









Review

Autonomous Vehicles: Sophisticated Attacks, Safety Issues, Challenges, Open Topics, Blockchain, and Future Directions

Anastasios Giannaros ¹, Aristeidis Karras ^{1,*}, Leonidas Theodorakopoulos ², Christos Karras ^{1,*},
Panagiotis Kranias ³, Nikolaos Schizas ¹, Gerasimos Kalogeratos ² and Dimitrios Tsolis ⁴

¹ Computer Engineering and Informatics Department, University of Patras, 26504 Patras, Greece; giannaros@ceid.upatras.gr (A.G.); nschizas@ceid.upatras.gr (N.S.)

² Department of Management Science and Technology, University of Patras, 26334 Patras, Greece; theodleo@upatras.gr (L.T.); gkalogeratos@upatras.gr (G.K.)

³ School of Electrical and Computer Engineering, National Technical University of Athens, 15773 Athens, Greece; el16729@mail.ntua.gr

⁴ Department of History and Archaeology, University of Patras, 26504 Patras, Greece; dtsolis@upatras.gr

* Correspondence: akarras@ceid.upatras.gr (A.K.); c.karras@ceid.upatras.gr (C.K.)

Abstract: Autonomous vehicles (AVs), defined as vehicles capable of navigation and decision-making independent of human intervention, represent a revolutionary advancement in transportation technology. These vehicles operate by synthesizing an array of sophisticated technologies, including sensors, cameras, GPS, radar, light imaging detection and ranging (LiDAR), and advanced computing systems. These components work in concert to accurately perceive the vehicle's environment, ensuring the capacity to make optimal decisions in real-time. At the heart of AV functionality lies the ability to facilitate intercommunication between vehicles and with critical road infrastructure—a characteristic that, while central to their efficacy, also renders them susceptible to cyber threats. The potential infiltration of these communication channels poses a severe threat, enabling the possibility of personal information theft or the introduction of malicious software that could compromise vehicle safety. This paper offers a comprehensive exploration of the current state of AV technology, particularly examining the intersection of autonomous vehicles and emotional intelligence. We delve into an extensive analysis of recent research on safety lapses and security vulnerabilities in autonomous vehicles, placing specific emphasis on the different types of cyber attacks to which they are susceptible. We further explore the various security solutions that have been proposed and implemented to address these threats. The discussion not only provides an overview of the existing challenges but also presents a pathway toward future research directions. This includes potential advancements in the AV field, the continued refinement of safety measures, and the development of more robust, resilient security mechanisms. Ultimately, this paper seeks to contribute to a deeper understanding of the safety and security landscape of autonomous vehicles, fostering discourse on the intricate balance between technological advancement and security in this rapidly evolving field.



Citation: Giannaros, A.; Karras, A.; Theodorakopoulos, L.; Karras, C.; Kranias, P.; Schizas, N.; Kalogeratos, G.; Tsolis, D. Autonomous Vehicles: Sophisticated Attacks, Safety Issues, Challenges, Open Topics, Blockchain, and Future Directions. *J. Cybersecur. Priv.* **2023**, *3*, 493–543. <https://doi.org/10.3390/jcp3030025>

Academic Editor: Danda B. Rawat

Received: 29 June 2023

Revised: 24 July 2023

Accepted: 31 July 2023

Published: 5 August 2023

Keywords: autonomous vehicles; cyber security AV attacks; AV attacks; AV safety; emotional intelligence; blockchain in AVs; big data and AVs; real-time decision making



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The advent of autonomous vehicles (AVs) represents an important progression toward the development of intelligent transportation systems. This development prepares the way for the emergence of brand-new opportunities to improve mobility, environmental sustainability, and other related sectors of transportation. As a result of the development and progression of this technology, a rising focus has been placed on fully autonomous vehicles, also known as FAVs. FAVs represent the most advanced form of vehicular automation. In terms of the Society of Automotive Engineers (SAE) categorization, full autonomy corresponds to level 5, which denotes complete driving automation. Vehicles at this level

are engineered to handle all aspects of dynamic driving tasks under all conditions. They are capable of independently operating, even when faced with challenging road and climatic circumstances. The onus of safe operation under every driving condition is entirely on the vehicle's systems, requiring no human intervention. These vehicles have been developed to be capable of handling all parts of dynamic driving activities on their own, even when faced with difficult road and climatic circumstances. The utilization of accurate, trustworthy, and dependable sensor technologies is essential to their functioning. A conceptual representation of the functional architecture of these FAVs can be viewed in Figure 1.

Prominent examples of such vehicles in today's landscape include the Google Driverless Car [1], AnnieWAY [2], and Stanford Shelley [3]. These vehicles leverage light imaging detection and ranging (LiDAR) technology to detect objects and recognize traffic signs. The sensor data collected by these technologies form a foundation in mission planning, and the onboard automated systems use this information to make key operational decisions. For instance, if an obstacle is detected by LiDAR, the mission plan of the vehicle adjusts to evade a potential collision.

On the other hand, the growing complexity of AVs also brings about the emergence of new difficulties. An important concern that is emerging is the urge to ensure the safety and resilience of AV sensors in the face of cyber attacks. The implications of this kind of attack have the potential to be devastating due to the fact that compromised sensor data might lead to improper driving reactions, accidents, and even deaths [4]. Camera hacking is one major concern. In addition to incorrectly reading road signs, an attacker could also manipulate the camera feed to hide obstacles or other vehicles or create phantom objects, leading to incorrect and potentially disastrous decision-making by the vehicle's AI. Similarly, LiDAR and radar systems, which are used by AVs to create a detailed 3D map of their surroundings, could also be targeted. An attacker could potentially feed the system false data, causing it to 'see' obstacles that do not exist, or fail to detect those that do. The GPS system, which is crucial for navigation, can also be a target. For instance, GPS spoofing attacks can feed false location information to the AV, leading it to go off course or even to dangerous locations. As an example, a hacked camera can incorrectly read a speed limit sign, putting the lives of the vehicle's passengers and anybody else who uses the road in danger.

Beyond the vehicle itself, the era of interconnected autonomous vehicles is upon us, where vehicles can communicate and share environmental data not just amongst themselves but also with wider infrastructural systems [5]. Although this networking capability enhances operational efficiency, it is susceptible to potential cyber-attacks. Embedded control systems such as engine control units (ECUs), which currently manage functions like electric window controls, may become vulnerable. Any malicious alteration in the programming code of these critical components during design or implementation can degrade hardware performance or remove crucial data, leading to potentially serious consequences [6].

A noteworthy instance of such an intrusion was documented in [7], where a virus was developed to manipulate messages transmitted via the controller area network (CAN) bus, a vital communication system linking all vehicle components. This malware was capable of remotely locking the doors of a vehicle by intercepting the corresponding communications of the core system. Such security vulnerabilities related to the CAN bus pose significant threats to driver safety and privacy, and it is crucial to undertake countermeasures [8]. In this survey, and, in particular, in Table 1, we review and present the state-of-the-art surveys in the field of autonomous vehicles and categorized them based on their scope. Moreover, after presenting each work, we highlight the scope of our work and the gaps in the different fields of autonomous vehicles that we aim to reduce.

Table 1. Summary of surveys of autonomous vehicles.

Reference	Survey	Scope
[9]	A survey of autonomous vehicles: Enabling communication technologies and challenges	Focuses on the development of vehicular communication technologies and AVs surrounding data gathering using sensors.
[10]	Artificial intelligence applications in the development of autonomous vehicles: A survey	Provides a detailed review of the utilization of AI in supporting primary applications in AVs, namely perception, localization & mapping, and decision making.
[11]	Autonomous vehicles that interact with pedestrians: A survey of theory and practice	Explores factors influencing pedestrian behavior studies, featuring both classical works on pedestrian–driver interaction and contemporary ones involving autonomous vehicles.
[12]	Computer vision for autonomous vehicles: Problems, datasets and state of the art	Examines perception-related issues for autonomous vehicles, discussing the modular pipeline and end-to-end learning-based approaches.
[13]	Planning and decision-making for autonomous vehicles	Offers an overview of emerging trends and challenges in the realm of intelligent and self-driving vehicles.
[14]	A review on autonomous vehicles: Progress, methods, and challenges	Investigates the current state of research in environmental detection, pedestrian detection, path planning, motion control, and vehicle cyber security for autonomous vehicles.
Our Work	Autonomous Vehicles: Sophisticated Attacks, Safety Issues, Challenges, Open Topics, Blockchain, and Future Directions	Our survey comprehensively investigates safety and attack vectors associated with autonomous vehicles, identifying novel threats and suggesting potential blockchain applications and future research directions.

The purpose of this work is to investigate, highlight, and contribute to the understanding and mitigation of the difficulties that exist in AVs by presenting all factors that frame them, including the following:

- We present an overview of the state of the art in this field of study by providing an analysis that is comprehensive, specific, and up-to-date on the safety problems that are associated with autonomous cars and the countermeasures that are related to them;
- We analyze all potential attack vectors on autonomous vehicles, an endeavor that has not been previously undertaken to this extent. To the best of our knowledge, this paper represents the first comprehensive exploration of such a wide range of potential threats—a significant contribution relative to previous surveys, which typically address only a subset of these threats;
- We highlight and explore unresolved issues and potential research directions in this domain, thereby creating a roadmap for future studies in academia;
- We present a concrete survey that aims to help readers understand the broader scope of AVs by navigating different sections in the survey and gaining knowledge that is summarized based on all references presented here, without requiring review of all recent works.

The remainder of this article is organized as follows. In Section 2, an overview of autonomous vehicles (AVs) is presented. Section 3 highlights security attacks on sensor systems of AVs. In Section 4, cyber security attacks on vehicular networks are analyzed, while in Section 5, the vulnerabilities of AVs are discussed. In Section 6, vulnerabilities in deep neural networks and machine learning are shown, while Section 7, highlights how big data can be applied to AVs. In Section 8, the use of blockchain in AVs is presented, with an exploration of how it enhances security. Lastly, in Section 9, a discussion takes place, and Section 10 concludes the article by presenting summarizing points and potential future directions.

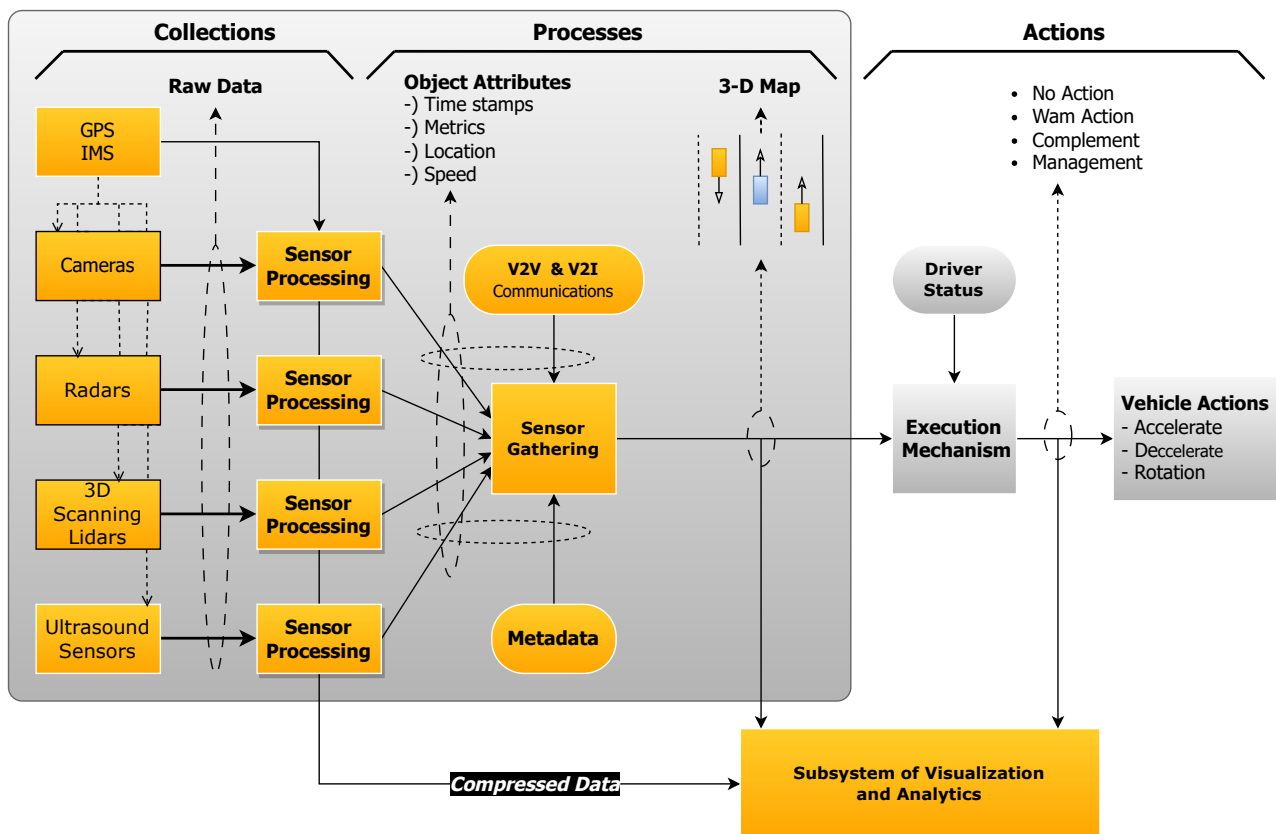


Figure 1. Autonomous vehicle overview.

