explains modern automotive instrument cluster (IC) features and connections. The IC's role in the bus system and ADAS data display make it important to modern automobiles. This page

discusses IC assaults in cars, including manipulating the speedometer and fuel gauge. A risk assessment that considers security, cost, and operational interruption evaluates the potential impact and complexity of such IC attacks [35]. The research provides a framework for modeling autonomous vehicle behavior at industry standards. Yet, the research suggests approaches to enhance and realistically improve future platforms. The paper suggests two ways to improve image-based visual servo, including making it more robust. Reinforcement learning, which uses trial and error to determine the best car behavior, might also be used on miniature autonomous vehicle models. The paper also discusses 5G wireless communication and LiDAR's potential for modeling self-driving cars on a modest scale [196].

5.4. Threat Modeling Approaches

The authors modeled the hostile environment by using SPICE to observe how the transmission line and the parasitic capacitance of the FETs in the transceiver affected the signal. Their goal was to determine whether or not these factors affected the signal. After performing a detailed schematic analysis, the CAN transceivers were modeled with the help of realistic channel and n-channel MOSFETs [197]. The two most important contributions this study makes are an adaptation of the TMT that makes it applicable to automotive threat modeling and a demonstration of the actual application of the approach to the identification of security threats in the control unit of a vehicle. Both of these are presented here [198]. Electronic Control Units (ECUs), sensors, and inter-vehicle communications were the primary areas of concentration for the authors of the article as they offered an in-depth analysis of these components in relation to autonomous vehicles. They categorized ECUs according to the significance of their roles and provided an overview of the numerous sensor technologies utilized in autonomous vehicles. The authors also discussed the many channels through which self-driving vehicles can communicate with one another, such as the Internet stack and the VANET stack [199].

Attacks on and defenses against autonomous cars are organized by time period to show technology evolution. An overview of 15 research papers from 2008 to 1029 on autonomous vehicle assaults and reactions is available. A full examination of autonomous vehicle attacks shows that future attacks will target vehicle-to-everything (V2X) communication technology rather than other vehicle components. Autonomous vehicle security research involves using artificial intelligence and big data to protect them [17]. The paper's authors made four significant contributions. First, they identified potential cyber risks by categorizing current cyber security risks and vulnerabilities in the environment of CAVs based on types of communication networks and attack objects. Unlike past similar efforts, this one treats cyber risk as just another threat in CAVs' natural habitat. Finally, they determined that most research in CAVs is still at the theoretical level and recommended bridging the gap between theory and practice by synthesizing existing cyber security and safety standards in the CAV environment [200]. The results of this research primarily fall into two categories. First, it performs an in-depth analysis of cyber-attacks against CAVs and AVs; then it models the most severe threats to reveal them. Second, it recreates the most serious cyber attacks to demonstrate the impact they might have on various organizations [201].

This report analyzes current research on Intelligent Automation (IA) in autonomous cars, which uses RPA and AI to enable digital transformation. AI, ML, and IoT-based autonomous automobile methods are the core topics. The extensive literature evaluation makes this paper valuable. The article discusses autonomous vehicle safety regulations, choices, and challenges [202].

5.5. Authentication Schemes

The security and integrity of the vehicle's control systems and the safety of the passengers and other road users depend on authentication techniques in autonomous vehicles. Authentication procedures ensure that only approved systems and software are operating on the vehicle to avoid unauthorized access or modifications jeopardizing the car's safety.

Autonomous vehicles are susceptible to cyberattacks, including man-in-the-middle, denial-of-service, and spoofing [203]. By confirming the vehicle's identity and the veracity of messages, authentication techniques can assist in defending against these kinds of assaults. By limiting access to the vehicle's control systems or personal data to only those permitted, biometric-based authentication schemes can be utilized to protect passengers' privacy. By enabling vehicles to confirm the identification of other vehicles and trust the information they receive, such as traffic and weather conditions, can increase road safety. To enable secure communication between vehicles and between vehicles and infrastructure, such as traffic lights, toll booths, and parking garages, authentication systems are crucial [97]. Details of various authentication techniques employed in autonomous vehicles are provided in the subsections.

5.5.1. Public Key Infrastructure (PKI) Based Schemes

These schemes use digital certificates and public key infrastructure (PKI) to authenticate cars and messages. To guarantee anonymity, [35] presented a technique for anonymous authentication that used anonymous public keys rather than just one. By doing this, the recipient is kept in the dark regarding the keys' owner. The increased revocation of malicious nodes causes the list to grow. The complexity of setting up and maintaining a PKI system, which may be expensive and time-consuming, is one of the key issues. PKI systems could also be subject to attacks that take advantage of flaws in key management or encryption techniques. Another drawback is the PKI-based schemes' inability to scale when more connected devices and systems are added to the autonomous vehicle environment. As a result, there will be more keys and certificates to handle, which could cause performance problems and key management challenges.

5.5.2. Hardware-Based Authentication

These techniques verify the car using particular hardware components like the ECU (Electronic Control Unit) or GPS [204]. To address these faults and formally demonstrate the novelty features of our innovative hardware-based approach, Ref. [205] explored approaches that had flaws that are challenging, if not impossible, to correct within the confines of their particular methodologies. Given how expensive it may be to design, produce, and distribute hardware devices, one of the key issues is the expense of establishing and maintaining hardware-based authentication. Hardware-based authentication is also susceptible to physical assaults like theft or tampering with the authentication device, which might give a hacker access to the car's systems without authorization. As replacing or upgrading the hardware components may be challenging, hardware-based authentication systems may not be adaptable enough to the rapidly changing autonomous vehicle ecosystem. This might cause issues when new features or capabilities are added.

5.5.3. BiometricBased Authentication

These systems use biometric data, like fingerprints or facial recognition, to identify the driver and occupants of the car. Authors in [206] suggested a user biometric-based and password-based two-factor authentication protocol that can work in scenarios with little or no VANET infrastructure. As mentioned earlier, the security elements of the protocol were also examined as part of a loose security study. Biometric-based authentication is susceptible to spoofing attacks, such as impersonating a user using a fake fingerprint or a picture of their face, which might give an attacker access to the car's systems without their consent. The privacy issues raised by the usage of biometric data are another drawback. These data are considered sensitive personal information, can be used to track, monitor, or identify specific people, and may be challenging to keep secure against hacks or unauthorized access.

5.5.4. Secure Boot

By confirming the integrity of the boot process, this approach ensures the authenticity of the firmware and software used by the vehicle's control systems. Autonomous vehicles use the secure boot as an authentication technique to ensure that only approved software is operating on the vehicle's computer systems. Authors in [207] achieved this by checking the software's integrity during the boot process before the operating system is loaded. This aids in preventing the installation of harmful software or firmware on the car, which can endanger its functionality or safety. A secure bootloader is used in the procedure, and it uses techniques like cryptographic hashing and digital signature verification to check the software's validity before allowing it to function. In addition to offering a high level of protection against cyberattacks, this can ensure that only software approved by the vehicle manufacturer or other trustworthy parties can run on the vehicle's systems.

Implementing and maintaining secure boot authentication can be challenging since it requires high technical know-how and regular system monitoring to ensure everything runs well. Furthermore, physical assaults, such as tampering with the vehicle's firmware or software, could allow attackers to go around the authentication process and circumvent secure boot authentication.

5.5.5. Remote Attestation

This method enables a distant third party to check the accuracy of the vehicle's control systems and find any unapproved alterations. A remote attestation system that proposes [208] is used to check the validity and integrity of an autonomous vehicle. Remote attestation ensures that the vehicle's hardware and software are working as they should and that it is not infected with malware or other dangerous software.

Critical Analysis: In the Remote attestation scheme, there is a concern of privacy invasion by providing a third party with access to the vehicle's system status, as it may reveal sensitive information about the vehicle or the user.

5.6. Over-The-Air (OTA) Updates

This solution enables wireless updates to the vehicle's control systems that are secure and authenticated. Similar to how smartphones and other connected devices receive updates, autonomous vehicles can download and install software remotely with OTA updates [209]. Bug fixes, security patches, and new features or capabilities can all be included in these upgrades. OTA updates are crucial for autonomous vehicles because they enable ongoing system maintenance and enhancement without requiring the car to be physically taken in for servicing. Additionally, in the event of a security vulnerability or other problem, OTA updates can be utilized to distribute and deploy necessary updates rapidly. Article [210] created a framework that successfully distinguishes between harmful and benign software executables. Windows and Linux operating system executables were collected to create two datasets for testing and training. They supported transfer learning by utilizing the created CNN models to identify dangerous executables created for autonomous vehicles.

The security of the OTA update process is one of the primary issues since it necessitates a safe and impenetrable way of confirming the validity and integrity of the update. It is crucial to have a strong authentication system in place since an attacker could tamper with the update and harm the user or the car. For OTA updates to function correctly, a dependable and consistent Internet connection may not be accessible in all locations or at all times.

5.7. Zero-Trust Architecture

A zero-trust architecture for AVs can provide a secure and scalable solution for the security of connected vehicles, and it can help promote the widespread adoption and deployment of these technologies. To reduce the hazards associated with conventional centralized systems, a decentralized and secure communication infrastructure for automo-

biles has been proposed in ref. [211]. The zero-trust architecture is founded on the ideas of safe data transfer and secure device management, and it is made to give car owners and passengers more security and privacy. A cryptographic protocol system enables safe communication between vehicles and between vehicles and other systems, such as secure pairing and authentication. To guarantee the validity and integrity of the software running on automobiles, they also advocate the usage of secure software updates.

Next-generation cars can benefit from zero-trust architecture's security and scalability, and it has the potential to become a pillar of connected vehicle security. In addition to helping to encourage the widespread acceptance and deployment of these technologies, the proposed design can be crucial in reducing the dangers related to autonomous vehicles and the Internet of Things [212,213].

5.7.1. Decentralized Communication

Communication between vehicles and between vehicles and external systems is decentralized and secured using cryptographic protocols, such as secure pairing and authentication. Decentralized communication also offers increased privacy and security. In a centralized communication system, all communication passes through a central authority, which creates a single point of failure and a potential target for attackers. In a P2P network, communication is distributed across multiple nodes, making it more difficult for attackers to disrupt the network or intercept communication. This can help to protect sensitive information and ensure the privacy of AV occupants.

5.7.2. Secure Device Management

Vehicles are equipped with secure software updates and device management protocols to ensure the integrity and authenticity of the software running on vehicles. To address these challenges, secure device management in AVs should be based on a defense-in-depth approach incorporating multiple security layers. This includes physical security measures such as tamper-proofing and anti-tamper mechanisms and software security measures such as code signing and secure boot. Secure communication protocols such as Transport Layer Security (TLS) should also protect communication channels between devices, as shown in Figure 11.

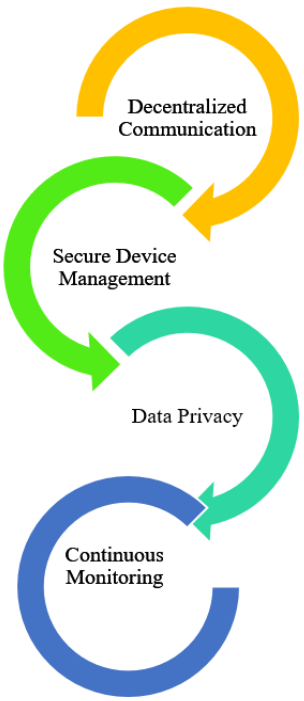

Figure 11. Zero-Trust Architecture in AVs.

5.8. Data Privacy

Personal data are collected, processed, and stored securely and privacy-preserving by data protection regulations. The system is continuously monitored for security vulnerabilities, and security patches are applied as needed to address any issues discovered [214]. It is also designed to detect and respond to real-time security threats like cyber-attacks and data breaches.

6. Forensics Approaches

This section provides a brief overview of the forensics approaches, tools used, standards involved, and challenges associated with conducting digital forensics in the context of autonomous vehicles. Digital Forensics is a rapidly developing field as a brand-new area of study. Information and communication technology (ICT) cyber security is receiving more and more attention. An information security breach necessitates using digital forensics to gather the digital evidence and determine who was responsible, what was performed maliciously, how to assess the danger that may result, and many other things. Digital forensics has been experiencing even greater challenges than the initial digital breach investigations, particularly in cases involving attacks on smart cities [215,216].

Digital forensics for autonomous vehicles involves the investigation of digital evidence related to a particular incident, such as a collision, malfunction, or cyber-attack, in an autonomous vehicle (AV) environment. AVs rely on various digital systems and components, including sensors, processors, and communication networks, which can be valuable data sources in a forensic investigation [217]. Investigators need to be aware of this environment's unique challenges and limitations when conducting digital forensics in an AV environment. The data may be distributed across multiple systems and components and may be encrypted or otherwise protected, requiring specialized tools and techniques to access and analyze it. Additionally, because AVs are designed to operate autonomously, it can be difficult to determine which specific systems or components were involved in a particular incident. This requires careful analysis and correlation of data from different sources, such as sensor data, system logs, and communication records [218]. Forensic investigators may need to access the vehicle's onboard computer systems and data storage devices to retrieve and analyze the relevant data in an autonomous vehicle incident. This can involve working with the vehicle manufacturer or other relevant parties to obtain the necessary access and tools to perform the analysis. Understanding the causes of CAV accidents and mishaps is essential to designing robust and safe CAVs. As a result, it is crucial to gather logs from various CAV artifacts and store them securely. According to theory, forensics can be performed in one of two methods. The post-marten method of looking into digital crimes is known as the reactive technique. Finding, keeping, gathering, studying, and producing a final report are vital steps in this process [219]. When conducting an investigation, an investigator may ask questions about the incident. Investigators will likely ask questions about the incident, such as when it occurred, who was involved, what happened, and what the impact was. The systems involved in the incident, how they are connected, and their function. Who had access to the systems and data involved in the incident, and what level of access they had? The logging and monitoring systems were in place during the incident and effectively captured relevant data. This will help them to identify potential sources of evidence and determine the scope of the incident [220].

This study has demonstrated that extracting, preserving, and displaying vehicular evidence data using conventional techniques and methodologies by the ACPO criteria is possible. Still, the investigator needs to be careful and diligent. The problem, as the research explains it, is that the data are changed when vehicles are removed from the incident scene, leading to an erroneous result compared to the one that would have been obtained from the point of an event. Additionally, in some circumstances, it is only possible to identify some interested parties when the evidence is extracted. An investigator's ability to perform a typical inquiry needs to be improved by the absence of witnesses, making things more challenging for first responders. In the smart city framework, this

research endeavor has looked into the current vulnerabilities of smart autonomous vehicles. Although data on networks and clouds can be trusted, a difficulty with vehicle digital data is how easily data and evidence files can be altered. The data integrity exposed to adverse and unfavorable circumstances is another issue with car ECMs' construction technique. Therefore, it is important to include safeguards against intentional and unintentional network data manipulation while designing these systems. The research suggests archiving, hashing, and encrypting this network data to prevent tampering and comparing it to trusted external sources [221].

6.1. Forensic Tools

Digital forensics in cloud computing involves the investigation of digital evidence related to a particular incident, such as a cyber-attack, data breach, or another security incident, in a cloud computing environment. In cloud computing, data and services are stored and accessed remotely, making investigations more complex and challenging. Data collection methods include using tools (like those used to track file activity), artifacts (such as virtual machine images), & logs (e.g., audit logs). Keeping the data secure is the responsibility of the storage activity, while the management activity conducts a forensics investigation and information extraction for reconstructing the incident's timeline [218]. Table 14 shows a complete summary of forensic tools. FROST is intended to provide a reliable and efficient storage solution for IaaS platforms. Its scalability, fault tolerance, and object storage model make it well-suited for cloud computing environments where data storage needs can be complex and constantly evolving [187]. Using Map Reduce in a cloud forensic analysis context can be particularly useful when dealing with large volumes of data, such as log files or network traffic data. The analysis can be performed much more quickly by processing data in parallel across multiple nodes [222].

Table 14. Tools Used for Forensics of Autonomous Vehicles.

Sr No	Tool /Model	Platform	Comments
1	FROST [223]	Open Stack Cloud Platform (IaaS)	•Gathered at the host operating system •Negating the need for cloud provider involvement in data collecting •No mechanism for Preserving the data
2	Cloud Forensic Readiness Evidence Analysis System (CFREAS) [224]	Map Reduce paradigm –Cloud-based	•Reduces the amount of time needed to analyze extensive evidence. •Handles the risk of the cloud being used to store the chain of custody and the absence of a single, centralized legal authority
3	Vehicle Data Recorders [220]	•Embedded Systems •Standalone devices •Cloud-based platform •Telemetries System	•Record various vehicle parameters such as speed, acceleration, steering, and sensor data, which can be used to recreate the events leading up to an incident. •Issues: Compromised Data •Integrity/Accessibility, Data Loss
4	Black Boxes [221]	•Magnetic Tape •Solid-state memory devices	•Specialized recorders that can capture data from the vehicle's sensors, control systems, and other components.
5	Vehicle Telemetry Systems [225]	•Embedded Systems •Standalone devices •Cloud-based platform •Telemeters System	•Collect and transmit data in real-time from various vehicle sensors, allowing investigators to track the vehicle's movements leading up to an incident.
6	Imaging Technologies [222]	Cameras	•Autonomous vehicles often use cameras and other imaging technologies to gather information about their surroundings. •Forensic tools can be used to analyze this data and recreate a visual representation of the events leading up to an incident.
7	Simulation and Reconstruction Software [3]		•These Tools allow investigators to simulate the movements and behavior of an autonomous vehicle leading up to an incident, helping to determine the cause.

As autonomous vehicles produce a significant amount of data, it is critical to have reliable forensic technologies that can assist in accident investigations and pinpoint the origin of any mishaps. Typical forensic tools for autonomous vehicles include:

6.2. Forensics Standards for Autonomous Vehicles

Autonomous, connected vehicles operate without human interaction, relying on onboard sensor computations. However, CAV decision-making could go wrong for various reasons, resulting in undesirable events. The connected autonomous driving compliance safety rules are now only possible with a solid forensic investigative framework or standard. NIST has been working to develop the framework for interoperability standards for CAVs and other intelligent transportation systems. ISO/IEC 27037 is the sole forensics standard for processing digital data. The standard outlines procedures for identifying, gathering, acquiring, and storing any digital evidence that could be crucial to a legal proceeding [3].

There currently needs to be widely accepted standards for autonomous vehicle forensics. However, several organizations and initiatives are working to develop guidelines and best practices for investigating incidents involving autonomous vehicles. The NIST has developed a research program to provide standards and best practices for automated vehicles' reliable and secure operation. The program addresses privacy, security, safety, and ethical considerations in designing and using autonomous systems. In addition, The National Highway Traffic Safety Administration (NHTSA) is a U.S. government agency responsible for regulating and enforcing safety standards for automobiles and other motor vehicles. It includes the testing and deploying of autonomous vehicles with recommendations for data recording and retention in the event of a crash. The guidelines also emphasize the importance of cooperation between the vehicle manufacturer and relevant authorities in the event of an incident. The SAE has also published standards for autonomous vehicles, including data logging and retention recommendations. The standards are intended to ensure the reliable and consistent operation of autonomous cars and to give investigators a framework for analyzing accidents involving these vehicles. As the use of autonomous vehicles continues to grow, additional standards and guidelines will likely be developed to address specific issues related to autonomous vehicle forensics. However, at this time, there are yet to be widely accepted standards for this field. The digital forensics factors are the two components of a framework created for managing DFR [226].

Digital Forensics Investigation Readiness Procedures (DFIRP) is a set of measures an organization can implement to ensure they are prepared to respond effectively to potential cyber security incidents. These procedures are given a uniform approach, which ISO/IEC 27043:2015 eventually adopted. Three phases comprise their methodology, which can be used to implement DFR in businesses: planning, implementation, and assessment [227]. There are six components in the proposed forensic-by-design paradigm for a cyber-physical system (CPS), including best practices and guiding principles for managing risks, forensics preparation, incident handling, legal requirements, specifications for CPCS, both hardware and software & industry-specific specifications [228].

6.3. Forensics Challenges in Autonomous Vehicles

Communications between vehicles, infrastructure, networks, and pedestrians are part of the dynamic ecosystem that makes up an autonomous vehicle (V2V, V2I, V2N, and V2P). It is a more challenging setting than other IoT systems because it includes mobile restrictions, a huge network scale, non-uniform node distribution, and dynamic topological structures [229]. CAVs are complex systems that hold much digital data, including sensitive personal data, which presents various challenges. Data are transferred through buses for internal communication stored in physical memory, and external network connection is saved in the cloud. Many components for communication and storage result in a need for more norms and frameworks for CAV forensics, and the complicated requirements and design of CAVs prevent the use of traditional digital forensic techniques. It is important to note that autonomous vehicle forensics is a rapidly evolving field, and technical and legal challenges may be associated with accessing and analyzing the data generated by these vehicles. However, as autonomous vehicles become increasingly widespread, the importance of autonomous vehicle forensics is likely to grow, and it will become increasingly important to develop standard practices and techniques for investigating incidents

involving these vehicles [216]. It is challenging to obtain evidence because of the variety of data sources, complexity, and quantity. A few technical challenges are listed below.

- How can we identify which information should be kept onboard the car and which should be stored on the cloud?
- What software program or architecture is suitable for collecting a large volume of online and offline data simultaneously without endangering its integrity?
- Which software and programs are suitable for collecting the data live or offline without compromising its integrity?
- What location does the internal data storage have? RAM, USB drive, EPROM, or flash memory.
- On-the-fly data collecting and analysis by CAVs may utilize a variety of processing protocols. How are these kinds of data handled?

Vehicle forensics must meet certain data quality requirements to be admitted into legal proceedings. The following are some legal concerns about CAV forensics:

- Critical evidence is invalidated if the evidence is not sealed before the files are opened.
- To comprehend their surroundings and operate effectively, CAVs must scan their surroundings; nevertheless, mapping private property may be viewed as an intrusion. Clear criteria must be established for what data CAVs can collect and maintain to protect privacy.
- For gathering digital evidence and a solid understanding of the software, hardware, and networks, specialists need to have solid expertise and specialized abilities. Therefore, technicians need extensive training in technical capabilities and legal procedures before being involved in CAV forensics.

7. Simulators

This section overviews the simulators used in developing and testing autonomous vehicles. Simulators play a crucial role in evaluating autonomous vehicle systems, providing a safe and controlled environment to test various scenarios and algorithms. The development and testing of autonomous cars rely heavily on simulators. They offer a secure and controlled environment for testing the vehicle's sensors, perception, planning, and control systems without real-world testing. This enables engineers to test and optimize the vehicle's behavior in various situations, including challenging or hazardous ones that would be difficult or impossible to test in the real world [200]. Developers can evaluate a vehicle's performance in simulations under various environmental factors, including weather, lighting, and traffic density, which might be challenging or impossible to recreate in actual testing. Simulators can also test a vehicle's performance in hypothetical locations that may or may not ever be constructed in the actual world. Simulators are crucial for testing the robustness and safety of autonomous vehicles. Before the car is tested on public roads, developers can find and address possible problems by evaluating the vehicle's behavior in various scenarios. Before the vehicle is used in the real world, this guarantees that it is secure and dependable.

7.1. CARLA

Intel Labs created the open-source CARLA (Car Learning to Act) simulator for research on autonomous vehicles. It offers a highly detailed and realistic urban environment for testing and developing autonomous vehicles and other agents like pedestrians and bicycles. The simulator has a lot of features, including:

- A sizable, intricate urban area including streets, buildings, traffic lights, and other elements typical of cities.
- Realistic lighting and weather conditions, including varying day lengths, seasons, and weather phenomena like snow, rain, and fog [230].
- Support for various sensors, including LiDAR, radar, and cameras, which may be set up to imitate various sensor kinds and noise levels.

- A scenario system that is flexible and adaptable, enabling developers to generate and test a variety of situations, including various traffic densities, driving behaviors, and weather conditions.
- A Python API that makes it simple for developers to build custom agents and behaviors and control and interact with the simulation [231].
- Support for the Open DRIVE format enables simulation developers to import actual road networks.
- Support for the Unreal Engine enables physics-based interactions between agents and realistic graphics.

7.2. Apollo

Baidu created the open-source Apollo platform for autonomous vehicles. It has various resources and technologies, including a simulator, for the research and development of autonomous vehicles. The following elements are part of the Apollo platform

- The Apollo Simulator is a physics-based, highly realistic simulator that may be used to test and create autonomous vehicle systems. It supports several sensors, including LiDAR, radar, and cameras, and contains a variety of realistic landscapes [232].
- Perception is a module collection that analyzes sensor data and identifies environmental items such as lane markers, traffic lights, and other cars.
- Planning is a collection of modules for creating plans for the vehicle's motion, such as trajectory and path planning.
- Control, A group of modules that carry out instructions and manage the vehicle's motion, including low-level steering, throttle, and braking controllers [123].
- HD Map is a high-definition map that can give the car precise information about its surroundings, such as the road's geometry, lane markings, and traffic lights.
- Cybersecurity is a collection of modules to protect autonomous vehicle systems against cyberattacks.
- Cloud-based services is a group of cloud-based services that can be used to remotely access the car and store and exchange data [36].

7.3. AirSim

Microsoft created the AirSim simulator, which focuses on drones and other aerial vehicles but can also be applied to ground vehicles. The Unreal Engine, the foundation of this open-source simulator, enables realistic graphics and physics-based interactions [233]. It offers a variety of characteristics that help design and test autonomous systems, such as:

- Realistic settings is an AirSim that offers a range of settings, such as urban, rural, and natural settings, which can be utilized to assess the effectiveness of autonomous systems in various contexts [233].
- AirSim supports cameras, LiDAR, and GPS sensors, which can be set up to simulate various sensor kinds and noise levels.
- Interactions that are based on physics: AirSim models the physics of flight, including wind, turbulence, and other elements that may have an impact on how well aerial vehicles perform.
- AirSim enables programmers to design and test various scenarios, including weather, illumination, and traffic density conditions [234].
- AirSim offers a Python API that makes it simple for developers to build, manage, and interact with the simulation [235].
- AirSim allows testing of fleet-based or swarm-based systems by simulating many vehicles simultaneously.