2. Overview of Autonomous Vehicles (AVs)

The reviewed research papers delve into the various aspects of autonomous vehicles (AVs), ranging from sensor technologies to user acceptance. Vargas et al. provided insights into the roles of RADAR, LiDAR, ultrasonic cameras, and GNSS sensors in AVs and highlighted their performance under different weather conditions [15]. Parekh et al. comprehensively evaluated the technologies integral to AVs, encompassing environment detection, pedestrian identification, path planning, motion control, and cyber security [14]. Tian et al. underscored the criticality of testing deep-neural-network-driven autonomous cars to expose and rectify behaviors that could trigger potentially fatal incidents [16]. Lastly, Jing et al. investigated the multitude of factors influencing public acceptance of AVs, including perceived ease of use, attitude, social norms, trust, perceived usefulness, risk perception, compatibility, safety, performance-to-price value, mobility, symbolic value, and environmental friendliness [17]. In essence, these studies present a holistic understanding of the complexities, technologies, and societal factors contributing to the development and adoption of autonomous vehicles.

In terms of an overview, autonomous vehicles represent the convergence of advanced technologies aimed at revolutionizing transportation. These vehicles leverage a spectrum of sensors and artificial intelligence to perceive the surrounding environment and make independent decisions. From enhancing road safety by minimizing human error to providing mobility for individuals unable to operate traditional vehicles, AVs hold significant promise. However, their successful integration into everyday life hinges on overcoming various challenges, including robustness against diverse weather conditions, foolproof cyber security, and public acceptance. As they stand on the precipice of widespread adoption, autonomous vehicles represent a transformative potential that could redefine the landscape of transportation.

2.1. Essential Security Principles

Definition 1 (Data Processing). *Data processing, which is at the core of computer security, has an intricate connection with information security as an entire area, which is an even broader area of study.*

Description 1 (Security Measures). *Antivirus software, which must carefully evaluate sensor data in order to allow for proper responses, is an excellent example of this connection as a result of the manner in which it works. In the process of performing their primary tasks, such systems run the risk of accidentally turning into attractive targets for attackers who seek to take advantage of the data-rich features they provide.*

As a consequence of this, it is very necessary to apply the concepts of privacy and security to autonomous vehicles in order to strengthen their defensive systems against possible attacks. The basic triangle is the driving force behind these fundamental principles. Figure 2 illustrates a visual representation of the way in which the triangle of confidentiality, integrity, and availability (CIA) applies to the data security principles of autonomous vehicles.

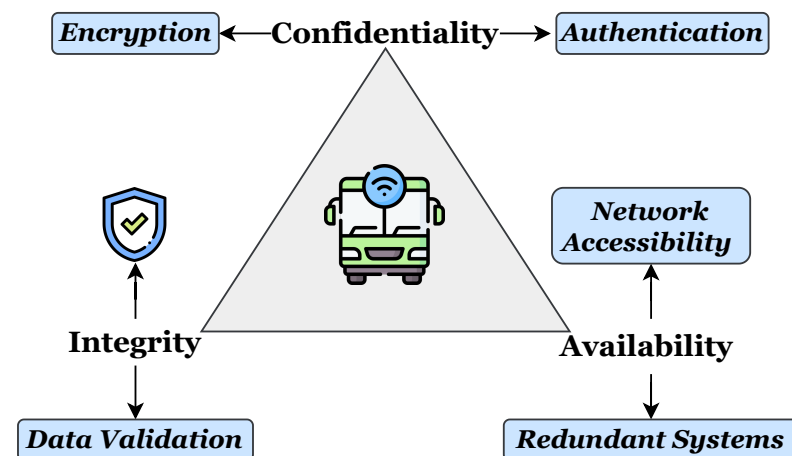


Figure 2. Triangle of confidentiality, integrity, and availability for AVs.

- **Confidentiality** : This principle underscores the importance of preventing unauthorized data access. Upholding confidentiality is crucial to preempt potential misappropriation or exploitation of sensitive information, which, if mishandled, could compromise the safe and reliable operation of AV systems.
- **Integrity**: Integrity ensures the authenticity, accuracy, and consistency of data over their entire life cycle. This involves not only detecting unauthorized data access but also thwarting unsanctioned data modification. Preservation of data integrity is critical to maintaining the trustworthiness of a system and its decision-making abilities.
- **Availability**: A system's effectiveness is contingent upon the consistent availability of its functionalities and its ability to perform as expected. In the context of AVs, any compromise in availability could have immediate and severe safety implications.

Besides these fundamental concepts, AV security may also attempt to accomplish additional attributes, depending on the specific circumstances and application, including privacy, authenticity, accountability, non-repudiation, and reliability. These characteristics, when considered together, help to provide an integrated and all-encompassing security framework for autonomous vehicles, which helps to protect such vehicles from a wide variety of possible threats.

2.2. Spectrum of Autonomous Vehicles

As mentioned earlier, the automation process in vehicles comprises several levels, each denoting varying degrees of autonomy. The National Highway Traffic Safety Administration (NHTSA) [18] has proposed a detailed six-tier categorization to encapsulate the spectrum of vehicle automation:

- **No Automation (Level 0):** At this level, vehicle operation is entirely under the control of the human driver, including the core functions of steering, brakes, throttle, and motive power.
- **Driver assistance (Level 1):** At this level, while the vehicle operation continues to be largely controlled by the driver, certain driving assistance features, such as automatic braking or lane assistance, may be integrated into the vehicle's system.
- **Partial Automation (Level 2):** At this level, the vehicle is equipped with advanced automated capabilities that can control both steering and acceleration/deceleration, but the driver must maintain active engagement with the driving environment and be ready to take control if required.
- **Conditional Automation (Level 3):** Vehicles at this level can handle all critical driving functions under certain conditions. However, the driver must be ready to retake control when the system requests, thus maintaining an active supervisory role.
- **High Automation (Level 4):** Vehicles at this level can perform all necessary driving tasks autonomously under specific conditions. The driver has the option to control the vehicle, but it is not a requirement, and the vehicle can operate independently when conditions permit.
- **Full Automation (Level 5):** This level represents the epitome of vehicular automation, where the vehicle is capable of executing all necessary driving functions throughout an entire journey, under all driving conditions, without any form of human intervention.

2.3. Emotional Intelligence in Autonomous Vehicles

As we approach an era of fully automated vehicles, emotional intelligence has emerged as a vital area of exploration. Emotional intelligence, defined as the capacity to comprehend, manage, and respond appropriately to emotions in oneself and others, is a characteristic typically attributed to humans. However, the integration of emotional intelligence into autonomous vehicles is becoming increasingly feasible with the rapid advancements in artificial intelligence (AI) and machine learning [19].

Autonomous vehicles, through sensor technologies, AI, and sophisticated algorithms, already demonstrate cognitive intelligence in terms of navigating complex environments, making split-second decisions, and communicating with other vehicles or infrastructure. Nevertheless, to fully understand and interact with their human passengers, these vehicles also need to possess emotional intelligence. This intersection between autonomous vehicles and emotional intelligence could transform the passenger experience, safety, and public acceptance of these vehicles [20]. Research is underway to develop systems that can identify, comprehend, and react to the emotional states of passengers. For instance, if the vehicle detects signs of passenger anxiety during a high-speed drive, it could respond by slowing down or by providing reassuring communication about the journey's safety. Furthermore, it could tailor the in-vehicle environment, adjusting elements like lighting, temperature, or music to help calm the passenger [21].

The integration of emotional intelligence in AVs can also enhance safety. A vehicle that can recognize a passenger's fatigue or medical distress could take preventative actions such as slowing down, stopping, or even calling for medical assistance [22]. Moreover, emotional intelligence in AVs could promote public acceptance. As these vehicles become more attuned to human emotions and responsive in a human-like manner, they may help mitigate the uncertainty or discomfort associated with relinquishing control to a machine. It is important to note that the integration of emotional intelligence into autonomous vehicles raises several challenges and ethical considerations, including privacy, data security, and the risk of over-reliance on technology. Nevertheless, it represents an exciting frontier in the

evolution of autonomous vehicles, potentially contributing to a safer, more personalized, and more human-like autonomous driving experience [23].

3. Security Attacks on AV Sensors: A Closer Examination of GPS Systems

Autonomous vehicles (AVs) substantially draw upon sensor systems for navigation and critical decision-making. Among these, the global positioning system (GPS) holds notable significance, providing precise geolocation, speed, and temporal data, regardless of the vehicle's global position and meteorological conditions. Nevertheless, as with any technologically sophisticated system, GPS is not immune to potential security compromises.

Security compromises generally manifest in various types, classified as:

1. **Spoofing Attacks:** In such instances, adversaries generate synthetic signals to mimic legitimate GPS signals. These deceptive signals, once received by the AV, are mistaken as authentic, thereby misleading the AV into calculating its location inaccurately.
2. **Jamming Attacks:** During these attacks, the perpetrator utilizes devices that transmit signals matching the frequency of the GPS signals, with the intent to overwhelm the authentic signals. This interference inhibits the GPS receiver's ability to establish a connection with the original GPS signals, effectively impeding its geolocation determination.
3. **Meaconing Attacks:** These attacks entail the interception of GPS signals, which are then deliberately delayed before retransmission. This activity can cause the GPS receiver to miscalculate its position.
4. **Replay Attacks:** These consist of capturing GPS signals and retransmitting them at an alternative time or location. This action can mislead the GPS receiver into miscomputing its position or time.

Each of these attacks has severe implications for AVs, potentially leading to navigational inaccuracies or even disastrous vehicular collisions. Thus, the implementation of robust security countermeasures to protect GPS systems against these breaches becomes an academic and industrial priority.

3.1. The Significance and Applicability of Sensor Security in Autonomous Vehicles

Security breaches targeted at sensor systems in autonomous vehicles (AVs) have emerged as a significant cause for concern due to their potential to compromise the vehicle's safety and the well-being of its passengers. AVs deploy a complex array of sensors, including but not limited to cameras, LiDAR, and radar. These sensors are essential for interpreting the surrounding environment and facilitating crucial decision-making processes. The compromise of these sensor systems could result in a distorted understanding of the environment, which could, in turn, elevate the risk of accidents and safety hazards.

Historically, there have been various demonstrations highlighting the potential of such security attacks on AV sensors. These include sophisticated spoofing attacks capable of deceiving sensors into acknowledging non-existent obstacles and jamming attacks that effectively interrupt the sensors' capabilities in accurately detecting objects. Worryingly, the equipment needed to execute these attacks can often be simple and easy to procure, such as a laser pointer or a radio transmitter, thus increasing the potential pool of attackers.

As AVs become more commonplace in our transportation landscape, the importance of addressing the security vulnerabilities of AV sensors becomes increasingly clear. This recognition underpins the need for the development and implementation of rigorous security measures tailored to detect and neutralize attacks on AV sensors. Alongside these security provisions, it is critical to raise public awareness regarding the potential risks associated with security attacks on AVs.

Additionally, the creation and enforcement of comprehensive standards play a critical role in ensuring the safety and security of AVs. These standards would serve to reinforce the safety framework for autonomous vehicles, managing and mitigating the risks associated with potential security breaches of their sensor systems.

In conclusion, the potential consequences of security intrusions on AV sensors are dangerous and global, threatening the protection of both the vehicle and its occupants. As the community moves towards a future characterized by the increasing quantity of autonomous vehicles (AVs), it becomes vital to develop and implement robust security measures supported by comprehensive and extensive standards in order to ensure the ongoing safety and security of these advanced vehicles.

3.2. Vulnerability of Global Positioning Systems

In the spectrum of autonomous vehicles, global positioning systems (GPS) are integral, facilitating accurate location tracking and route navigation. However, this reliance creates a potential vulnerability that can be exploited by malicious entities. Given the open accessibility of GPS technology, an adversary could potentially manipulate signals, provide incorrect navigational instructions, or even trigger vehicle crashes, posing significant safety threats [24].

GPS-based attacks on autonomous vehicles take two primary forms: jamming and spoofing. Jamming involves an adversary broadcasting a more potent signal at the identical frequency as the GPS, consequently causing temporary interference [25]. This type of attack can significantly hinder the operation of autonomous vehicles, as these highly sophisticated vehicles rely heavily on accurate GPS data for efficient navigation and overall functionality.

Spoofing, a more invisible form of attack, involves an attacker disseminating falsified GPS signals designed to emulate authentic ones. This deceptive method leads the receiver to inadvertently acknowledge the fraudulent signals as genuine. Typically, the process of GPS spoofing incorporates an initial phase of GPS jamming to obstruct real signals, subsequently followed by the broadcast of counterfeit signals, thereby fooling the system [26].

Given the intrinsically unguarded nature of public GPS systems, the singular defense mechanism against GPS spoofing lies in the domain of authentication. Achieving this safeguard necessitates the use of precise encryption techniques [27]. Regardless of these concerns, the scientific community must address these vulnerabilities and develop effective countermeasures to ensure the safety and dependability of autonomous vehicles in an era of GPS-centric navigation.

Due to the design of GPS systems, which are inclined to accept stronger signals, a well-executed attack can imperceptibly alter a vehicle's location by transmitting a strong, fake signal [28]. Various countermeasures, such as monitoring of identification codes, satellite signals, and timing intervals, have been proposed to combat these attacks. It is known, for instance, that the expected signal strength is approximately 163 decibel watts, so a countermeasure could consist of blocking signals with higher frequencies [29]. In their research, the authors developed an antenna-array-based hybrid antijamming and antispoofing method for GPS receivers. Using a compressed sensing framework, they determine the direction of arrival (DOA) of the despreading satellite navigation signal and identify the deception signal following the elimination of the interference via subspace projection. The receiver uses adaptive multi-beamforming to accomplish undistorted reception of the authentic satellite signal and to suppress deception based on the DOA of the authentic and spoofing signals.

However, these measures can be circumvented if the attacker's signals are sophisticated enough to mimic genuine ones convincingly, causing the validation checks to fail and resulting in the manipulation of the GPS device. Currently, an entirely foolproof and practical solution to these GPS-based attacks remains inaccessible. The use of military-grade cryptography currently stands as the only feasible solution that can definitively prevent both GPS jamming and spoofing attacks.

In the broader perspective of emotional intelligence, the ability of autonomous vehicles to recognize and react appropriately to these threats is a significant challenge. Just as humans must navigate and respond to deceptive cues in social contexts, autonomous vehicles must discern between genuine and deceptive signals in their environment. This

ability to perceive and react appropriately under a potential attack is crucial to the future development and widespread acceptance of autonomous vehicles.

3.3. Exposure of Light Detection and Ranging (LiDAR) Systems to Security Attacks

LiDAR systems which are essential components in autonomous vehicles, function as range-finding sensors. By emitting light pulses and measuring the time taken for these pulses to reflect off distant surfaces, they generate a three-dimensional map of the vehicle's environment. These laser pulses, which are produced hundreds of times per second, are typically reflected off a rotating mirror, creating a scan. Extra pulses, referred to as echoes, contribute to the vehicle's ability to detect objects under varied weather conditions [30].

Despite their critical role in facilitating safe autonomous navigation, LiDAR systems are susceptible to potential security threats. One such threat is relay signal attacks, a variation of replay attacks, which aim to misplace targets from their actual positions by rebroadcasting the original signal provided by the target vehicle's LiDAR from an altered location. This attack can be executed inexpensively using just two transceivers, as demonstrated in [31].

Another concerning threat is spoofing signal attacks, an extension of relay signal attacks. An adversary can create phantom objects by transmitting a signal of the same frequency as the scanner. LiDAR systems typically listen for incoming reflections for a minimum of 1.33 microseconds. To successfully inject signals into LiDAR, the false signal must enter this window, which allows an attacker to manipulate the perceived location of objects by delaying the initial signal before relaying it.

Such attacks can cause autonomous vehicles to slow down or even stop, potentially resulting in fatal accidents, particularly on highways [32–34]. Several potential countermeasures can be employed, including the use of non-predictable LiDAR, which skips a pulse but continues to listen for incoming pulses. Another strategy is to reduce the LiDAR pulse time, thereby reducing the attack window in the sensor, although this also shortens the sensor's operational range [31]. Given that LiDAR pulses are not currently encoded, one promising direction for future research is the exploration of LiDAR pulse encoding as a potential means of mitigating these attacks. Figure 3 is a visual representation of the Relaying and Spoofing signal attacks on LiDAR.

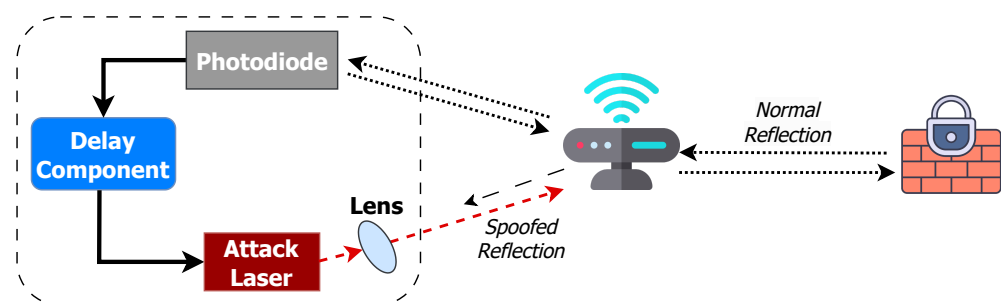


Figure 3. Relaying and spoofing signal attacks on LiDAR.

LiDAR systems in autonomous vehicles can be vulnerable to security attacks, which can have serious implications for road safety. Here are some examples of how security assaults on LiDAR sensors can manifest in real-world autonomous vehicles:

Spoofing attacks: Adversaries can create false signals that mimic the real signals received by LiDAR sensors, causing the autonomous vehicle to misinterpret its surroundings. For example, an attacker could create a fake obstacle close to the front of a victim AV to cause it to swerve or brake suddenly [32].

Cyber-level attacks: Attackers can disrupt sensor data by compromising the LiDAR system, even if they lack situational awareness. This can result in compromised perception and tracking in multisensor AVs, which can be critical for road safety [35].

Electromagnetic interference (EMI): LiDAR sensors can be vulnerable to IEMI, which affects the time-of-flight circuits that make up modern LiDAR systems. This can force

the AV perception system to misdetect or misclassify objects and perceive non-existent obstacles, which can be dangerous for road safety [36].

Adversarial objects: Attackers can generate adversarial objects that can evade LiDAR-based detection systems under various conditions. For example, an attacker could create an object that appears normal to a human observer but is misclassified by the LiDAR system, causing the AV to make incorrect decisions [37].

To mitigate these vulnerabilities, researchers have proposed various countermeasures, such as probabilistic data asymmetry monitors and security-aware fusion approaches [35]. It is important to take a sensible risk-management approach to tackle potential cyber security threats to ensure the successful embracing of autonomous vehicles in future transport systems [38,39].

3.4. The Vulnerability of AV Cameras to Security Attacks

Cameras serve as the optical eyes of autonomous vehicles, providing digital video feeds of the external world. They are employed in various capacities in AVs, including lane detection, traffic sign recognition, and headlight detection, among others [40–42].

One significant vulnerability of these camera systems lies in their susceptibility to being temporarily or permanently obscured by targeted light interference. Such a compromise could pose a substantial risk to passenger safety, particularly in instances where the vehicle's ability to detect essential road signage or traffic signals is undermined [31]. Notably, this has been acknowledged as a potential area of concern by leading industry stakeholders, with instances recorded of autonomous vehicles, such as those developed by Google, experiencing difficulties in low-light conditions [43].

A similar form of attack capitalizes on the period of recovery required by cameras after exposure to high-intensity light. During this interval, the autonomous vehicle may be more vulnerable to unperceived obstacles. Such an attack could be orchestrated by intermittently switching a light source on and off and could be initiated from any direction—the front, back, or side of the vehicle [31].

Several mitigation strategies could be employed to counteract these forms of attacks. For instance, employing a configuration of multiple cameras, each capturing the same visual field, could present an added layer of complexity for an attacker aiming to confuse all cameras at once. Alternatively, the integration of a detachable near-infrared-cut filter could provide the ability to selectively filter near-infrared light, enhancing the camera's resilience to light-based attacks. Moreover, photochromic lenses, with their unique capacity to change color and block specific light wavelengths, could also serve as a potential protective measure [31].

In the broader context of emotional intelligence, these threats underscore the need for autonomous vehicles to possess a degree of perceptual intelligence. This would enable them to recognize and adjust to potentially harmful inputs, similar to how humans process and react to threats in their environment. This aspect of emotional intelligence in AVs is critical for mitigating safety concerns and advancing the technology's development and acceptance.

3.5. The Susceptibility of Inertial Measurement Units (IMUs) to Security Attacks

The inertial measurement unit (IMU), an integral part of an autonomous vehicle's sensor ecosystem, integrates the functionalities of a gyroscope and an accelerometer. This combination produces vital information regarding the vehicle's orientation, acceleration, and velocity. The IMU also monitors changes in environmental dynamics, such as the gradient of the road, enabling the vehicle to navigate varied terrains efficiently.

Nevertheless, the IMU is not invulnerable to potential direct security threats. For example, an attacker could manipulate the sensor data to misrepresent the road's gradient, disrupting the autonomous vehicle's ability to interpret and react to its environment correctly. Such an attack could lead to significant safety risks, as the vehicle's behavior might not align with the actual environmental conditions.

This potential threat was exemplified by the work reported in [44], where the authors developed the CarShark tool to monitor data flow in the vehicle's controller area network (CAN) bus system. Thorough packet analysis and modification, the tool enabled the simulation of a man-in-the-middle attack on the CAN network. By altering the data packet, they could manipulate the sensor's readings, demonstrating the potential implications of such an attack on autonomous vehicles.

A variety of countermeasures might help mitigate such a security threat. One potential strategy involves implementing encrypted communication within the vehicle's network, adding a layer of protection against unauthorized data manipulation. Another approach could be the use of additional, redundant sensors to provide backup measurements. This could involve using GPS data to verify the vehicle's inclination, providing an extra check against erroneous readings from a compromised IMU.

In the context of the emphasis of this article on emotional intelligence, it is essential to extend this concept to how a self-driving vehicle interprets and responds to sensor data. Similar to how humans use emotional intelligence to traverse complex social situations, an autonomous vehicle could use perceptual intelligence to recognize and respond adequately to potential hazards to its sensor inputs. This additional intelligence could considerably contribute to the overall safety and dependability of autonomous vehicles while also opening up new research avenues in the field.