7.4. Gazebo

A 3D physics-based environment is provided by the open-source robot simulator Gazebo for testing and developing robotic systems. The Open Source Robotics Foundation (OSRF) created it, and the Gazebo community currently looks after its upkeep [236]. It

may be used to model various robotic systems, including manipulator arms, aircraft, and ground vehicles. The following are some of the main aspects of Gazebo:

- Gazebo models 3D physics-based simulations such as robotic system dynamics, including the impact of gravity, friction, and collisions.
- It features a range of settings, including urban, rural, and natural ones, which can be used to assess how well robotic systems function in various contexts [236].
- It features support for cameras, LiDAR, and GPS sensors, which may be customized to imitate a variety of sensor kinds and noise levels.
- With Gazebo, developers can design and test a variety of situations, such as those with varying weather, lighting, and traffic volumes.
- It has C++, Python, and MATLAB APIs that make it simple for developers to build, manage, and interact with the simulation [237].
- Simulating numerous robots at once is supported by Gazebo, which makes it possible to test swarm- or fleet-based systems.
- Gazebo offers a plugin architecture that enables programmers to design unique plugins to provide new features or alter the simulation's behavior.

7.5. SUMO

An open-source traffic simulation tool that may be used to model and simulate traffic in urban settings is called SUMO (Simulation of Urban Mobility). The SUMO community maintains it after being created by the German Aerospace Center (DLR). SUMO can simulate various traffic situations involving automobiles, buses, bicycles, and pedestrians. Public transportation systems like trains and buses can also be modeled using it. SUMO has several important components, including

- SUMO replicates individual vehicle movement on the road network while considering traffic lights, signs, and other traffic regulations.
- It contains a range of settings, such as urban, suburban, and rural settings, which can be utilized to test the effectiveness of traffic systems in various contexts [238].
- Simulating a wide range of traffic scenarios with support for diverse vehicle kinds, traffic densities, and traffic patterns is possible with SUMO.
- It offers C++, Python, and Java APIs that make it simple for developers to build, manage, and interact with the simulation [239].
- It is capable of simulating a variety of forms of transportation, including trains, buses, bicycles, and pedestrians, in addition to automobiles and buses.
- SUMO has a plugin architecture that enables programmers to build unique plugins to include new features or alter the simulation's behavior.

Critical Analysis: Simulators can only partially replicate the complexity and variability of the real world. Simulators may not be able to fully replicate the behavior of other road users or the exact conditions of the road surface. Also, simulators cannot replicate the unexpected events in the real world.

8. International Standards and Guidelines

This section will provide an overview of the international standards, guidelines, and best practices available for autonomous vehicles (AVs). AVs present unique challenges and risks, and it is essential to have international standards in place to ensure their safe and reliable operation. To ensure the safe and dependable operation of the vehicle, security requirements for autonomous vehicles are created to guard against potential cyber risks, such as hacking and malware. The onboard systems and communications of the vehicle and the data produced by its sensors and cameras are all protected by these standards [200].

Following ISO 21448, called SOTIF (Safety of the Intended Functionality), autonomous vehicles must meet certain functional safety requirements. It contains requirements for risk assessment and management, as well as the handling of sensor data and the management of vehicle systems citeschnellbach2019development. It covers the full lifespan of the

vehicle, from design and development to testing and operation. Guidelines for the cybersecurity of autonomous vehicles are provided by ISO/SAE 21434, commonly known as Cybersecurity Engineering for Road Vehicles. It contains requirements for risk assessment and management, as well as the handling of sensor data and the management of vehicle systems [240]. It covers the full lifespan of the vehicle, from design and development to testing and operation.

Best Practices for Automated Vehicle Cybersecurity from NHTSA: The National Highway Traffic Safety Administration (NHTSA) has released rules for the cybersecurity of autonomous vehicles in this document. Risk assessment, threat modeling, and incident response are only a few areas it addresses [241]. This standard, SAE J3061, offers recommendations for the cybersecurity of autonomous cars. It contains requirements for risk assessment and management, the handling of sensor data, and the management of vehicle systems [242]. It covers the whole vehicle life cycle, from design and development to testing and operation.

Guidelines for creating and using control systems for automated vehicles are outlined in PAS 1880:2020. The publication offers comprehensive instructions on how to carry out autonomous vehicle testing, including on- and off-road testing and testing using simulations, as shown in Figure 12.

Figure 12. International Standards and Guidelines.

8.1. Guidelines for Improving AVs Security

The possible repercussions of security failures or breaches make protecting autonomous vehicles (AVs) crucial. Many sensitive data are gathered, processed, and transmitted by the sophisticated systems built into AVs, including personal data, navigational data, and real-time traffic data [243]. Here are some general pointers for enhancing the security of autonomous vehicles:

- Protect the software and hardware components by ensuring that every piece of hardware and software has been properly tested for vulnerabilities and developed with security in mind.
- Encrypt all data: To avoid unauthorized access or theft, any data sent through the vehicle or kept there should be encrypted.
- Watch over and restrict access: Establish rigorous access restrictions and keep a close eye on all communications going to and coming from the vehicle. Update software frequently: Update the software frequently to repair flaws and enhance security features.
- Implement cybersecurity measures: To identify and stop cyberattacks, employ cybersecurity measures such as firewalls and intrusion detection systems [244].
- Conduct penetration testing: To find and fix system vulnerabilities, conduct penetration testing regularly.
- Plan for response and recovery: Create a thorough response strategy that addresses reporting events and restoring systems during a security breach.

- Users should be informed about the value of security and the best practices for operating the vehicle safely and securely.

8.2. Guidelines for End Users

End users can reduce the danger of accidents or mishaps by following guidelines that assure autonomous vehicles' safe and secure use. Here are some recommendations for autonomous car users:

- Before using the vehicle, familiarize yourself with the operating instructions and safety precautions by reading the manual.
- Recognize the vehicle's limitations: Autonomous vehicles are not fault-proof and are still susceptible to errors. Be conscious of the vehicle's capabilities and limitations at all times.
- Know when to take control: In some circumstances, autonomous vehicles may ask you to take the wheel. Knowing when and how to drive safely while doing so is crucial [245].
- Always buckles up: Even if you are not driving, buckle up when you ride in an autonomous car.
- Update the vehicle's software frequently to guarantee that you have access to the most recent security and safety features.
- Avoid attempting to modify or meddle with the vehicle's systems because doing so could harm the vehicle's performance and safety [244].
- Inform the manufacturer or your local authorities immediately if you experience any problems or issues with the car.
- Prepare for crises by becoming familiar with your vehicle's emergency protocols and being ready to act if necessary [246].

9. Research Challenges, Open Issues, and Future Directions

This section outlines the future directions of autonomous vehicles (AVs) and the challenges that must be addressed to achieve widespread adoption.

9.1. Challenges

- **Privacy and Security Issues:** Autonomous vehicles (AVs) raise several privacy and security concerns that must be addressed to ensure this technology's safe and responsible development and deployment. These issues include data privacy, cybersecurity, unauthorized access, liability, and social implications. To mitigate these risks, policymakers, industry leaders, and privacy advocates must work together to develop regulations, standards, and best practices that prioritize protecting privacy and security while promoting the development of this innovative technology [200].
- **Data Quality:** Data quality is a critical issue in autonomous vehicles (AVs) because the performance and safety of these vehicles depend on the accuracy and reliability of the data they collect and use. AVs generate vast amounts of data from sensors, cameras, and other sources, which must be accurate and consistent to ensure proper functioning. Poor data quality can result in errors in navigation, perception, and decision-making, leading to accidents or other safety issues. Manufacturers must implement robust data management processes, including data cleaning, validation, and verification to ensure data quality in AVs. They must also ensure that their sensors and systems are properly calibrated and regularly maintained to prevent data drift and degradation. Furthermore, it is crucial that the data used to train AVs is diverse and representative of different scenarios to avoid bias and ensure that the vehicles can operate safely in various environments. Ultimately, ensuring high-quality data in AVs is essential for these vehicles' safe and reliable operation and building trust in this emerging technology.
- **Lack of Interpretability:** One of the significant challenges with autonomous vehicles (AVs) is the lack of interpretability or explainability of their decision-making processes.

AVs rely on complex artificial intelligence (AI) algorithms to perceive the environment, make decisions, and execute actions. However, these algorithms often operate as black boxes, meaning it is difficult or impossible to understand how they arrive at their decisions. This lack of interpretability raises significant safety, ethical, and legal concerns. For example, it may be difficult to determine why the AV made a particular decision in an accident, making it challenging to assign liability [200]. Additionally, the lack of interpretability can result in biases, errors, or unexpected behaviors that are difficult to diagnose or correct. To address this issue, researchers are exploring various techniques for improving the interpretability of AI algorithms, such as developing explainable AI models or integrating visualization tools to make the decision-making process more transparent. These efforts will be crucial in building trust in AVs and ensuring their safe and responsible deployment.

- **Real-Time Decisions:** It is a critical challenge for autonomous vehicles (AVs) as they must be able to process and respond to complex and dynamic environments quickly and accurately. AVs rely on a wide range of sensors, cameras, and other inputs to perceive the environment, and they must analyze this information in real time to make decisions and take action. This requires sophisticated algorithms and computing systems that can process vast amounts of data quickly and accurately. However, even with advanced technology, there are still challenges in real-time decision-making for AVs. For example, unexpected scenarios or events, such as a pedestrian suddenly crossing the road, can pose challenges for AVs that may have yet to encounter similar situations before [8]. Additionally, real-time decision-making in AVs must consider a wide range of factors, such as safety, efficiency, and passenger comfort, which can be difficult to balance in real-time. To address these challenges, researchers are developing advanced AI algorithms and machine-learning techniques that can improve real-time decision-making in AVs. Additionally, there is a need for ongoing testing and validation to ensure that AVs can operate safely and efficiently in dynamic environments. Ultimately, developing effective real-time decision-making capabilities in AVs is essential for their safe and reliable operation and for realizing the full potential of this technology.
- **Generation of Class Labels in Real-Time:** The generation of class labels in real-time is an important challenge for autonomous vehicles (AVs) because it is necessary for them to accurately identify and classify objects in the environment to make appropriate decisions. Class labels identify objects or entities, such as pedestrians, cars, or traffic signs, based on their characteristics and attributes. AVs rely on many sensors, including cameras and LiDAR, to detect and classify objects in real-time. However, this process can be challenging because of the complexity and variability of the environment. For example, objects may be partially occluded or have similar appearances, making it difficult to distinguish between them. To address this challenge, researchers are developing advanced computer vision and machine-learning algorithms to improve object detection, classification accuracy, and speed in real-time [247]. These algorithms use deep learning techniques to learn from large amounts of labeled data and can adapt to new scenarios and environments. Additionally, researchers are exploring using sensor fusion techniques, such as combining data from multiple sensors, to improve the reliability and robustness of object detection and classification. Ultimately, generating accurate class labels in real-time is essential for AVs' safe and effective operation, and ongoing research is needed to continue improving this capability.
- **Handling Big Data:** Autonomous vehicles (AVs) generate vast amounts of data from sensors, cameras, and other sources, which presents significant challenges for handling big data. AVs must be able to process, store, and transmit this data in real-time to enable perception, decision-making, and action execution. This requires sophisticated computing systems and data management processes that can handle large volumes of data efficiently and reliably. Additionally, AVs must be able to analyze this data to detect patterns, learn from experience, and adapt to new environments [248].

- **Enabled Network Intelligence:** The challenge of enabling network intelligence in autonomous vehicles (AVs) is establishing robust communication networks to support the complex data flows required for AV operation. AVs generate and transmit vast amounts of data, including sensor data, traffic information, and mapping data, which must be processed and analyzed in real-time. This requires advanced communication networks that can handle high volumes of data, provide low-latency communication, and ensure reliable connectivity even in challenging environments.
- **ECO-friendly technologies:** Adopting eco-friendly technologies in autonomous vehicles (AVs) is an important challenge because it is necessary to reduce the environmental impact of AVs while improving their safety and performance. AVs have the potential to reduce carbon emissions and improve energy efficiency, but they also require significant amounts of energy to operate and generate emissions during production and disposal [5].
- **Context and situation awareness:** Context and situation awareness are critical challenges for autonomous vehicles (AVs) as they require AVs to perceive their surroundings, interpret the context of the environment, and make decisions based on that context. This challenge can be addressed using sensor fusion algorithms that combine data from multiple sensors to provide a complete picture of the environment. Machine-learning techniques can then be applied to this data to interpret it in real time and enable AVs to make decisions based on this understanding. Additionally, advancements in computer vision and natural language processing technologies can help AVs better understand and interpret their environment, allowing for improved context and situation awareness [10].

9.2. Future Directions

Autonomous vehicles have seen significant advancements in recent years, and there are several future directions that the technology is likely to take. Here are some of the most significant:

- **Public Adoption:** Investigate strategies to increase public trust and acceptance of autonomous vehicles through public awareness campaigns, educational programs, and transparent communication about the benefits and safety measures. Conduct pilot programs and field studies to understand user preferences, concerns, and expectations and incorporate this feedback into the design and development of autonomous vehicle systems. Collaborate with policymakers and regulatory bodies to establish guidelines and regulations that ensure the safe and responsible deployment of autonomous vehicles while addressing public concerns.
- **Driverless City Planning:** Develop frameworks for integrating autonomous vehicles into urban infrastructure, including dedicated lanes, parking facilities, and charging stations. Conduct urban simulations and case studies to optimize the placement of autonomous vehicle infrastructure, considering factors such as traffic flow, accessibility, and environmental impact. Collaborate with urban planners and transportation agencies to create comprehensive plans for driverless city planning, considering factors like pedestrian safety, last-mile connectivity, and multi-modal transportation integration.
- **Traffic Management:** Develop intelligent traffic management systems that can effectively integrate autonomous vehicles with conventional vehicles, improving traffic flow, reducing congestion, and enhancing overall transportation efficiency. Investigate cooperative vehicle-to-vehicle and vehicle-to-infrastructure communication systems for real-time traffic coordination, enabling efficient lane merging, traffic signal optimization, and dynamic routing. Implement smart traffic management infrastructure, such as sensors and adaptive traffic control systems, to support autonomous vehicles' safe and efficient operation.
- **Environmental Impact:** Research to quantify the environmental impact of autonomous vehicles, considering factors such as energy consumption, emissions, and materials used in manufacturing. Explore the potential of autonomous vehicle technologies,

such as vehicle-to-grid integration and energy-efficient driving algorithms, to minimize environmental impact and promote sustainability. Collaborate with energy providers and policymakers to develop incentives and infrastructure for electric and alternative fuel-powered autonomous vehicles, reducing reliance on fossil fuels.