4. Cyber Security Attacks in Vehicular Ad Hoc Networks (VANETs)

Autonomous vehicles (AVs) operate utilizing two principal communication channels, namely vehicle-to-vehicle (V2V) and Vehicle-to-infrastructure (V2I) communications, which are critical components of the broader Vehicular ad hoc network (VANET) ecosystem. A detailed analysis of the structure and operations of a VANET is depicted in Figure 4.

The V2V communication paradigm leverages the principles of peer-to-peer networking, enabling vehicles to establish mutual connections. This system is underpinned by the IEEE 802.11p protocol and is designed based on the assumption that vehicles within a specified range of radio communication can automatically form an ad hoc network. Within this network, nodes represented by the vehicles can share vital data points such as positional coordinates, speed metrics, directional vectors, and more. Combined with V2V, the V2I communication mechanism allows vehicles to establish connections with embedded electronic devices in the broader transportation infrastructure. The information exchanged between vehicles and infrastructure can be utilized for various applications, including enhancing traffic management, optimizing traffic flow, promoting fuel efficiency, and reducing environmental impact.

Vehicular communication systems, underpinned by the IEEE 802.11p protocol, have emerged as a transformative force for improving road safety and traffic efficiency [45]. These systems leverage vehicle-to-vehicle (V2V) communication for sharing of pivotal data points such as positional coordinates and speed metrics, and vehicle-to-infrastructure (V2I) communication to interface with the embedded electronic devices in transportation infrastructure. However, the effectiveness of these communication methods relies heavily on the accuracy of wireless channel estimates, such as channel state information (CSI) and received signal strength. Consequently, researchers have been mobilizing efforts towards the development of deep-learning-based channel prediction algorithms and conducting measurement campaigns to generate reliable wireless channel estimates [45].

Simultaneously, road traffic safety remains a vital concern in the domain of vehicular communication. Mehdizadeh et al. highlighted the development of predictive models to gauge crash risks based on varying driving conditions and the implementation of optimization techniques such as path selection and rest-break scheduling to augment road safety [46]. However, bridging the gap between research outcomes and real-time crash risk optimization remains a challenge. Complementing safety, security issues have gained attention due to the highly active and ever-changing topology of vehicular environments. Proposals for security models grounded in evolutionary game theory aim to identify

common attacks and establish defenses [47]. Concurrently, the rise in smart car sensors and applications reliant on artificial intelligence and augmented reality has escalated challenges related to computational resources and latency requirements. Efforts are underway to advance secure multiaccess edge computing and intelligent vehicle control systems to meet these demands [48]. Overall, vehicular communication systems present an array of opportunities alongside a spectrum of challenges, underscoring the need for ongoing research and innovation.

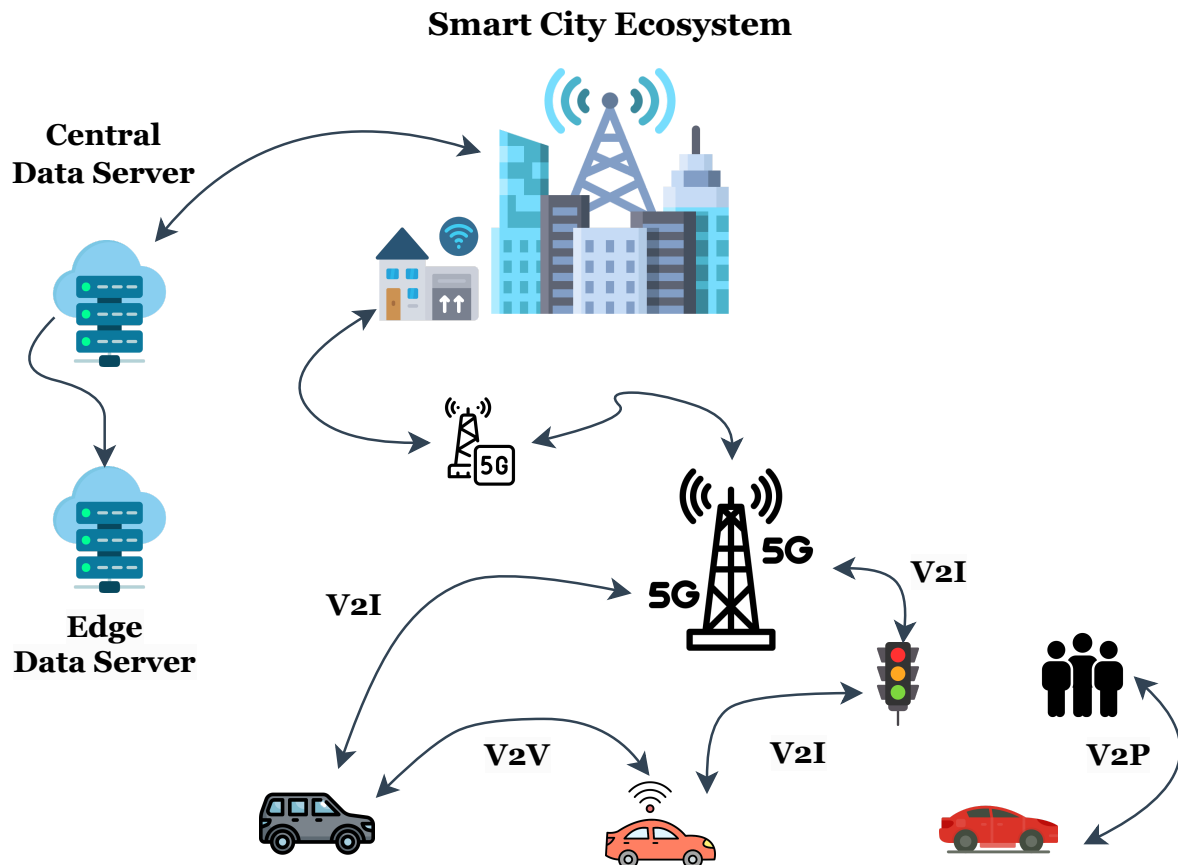


Figure 4. VANET.

4.1. Autonomous Vehicles: Security Measures and Technological Interplay

Artificial intelligence (AI) and machine learning (ML) technologies have empowered the development and efficiency of autonomous vehicles, catalyzing intelligent decision making and improved security. However, just like vehicle ad hoc networks (VANETs), autonomous vehicles are also vulnerable to various cyber threats. In particular, these vehicles integrate technologies like LiDAR, Radar, GPS, and computer vision, which also become potential targets for cyber attacks. Notable threats include Sybil and replication attacks, which involve spoofing and identity theft, capable of causing critical operational issues [49,50]. Countermeasures against these threats, some of which were initially developed for VANETs, have been adapted for autonomous vehicles. For instance, digital signatures and time stamps help authenticate messages and data sources [51,52]. Mechanisms that detect disparities in motion trajectories and, hence, identify potential Sybil attacks, can also be applied in the context of autonomous vehicles [51].

Additionally, Hao et al. [53] presented a cooperative message authentication protocol (CMAP), which includes the sender vehicle's location data in each safety message. This protocol can be adopted in autonomous vehicles to counter replication attacks, thus significantly improving security [53]. Furthermore, techniques such as the anonymous batch authenticated and key agreement (ABAKA) scheme, which was initially introduced in

VANETs [50], can be tailored for autonomous vehicles to authenticate multiple requests and generate multiple session keys simultaneously. It aids in quick validation and session key negotiation, thus minimizing transmission overhead and verification latency.

To tackle the evolving security landscape, the development of advanced intrusion detection systems (IDS) is crucial. By leveraging anomaly detection techniques, autonomous vehicles can quickly detect and react to deviations from normal operations triggered by potential cyber attacks. Finally, secure communication protocols can be incorporated into the vehicle's systems to safeguard sensitive data, thereby further improving the overall security of autonomous vehicles [54–56].

4.2. Availability Attacks, Benefits, and Security Solutions in Autonomous Vehicles

Ensuring system availability is a crucial aspect of the security framework for autonomous vehicles. Autonomous vehicles, like vehicular ad hoc networks (VANETs), face threats such as denial of service (DoS) attacks, which can exhaust network resources and disrupt vehicle operations. Effective countermeasures include authentication measures, anomaly detection systems, and cryptographic solutions.

Malware attacks pose a significant risk, as they involve the deployment of malicious software, such as computer viruses, which can compromise the software infrastructure of autonomous vehicles. To protect against such threats, firewall technologies and antimalware systems are instrumental [57].

Denial of service (DoS) attacks aimed at blocking legitimate entities from accessing resources and services are another significant threat. A more pervasive form of DoS attack is the distributed denial-of-service (DDoS) attack, which utilizes multiple computing devices or Internet connections. These attacks can severely impact the functionality and service availability of autonomous vehicles [58–60].

The benefits associated with addressing availability attacks and implementing the related countermeasures are manifold:

- **Robust operational stability:** Effective countermeasures against DoS and DDoS attacks can ensure that autonomous vehicles continue to operate without disruption. This enhances the reliability and robustness of autonomous vehicles in various driving conditions.
- **Enhanced security infrastructure:** Utilizing robust firewall technologies and antimalware systems not only shields autonomous vehicles from malware attacks but also significantly fortifies the vehicle's overall security infrastructure.
- **Improved user trust and confidence:** As autonomous vehicles become more secure and less susceptible to attacks, user trust and confidence in this technology can be expected to increase. This can facilitate the broader acceptance and adoption of autonomous vehicles.
- **Prevention of potential misuse:** Effective countermeasures can prevent potential misuse of autonomous vehicles, such as using them as nodes in distributed denial-of-service attacks.
- **Guaranteed service accessibility:** By effectively mitigating DoS and DDoS attacks, the continuous availability of essential vehicle services and resources can be guaranteed, which is crucial for the functionality of autonomous vehicles.
- **Accurate vehicle routing:** By mitigating wormhole attacks, accurate distance calculations between nodes, which are essential for precise vehicle routing, can be ensured.
- **Versatility and performance:** Techniques like HEAP offer a versatile solution that works across various applications and provides superior performance, making them well-suited for autonomous vehicles.

Incorporating these countermeasures into the design and operation of autonomous vehicles provides a significant benefit by increasing their resilience against cyber attacks and thus ensuring their reliable and secure operation. As a result, the safety and efficiency of these vehicles are significantly improved, contributing to the broader aim of safe and reliable autonomous driving.

He et al. proposed a preauthentication solution to counteract DoS attacks, which uses a group rekeying mechanism, along with a one-way hash chain [60]. Additionally, Verma et al. suggested a method for packet filtering and abrupt change detection to prevent DoS attacks in autonomous vehicles [61]. With the development of these countermeasures, it can be inferred that DoS attacks have been considerably mitigated.

A wormhole attack, which involves transporting packets from one network segment to another, can significantly disrupt routing algorithms in autonomous vehicles that rely on accurate distance calculations between nodes [61]. A countermeasure proposed by Safi et al. restricts the maximum transmission range of packets, ensuring that the received packet is within a practical range of the sender. This method, known as HEAP, provides superior performance compared to other authentication techniques, making it particularly suitable for autonomous vehicles. HEAP can be utilized across unicast, multicast, and broadcast applications and can authenticate all types of packets [62].

In conclusion, addressing availability threats in autonomous vehicles is paramount for ensuring their functionality and safety. The application of robust defensive strategies and countermeasures against these attacks is essential for safeguarding these vehicles against potential threats.

4.3. Data Integrity Attacks in Autonomous Vehicles

Data integrity is pivotal in autonomous vehicle systems, forming the bedrock of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. It is crucial for everything from navigation to collision avoidance [63]. However, the risk of data manipulation is omnipresent, either through unauthorized intrusion or malicious intent. To preserve data integrity, autonomous vehicles employ secure communication protocols and advanced encryption methods.

One commonly encountered breach is the *masquerading attack*, where the perpetrator impersonates a legitimate entity within the system. This can cause traffic disruption, trigger accidents, or potentially allow the attacker to control vehicle systems or extract sensitive data [39]. Therefore, autonomous vehicles must incorporate systems to authenticate the received information or signals.