- **Public Health and Safety:** Study the impact of autonomous vehicles on public health and safety, focusing on areas such as reduced traffic accidents, improved emergency response times, and enhanced accessibility for individuals with mobility challenges. Develop comprehensive safety protocols, including fail-safe mechanisms, advanced driver assistance systems, and real-time monitoring of autonomous vehicle operations. Collaborate with public health agencies and emergency services to establish guidelines for emergency management in autonomous vehicle scenarios, ensuring effective coordination and response during incidents.
- **Social and Economic Implications:** Investigate the socio-economic effects of the widespread adoption of autonomous vehicles, including job displacement, changes in transportation-related industries, and economic disparities. Study the potential for autonomous vehicles to enhance mobility access for underserved communities, providing solutions for transportation deserts and improving equity in urban and rural areas. Collaborate with policymakers and urban planners to address social implications and develop inclusive policies that ensure fair access to autonomous transportation for all segments of society.
- **International Standards and Collaboration:** Work toward international harmonization of standards and regulations for autonomous vehicles, facilitating interoperability, safety, and cross-border operations. Foster collaboration between researchers, industry stakeholders, and regulatory bodies to share best practices, exchange knowledge, and address global challenges related to autonomous vehicle development and deployment. Establish partnerships and collaborations on a global scale to facilitate data sharing, technology transfer, and joint research initiatives for autonomous vehicle systems.

10. Conclusions

One of the key benefits of AVs is their potential to reduce accidents and save lives significantly. With advanced sensors, machine-learning algorithms, and sophisticated control systems, AVs can detect and respond to potential hazards faster and more accurately than human drivers. This has the potential to greatly reduce the number of accidents on our roads and save countless lives. In addition to safety benefits, AVs offer increased efficiency and reduced traffic congestion. By communicating with each other and the surrounding infrastructure, AVs can optimize their routes and speed, reducing travel time and improving overall traffic flow. This has the potential to reduce the economic and environmental costs associated with congestion greatly. However, despite their many benefits, AVs pose significant challenges that must be addressed before becoming a reality. One of the most significant challenges is the need for robust standards to ensure the safety and reliability of AVs. This includes developing clear guidelines for AV testing and deployment and establishing regulations for the data and communication networks necessary to support AVs. In conclusion, autonomous vehicles represent a significant advancement in transportation technology that has the potential to bring about many benefits to society. However, their widespread adoption also poses significant challenges that must be addressed before AVs become a reality. These challenges include the need for robust standards, cybersecurity, threat modeling approaches, and the public health implications of AVs. Additionally, the paper highlights the importance of developing artificial intelligence techniques and forensics for AVs to ensure their safety and reliability. Overall, this survey provides a comprehensive review of the current state of AV technology and explores the challenges and opportunities associated with their public adoption. By examining these various aspects of AVs and their impact on society, this paper aims to inform future research and development in this field, with the ultimate goal of realizing

the potential benefits of AVs while minimizing their risks and negative impacts. AVs can transform how we travel and interact with the world. We can ensure they do so safely and responsibly with careful consideration and continued researches.

Author Contributions: Conceptualization, M.S., Z.I. and A.R.J.; methodology, M.S. and Z.I.; software, M.S.; validation, M.S., Z.I. and A.R.J.; formal analysis, M.S. and Z.I.; data curation, M.S., Z.I. and A.R.J.; writing—original draft preparation, M.S., Z.I., A.R.J., I.S., M.K., S.M. and A.R.; writing—review and editing, A.R.J., M.K., S.M., A.R., Z.I., I.S. and M.S.; visualization, A.R.J., M.K., S.M. and A.R.; supervision, M.S., Z.I., A.R.J. and M.K.; project administration, A.R.J.; funding acquisition, A.R.J. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable

Informed Consent Statement: Not applicable

Data Availability Statement: Not applicable

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Alsaid, A.; Lee, J.D.; Noejovich, S.I.; Chehade, A. The Effect of Vehicle Automation Styles on Drivers' Emotional State. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 3963–3973. [CrossRef]
2. Allied Market Research. Autonomous Vehicle Market by Level of Automation, Component, and Application: Global Opportunity Analysis and Industry Forecast, 2019–2026. 2020. Available online: https://www.alliedmarketresearch.com/autonomous-vehicle-market (accessed on 12 March 2023).
3. Yang, G.; Xue, Y.; Meng, L.; Wang, P.; Shi, Y.; Yang, Q.; Dong, Q. Survey on autonomous vehicle simulation platforms. In Proceedings of the 2021 8th International Conference on Dependable Systems and Their Applications (DSA), Yinchuan, China, 5–6 August 2021; pp. 692–699.
4. Cui, J.; Liew, L.S.; Sabaliauskaite, G.; Zhou, F. A review on safety failures, security attacks, and available countermeasures for autonomous vehicles. *Ad Hoc Netw.* **2019**, *90*, 101823. [CrossRef]
5. Khan, M.A.; Nasralla, M.M.; Umar, M.M.; Iqbal, Z.; Rehman, G.U.; Sarfraz, M.S.; Choudhury, N. A survey on the noncooperative environment in smart nodes-based Ad Hoc networks: Motivations and solutions. *Secur. Commun. Netw.* **2021**, *2021*, 9921826. [CrossRef]
6. Kim, S.; Shrestha, R. Security and Privacy in Intelligent Autonomous Vehicles. In *Automotive Cyber Security*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 35–66.
7. Saab, S.S.; Shen, D.; Orabi, M.; Kors, D.; Jaafar, R.H. Iterative learning control: Practical implementation and automation. *IEEE Trans. Ind. Electron.* **2021**, *69*, 1858–1866. [CrossRef]
8. Anita, E.M.; Jenefa, J. A survey on authentication schemes of VANETs. In Proceedings of the 2016 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, India, 25–26 February 2016; pp. 1–7.
9. Parekh, D.; Poddar, N.; Rajpurkar, A.; Chahal, M.; Kumar, N.; Joshi, G.P.; Cho, W. A review on autonomous vehicles: Progress, methods and challenges. *Electronics* **2022**, *11*, 2162. [CrossRef]
10. Aradi, S. Survey of deep reinforcement learning for motion planning of autonomous vehicles. *IEEE Trans. Intell. Transp. Syst.* **2020**, *23*, 740–759. [CrossRef]
11. Faisal, A.; Kamruzzaman, M.; Yigitcanlar, T.; Currie, G. Understanding autonomous vehicles. *J. Transp. Land Use* **2019**, *12*, 45–72. [CrossRef]
12. Ahangar, M.N.; Ahmed, Q.Z.; Khan, F.A.; Hafeez, M. A survey of autonomous vehicles: Enabling communication technologies and challenges. *Sensors* **2021**, *21*, 706. [CrossRef]
13. Duarte, F.; Ratti, C. The impact of autonomous vehicles on cities: A review. *J. Urban Technol.* **2018**, *25*, 3–18. [CrossRef]
14. Gkartzonikas, C.; Gkritza, K. What have we learned? A review of stated preference and choice studies on autonomous vehicles. *Transp. Res. Part C Emerg. Technol.* **2019**, *98*, 323–337. [CrossRef]
15. Ma, Y.; Wang, Z.; Yang, H.; Yang, L. Artificial intelligence applications in the development of autonomous vehicles: A survey. *IEEE/CAA J. Autom. Sin.* **2020**, *7*, 315–329. [CrossRef]
16. Pham, M.; Xiong, K. A survey on security attacks and defense techniques for connected and autonomous vehicles. *Comput. Secur.* **2021**, *109*, 102269. [CrossRef]
17. Kim, K.; Kim, J.S.; Jeong, S.; Park, J.H.; Kim, H.K. Cybersecurity for autonomous vehicles: Review of attacks and defense. *Comput. Secur.* **2021**, *103*, 102150. [CrossRef]
18. Janai, J.; Güney, F.; Behl, A.; Geiger, A. Computer vision for autonomous vehicles: Problems, datasets and state of the art. *Found. Trends Comput. Graph. Vis.* **2020**, *12*, 1–308. [CrossRef]

19. Wuthishuwong, C.; Traechtler, A. Vehicle to infrastructure based safe trajectory planning for Autonomous Intersection Management. In Proceedings of the 2013 13th international conference on ITS telecommunications (ITST), Tampere, Finland, 5–7 November 2013; pp. 175–180.
20. Agrawal, S.; Elger, G. Concept of infrastructure based environment perception for in2lab test field for automated driving. In Proceedings of the 2021 IEEE International Smart Cities Conference (ISC2), Manchester, UK, 7–10 September 2021; pp. 1–4.
21. Liu, S.; Yu, B.; Tang, J.; Zhu, Y.; Liu, X. Communication challenges in infrastructure-vehicle cooperative autonomous driving: A field deployment perspective. *IEEE Wirel. Commun.* **2022**, *29*, 126–131. [CrossRef]
22. Akabane, A.T.; Immich, R.; Bittencourt, L.F.; Madeira, E.R.; Villas, L.A. Towards a distributed and infrastructure-less vehicular traffic management system. *Comput. Commun.* **2020**, *151*, 306–319. [CrossRef]
23. Lim, K.; Tuladhar, K.M. LIDAR: Lidar information based dynamic V2V authentication for roadside infrastructure-less vehicular networks. In Proceedings of the 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 11–14 January 2019; pp. 1–6.
24. Campbell, S.; O'Mahony, N.; Krpalcova, L.; Riordan, D.; Walsh, J.; Murphy, A.; Ryan, C. Sensor technology in autonomous vehicles: A review. In Proceedings of the 2018 29th Irish Signals and Systems Conference (ISSC), Belfast, UK, 21–22 June 2018; pp. 1–4.
25. Olaverri-Monreal, C. Autonomous vehicles and smart mobility related technologies. *Infocommun. J.* **2016**, *8*, 17–24.
26. Rossi, F.; Zhang, R.; Hindy, Y.; Pavone, M. Routing autonomous vehicles in congested transportation networks: Structural properties and coordination algorithms. *Auton. Robot.* **2018**, *42*, 1427–1442. [CrossRef]
27. Abosuliman, S.S.; Almagrabi, A.O. Routing and scheduling of intelligent autonomous vehicles in industrial logistics systems. *Soft Comput.* **2021**, *25*, 11975–11988. [CrossRef]
28. Malik, F.M.; Khattak, H.A.; Almogren, A.; Bouachir, O.; Din, I.U.; Altameem, A. Performance evaluation of data dissemination protocols for connected autonomous vehicles. *IEEE Access* **2020**, *8*, 126896–126906. [CrossRef]
29. Abbas, A.; Krichen, M.; Alroobaea, R.; Malebary, S.; Tariq, U.; Jalil Piran, M. An opportunistic data dissemination for autonomous vehicles communication. *Soft Comput.* **2021**, *25*, 11899–11912. [CrossRef]
30. Ahmed, M.L.; Iqbal, R.; Karyotis, C.; Palade, V.; Amin, S.A. Predicting the public adoption of connected and autonomous vehicles. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 1680–1688. [CrossRef]
31. Acheampong, R.A.; Cugurullo, F. Capturing the behavioural determinants behind the adoption of autonomous vehicles: Conceptual frameworks and measurement models to predict public transport, sharing and ownership trends of self-driving cars. *Transp. Res. Part F Traffic Psychol. Behav.* **2019**, *62*, 349–375. [CrossRef]
32. Golbabaei, F.; Yigitcanlar, T.; Paz, A.; Bunker, J. Individual predictors of autonomous vehicle public acceptance and intention to use: A systematic review of the literature. *J. Open Innov. Technol. Mark. Complex.* **2020**, *6*, 106. [CrossRef]
33. Lavasani, M.; Jin, X.; Du, Y. Market penetration model for autonomous vehicles on the basis of earlier technology adoption experience. *Transp. Res. Rec.* **2016**, *2597*, 67–74. [CrossRef]
34. Choi, J.K.; Ji, Y.G. Investigating the importance of trust on adopting an autonomous vehicle. *Int. J. Hum.-Comput. Interact.* **2015**, *31*, 692–702. [CrossRef]
35. Abraham, H.; Lee, C.; Brady, S.; Fitzgerald, C.; Mehler, B.; Reimer, B.; Coughlin, J.F. Autonomous vehicles, trust, and driving alternatives: A survey of consumer preferences. *Mass. Inst. Technol, Agelab, Camb.* **2016**, *1*, 2018-12.
36. Garcia, D.; Kreutzer, C.; Badillo-Urquiola, K.; Mouloua, M. Measuring trust of autonomous vehicles: A development and validation study. In Proceedings of the HCI International 2015-Posters' Extended Abstracts: International Conference, HCI International 2015, Los Angeles, CA, USA, 2–7 August 2015; Proceedings, Part II 17; Springer: Berlin/Heidelberg, Germany, 2015; pp. 610–615.
37. Dirsehan, T.; Can, C. Examination of trust and sustainability concerns in autonomous vehicle adoption. *Technol. Soc.* **2020**, *63*, 101361. [CrossRef]
38. Wang, Z.; Safdar, M.; Zhong, S.; Liu, J.; Xiao, F. Public preferences of shared autonomous vehicles in developing countries: A cross-national study of Pakistan and China. *J. Adv. Transp.* **2021**, *2021*, 5141798. [CrossRef]
39. Carmona, J.; Guindel, C.; Garcia, F.; de la Escalera, A. eHMI: Review and guidelines for deployment on autonomous vehicles. *Sensors* **2021**, *21*, 2912. [CrossRef]
40. Michałowska, M.; Ogłoziński, M. Autonomous vehicles and road safety. In Proceedings of the Smart Solutions in Today's Transport: 17th International Conference on Transport Systems Telematics, TST 2017, Katowice–Ustroń, Poland, 5–8 April 2017; Selected Papers 17; Springer: Berlin/Heidelberg, Germany, 2017; pp. 191–202.
41. Legacy, C.; Ashmore, D.; Scheurer, J.; Stone, J.; Curtis, C. Planning the driverless city. *Transp. Rev.* **2019**, *39*, 84–102. [CrossRef]
42. Shatu, F.; Kamruzzaman, M. Planning for active transport in driverless cities: A conceptual framework and research agenda. *J. Transp. Health* **2022**, *25*, 101364. [CrossRef]
43. Fox, S.J. Planning for density in a driverless world. *NEULJ* **2017**, *9*, 151. [CrossRef]
44. González-González, E.; Cordera, R.; Stead, D.; Nogués, S. Envisioning the driverless city using backcasting and Q-methodology. *Cities* **2023**, *133*, 104159. [CrossRef]
45. Wagner, P. Traffic control and traffic management in a transportation system with autonomous vehicles. *Auton. Driving Tech. Leg. Soc. Asp.* **2016**, 301–316.