Addressing these challenges, T.W. Chim et al. introduced the secure and privacy-enhancing communications schemes (SPECS) system [64]. SPECS leverages pseudo identification and a shared secret key between an autonomous vehicle and roadside units (RSUs) to maintain the vehicle's identity confidentiality. Even when pseudonyms are used for communications, RSUs can verify the signatures, thus preventing masquerading attacks [63,64].

Another potential breach of data integrity is represented by the replay attack or playback attack. This attack involves the malicious repetition or delay of valid data transmissions [39]. Modern security designs using robust cryptographic systems, including digital signatures and nonce inclusion in messages, are typically effective at countering these attacks.

However, the challenge is amplified when the attacker is a trusted insider, like a compromised vehicle with a valid certificate. Anomaly or misbehavior detection systems, such as those discussed in [65], are often employed to manage these scenarios. However, these systems have inherent limitations concerning false negatives and positives and rely on a variety of data sources that might not always be available. Consequently, further research is required in anomaly detection to ensure the robust operation of these algorithms and the consequent protection of autonomous vehicles.

4.4. Threats to Confidentiality in Emotionally Intelligent Autonomous Vehicles

Confidentiality attacks, although not perceived as the most significant threats to vehicular system security, nevertheless constitute considerable privacy risks. Preserving the confidentiality of data transmitted within vehicular networks, such as the geographical location of autonomous vehicles, intelligent transport systems (ITS) safety alerts, and

driver information, is paramount. Possible data breaches can be deterred through secure transmission techniques and fortified data encryption protocols.

An illustrative confidentiality threat in the realm of vehicular networks is the eavesdropping attack. During standard vehicle operation, vehicles frequently broadcast beacon signals encapsulating a wealth of data, such as the vehicle's identity, current location, velocity, and acceleration. This disseminated information is vulnerable to unauthorized interception, potentially breaching the privacy of the system. An adversary armed with the appropriate tools could execute an eavesdropping attack, harvesting precious data from the transmitted information. By associating this extracted location data over time, the adversary could track the vehicle's path and possibly manipulate it for malicious activities.

Given its passive nature, eavesdropping presents a formidable challenge, as its detection is difficult, especially in a broadcast wireless communication context. Nonetheless, the successful orchestration of eavesdropping can be thwarted by employing data encryption protocols to shield data privacy or anonymization techniques to protect identity and location data. Anonymity is generally realized using group signatures [66] or temporary certificates, also known as pseudonyms [67].

In the context of emotionally intelligent autonomous vehicles, confidentiality attacks bear an additional layer of intricacy and risk. "Emotionally intelligent autonomous vehicles" refer to autonomous vehicles that are equipped with the ability to perceive, comprehend, and appropriately react to human emotions. These vehicles utilize a range of technologies, such as AI, ML, and sensor technologies, complemented by effective computing capabilities. They can identify and respond to emotional cues by recognizing facial expressions, interpreting voice sentiments, processing physiological signals, and more. Their goal is to enhance the passengers' comfort, safety, and overall experience by adapting to their emotional states.

The emotional data in these vehicles represent a core component of their intelligent system and are highly personal and sensitive. Thus, the implications of an eavesdropping attack could extend beyond mere vehicle tracking, potentially leading to unauthorized access and exploitation of a passenger's emotional data. To effectively safeguard this sensitive information, advanced encryption, and anonymization techniques must be amalgamated within the system's data communication protocol. This integration should ensure that even in the event of an eavesdropping attack, the intercepted data would not be useful to the adversary.

Moreover, emotionally intelligent autonomous vehicles may necessitate additional privacy protection layers due to the nature of the processed data. For instance, homomorphic encryption could be employed to allow the system to analyze and react to emotional data without ever needing to decrypt them, thereby maintaining privacy. Additionally, differential privacy concepts could be applied to ensure that the system's responses do not inadvertently disclose sensitive information about the passengers' emotional states. These advanced methods could form a vital part of a comprehensive strategy for preserving data confidentiality in emotionally intelligent autonomous vehicles.

4.5. Vehicle-to-Pedestrian (V2P) Network and Its Implications

As we navigate an increasingly digitized world, the ubiquity of smartphone usage among both drivers and vulnerable road users (VRUs) has grown exponentially. To mitigate the potential hazards associated with this trend, particularly in contexts where traffic is a primary concern, it is essential to develop novel approaches for enhancing road safety. One such strategy involves the implementation of collision prediction algorithms, capitalizing on pedestrian-to-vehicle (P2V) and vehicle-to-pedestrian (V2P) communication technologies [68]. A. Hussein et al. presented a sophisticated example of this approach, proposing an algorithm that uses global positioning system (GPS) data and magnetometer readings from a pedestrian's smartphone in conjunction with sensor data from an autonomous vehicle to predict potential collision scenarios.

Figure 5 provides a schematic representation of this innovative algorithm's functionality. It highlights the method by which the algorithm calculates the potential angle of collision, thereby informing preventative measures.

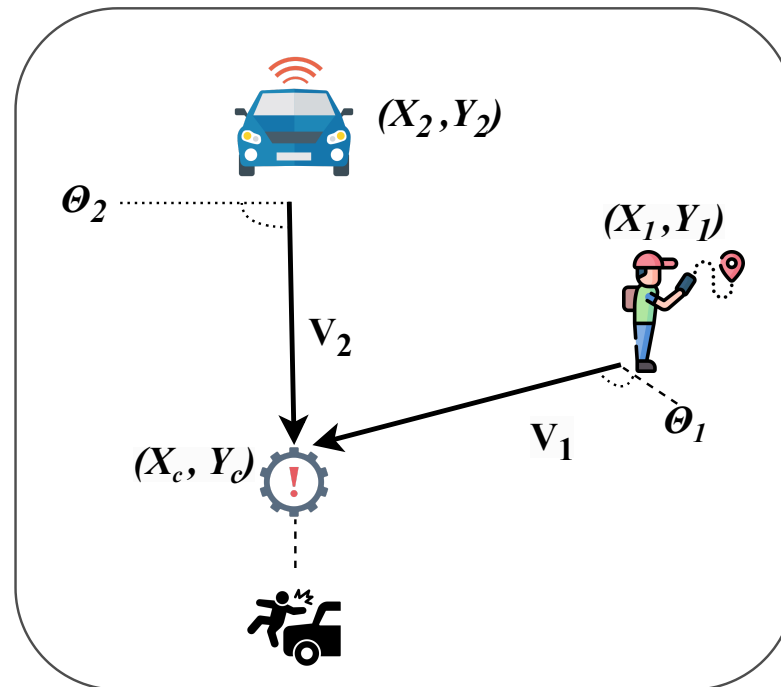


Figure 5. Schematic representation of the collision prediction algorithm.

Upon the prediction of a possible collision, the system alerts both the pedestrian and the autonomous vehicle, enabling them to take necessary evasive action and replan their routes accordingly. This immediate response facilitates the prevention of accidents, enhancing the safety of all road users.

While V2P communication is an emerging area of exploration, its potential for improving road safety cannot be underestimated. Nonetheless, given its nascent stage, it requires substantial research and development to ensure its robustness and security. Future aspirations of achieving a fully integrated Internet of Things (IoT) are reliant on the resolution of current security vulnerabilities. As such, it is crucial that further advancements in this field be underpinned by an unwavering commitment to ensuring the security and safety of all connected devices. By doing so, we can progress towards realizing the full potential of V2P communications, contributing significantly to the development of emotionally intelligent autonomous vehicles.

5. Autonomous Vehicle Vulnerabilities

Autonomous vehicles, despite their potential to revolutionize transportation, are not immune to the growing complexity of cyber threats due to their dependence on advanced digital technologies [69]. Potential hackers may exploit these cyber vulnerabilities, creating a threat to the safety and privacy of individuals, regardless of whether they are motivated by malicious goals or simple curiosity [69]. Detailed analyses of these cyber threats can be discovered on informative platforms such as HackerNoon [70].

The following sections highlight some of the prominent attack vectors that could potentially compromise the integrity of autonomous vehicles:

- **Key fob hacking:** Remote vehicle access and ignition made possible by key fob technology can be compromised. By using devices to strengthen the signal transmitted by a vehicle's key transponder, hackers can gain unauthorized entry and even remotely start the vehicle [71].

- Control area network (CAN) bus attacks: The CAN bus, which operates as the electrical network that connects the various electronic control units (ECUs) within a vehicle, is an attractive target for hackers. By exploiting vulnerabilities in the CAN bus, hackers can take control of fundamental vehicle functions such as braking and steering [71].
- Entertainment system hacking: Given its connection to the CAN bus, a vehicle's entertainment system can provide a back door for hackers, which, once breached, could potentially grant a hacker full control over the vehicle's systems [71].
- Adversarial machine learning techniques: Autonomous vehicles rely heavily on machine learning algorithms to interpret sensor data and make operational decisions. By employing adversarial machine learning techniques, such as evasion or poisoning attacks, hackers can manipulate sensor data, causing the vehicle to make faulty and potentially hazardous decisions [72].
- User data theft: Considering the plethora of user data stored in autonomous vehicles, these vehicles become prime targets for cyber criminals. A hacked vehicle can lead to significant privacy violations and impose safety risks to the driver and others on the road.
- Remote vehicle hijacking: In a potentially dangerous scenario, hackers might gain remote control of a self-driving car, causing passengers to experience difficulty.
- Denial-of-service (DoS) attacks: The launching of DoS attacks against the vehicle's systems could lead to system shutdown or failure.

The extensive range of potential attack vectors underscores the imperative to enhance cyber security measures in autonomous vehicles. A compromised vehicle becomes a significant threat to all road users, necessitating immediate rectification of these vulnerabilities for public safety [69]. To fully understand the scope of these vulnerabilities, it is necessary to delve into the hardware aspects, specifically focusing on critical components such as the onboard diagnostic port (OBD) and the engine control unit (ECU).

5.1. Hardware Vulnerabilities: Onboard Diagnostic Port (OBD)

The onboard diagnostic (OBD) port, a critical component in modern vehicles, provides a critical gateway to gathering diagnostic information. These vital data include an array of performance metrics and potential system faults, which the port communicates directly to the electronic control unit (ECU) via the controller area network (CAN) bus. Typically, the OBD port interface is a compact device akin to a standard USB drive, usually situated beneath the dashboard near the driver's seat. This interface can be connected to external computational devices, either via physical tethering or wireless connectivity, facilitating bidirectional data transfer between the vehicle's ECU and the connected device.

This communication system can have various applications. For example, it can be used to orchestrate cars as discussed in [73] or to analyze the effects of an onboard unit on the driving behavior of cars in connected vehicle flow, as detailed in [74]. With the emergence of advanced technologies, the OBD port can also be leveraged for more sophisticated tasks, such as suppressing selfish node attack motivation in vehicular ad hoc networks through deep reinforcement learning and blockchain, as proposed in [75], or assessing the trust level of a driverless car using deep learning techniques, as investigated by [76]. These innovative applications highlight the critical role of the OBD port in enhancing the functionality and safety of autonomous vehicles.

Zhang et al. [77], in their work, illustrated the vulnerabilities inherent in this system by successfully breaching multiple automobile models through the OBD port. The potential consequences of such breaches are severe, extending to remote control of the vehicles, highlighting the urgent need for robust security measures within OBD port systems.

Once an external device is linked to the OBD, it gains the ability to send and receive data to and from the vehicle's ECUs. Such an open connection can be exploited to introduce malicious payloads into vehicle networks. This threat was further underscored by W. Yan's research [78], which demonstrated the feasibility of manipulating data packets to initiate such attacks. In addition to posing a direct threat to vehicle operations, such vulnerabilities

also carry potential ramifications for intellectual property theft. Criminal organizations could leverage these security gaps to steal proprietary information relating to suppliers' and original equipment manufacturers' (OEM) production processes. This not only enables the production of counterfeit parts but also breaches driver privacy by exposing sensitive information such as driving habits.

In response to these threats, countermeasures have been proposed by various researchers. Yadav et al. [79] introduced a defense mechanism that combines the seed key protocol with a two-way authentication method and a timer method. This approach seeks to enhance security by making the seed and key values more difficult to decrypt. Likewise, Oka and Larson [80] proposed the use of cryptographic techniques to authenticate messages on the CAN, thus limiting the transmission of unauthorized data.

However, despite these efforts, a comprehensive and foolproof solution to secure OBD port systems remains elusive. This area of research is still in its first steps and requires further in-depth investigation. This is particularly true in the context of emotionally intelligent autonomous vehicles, where ensuring the security of the OBD port system is fundamental to maintaining the operational integrity of these vehicles and protecting the privacy of their users.

5.2. Hardware Vulnerabilities: Engine Control Unit (ECU)

The engine control unit (ECU) plays a vital role in the orchestration of a vehicle's functionalities, acting as the central processing entity for a range of control functions within an automotive system. By interpreting, analyzing, and managing a myriad of electronic signals, the ECU oversees critical operational aspects of vehicles, including fundamental features such as the core braking system.

Various studies have underscored the vulnerability of ECUs to sophisticated infiltration strategies. The work of Vallance [81] is particularly instructive, revealing how intruders can exploit the onboard digital audio broadcasting radio as an entry point to gain unauthorized access to ECUs. Upon breaching this boundary, malicious attackers have the capacity to manipulate the CAN (controller area network), a critical communication highway that interconnects different vehicular subsystems. Such disruptions can have profound implications, potentially compromising the core functionalities of the vehicle and thereby posing significant safety risks.

The potential gravity of such security breaches is further underscored by the observations of Checkoway et al. [82]. Their findings indicate that the security measures currently implemented in ECUs are often insufficient in thwarting attempts at unauthorized firmware access or modification. Given that firmware alterations have the potential to completely reprogram a vehicle's behavior, this vulnerability is of significant concern in the context of public safety. However, their research is not only diagnostic but also offers a path toward remediation. They propose the adoption of an asymmetric cryptographic framework rooted in the use of public-private key pairings. This approach helps to ensure that any firmware introduced to the system originates from a verified and trusted source. In this way, the risk of unauthorized firmware modifications can be considerably mitigated, helping to safeguard against malicious intent.

Despite this, guaranteeing the robustness of ECU security is a difficult task, given the complexity and evolution of cyber security threats. Not only is the scope of possible infiltration techniques a challenge, but so is the depth of possible exploits once access has been gained. The discovery of these latent vulnerabilities requires exhaustive testing and evaluation, utilizing both proven cryptographic techniques and emergent cyber security methodologies.

5.3. Countermeasures for Autonomous Vehicles

The classification of various types of attacks on autonomous vehicles and their respective countermeasures are shown in Table 2. In this table, we emphasize the scope and complexity of the threats that autonomous vehicles face. Although significant strides

have been made in countering some types of attacks, a number of vulnerabilities, such as those associated with OBD port tampering, man-in-the-middle attacks on the CAN bus, and replay attacks by insider adversaries, remain unaddressed. A comprehensive understanding and solution for these vulnerabilities are crucial to realize the full potential of emotionally intelligent autonomous vehicles.

Table 2. Data Security attacks and mitigation strategies in autonomous vehicles.

Attack Type	Specific Attack	Proposed Countermeasures	Ref.	Mitigation Status
Data Security	Data Authenticity	Signal strength monitoring	[28]	Partially mitigated
		Military-grade cryptography	[28]	Partially mitigated
		Antispoofing methods	[29]	Partially mitigated
	Man-In-The-Middle	Cryptography on CAN	[44]	Not addressed
		Secondary measurement source	[44]	Not addressed
	Data Availability	GPS jamming	[28]	Partially mitigated
		Antijamming methods	[29]	Partially mitigated
		LiDAR jamming	[31]	Fully mitigated
		Use of alternate data sources	[31]	Fully mitigated
		Camera blinding	[31]	Fully mitigated
		Malware attack	[83]	Partially mitigated
		DoS/DDoS attack	[60,61]	Fully mitigated
		Replay attack on LiDAR	[31]	Fully mitigated
	Data Integrity	Auto control confusion	[31]	Fully mitigated
		OBD port tampering	[84]	Not addressed
		Exploitation and injection in CAN bus	[79,85]	Not addressed
		Masquerading attack	[64]	Fully mitigated
		Replay attack (outsider adversary)	[39]	Fully mitigated
		Replay attack (insider adversary)	[65]	Not addressed
Data Confidentiality	Eavesdropping	Cryptographic solution (group signatures)	[66]	Partially mitigated
	Eavesdropping	Cryptographic solution (short-term certificates)	[67]	Partially mitigated

Autonomous vehicles (AVs) introduce numerous unique security challenges that have the potential to create safety consequences on the road [86]. Therefore, security measures are paramount to the implementation of AV networks [87]. Here are some countermeasures being developed and deployed to solve the security flaws of autonomous vehicles:

- **Game-theory-based solutions:** Game-theory-based solutions could offer resilience in the context of AVs [88]. Game theory is a mathematical framework for modelling decision-making in situations where multiple parties have conflicting interests. It can be used to model the behavior of attackers and defenders in a cyber security context and to develop optimal strategies for both parties [88].
- **Benchmarking frameworks:** AVs lack a proper benchmarking framework to evaluate attack and defense mechanisms and quantify safety measures [86]. BenchAV is a security benchmark suite and evaluation framework for AVs that addresses current limitations and pressing challenges of AD security. The benchmark suite contains 12 security and performance metrics and an evaluation framework that automates the metric collection process using the Carla simulator and robot operating system (ROS) [86].

- **Opportunistic networking protocols:** Novel networking protocols in vehicular ad hoc networks (VANETs) are being developed to provide data to autonomous trams and buses in a smart city [87]. Opportunistic networking protocols are used to bridge the gap between fully distributed vehicular networks based on short-range vehicle-to-vehicle communication and cellular-based infrastructure for centralized solutions [87]. The state-of-the-art MaxProp algorithm outperforms the benchmark, as well as other more complex routing protocols, in most of the categories [87].
- **Blockchain-based architecture:** A blockchain-based architecture could provide a promising solution to the threats of cyber attacks that jeopardize the security and connectivity of CAVs [89]. Blockchain technology can be used to secure communication between vehicles and infrastructure and to ensure the integrity and confidentiality of data [89]. It can also be used to provide a secure and decentralized platform for vehicle-to-vehicle and vehicle-to-infrastructure communication [89].

These countermeasures aim to address the security challenges facing AVs, including trustworthiness, security, safety, and complexity. By developing and deploying these solutions, AVs can become more reliable and safe, which is crucial for the adoption of such technology in smart projects [88].

Specific cyber security measures and examples of security solutions implemented in autonomous vehicles include:

- **Secure communication protocols:** Implementing secure communication protocols, such as transport-layer security (TLS), can help protect the vehicle's connectivity and prevent unauthorized access to the vehicle's network [90].
- **Encryption:** Utilizing encryption techniques can safeguard the data transmitted between different components of the autonomous vehicle system, including sensors, controllers, and communication interfaces [91].
- **Intrusion Detection systems (IDS):** IDS can be deployed in autonomous vehicles to monitor the network and detect any suspicious or malicious activities. IDS can identify potential cyber attacks and trigger appropriate responses to mitigate the risks [92].
- **Secure over-the-air (OTA) updates:** OTA updates allow for the remote updating of software and firmware in autonomous vehicles. Implementing secure OTA mechanisms ensures that updates are authenticated, encrypted, and tamper-proof, reducing the risk of unauthorized modifications or malware injection [91].
- **Access control and authentication:** Implementing strong access control mechanisms and multifactor authentication can prevent unauthorized access to critical vehicle systems. This includes securing access to the vehicle's control systems, sensors, and communication interfaces [90].
- **Secure sensor fusion:** Sensor fusion is crucial for perception in autonomous vehicles. Ensuring the security of sensor data fusion is important to prevent the injection of false or manipulated sensor data, which could lead to incorrect decisions by the autonomous system [93].
- **Behavioral anomaly detection:** Implementing behavioral anomaly detection techniques can help identify abnormal behavior in the vehicle's network or system, indicating a potential cyber attack. This can include monitoring network traffic patterns, system performance, and sensor data consistency [94].
- **Redundancy and fail-safe mechanisms:** Building redundancy and fail-safe mechanisms into autonomous vehicle systems can help mitigate the impact of cyber attacks. This includes redundant sensors, controllers, and communication channels to ensure that the vehicle can still operate safely, even if one component is compromised [93].
- **Continuous monitoring and updates:** Regularly monitoring the security of the autonomous vehicle system and applying security updates and patches is essential to address newly discovered vulnerabilities and protect against emerging cyber threats [92].

These cyber security measures are crucial to ensure the safety and integrity of autonomous vehicles in the face of potential cyber attacks. By implementing these measures,

manufacturers and researchers aim to minimize the risks associated with autonomous vehicle cyber security and enhance the overall security posture of these vehicles.

Current Status and Future Directions of Sensor Security in Autonomous Vehicles

As the complexity and ubiquity of autonomous vehicles (AVs) continue to increase, the current state of their sensor security and future directions for research become critical topics. The current landscape of AV sensor security involves a plethora of techniques developed to counteract the broad spectrum of potential threats. These techniques encompass a multitude of disciplines, such as encryption, anomaly detection, intrusion detection systems, and secure communication protocols.

The field of encryption, for example, is being utilized to protect data in transit from sensors to the vehicles' central processing units and cloud-based systems. Secure communication protocols, such as transport layer security (TLS) and Internet protocol security (IPSec), are being employed to ensure that data communicated between vehicles and infrastructure are authenticated and encrypted. Moreover, techniques from the realm of machine learning and data science are being incorporated to develop sophisticated anomaly detection systems that can identify unusual patterns in sensor data that are indicative of a potential attack.

Despite these advancements, the industry faces considerable challenges that need to be addressed to increase AVs' resilience against threats. First, due to the complex nature of AVs and the environments they operate within, creating a comprehensive and foolproof security solution is inherently difficult. Additionally, the rapidly evolving nature of cyber threats necessitates constant vigilance and adaptation in the field of AV sensor security.

The future of AV sensor security research holds promising directions. Enhancing machine learning algorithms to detect subtle and complex attacks, developing more sophisticated encryption techniques, and integrating blockchain technology for secure data recording and transaction are some of the notable future directions. However, a critical part of the future lies in developing security measures that are proactive rather than reactive, preventing attacks before they occur rather than responding to them post event.

Furthermore, it is essential to ensure that security measures do not impede the functionality and efficiency of AVs. Achieving this balance will require advancements in both hardware and software, necessitating ongoing research and development. In summary, the current status of sensor security in AVs presents a dynamic landscape fraught with challenges and opportunities. The future is ripe for research that addresses these challenges head-on, advancing the safety and security of AVs.

6. Vulnerabilities of Deep Neural Networks in the Face of Adversarial Machine Learning: Implications for Autonomous Vehicles

The field of adversarial machine learning has demonstrated that it is possible to exploit the weaknesses that are built into deep neural networks (DNNs). This potential has been confirmed in state-of-the-art research. The first adversarial machine learning attacks on DNNs were proven in a significant study that was conducted by Szegedy et al. [95]. During the experimental phase, the researchers introduced the idea of adversarial instances, which are small modifications made to the input images. These modifications have the potential to influence DNNs and result in inaccurate categorization. This method, which is based on a gradient-based attack, devises adversarial instances that are only slightly different from the original. By tricking image classifiers with these inputs that had been deceptively manipulated, the method was successful.

In response to this groundbreaking work, Goodfellow et al. [96] formulated adversarial machine learning as a min-max problem and developed an alternative gradient-based method. This technique now commonly referred to as the fast gradient sign method (FGSM) was an effective tool for generating adversarial instances. The researchers also introduced adversarial training, a technique used to fortify DNNs against such adversarial instances, advancing our knowledge of both the vulnerabilities and potential defenses in

this field. The vulnerabilities of DNNs were further highlighted by Ian Goodfellow and Bengio [97]. Utilizing adversarial examples derived from images taken by a mobile phone camera, they revealed the susceptibility of machine learning (ML) and deep learning (DL) techniques to attacks in real-world scenarios. Using the basic iterative method (BIM), a more sophisticated version of FGSM, they produced adversarial examples that successfully deceived advanced image classifiers.