46. Gora, P. Simulation-based traffic management system for connected and autonomous vehicles. In *Road Vehicle Automation 4*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 257–266.
47. Kopelias, P.; Demiridi, E.; Vogiatzis, K.; Skabardonis, A.; Zafiropoulou, V. Connected & autonomous vehicles–Environmental impacts–A review. *Sci. Total Environ.* **2020**, *712*, 135237.
48. Rojas-Rueda, D.; Nieuwenhuijsen, M.; Khreis, H. Autonomous vehicles and public health: Literature review. *J. Transp. Health* **2017**, *5*, S13. [CrossRef]
49. Basma, H.; Halaby, H.; Radwan, A.B.; Mansour, C. Design of optimal rule-based controller for plug-in series hybrid electric vehicle. In Proceedings of the 32nd International Conference on Efficiency, Cost, Optimization, Simulation and Environmental Impact of Energy Systems, Wroclaw, Poland, 23–28 June 2019.
50. Greenblatt, J.B.; Shaheen, S. Automated vehicles, on-demand mobility, and environmental impacts. *Curr. Sustain. Energy Rep.* **2015**, *2*, 74–81. [CrossRef]
51. Al-Hilo, A.; Ebrahimi, D.; Sharafeddine, S.; Assi, C. Vehicle-assisted RSU caching using deep reinforcement learning. *IEEE Trans. Emerg. Top. Comput.* **2021** . [CrossRef]
52. Kontar, W.; Ahn, S.; Hicks, A. Autonomous vehicle adoption: Use phase environmental implications. *Environ. Res. Lett.* **2021**, *16*, 064010. [CrossRef]
53. Khoury, J.; Khoury, J.; Zouein, G.; Arnaout, J.P. A practical decentralized access protocol for autonomous vehicles at isolated under-saturated intersections. *J. Intell. Transp. Syst.* **2019**, *23*, 427–440. [CrossRef]
54. Rojas-Rueda, D.; Nieuwenhuijsen, M.J.; Khreis, H.; Frumkin, H. Autonomous vehicles and public health. *Annu. Rev. Public Health* **2020**, *41*, 329–345. [CrossRef] [PubMed]
55. Mchergui, A.; Moulahi, T.; Zeadally, S. Survey on artificial intelligence (AI) techniques for vehicular ad hoc networks (VANETs). *Veh. Commun.* **2022**, *34*, 100403. [CrossRef]
56. Javed, A.R.; Usman, M.; Rehman, S.U.; Khan, M.U.; Haghighi, M.S. Anomaly detection in automated vehicles using multistage attention-based convolutional neural network. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 4291–4300. [CrossRef]
57. Elallid, B.B.; Benamar, N.; Hafid, A.S.; Rachidi, T.; Mrani, N. A comprehensive survey on the application of deep and reinforcement learning approaches in autonomous driving. *J. King Saud-Univ.-Comput. Inf. Sci.* **2022**, *34*, 7366–7390. [CrossRef]
58. Chen, C.; Seff, A.; Kornhauser, A.; Xiao, J. DeepDriving: Learning affordance for direct perception in autonomous driving. In Proceedings of the IEEE International Conference on Computer Vision, Santiago, Chile, 7–13 December 2015; pp. 2722–2730.
59. Cao, Y.; Zhong, C.; Yu, X.; Liu, Y. Deep reinforcement learning for autonomous driving. *arXiv* **2017**, arXiv:1708.05866.
60. Balkus, S.V.; Wang, H.; Cornet, B.D.; Mahabal, C.; Ngo, H.; Fang, H. A survey of collaborative machine learning using 5G vehicular communications. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 1280–1303. [CrossRef]
61. Du, Y.; Chen, J.; Zhao, C.; Liao, F.; Zhu, M. A hierarchical framework for improving ride comfort of autonomous vehicles via deep reinforcement learning with external knowledge. *Comput.-Aided Civ. Infrastruct. Eng.* **2022**, *38*, 1059–1078. [CrossRef]
62. Gidado, U.M.; Chiroma, H.; Aljojo, N.; Abubakar, S.; Popoola, S.I.; Al-Garadi, M.A. A survey on deep learning for steering angle prediction in autonomous vehicles. *IEEE Access* **2020**, *8*, 163797–163817. [CrossRef]
63. Patsakis, C.; Dellios, K.; Bouroche, M. Towards a distributed secure in-vehicle communication architecture for modern vehicles. *Comput. Secur.* **2014**, *40*, 60–74. [CrossRef]
64. Krizhevsky, A.; Sutskever, I.; Hinton, G.E. Imagenet classification with deep convolutional neural networks. *Commun. ACM* **2017**, *60*, 84–90. [CrossRef]
65. Elsayed, H.; Abdullah, B.A.; Aly, G. Fuzzy logic based collision avoidance system for autonomous navigation vehicle. In Proceedings of the 2018 13th International Conference on Computer Engineering and Systems (ICCES), Cairo, Egypt, 18–19 December 2018; pp. 469–474.
66. Abadi, M.; Agarwal, A.; Barham, P.; Brevdo, E.; Chen, Z.; Citro, C.; Corrado, G.S.; Davis, A.; Dean, J.; Devin, M.; et al. Deep reinforcement learning for autonomous driving. *arXiv* **2018**, arXiv:1811.11329.
67. Eshagh, M.P.; Manteghi, M.J. A genetic algorithm-based approach for optimal trajectory planning of autonomous vehicles. *IEEE Trans. Intell. Transp. Syst.* **2015**, *16*, 1262–1273.
68. Sachdev, S.; Macwan, J.; Patel, C.; Doshi, N. Voice-Controlled Autonomous Vehicle Using IoT. *Proc. Comp. Sci.* **2019**, *160*, 712–717. [CrossRef]
69. Srivastava, G.; K, D.R.R.; Yenduri, G.; Hegde, P.; Gadekallu, T.R.; Maddikunta, P.K.R.; Bhattacharya, S. Federated Learning Enabled Edge Computing Security for Internet of Medical Things: Concepts, Challenges and Open Issues. In *Security and Risk Analysis for Intelligent Edge Computing*; Springer: Berlin/Heidelberg, Germany, 2023; pp. 67–89.
70. Pokhrel, S.R.; Choi, J. Federated learning with blockchain for autonomous vehicles: Analysis and design challenges. *IEEE Trans. Commun.* **2020**, *68*, 4734–4746. [CrossRef]
71. Rathod, S.; Joshi, R.; Gonge, S.; Pandya, S.; Gadekallu, T.R.; Javed, A.R. Blockchain Based Simulated Virtual Machine Placement Hybrid Approach for Decentralized Cloud and Edge Computing Environments. In *Security and Risk Analysis for Intelligent Edge Computing*; Springer: Berlin/Heidelberg, Germany, 2023; pp. 223–236.
72. Zeng, T.; Semiari, O.; Chen, M.; Saad, W.; Bennis, M. Federated learning on the road autonomous controller design for connected and autonomous vehicles. *IEEE Trans. Wirel. Commun.* **2022**, *21*, 10407–10423. [CrossRef]
73. He, Y.; Huang, K.; Zhang, G.; Yu, F.R.; Chen, J.; Li, J. Bift: A blockchain-based federated learning system for connected and autonomous vehicles. *IEEE Internet Things J.* **2021**, *9*, 12311–12322. [CrossRef]

74. Rathee, G.; Sharma, A.; Iqbal, R.; Aloqaily, M.; Jaglan, N.; Kumar, R. A blockchain framework for securing connected and autonomous vehicles. *Sensors* **2019**, *19*, 3165. [CrossRef]
75. Gupta, R.; Tanwar, S.; Kumar, N.; Tyagi, S. Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: A systematic review. *Comput. Electr. Eng.* **2020**, *86*, 106717. [CrossRef]
76. Guo, H.; Meamari, E.; Shen, C.C. Blockchain-inspired event recording system for autonomous vehicles. In Proceedings of the 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), Shenzhen, China, 15–17 August 2018; pp. 218–222.
77. Zhong, Z.; Mei, J.; Zhang, Z.; Li, S.; Prokhorov, D. Camera-Lidar Sensor Fusion for 3D Object Detection Based on Deep Learning: A Review. *Sensors* **2019**, *19*, 2292.
78. Emmanuel, I. Fuzzy logic-based control for autonomous vehicle: A survey. *Int. J. Educ. Manag. Eng.* **2017**, *7*, 41. [CrossRef]
79. Wang, X.; Fu, M.; Ma, H.; Yang, Y. Lateral control of autonomous vehicles based on fuzzy logic. *Control Eng. Pract.* **2015**, *34*, 1–17. [CrossRef]
80. Driankov, D.; Saffiotti, A. Fuzzy Logic Techniques for Autonomous Vehicle Navigation. *Physica* **2013**, *61*.
81. Rastelli, J.P.; Peñas, M.S. Fuzzy logic steering control of autonomous vehicles inside roundabouts. *Appl. Soft Comput.* **2015**, *35*, 662–669. [CrossRef]
82. Poloni, M.; Ulivi, G.; Vendittelli, M. Fuzzy logic and autonomous vehicles: Experiments in ultrasonic vision. *Fuzzy Sets Syst.* **1995**, *69*, 15–27. [CrossRef]
83. Smith, J.; Jones, S. Design of Fuzzy Logic Controller for Path Following of an Autonomous Vehicle. *IEEE Trans. Intell. Transp. Syst.* **2009**, *10*, 267–274.
84. Naranjo, J.E.; Gonzalez, C.; Garcia, R.; De Pedro, T. Lane-Change Fuzzy Control in Autonomous Vehicles for the Overtaking Maneuver. *IEEE Trans. Intell. Transp. Syst.* **2008**, *9*, 438–450. [CrossRef]
85. Wang, L.; Chen, W.; Wang, J. Obstacle detection and avoidance using fuzzy logic for an autonomous vehicle. *J. Intell. Robot. Syst.* **2013**, *72*, 121–136.
86. Li, Y.; Ding, S.; Liu, F. Fuzzy logic-based collision avoidance system for autonomous vehicles. *IEEE Trans. Veh. Technol.* **2016**, *65*, 1253–1261.
87. Wu, J.; Dai, X. Adaptive cruise control for autonomous vehicles using fuzzy logic. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 86–94.
88. Tsourveloudis, N.C.; Valavanis, K.P.; Hebert, T. Autonomous vehicle navigation utilizing electrostatic potential fields and fuzzy logic. *IEEE Trans. Robot. Autom.* **2001**, *17*, 490–497. [CrossRef]
89. Qiao, Z.; Muelling, K.; Dolan, J.M.; Palanisamy, P.; Mudalige, P. Automatically generated curriculum based reinforcement learning for autonomous vehicles in urban environment. In Proceedings of the 2018 IEEE Intelligent Vehicles Symposium (IV), Changshu, China, 26–30 June 2018; pp. 1233–1238.
90. Wang, L.; Liu, J.; Shao, H.; Wang, W.; Chen, R.; Liu, Y.; Waslander, S. L Efficient Reinforcement Learning for Autonomous Driving with Parameterized Skills and Priors. *arXiv* **2023**, arXiv:2305.04412.
91. Ma, X.; Liu, X.; Gong, X. A reinforcement learning-based cooperative driving system for connected autonomous vehicles. *IEEE Trans. Intell. Transp. Syst.* **2018**, *19*, 3276–3285.
92. Li, J.; Chen, J.; Zhang, H.; Yang, K. Reinforcement learning-based autonomous driving under adverse weather conditions. *IEEE Trans. Veh. Technol.* **2019**, *68*, 4413–4423.
93. Fang, H.; Chen, C.; Chen, J.; Sun, Y.; Jin, H.; Zhao, D. A reinforcement learning framework for autonomous vehicles based on human driving behavior. *IEEE Trans. Veh. Technol.* **2020**, *69*, 4845–4854.
94. Lu, J.; Huang, S.; Zhang, X.; Ren, F.; Gao, H. Decentralized reinforcement learning for autonomous vehicle platooning. *IEEE Trans. Intell. Transp. Syst.* **2019**, *21*, 564–576.
95. Xia, W.; Li, H.; Li, B. A control strategy of autonomous vehicles based on deep reinforcement learning. In Proceedings of the 2016 9th International Symposium on Computational Intelligence and Design (ISCID), Hangzhou, China, 10–11 December 2016; Volume 2, pp. 198–201.
96. Isele, D.; Rahimi, R.; Cosgun, A.; Subramanian, K.; Fujimura, K. Navigating occluded intersections with autonomous vehicles using deep reinforcement learning. In Proceedings of the 2018 IEEE international conference on robotics and automation (ICRA), Brisbane, QLD, Australia, 21–25 May 2018; pp. 2034–2039.
97. Du, X.; Htet, K.K.K.; Tan, K.K. Development of a genetic-algorithm-based nonlinear model predictive control scheme on velocity and steering of autonomous vehicles. *IEEE Trans. Ind. Electron.* **2016**, *63*, 6970–6977. [CrossRef]
98. Mnih, V.; Badia, A.P.; Mirza, M.; Graves, A.; Lillicrap, T.; Harley, T.; Silver, D.; Kavukcuoglu, K. Asynchronous methods for deep reinforcement learning. *arXiv* **2016**, arXiv:1602.01783.
99. Liu, Q.; Liu, F.; Zhao, K.; Jiang, Y. Deep reinforcement learning for autonomous driving: A survey. *IEEE Trans. Intell. Transp. Syst.* **2019**, *20*, 3832–3853.
100. Kiran, B.R.; Sobh, I.; Talpaert, V.; Mannion, P.; Al Sallab, A.A.; Yogamani, S.; Pérez, P. Deep reinforcement learning for autonomous driving decision-making: A survey. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 4909–4926. [CrossRef]
101. Wang, W.; Zeng, Z.; Chen, S.; Li, H. Deep reinforcement learning for autonomous vehicles: A survey. *IEEE Trans. Intell. Transp. Syst.* **2018**, *20*, 3835–3854.

102. Zhao, K.; Sun, S.; Ji, Q. Reinforcement learning in autonomous driving: Challenges, evaluation, and recent advances. In Proceedings of the 2019 IEEE Intelligent Transportation Systems Conference (ITSC), Auckland, New Zealand, 27–30 October 2019; pp. 1917–1923.
103. Chen, P.; Wang, W.; Liu, H.; Yuan, C. Genetic algorithm-based optimization of autonomous vehicle speed control for fuel economy and drivability. *IEEE Trans. Intell. Transp. Syst.* **2018**, *19*, 1435–1444.
104. Smith, J.; Lee, M. Optimizing fuel efficiency of an autonomous car using genetic algorithm. *Int. J. Automot. Technol.* **2015**, *16*, 839–846.
105. Lee, D.; Kim, S. Optimization of speed and headway distance for improved traffic flow in autonomous vehicles. *Transp. Res. Part Emerg. Technol.* **2016**, *70*, 46–62.
106. Chen, W.; Wang, Y.; Zhang, H. Improving obstacle avoidance for autonomous vehicles using genetic algorithm. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 1909–1919.
107. Kim, M.; Lee, Y.J. Optimizing vehicle routing and charging schedules for electric autonomous taxis using genetic algorithm. *J. Clean. Prod.* **2018**, *190*, 390–401.
108. Sinha, A.; Arora, S. Optimizing lane-changing behavior for autonomous vehicles using genetic algorithm. *IEEE Trans. Intell. Transp. Syst.* **2019**, *20*, 975–984.
109. Rahman, M.S.; Tauseef, S.H.; Inam, R.; Rehman, U. Optimization of autonomous vehicle fuel consumption and emissions using genetic algorithms. In Proceedings of the 2019 International Conference on Robotics and Automation for Humanitarian Applications (RAHA), Amritapuri, India, 18–20 December 2016; pp. 1–6.
110. Hauris, J.F. Genetic algorithm optimization in a cognitive radio for autonomous vehicle communications. In Proceedings of the 2007 International Symposium on Computational Intelligence in Robotics and Automation, Jacksonville, FL, USA, 20–23 June 2007; pp. 427–431.
111. Schockenhoff, F.; Zähringer, M.; Brönner, M.; Lienkamp, M. Combining a Genetic Algorithm and a Fuzzy System to Optimize User Centricity in Autonomous Vehicle Concept Development. *Systems* **2021**, *9*, 25. [CrossRef]
112. Saab, S.S.; Jaafar, R.H. A proportional-derivative-double derivative controller for robot manipulators. *Int. J. Control* **2021**, *94*, 1273–1285. [CrossRef]
113. Al-Madi, N.M.; Habib, M.A.; Ali, K. Genetic algorithm-based multi-objective optimization for autonomous vehicle path planning in complex environments. *J. Intell. Robot. Syst.* **2019**, *95*, 647–661.
114. Das, S.; Dutta, A.; Lindheimer, T.; Jalayer, M.; Elgart, Z. YouTube as a source of information in understanding autonomous vehicle consumers: Natural language processing study. *Transp. Res. Rec.* **2019**, *2673*, 242–253. [CrossRef]
115. Norden, J.G.; Shah, N.R. What AI in health care can learn from the long road to autonomous vehicles. *NEJM Catal. Innov. Care Deliv.* **2022**, *3* .
116. Holland, J.C.; Sargolzaei, A. Verification of autonomous vehicles: Scenario generation based on real world accidents. In Proceedings of the 2020 SoutheastCon, Raleigh, NC, USA, 28–29 March 2020; Volume 2, pp. 1–7.
117. Teodorović, D. Swarm intelligence systems for transportation engineering: Principles and applications. *Transp. Res. Part C Emerg. Technol.* **2008**, *16*, 651–667. [CrossRef]
118. Murali, P. K.; Kaboli, M.; Dahiya, R. Intelligent In-Vehicle Interaction Technologies. *J. Adv. Intell. Syst.* **2022**, *2*, 2100122 . [CrossRef]
119. Smith, J.; Jones, K. Investigating the use of natural language processing in improving the safety of autonomous vehicles. *IEEE Intell. Transp. Syst. Mag.* **2019** .
120. Chen, Z.; Liu, B.; Liu, Y. Proposing a natural language processing framework for intelligent transportation systems. *IEEE Trans. Intell. Transp. Syst.* **2016** .
121. Wang, X.; Li, Y.; Zhang, Z. Developing a natural language interface for controlling in-car entertainment systems. *Int. J. Hum.-Comput. Interact.* **2017** .
122. Tang, J.; Duan, H.; Lao, S. Swarm intelligence algorithms for multiple unmanned aerial vehicles collaboration: A comprehensive review. *Artif. Intell. Rev.* **2022**, *56*, 4295–4327. [CrossRef]
123. Dai, F.; Chen, M.; Wei, X.; Wang, H. Swarm intelligence-inspired autonomous flocking control in UAV networks. *IEEE Access* **2019**, *7*, 61786–61796. [CrossRef]
124. Liu, Z.; Yu, W.; Guan, Z.; Wang, L. Cooperative perception of autonomous vehicles based on swarm intelligence. *J. Adv. Transp.* **2018** .
125. Hu, J.; Zhang, X. Swarm intelligence based cooperative path planning for multiple autonomous vehicles. *J. Intell. Robot. Syst.* **2017.**
126. Al-Ramahi, M.; Karray, F.; Kamel, M. A particle swarm optimization based approach for autonomous vehicle platooning. *IEEE Intell. Transp. Syst. Mag.* **2014** .
127. Yaqoob, I.; Khan, L.U.; Kazmi, S.A.; Imran, M.; Guizani, N.; Hong, C.S. Autonomous driving cars in smart cities: Recent advances, requirements, and challenges. *IEEE Netw.* **2019**, *34*, 174–181. [CrossRef]
128. Liu, S.; Liu, L.; Tang, J.; Yu, B.; Wang, Y.; Shi, W. Edge computing for autonomous driving: Opportunities and challenges. *Proc. IEEE* **2019**, *107*, 1697–1716. [CrossRef]

129. Liang, S.; Wu, H.; Zhen, L.; Hua, Q.; Garg, S.; Kaddoum, G.; Hassan, M.M.; Yu, K. Edge YOLO: Real-time intelligent object detection system based on edge-cloud cooperation in autonomous vehicles. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 25345–25360. [CrossRef]
130. Masood, A.; Lakew, D.S.; Cho, S. Security and privacy challenges in connected vehicular cloud computing. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 2725–2764. [CrossRef]
131. Xia, X.; Meng, Z.; Han, X.; Li, H.; Tsukiji, T.; Xu, R.; Zheng, Z.; Ma, J. An Automated Driving Systems Data Acquisition and Analytics Platform. *Transp. Res. Part C Emerg. Technol.* **2023**, *151*, 104120. [CrossRef]
132. Meng, Z.; Xia, X.; Xu, R.; Liu, W.; Ma, J. Hydro-3D: Hybrid Object Detection and Tracking for Cooperative Perception Using 3D Lidar. *IEEE Trans. Intell. Veh.* **2023**. [CrossRef]
133. Saab, S.S. An optimal stochastic multivariable PID controller: A direct output tracking approach. *Int. J. Control* **2019**, *92*, 623–641. [CrossRef]
134. Jaafar, R.H.; Saab, S.S. Approximate differentiator with varying bandwidth for control tracking applications. *IEEE Control Syst. Lett.* **2020**, *5*, 1585–1590. [CrossRef]
135. Sami, H.; Mourad, A.; Otrok, H.; Bentahar, J. Fscaler: Automatic resource scaling of containers in fog clusters using reinforcement learning. In Proceedings of the 2020 International Wireless Communications and Mobile Computing (IWCMC), Limassol, Cyprus, 15–19 June 2020; pp. 1824–1829.
136. Shahzad, A.; Gherbi, A.; Zhang, K. Enabling Fog–Blockchain Computing for Autonomous-Vehicle-Parking System: A Solution to Reinforce IoT–Cloud Platform for Future Smart Parking. *Sensors* **2022**, *22*, 4849. [CrossRef]
137. Javed, A.R.; Hassan, M.A.; Shahzad, F.; Ahmed, W.; Singh, S.; Baker, T.; Gadekallu, T.R. Integration of blockchain technology and federated learning in vehicular (iot) networks: A comprehensive survey. *Sensors* **2022**, *22*, 4394. [CrossRef] [PubMed]
138. Lu, H.; Liu, Q.; Tian, D.; Li, Y.; Kim, H.; Serikawa, S. The cognitive internet of vehicles for autonomous driving. *IEEE Netw.* **2019**, *33*, 65–73. [CrossRef]
139. Javed, A.R.; Ur Rehman, S.; Khan, M.U.; Alazab, M.; Reddy, T. CANintelliIDS: Detecting in-vehicle intrusion attacks on a controller area network using CNN and attention-based GRU. *IEEE Trans. Netw. Sci. Eng.* **2021**, *8*, 1456–1466. [CrossRef]
140. Ahmad, W.; Rasool, A.; Javed, A.R.; Baker, T.; Jalil, Z. Cyber security in iot-based cloud computing: A comprehensive survey. *Electronics* **2022**, *11*, 16. [CrossRef]
141. Moulahi, T.; Jabbar, R.; Alabdulatif, A.; Abbas, S.; El Khediri, S.; Zidi, S.; Rizwan, M. Privacy-preserving federated learning cyber-threat detection for intelligent transport systems with blockchain-based security. *Expert Syst.* **2023**, *40*, e13103. [CrossRef]
142. Rehman Javed, A.; Jalil, Z.; Atif Moqurrab, S.; Abbas, S.; Liu, X. Ensemble adaboost classifier for accurate and fast detection of botnet attacks in connected vehicles. *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e4088. [CrossRef]
143. Zhuang, Y.; Wang, C.; Zheng, W.; Victor, N.; Gadekallu, T.R. ERACMA: Expressive and Revocable Access Control With Multi-Authority for AIoT-Enabled Human Centric Consumer Electronics. *IEEE Trans. Consum. Electron.* **2023** . [CrossRef]
144. Mukherjee, A.; Keshary, V.; Pandya, K.; Dey, N.; Satapathy, S.C. Flying ad hoc networks: A comprehensive survey. In *Information and Decision Sciences, Proceedings of the 6th International Conference on FICTA*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 569–580.
145. Shahwani, H.; Shah, S.A.; Ashraf, M.; Akram, M.; Jeong, J.P.; Shin, J. A comprehensive survey on data dissemination in Vehicular Ad Hoc Networks. *Veh. Commun.* **2022**, *34*, 100420. [CrossRef]
146. Sanguesa, J.A.; Torres-Sanz, V.; Garrido, P.; Martinez, F.J.; Marquez-Barja, J.M. A review on electric vehicles: Technologies and challenges. *Smart Cities* **2021**, *4*, 372–404. [CrossRef]
147. Sun, X.; Li, Z.; Wang, X.; Li, C. Technology development of electric vehicles: A review. *Energies* **2019**, *13*, 90. [CrossRef]
148. Wang, Y.; Liu, Q.; Mihankhah, E.; Lv, C.; Wang, D. Detection and isolation of sensor attacks for autonomous vehicles: Framework, algorithms, and validation. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 8247–8259. [CrossRef]
149. Majid, M.; Habib, S.; Javed, A.R.; Rizwan, M.; Srivastava, G.; Gadekallu, T.R.; Lin, J.C.W. Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review. *Sensors* **2022**, *22*, 2087. [CrossRef] [PubMed]
150. Liu, J.; Yan, C.; Xu, W. Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicles. *Las Vegas DEF CON* **2016**, *24*, 109.
151. Hikita, M. An introduction to ultrasonic sensors for vehicle parking. *New Electron.* **2010**, *12* .
152. Xu, W.; Yan, C.; Jia, W.; Ji, X.; Liu, J. Analyzing and enhancing the security of ultrasonic sensors for autonomous vehicles. *IEEE Internet Things J.* **2018**, *5*, 5015–5029. [CrossRef]
153. Wang, W.; Yao, Y.; Liu, X.; Li, X.; Hao, P.; Zhu, T. I can see the light: Attacks on autonomous vehicles using invisible lights. In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, Republic of Korea, 15–19 November 2021; pp. 1930–1944.
154. Cao, Y.; Wang, N.; Xiao, C.; Yang, D.; Fang, J.; Yang, R.; Chen, Q.A.; Liu, M.; Li, B. Invisible for both camera and lidar: Security of multi-sensor fusion based perception in autonomous driving under physical-world attacks. In Proceedings of the 2021 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 23 May 2021; pp. 176–194.
155. Zhu, Y.; Miao, C.; Hajiaghajani, F.; Huai, M.; Su, L.; Qiao, C. Adversarial Attacks against LiDAR Semantic Segmentation in Autonomous Driving. In Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems, Coimbra, Portugal, 15–17 November 2021; pp. 329–342.