Further research [98] highlighted the susceptibility of convolutional neural networks (CNNs), the most sophisticated deep-learning-based image categorization algorithms, to simple manipulations such as rotations and translations. Another study [99] emphasized this vulnerability, demonstrating that even basic geometric transformations like translation, rotation, and blurring could confound ten state-of-the-art CNNs. Meanwhile, Liu et al. [100] offered a different approach by modifying the neurons of an already trained model, demonstrating a stealthy back-door attack on the model. The researchers maliciously injected the ML model and applied it to an autonomous vehicle, where a specific trigger, a particular billboard in this case, caused the vehicle to behave unpredictably.

With a different strategy, Papernot et al. [101] constructed a white-box Jacobian saliency-based adversarial attack (JSMA), which manipulated the mapping between the input and output of DNNs to deceive the classifiers. They also proposed a defensive technique, namely defensive distillation, where a model is trained to predict the probabilities of another model trained on the baseline standard. This aimed to foster a higher emphasis on accuracy, serving as protection against adversarial perturbations. Papernot et al. [102] extended their work to present a black-box adversarial ML attack that exploited the transferability property of adversarial examples. This method not only deceived ML/DL classifiers but also bypassed the defensive distillation mechanism, highlighting the sophistication of adversarial attacks. Carlini and Wagner [103] introduced a synergy of adversarial techniques known as C&W attacks, utilizing three distinct distance metrics: L1, L2, and L_∞ . These attacks were successful in evading both defensive distillation and DNN classifiers, exposing the inadequacy of existing defensive strategies. In another study Carlini and Wagner [104] demonstrated that their adversarial attacks could bypass ten commonly used defensive techniques against adversarial instances, further emphasizing the complexity of the problem.

Another alarming vulnerability was demonstrated by Brown et al. [105], who reported that a malicious patch, when applied to an original image, led the deep model to misclassify that image. These universal adversarial patches could deceive classifiers without the need to know about other objects present in the image, allowing for the offline creation and dissemination of such patches. Su et al. [106] adopted an alternative approach by employing differential evolution to generate one-pixel adversarial perturbations. This novel attack demonstrated the capability of minimal yet calculated manipulations to compromise a variety of neural networks.

Despite substantial progress in identifying and comprehending these weaknesses, effective defense mechanisms against adversarial attacks remain elusive, while some countermeasures have proven to be somewhat effective against low-level attacks, they are ineffective against a broader range of sophisticated attacks. In order to ensure the security and dependability of autonomous vehicles in the context of adversarial ML attacks, it is crucial that future research focuses on the development of more robust defensive strategies. This critical requirement highlights the scale of the challenge and the significance of ongoing research in this crucial area in order to ultimately secure autonomous vehicles against malicious threats.

7. Big Data in Autonomous Vehicles

The use of large amounts of data is crucial to the successful operation of autonomous vehicles from both a safety and productivity perspective. The list that follows is an overview of crucial details discovered as a result of our study:

- **Security Challenges due to big data utilization in AVs:** As autonomous vehicles (AVs) increasingly exploit big data to enhance their operations, they are simultaneously exposed to a range of security concerns, including cyber security vulnerabilities. One such difficulty is that autonomous vehicles (AVs) are more vulnerable to cyber-attacks. According to [71], the nature of these vulnerabilities is multifaceted, including data breaches, illegal access, and the manipulation of vehicle sensor data. According to the findings of this study, in order to further enhance the safety of the utilization of big data applications in autonomous vehicles, it is essential to create complex encryption strategies and to create algorithms based on machine learning for anomaly detection.
- **Designing robust path-following functionality through big data analysis:** The ability of autonomous vehicles to navigate predetermined routes in a manner that is both secure and economical is one of the most important characteristics of these vehicles. According to [107], the processing of a significant amount of data on road conditions, vehicle dynamics, and environmental factors could potentially make it feasible to perform big data analysis by simplifying the process for scientists to develop robust path-following algorithms. By synthesizing these data, autonomous vehicles have the ability to generate appropriate motion profiles and dynamically change velocities. This ensures that tire–road contact remains intact under a variety of circumstances, which leads to a higher standard of safety.
- **Environmental sensing through numerous sensing modalities:** In order for autonomous cars to be able to make intelligent decisions, it is crucial for these vehicles to have an extended understanding of their surroundings. As indicated by the research presented in [108], autonomous vehicles are equipped with a variety of sensors, including LiDAR, radar, ultrasonic sensors, and cameras, which continuously collect high-dimensional data on their surrounding area. Big data analytics could potentially be utilized for analysis of these sensor data in real-time, granting the vehicle the ability to generate a high-definition image of its surrounding environment, which is vital for both navigation and the avoidance of obstacles.
- **Interconnected vehicle platform for enhanced driver convenience and safety:** In accordance with the hypothesis presented in [109], the incorporation of connected car technologies with big data analytics has the potential to ultimately bring about an innovative improvement in the services and functions that become available to drivers. A connected vehicle platform could provide customized services that are targeted to the driver's comfort and safety by analyzing large datasets that are derived from vehicular sensors, user preferences, and other sources of information. These services are aimed at improving the driver's experience. This includes things like real-time traffic information, adaptive ambient settings, predictive maintenance, and automated emergency response systems.

Towards the final analysis, the collection and management of large amounts of data have become an essential component in the development of technology related to AI. In particular, the fields of automated machine learning, clustering, Gibbs sampling, and data structures [110–113] have emerged in recent days due to their robustness. Particularly in managing big data on AVs, there is a vital part in the pipeline by which autonomous vehicles consume and process a vast amount and variety of data, which is essential for improving safety, security, efficiency, and the overall user experience. However, the volume and complexity of big data simultaneously induce a range of security difficulties. These challenges need ongoing study and improvement in data protection and cyber security solutions, since they are always evolving. Towards the final analysis, the collection and analysis of large amounts of data have become an essential component in the development of the technology behind autonomous vehicles, playing a vital part in the pipeline by which autonomous vehicles consume and process a vast amount and variety of data, which is essential for improving safety, security, efficiency, and the overall user experience.

8. Blockchain in Autonomous Vehicles

The potential of blockchain technology could revolutionize the operations and functionality of autonomous vehicles. As a distinctive form of distributed ledger technology (DLT), blockchain provides a platform for secure and transparent transactions and data exchanges, which are pivotal to autonomous vehicles. It strengthens security, maintains privacy, and builds trust among users, vehicles, and the various entities embedded in the transportation ecosystem. Moreover, it facilitates real-time data exchange, enhances the decision-making abilities of autonomous vehicles, and paves the way for innovative business models. With the integration of blockchain technology, a more efficient, interconnected, and intelligent transportation system can be envisaged.

Blockchain technology can be used in autonomous vehicles in several ways:

1. **Enhanced situation awareness:** Blockchain technology offers a secure and reliable mechanism for autonomous vehicles to share information, elevating their situational awareness and decision-making capabilities. It enables vehicles to exchange real-time data regarding traffic conditions, potential road hazards, and other relevant factors. This collected information is stored in the blockchain, which provides a transparent and tamper-resistant record [114].
2. **Reputation management:** Employing blockchain technology enables the development of a reputation system for autonomous vehicles in which reputation points are awarded for the sharing of accurate and beneficial data. This enables vehicles to actively contribute to the network and ensures the transmission of high-quality data [115].
3. **Security for firmware updates:** Blockchain can be utilized to secure firmware updates in autonomous vehicles, mitigating the risk of harmful attacks that could compromise the vehicle systems [116].
4. **Liability attribution:** In scenarios involving accidents with autonomous vehicles, blockchain technology can play a crucial role in accurately identifying the vehicle at fault. This assists in resolving disputes and ascertaining fair liability assignment [117].
5. **Ride-hailing platforms:** Blockchain technology is applicable in the creation of secure, decentralized ride-hailing platforms for autonomous vehicles. Such platforms provide a secure and transparent process for users to arrange rides and for vehicles to receive appropriate compensation for their services [118].
6. **Internet of Vehicles:** The implementation of blockchain can facilitate a secure, decentralized network of vehicles or devices, drawing parallels to the Internet of Things. This would enable vehicles to communicate amongst themselves, share data, and coordinate actions in a secure, transparent manner [119,120].

8.1. Blockchain Applications

According to the published research in this field, blockchain technology has the potential to transform a variety of different aspects of autonomous cars. According to Kamble [121] and Show [122], utilizing blockchain technology may strengthen security measures, expedite vehicular operations, and make collaborative storage options more accessible. Pedrosa and Pau [123] focused on the application of blockchain technology in intelligent transportation settings, with a specific emphasis on the function that blockchain technology plays in the automation of contracts and transactions for the recharging process in autonomous electric cars. Furthermore, Jain et al. [124] investigated the numerous applications of blockchain technology in a variety of autonomous vehicles and systems. These include autonomous electric vehicles (AEVs), autonomous underwater vehicles (AUVs), automated guided vehicles (AGVs), autonomous aerial electric vehicles (AAEVs), and autonomous driving systems. In conjunction, the findings of this research highlight how the use of blockchain technology in the field of autonomous cars may improve trustworthiness, operational dependability, and system efficiency.

When cyber security is in the spotlight, blockchain is at the forefront of mitigating the numerous risks associated with autonomous vehicles [125]. Securing over-the-air (OTA)

software and firmware updates, a crucial aspect of the maintenance and performance of autonomous vehicles, is a prominent example of blockchain's capabilities [126]. By employing a blockchain-based framework, the integrity of the update procedure is maintained, allowing only authentic original equipment manufacturers (OEMs) to distribute software upgrades and updates. In conjunction with ensuring that only authenticated vehicles can access and deploy these upgrades, this creates an impenetrable security perimeter around the OTA procedure [126].

This combination is not without its challenges and potential traps, and it is imperative that this amalgamation be approached with discernment. The complexities of the data transmission networks that enable autonomous cars, when combined with the inherent symmetries of cyber security, have the potential to accidentally pave the path for new vulnerabilities during data transfers between vehicles and IoT devices [71]. This necessitates a relentless commitment to innovation and the construction of complex countermeasure models and cutting-edge security algorithms, both of which are specifically geared to neutralize cyber security vulnerabilities and prevent incidents of data loss [71].

Ultimately, blockchain technology is well-positioned to play an essential role in the paradigm change that will be brought about by autonomous cars. This will be accomplished via the implementation of strong security and the guarantee of unrivaled privacy. Although blockchain is a reliable ally in reducing risks, especially with respect to over-the-air (OTA) updates, it is essential to remain vigilant and proactive in order to successfully navigate the problems and vulnerabilities that are brought about by the combination of blockchain technology with autonomous cars.

8.2. Benefits in AVs

Most research has focused on the crucial role that blockchain technology may play in the process of transforming autonomous cars. Both the [119,127] are investigating the myriad of ways that blockchain technology might enhance cyber security, consequently producing an impenetrable and reliable infrastructure for the real-time transfer of vehicle telemetry data. The safety of sensitive vehicle data may be significantly improved by using the features of blockchain technology that make it inherently secure and impervious to change.

The discussion is brought to a higher level by Wang's presentation of a novel framework known as the blockchain-enabled autonomous vehicular social network (AVSN) [128]. This cutting-edge architecture not only protects information transmission using cryptographic protocols but also deftly orchestrates an incentive system for connected autonomous vehicles (CAVs), which encourages them to distribute material that can be verified and trusted. This helps to maintain the integrity of the material while also building a culture of cooperation and trust among the many organizations that make up the network. This brings the ecosystem closer to being in balance.

Alladi et al. [129] presented a larger perspective and provided a complete examination of the several ways in which blockchain technology might be used inside networks of unmanned aerial vehicles (UAVs). This research study investigated a wide range of applications, including but not limited to enhancing network security, accelerating decentralized storage paradigms, fine-tuning inventory management, and boosting cutting-edge surveillance methodologies.