156. Sun, H.T.; Peng, C.; Ding, F. Self-discipline predictive control of autonomous vehicles against denial of service attacks. *Asian J. Control* **2022**, *24*, 3538–3551. [CrossRef]
157. Hallyburton, R.S.; Liu, Y.; Cao, Y.; Mao, Z.M.; Pajic, M. Security Analysis of {Camera-LiDAR} Fusion Against {Black-Box} Attacks on Autonomous Vehicles. In Proceedings of the 31st USENIX Security Symposium (USENIX Security 22), Boston, MA, USA, 10–12 August 2022; pp. 1903–1920.
158. Cao, Y.; Xiao, C.; Cyr, B.; Zhou, Y.; Park, W.; Rampazzi, S.; Chen, Q.A.; Fu, K.; Mao, Z.M. Adversarial sensor attack on lidar-based perception in autonomous driving. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, London, UK, 11–15 November 2019; pp. 2267–2281.
159. Rahman, S.A.; Mourad, A.; El Barachi, M. An infrastructure-assisted crowdsensing approach for on-demand traffic condition estimation. *IEEE Access* **2019**, *7*, 163323–163340. [CrossRef]
160. Abbas, N.; Hajj, H.; Sharafeddine, S.; Dawy, Z. Traffic offloading with channel allocation in cache-enabled ultra-dense wireless networks. *IEEE Trans. Veh. Technol.* **2018**, *67*, 8723–8737. [CrossRef]
161. Nsouli, A.; Mourad, A.; Azar, D. Towards proactive social learning approach for traffic event detection based on arabic tweets. In Proceedings of the 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), Limassol, Cyprus, 25–29 June 2018; pp. 1501–1506.
162. Rahman, S.A.; Mourad, A.; El Barachi, M.; Al Orabi, W. A novel on-demand vehicular sensing framework for traffic condition monitoring. *Veh. Commun.* **2018**, *12*, 165–178.
163. Thing, V.L.; Wu, J. Autonomous vehicle security: A taxonomy of attacks and defences. In Proceedings of the 2016 IEEE International Conference on Internet of Things (Ithings) and IEEE Green Computing and Communications (Greencom) and IEEE Cyber, Physical and Social Computing (Cpscom) and IEEE Smart Data (Smartdata), Chengdu, China, 15–18 December 2016; pp. 164–170.
164. Petit, J.; Stottelaar, B.; Feiri, M.; Kargl, F. Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR. *Black Hat Eur.* **2015**, *11*, 995.
165. Claybrook, J.; Kildare, S. Autonomous vehicles: No driver... no regulation? *Science* **2018**, *361*, 36–37. [CrossRef]
166. Khan, F.; Kumar, R.L.; Kadry, S.; Nam, Y.; Meqdad, M.N. Autonomous vehicles: A study of implementation and security. *Int. J. Electr. Comput. Eng.* **2021**, *11*, 2088–8708. [CrossRef]
167. Sheehan, B.; Murphy, F.; Mullins, M.; Ryan, C. Connected and autonomous vehicles: A cyber-risk classification framework. *Transp. Res. Part A Policy Pract.* **2019**, *124*, 523–536. [CrossRef]
168. Psiaki, M.L.; Powell, S.P.; O'Hanlon, B.W. GNSS spoofing detection using high-frequency antenna motion and carrier-phase data. In Proceedings of the 26th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2013), Nashville, TN, USA, 16–20 September 2013; pp. 2949–2991.
169. Tang, K.; Shen, J.S.; Chen, Q.A. Fooling Perception via Location: A Case of Region-of-Interest Attacks on Traffic Light Detection in Autonomous Driving. In Proceedings of the NDSS Workshop on Automotive and Autonomous Vehicle Security (AutoSec), Alexandria, VA, USA, 1 January 2021.
170. He, X.; Hashemi, E.; Johansson, K.H. Secure platooning of autonomous vehicles under attacked GPS data. *arXiv* **2020**, arXiv:2003.12975.
171. Abojaradeh, M.; Jrew, B.; Al-Ababsah, H.; Al-Talafeeh, A. The effect of driver behavior mistakes on traffic safety. *Civ. Environ. Res.* **2014**, *6*, 39–54.
172. Koscher, K.; Czeskis, A.; Roesner, F.; Patel, S.; Kohno, T.; Checkoway, S.; McCoy, D.; Kantor, B.; Anderson, D.; Shacham, H.; et al. Experimental security analysis of a modern automobile. In Proceedings of the 2010 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 16–19 May 2010; pp. 447–462.
173. Ernst, J.M.; Michaels, A.J. LIN bus security analysis. In Proceedings of the IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society, Washington, DC, USA, 21–23 October 2018; pp. 2085–2090.
174. Zhang, G.; Yan, C.; Ji, X.; Zhang, T.; Zhang, T.; Xu, W. Dolphinattack: Inaudible voice commands. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, TX, USA, 30 October–3 November 2017; pp. 103–117.
175. Zhou, M.; Qin, Z.; Lin, X.; Hu, S.; Wang, Q.; Ren, K. Hidden voice commands: Attacks and defenses on the VCS of autonomous driving cars. *IEEE Wirel. Commun.* **2019**, *26*, 128–133. [CrossRef]
176. Roy, N.; Shen, S.; Hassanieh, H.; Choudhury, R.R. Inaudible Voice Commands: The Long-Range Attack and Defense. In Proceedings of the 15th USENIX Symposium on Networked Systems Design and Implementation (NSDI 18), Renton, WA, USA, 9–11 April 2018; pp. 547–560.
177. Taraba, M.; Adamec, J.; Danko, M.; Drgona, P. Utilization of modern sensors in autonomous vehicles. In Proceedings of the 2018 ELEKTRO, Mikulov, Czech Republic, 21–23 May 2018; pp. 1–5.
178. Garcia, F.D.; Oswald, D.; Kasper, T.; Pavlidès, P. Lock It and Still Lose It—on the (In)Security of Automotive Remote Keyless Entry Systems. In Proceedings of the 25th USENIX Security Symposium (USENIX Security 16), Austin, TX, USA, 10–12 August 2016.
179. Shen, J.; Won, J.Y.; Chen, Z.; Chen, Q.A. Drift with Devil: Security of Multi-Sensor Fusion based Localization in High-Level Autonomous Driving under GPS Spoofing. In Proceedings of the 29th USENIX Security Symposium (USENIX Security 20), Boston, MA, USA, 12–14 August 2020; pp. 931–948.

180. Zhao, Y.; Fapojuwo, A.O. Secrecy Outage Probability and Secrecy Capacity for Autonomous Driving in a Cascaded Rayleigh Fading Environment. In Proceedings of the 2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall), Norman, OK, USA, 27–30 September 2021; pp. 01–05.
181. Al-Sabaawi, A.; Al-Dulaimi, K.; Foo, E.; Alazab, M. Addressing malware attacks on connected and autonomous vehicles: recent techniques and challenges. In *Malware Analysis Using Artificial Intelligence and Deep Learning*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 97–119.
182. van de Beek, S.; Vogt-Ardatjew, R.; Leferink, F. Robustness of remote keyless entry systems to intentional electromagnetic interference. In Proceedings of the 2014 International Symposium on Electromagnetic Compatibility, Gothenburg, Sweden, 1–4 September 2014; pp. 1242–1245.
183. Sánchez, H.S.; Rotondo, D.; Puig, V.; Escobet, T.; Quevedo, J. Detection of replay attacks in autonomous vehicles using a bank of QPV observers. In Proceedings of the 2021 29th Mediterranean Conference on Control and Automation (MED), Puglia, Italy, 22–25 June 2021; pp. 1149–1154.
184. Porter, M.; Hespanhol, P.; Aswani, A.; Johnson-Roberson, M.; Vasudevan, R. Detecting generalized replay attacks via time-varying dynamic watermarking. *IEEE Trans. Autom. Control* **2020**, *66*, 3502–3517. [CrossRef]
185. Shrestha, R.; Bajracharya, R.; Kim, S. 6G enabled unmanned aerial vehicle traffic management: A perspective. *IEEE Access* **2021**, *9*, 91119–91136. [CrossRef]
186. Wesson, K.D.; Gross, J.N.; Humphreys, T.E.; Evans, B.L. GNSS signal authentication via power and distortion monitoring. *IEEE Trans. Aerosp. Electron. Syst.* **2017**, *54*, 739–754. [CrossRef]
187. Kerns, A.J.; Wesson, K.D.; Humphreys, T.E. A blueprint for civil GPS navigation message authentication. In Proceedings of the 2014 IEEE/ION Position, Location and Navigation Symposium-PLANS, Monterey, CA, USA, 5–8 May 2014; pp. 262–269.
188. Lim, K.; Islam, T.; Kim, H.; Joung, J. A Sybil attack detection scheme based on ADAS sensors for vehicular networks. In Proceedings of the 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 10–13 January 2020; pp. 1–5.
189. Aliebrahimi, S.; Miller, E.E. Effects of Cybersecurity Knowledge and Situation Awareness During Cyberattacks on Autonomous Vehicles. *Transp. Res. Part F Traffic Psychol. Behav.* **2023**, *96*, 82–91. [CrossRef]
190. Saber, O.; Mazri, T. Security of Autonomous Vehicles: 5g Iov (internet of Vehicles) Environment. *Int. Arch. Photogramm. Remote Sens. Spat. Inf. Sci.* **2022**, *48*, 157–163. [CrossRef]
191. Hasan, M.K.; Islam, S.; Gadekallu, T.R.; Ismail, A.F.; Amanlou, S.; Abdullah, S.N.H.S. Novel EBBDSA based Resource Allocation Technique for Interference Mitigation in 5G Heterogeneous Network. *Comput. Commun.* **2023**, *209*, 320–330. [CrossRef]
192. Sajid, F.; Javed, A.R.; Basharat, A.; Kryvinska, N.; Afzal, A.; Rizwan, M. An efficient deep learning framework for distracted driver detection. *IEEE Access* **2021**, *9*, 169270–169280. [CrossRef]
193. Caballero, W.N.; Rios Insua, D.; Banks, D. Decision support issues in automated driving systems. *Int. Trans. Oper. Res.* **2023**, *30*, 1216–1244. [CrossRef]
194. Sharafeddine, S.; Islambouli, R. On-demand deployment of multiple aerial base stations for traffic offloading and network recovery. *Comput. Netw.* **2019**, *156*, 52–61. [CrossRef]
195. Rathore, R.S.; Hewage, C.; Kaiwartya, O.; Lloret, J. In-vehicle communication cyber security: Challenges and solutions. *Sensors* **2022**, *22*, 6679. [CrossRef]
196. Newman, J.; Sun, Z.; Lee, D.J. Self-Driving Cars: A Platform for Learning and Research. In Proceedings of the 2020 Intermountain Engineering, Technology and Computing (IETC), Orem, UT, USA, 2–3 October 2020; pp. 1–5.
197. Ma, Z.; Schmittner, C. Threat modeling for automotive security analysis. *Adv. Sci. Technol. Lett.* **2016**, *139*, 333–339.
198. Mohammed, A.Z.; Man, Y.; Gerdes, R.; Li, M.; Celik, Z.B. Physical layer data manipulation attacks on the can bus. In Proceedings of the Intl. Workshop on Automotive and Autonomous Vehicle Security (AutoSec), Online, 24–28 April 2022.
199. Al Zaabi, A.O.; Yeun, C.Y.; Damiani, E. Autonomous vehicle security: Conceptual model. In Proceedings of the 2019 IEEE Transportation Electrification Conference and Expo, Asia-Pacific (ITEC Asia-Pacific), Seogwipo, Republic of Korea, 8–10 May 2019; pp. 1–5.
200. Sun, X.; Yu, F.R.; Zhang, P. A survey on cyber-security of connected and autonomous vehicles (CAVs). *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 6240–6259. [CrossRef]
201. Malik, S.; Sun, W. Analysis and simulation of cyber attacks against connected and autonomous vehicles. In Proceedings of the 2020 International Conference on Connected and Autonomous Driving (MetroCAD), Detroit, MI, USA, 27–28 February 2020; pp. 62–70.
202. Bathla, G.; Bhadane, K.; Singh, R.K.; Kumar, R.; Aluvalu, R.; Krishnamurthi, R.; Kumar, A.; Thakur, R.; Basheer, S. Autonomous vehicles and intelligent automation: Applications, challenges, and opportunities. *Mob. Inf. Syst.* **2022**, *2022*, 7632892. [CrossRef]
203. Manvi, S.S.; Tangade, S. A survey on authentication schemes in VANETs for secured communication. *Veh. Commun.* **2017**, *9*, 19–30. [CrossRef]
204. Kumar, N.A.; Kumar, P.S.; Victor, N.; Gadekallu, T.R.; Mohiddin, M.K.; Tiwari, S.; Minchula, V.K. Development of a double resampling based least-squares particle filter for accurate position estimation of a GPS receiver in Visakhapatnam region of the Indian subcontinent. *IEEE Sens. J.* **2023** .

205. Gürgens, S.; Zelle, D. A hardware based solution for freshness of secure onboard communication in vehicles. In Proceedings of the Computer Security: ESORICS 2018 International Workshops, CyberICPS 2018 and SECPRE 2018, Barcelona, Spain, 6–7 September 2018; Revised Selected Papers 2; Springer: Berlin/Heidelberg, Germany, 2019; pp. 53–68.
206. Nandy, T.; Idris, M.Y.I.B.; Noor, R.M.; Ahmedy, I.; Bhattacharyya, S. An enhanced two-factor authentication protocol for V2V communication in VANETs. In Proceedings of the 3rd International Conference on Information Science and Systems, Cambridge, UK, 19–22 March 2020; pp. 171–176.
207. Yoo, J.; Yi, J.H. Code-based authentication scheme for lightweight integrity checking of smart vehicles. *IEEE Access* **2018**, *6*, 46731–46741. [CrossRef]
208. Xu, C.; Liu, H.; Li, P.; Wang, P. A remote attestation security model based on privacy-preserving blockchain for V2X. *IEEE Access* **2018**, *6*, 67809–67818. [CrossRef]
209. Khatun, M.; Glaß, M.; Jung, R. An approach of scenario-based threat analysis and risk assessment over-the-air updates for an autonomous vehicle. In Proceedings of the 2021 7th International Conference on Automation, Robotics and Applications (ICARA), Prague, Czech Republic, 4–6 February 2021; pp. 122–127.
210. Qureshi, A.; Marvi, M.; Shamsi, J.A.; Aijaz, A. eUF: A framework for detecting over-the-air malicious updates in autonomous vehicles. *J. King Saud-Univ.-Comput. Inf. Sci.* **2021**, *34*, 5456–5467. [CrossRef]
211. Kondaveety, V.B.; Lamkuche, H.; Prasad, S. A zero trust architecture for next generation automobiles. *AIP Conf. Proc.* **2022**, *2519*, 030088.
212. Alipour, M.A.; Ghasemshirazi, S.; Shirvani, G. Enabling a Zero Trust Architecture in a 5G-enabled Smart Grid. *arXiv* **2022**, arXiv:2210.01739.
213. Lian, Z.; Zeng, Q.; Wang, W.; Gadekallu, T.R.; Su, C. Blockchain-based two-stage federated learning with non-IID data in IoMT system. *IEEE Trans. Comput. Soc. Syst.* **2022**, *10*, 1701–1710. [CrossRef]
214. Sarkar, S.; Choudhary, G.; Shandilya, S.K.; Hussain, A.; Kim, H. Security of zero trust networks in cloud computing: A comparative review. *Sustainability* **2022**, *14*, 11213. [CrossRef]
215. Javed, A.R.; Shahzad, F.; ur Rehman, S.; Zikria, Y.B.; Razzak, I.; Jalil, Z.; Xu, G. Future smart cities requirements, emerging technologies, applications, challenges, and future aspects. *Cities* **2022**, *129*, 103794. [CrossRef]
216. Sharma, P.; Gillanders, J. Cybersecurity and Forensics in Connected Autonomous Vehicles: A Review of the State-of-the-Art. *IEEE Access* **2022**, *10*, 108979–108996. [CrossRef]
217. Feng, X.; Dawam, E.S.; Amin, S. A New Digital Forensics Model of Smart City Automated Vehicles. In Proceedings of the 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Exeter, UK, 21–23 June 2017; pp. 274–279. [CrossRef]
218. Alexakos, C.; Katsini, C.; Votis, K.; Lalas, A.; Tzovaras, D.; Serpanos, D. Enabling digital forensics readiness for internet of vehicles. *Transp. Res. Procedia* **2021**, *52*, 339–346. [CrossRef]
219. Sharma, P.; Austin, D.; Liu, H. Attacks on machine learning: Adversarial examples in connected and autonomous vehicles. In Proceedings of the 2019 IEEE International Symposium on Technologies for Homeland Security (HST), Woburn, MA, USA, 5–6 November 2019; pp. 1–7.
220. Toledo, T.; Musicant, O.; Lotan, T. In-vehicle data recorders for monitoring and feedback on drivers' behavior. *Transp. Res. Part C Emerg. Technol.* **2008**, *16*, 320–331. [CrossRef]
221. Norden, J.; O'Kelly, M.; Sinha, A. Efficient black-box assessment of autonomous vehicle safety. *arXiv* **2019**, arXiv:1912.03618.
222. Royo, S.; Ballesta-Garcia, M. An overview of lidar imaging systems for autonomous vehicles. *Appl. Sci.* **2019**, *9*, 4093. [CrossRef]
223. Dykstra, J.; Sherman, A.T. Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform. *Digit. Investig.* **2013**, *10*, S87–S95. [CrossRef]
224. Kebande, V.; Venter, H. A functional architecture for cloud forensic readiness large-scale potential digital evidence analysis. In Proceedings of the European Conference on Cyber Warfare and Security, 2015; Academic Conferences International Limited: 2015, University of Hertfordshire, Hatfield, United Kingdom (UK) ; p. 373.
225. Terán, J.; Navarro, L.; Quintero M, C.G.; Pardo, M. Intelligent driving assistant based on road accident risk map analysis and vehicle telemetry. *Sensors* **2020**, *20*, 1763. [CrossRef] [PubMed]
226. Elyas, M.; Maynard, S.B.; Ahmad, A.; Lonie, A. Towards a systemic framework for digital forensic readiness. *J. Comput. Inf. Syst.* **2014**, *54*, 97–105. [CrossRef]
227. Valjarevic, A.; Venter, H. A harmonized process model for digital forensic investigation readiness. In Proceedings of the Advances in Digital Forensics IX: 9th IFIP WG 11.9 International Conference on Digital Forensics, Orlando, FL, USA, 28–30 January 2013; Revised Selected Papers 9; Springer: Berlin/Heidelberg, Germany, 2013; pp. 67–82.
228. Ab Rahman, N.H.; Glisson, W.B.; Yang, Y.; Choo, K.K.R. Forensic-by-design framework for cyber-physical cloud systems. *IEEE Cloud Comput.* **2016**, *3*, 50–59. [CrossRef]
229. Sun, Y.; Wu, L.; Wu, S.; Li, S.; Zhang, T.; Zhang, L.; Xu, J.; Xiong, Y.; Cui, X. Attacks and countermeasures in the internet of vehicles. *Ann. Telecommun.* **2017**, *72*, 283–295. [CrossRef]
230. Vivan, G.P.; Goberville, N.; Asher, Z.D.; Brown, N.; Rojas, J.F. *No Cost Autonomous Vehicle Advancements in CARLA through ROS*; SAE International: Warrendale, PA, USA, 2021.

231. Pérez-Gil, Ó.; Barea, R.; López-Guillén, E.; Bergasa, L.M.; Gomez-Huelamo, C.; Gutiérrez, R.; Diaz-Diaz, A. Deep reinforcement learning based control for Autonomous Vehicles in CARLA. *Multimed. Tools Appl.* **2022**, *81*, 3553–3576. [CrossRef]
232. Bojarski, M.; Del Testa, D.; Dworakowski, D.; Firner, B.; Flepp, B.; Goyal, P.; Zhang, X. End to end learning for self-driving cars. *arXiv* **2016**, arXiv:1604.07316.
233. Shah, S.; Dey, D.; Lovett, C.; Kapoor, A. Airsim: High-fidelity visual and physical simulation for autonomous vehicles. In *Proceedings of the Field and Service Robotics: Results of the 11th International Conference*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 621–635.
234. Bondi, E.; Dey, D.; Kapoor, A.; Piavis, J.; Shah, S.; Fang, F.; Dilkina, B.; Hannaford, R.; Iyer, A.; Joppa, L.; et al. Airsim-w: A simulation environment for wildlife conservation with uavs. In Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies, Menlo Park and San Jose, CA, USA, 20–22 June 2018; pp. 1–12.
235. Yao, S.; Zhang, J.; Hu, Z.; Wang, Y.; Zhou, X. Autonomous-driving vehicle test technology based on virtual reality. *J. Eng.* **2018**, *2018*, 1768–1771. [CrossRef]
236. Koenig, N.; Howard, A. Design and use paradigms for gazebo, an open-source multi-robot simulator. In Proceedings of the 2004 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)(IEEE Cat. No. 04CH37566), Sendai, Japan, 28 September–2 October 2004; Volume 3, pp. 2149–2154.
237. Furrer, F.; Burri, M.; Achtelik, M.; Siegwart, R. Rotors—a modular gazebo mav simulator framework. *Robot. Oper. Syst. (Ros) Complet. Ref.* **2016**, *1*, 595–625.
238. Krajzewicz, D. Traffic simulation with SUMO–simulation of urban mobility. *Fundam. Traffic Simul.* **2010**, *145*, 269–293.
239. Krajzewicz, D.; Erdmann, J.; Behrisch, M.; Bieker, L. Recent development and applications of SUMO-Simulation of Urban MObility. *Int. J. Adv. Syst. Meas.* **2012**, *5* .
240. Schmittner, C.; Griessnig, G.; Ma, Z. Status of the Development of ISO/SAE 21434. In Proceedings of the Systems, Software and Services Process Improvement: 25th Eurtpean Conference, EuroSPI 2018, Bilbao, Spain, 5–7 September 2018; Proceedings 25; Springer: Berlin/Heidelberg, Germany, 2018; pp. 504–513.
241. Martin, J.; Carter, A. Nhtsa cybersecurity research. In Proceedings of the 25th International Technical Conference on the Enhanced Safety of Vehicles (ESV) National Highway Traffic Safety Administration, Washington, DC, USA, 5 June 2017.
242. Schmittner, C.; Ma, Z.; Reyes, C.; Dillinger, O.; Puschner, P. Using SAE J3061 for automotive security requirement engineering. In Proceedings of the Computer Safety, Reliability, and Security: SAFECOMP 2016 Workshops, ASSURE, DECSoS, SASSUR, and TIPS, Trondheim, Norway, 20 September 2016; Proceedings 35; Springer: Berlin/Heidelberg, Germany, 2016; pp. 157–170.
243. Udayakumar, P. Manage and Secure AVS. In *Design and Deploy Azure VMware Solutions: Build and Run VMware Workloads Natively on Microsoft Azure*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 341–387.
244. Anderson, J.M.; Nidhi, K.; Stanley, K.D.; Sorensen, P.; Samaras, C.; Oluwatola, O.A. *Autonomous Vehicle Technology: A Guide for Policymakers*; Rand Corporation: Santa Monica, CA, USA, 2014.
245. Abu Bakar, A.I.; Abas, M.A.; Muhamad Said, M.F.; Tengku Azhar, T.A. Synthesis of autonomous vehicle guideline for public road-testing sustainability. *Sustainability* **2022**, *14*, 1456. [CrossRef]
246. Mohsin, A.H.; Zaidan, A.; Zaidan, B.; Albahri, O.; Ariffin, S.A.B.; Alemran, A.; Enaizan, O.; Shareef, A.H.; Jasim, A.N.; Jalood, N.; et al. Finger vein biometrics: Taxonomy analysis, open challenges, future directions, and recommended solution for decentralised network architectures. *IEEE Access* **2020**, *8*, 9821–9845. [CrossRef]
247. Bouchouia, M.L.; Labiod, H.; Jelassi, O.; Monteuuis, J.P.; Jaballah, W.B.; Petit, J.; Zhang, Z. A survey on misbehavior detection for connected and autonomous vehicles. *Veh. Commun.* **2023**, *41*, 100586. [CrossRef]
248. De Marco, L.; Kechadi, M.T.; Ferrucci, F. Cloud forensic readiness: Foundations. In Proceedings of the Digital Forensics and Cyber Crime: Fifth International Conference, ICDF2C 2013, Moscow, Russia, 26–27 September 2013; Revised Selected Papers 5; Springer: Berlin/Heidelberg, Germany, 2014; pp. 237–244.