The use of blockchain technology in the field of autonomous vehicles (AVs) has the potential to usher in a number of significant developments and advantages over a wide variety of domains. Listed below is an in-depth analysis of these cutting-edge advantages:

- Blockchain-based collaborative crowd sensing (BCC) in autonomous vehicular networks (AVNs): Blockchain prepares the way for an unprecedented, safe environment that is favorable for intense data transfers and fair recompense. This is an important step in the development of pioneering vehicular crowd sensing. It does an excellent job of protecting the privacy of AVs while also assuring the efficient usage of resources in the process of completing tasks [130].

- **Impenetrable security and uncompromised privacy:** AVs, which are often afflicted by intrinsic security weaknesses, may find refuge in the arms of blockchain technology, which offers impenetrable security and does not compromise privacy. The blockchain eliminates reliance on any centralized entity, thanks to its decentralized philosophy, and the immutability of its ledger instills unshakable faith in the system. Its inherent design principles render it immune to both single points of failure and a wide variety of security flaws, making it a very secure system. The combination of blockchain technology and artificial intelligence (AI) creates a sturdy fortress that efficiently protects autonomous vehicles (AVs) from a wide variety of dangerous threats [131].
- **Uncompromisable data integrity:** The combination of blockchain technology and unmanned aerial vehicles (UAVs) that are incorporated into autonomous vehicles (AVs) acts as a stronghold for data-related security. This hybrid approach may be further strengthened by the use of AI, opening the path for an integrated security fabric that is both robust and adaptable [132].
- **Efficient privacy preservation** conventional federated learning (FL) systems, which utilize direct raw data transfers to servers, are known for the privacy issues that they invoke. Although blockchain may be a helpful tool in protecting users' privacy, doing so comes at the expense of increased computing load. The implementation of gradient encryption in FL makes it possible to encrypt data in situ. This is made possible by using the processing power of edge devices. This not only protects the privacy of the data but also eliminates the need for extra processing resources, and it does all of this without any additional cost in terms of performance [14].

In a nutshell, the combination of blockchain technology and autonomous vehicle technology heralds the beginning of a new age of innovation that will be characterized by groundbreaking vehicular crowd sensing, unshakable security, perfect data integrity, and resource-efficient privacy conservation solutions.

8.3. Blockchain Potential Risks in AVs

Blockchain technology, heralded as a game changer for numerous industries, also shows promise in transforming the realm of autonomous vehicles (AVs). However, it is imperative to carefully navigate the intricate web of challenges and risks associated with its implementation:

- **Scaling bottlenecks:** Major blockchain networks such as Ethereum and Bitcoin exhibit constrained processing capacities, hovering around 5 to 20 transactions per second [133]. When juxtaposed with the high-velocity data exchanges integral to vehicular networks, these limitations pose significant challenges. It is imperative to develop or adopt blockchain architectures that are nimble enough to accommodate the velocity and volume of data inherent in autonomous vehicular systems.
- **Cyber security threats:** The complex communication networks that form the backbone of AV interactions are not impervious to cyber threats. These networks could be prey to attacks that not only compromise data but also imperil human lives through accidents instigated by erroneous or manipulated data [133]. To address this, cyber security mechanisms need to be woven into the blockchain fabric to fortify the system against intrusions and hacks.
- **Navigating privacy concerns:** Although blockchain technology's decentralized ledger systems improve security, the irreversible nature of data that is held on blockchains may pose privacy problems if not managed properly. It is essential to make use of privacy-enhancing technology, either via zero-knowledge proofs or other cryptographic approaches, in order to bring blockchain's transparency into harmony with the need for user anonymity and data security.
- **Integration complexities:** The rapid rate of innovation in hardware and software stands in stark contrast to the longer service life cycles of vehicles [134]. The integration of blockchain into the dynamic ecosystem of autonomous vehicles demands an agile ap-

proach, possibly through modular and adaptable frameworks that can keep pace with technological advancements without necessitating wholesale infrastructural changes.

- **Environmental and resource stewardship:** Certain blockchain frameworks, particularly those reliant on proof-of-work consensus algorithms, are notorious for their prodigious energy consumption. Beyond the environmental repercussions, the resource intensiveness of these systems could also tax the computing capacities within vehicles. Alternative consensus algorithms such as proof of stake or proof of authority might mitigate these challenges, striking a balance between security and resource efficiency.

It is crucially important to adopt an intelligent and forward-thinking strategy in order to maximize the revolutionary potential of blockchain technology in autonomous cars and enjoy the benefits of this potential. This requires the development and implementation of blockchain frameworks that are scalable, secure, and resource-efficient, along with the integration of privacy protections and cyber security defenses. The academic literature emphasizes both the exciting prospects, as well as the inherently difficult obstacles, that are associated with the combination of blockchain technology and autonomous cars. The potential security flaws that are associated with connected autonomous vehicles (CAVs) were investigated in depth in critical research that was carried out by Rajendar et al. [135]. The study focused on the potential solutions that may be provided by blockchain technology. Notably, the study highlighted the potential of blockchain technology to improve the reliability and integrity of data transfers, as well as intervehicle communication.

In a study that echoes similar results, Gupta et al. [136] conducted an in-depth investigation of the threat scenario posed by CAVs and highlighted the potentially game-changing role that blockchain technology may play in the fortification of vehicle networks. Their research went beyond just praising the benefits of blockchain technology and instead provided concrete insights into how blockchain-based frameworks might be adapted to meet the specific safety criteria of CAVs.

In addition, Reyna et al. [137] investigated the symbiotic relationship between blockchain technology and the ecosystem of the Internet of Things (IoT). Blockchain emerges as a formidable tool for maintaining data security, allowing for smooth machine-to-machine transactions and limiting the single points of failure in centralized systems when connected autonomous vehicles (CAVs) are used in conjunction with Internet of Things (IoT) networks. This intersection is of special relevance.

In their comprehensive study of the uses of blockchain technology in intelligent transportation systems, which includes autonomous vehicles (CAVs), Jabbar et al. [138] provided a 360-degree perspective. Their research meticulously catalogs a variety of blockchain implementations, deconstructing their respective advantages and disadvantages and providing a comparative analysis of the outcomes. This thorough study provides vital insights for decision makers and engineers, assisting them in choosing the ideal blockchain architecture that is in harmony with the requirements and restrictions of intelligent transportation.

In conclusion, the academic discussion highlights the enormous potential of blockchain technology as a key component to improve the safety, dependability, and effectiveness of CAVs. However, it should also be noted that this is not a problem that can be solved with a single solution; rather, the deployment of blockchain technology requires careful evaluation of the obstacles and restrictions it presents. In order to maximize the benefits that may be derived from the groundbreaking combination of blockchain technology and autonomous car ecosystems, it is necessary to maintain a high rate of innovation and have a solid grasp of the complexity involved in both of these fields.

8.4. Blockchain-Based Solutions for AVs

The exploration of blockchain technology application in autonomous vehicles (AVs) is thoroughly presented across five distinctive aspects in Tables 3–7.

Table 3 focuses on the employment of blockchain to enhance the security of data storage in AVs. The presented solutions are built on Ethereum, Consortium BC, and Private BC platforms.

Table 4 highlights the potential of blockchain technology in securing communication channels, particularly those relating to vehicle-to-vehicle (V2V) networks and in-vehicle networks, with works using various platforms, including Ethereum, Bitcoin, and Lightweight BC.

In Table 5, the attention shifts towards the preservation of data integrity and privacy in AV systems. The presented solutions address concerns such as AV forensics and location privacy, employing platforms like Permissioned BC, IoTChain, and IOTA Tangle DLT.

Table 6 presents a comprehensive analysis of how blockchain technology can be leveraged for forensic purposes in the context of AVs, providing means for accident responsibility identification and event recording systems.

Table 7 expands on research and implementations that focus on utilizing blockchain for reputation and trust management among AVs. The discussed solutions utilize both the Public and Consortium BC platforms.

All of the tables below provide valuable insight into the multifaceted role that blockchain technology can play in addressing challenges in the autonomous vehicle sector. This ranges from enhancing data security to creating network trust, emphasizing the immense opportunity that blockchain presents for future research and development in this field.

Table 3. Blockchain applications in autonomous vehicles (AVs)—secure data storage.

Description	Blockchain Platform	Authors	Year
Secure cloud-based storage of AV data	Ethereum	Jiang et al. [139]	2019
Secure data storage and sharing between AVs and RSUs	Consortium BC	Zhang et al. [140]	2019
Encrypting and hashing the AV data for secure storage	Public/Private BCs	Singh et al. [141]	2021
Data storage system with incremental AV data updating	Ethereum	Yin et al. [142]	2021
Secure data storage and sharing among AVs	Ethereum	Riya et al. [143]	2022
Encrypting and hashing the AV data for secure storage	Private BC	Meghna et al. [144]	2022

Table 4. Blockchain applications in Autonomous vehicles (AVs)—secure communication channels.

Description	Blockchain Platform	Authors	Year
Securing V2V communications and privacy protection	Private BC	Singh et al. [145]	2017
Securing V2V communications (V2V network)	Ethereum	Rowan et al. [146]	2017
Securing the communications between AVs and RSUs	Bitcoin	Yang et al. [147]	2018
BC-based V2V data aggregation model	Hyperledger Fabric	Mitra et al. [148]	2018
Securing smart sensors of AVs (in-vehicle network)	Ethereum	Rathee et al. [149]	2019
Securing in-vehicle network components	Private BC	Oham et al. [150]	2021
Secure sensing and tracking of AVs	Ethereum	Dakshita et al. [151]	2021
Secure routing for swarm UAS networking	Lightweight BC	Wang et al. [152]	2021
BC-based system for secure V2V communication	Public BC	Kamal et al. [153]	2021
BC-based secure V2V communication using ICN	Public BC	Ali et al. [154]	2022

Table 5. Blockchain applications in autonomous vehicles (AVs)—data integrity and privacy.

Description	Blockchain Platform	Authors	Year
Records all necessary data for an AV forensics solution	Permissioned BC	Cebe et al. [155]	2018
Protecting the AV identity and location privacy	IoTChain [156]	Li et al. [157]	2018
Ensure safety and information integrity inside the AV	Bitcoin	Davi et al. [158]	2019
Data integrity by tracking the actions of AVs	Exonum platform	Narbayeva et al. [127]	2020
Protection against data-tampering attacks in AV network	IOTA Tangle DLT	Rathore et al. [159]	2020
BC key management framework and hash graphs	Permissioned BC	Jha et al. [133]	2022

Table 6. Blockchain applications in autonomous vehicles (AVs)—forensics applications.

Description	Blockchain Platform	Authors	Year
Fragmented ledger for forensic analysis of traffic accidents	Lightweight BC	Cebe et al. [155]	2018
Event recording system for vehicular digital forensics	Ethereum	Li et al. [160]	2021
BC-based accident responsibility identification model	Lightweight BC	Yao et al. [161]	2022
BC-based reputation system for AV accident forensics	Permissioned BC	Oham et al. [150]	2022

Table 7. Blockchain applications in Autonomous vehicles (AVs)—reputation and trust management.

Description	Blockchain Platform	Authors	Year
Data sharing in V2V using reputation and contract theory	Public BC	Kang et al. [162]	2019
BC-based solution for reputation management in IoV	Ethereum	Abbes et al. [163]	2021
Two-layered AV reputation BC system	Private/Public BCs	Lee et al. [164]	2021
BC-based trust scheme for cellular V2X ecosystems	Consortium BC	Bhattacharya et al. [165]	2022
BC-based reputation system for secure V2V communications	Public BC	Kianersi et al. [115]	2022

9. Discussion

9.1. Challenges, Open Issues, and Future Research Directions for EIAVs

The domain of autonomous vehicles (AVs) remains in its growth phase, laden with an abundance of sensitive information and fresh technical hurdles. The enormous breadth and complexity of the topic render it multifaceted terrain. This is further compounded by the current scarcity of comprehensive global standards that guide the development, safety, and security procedures for AVs. As a result, investigating and addressing issues regarding the security and safety of AVs is not only highly intricate but also of utmost importance.

As AVs continue to evolve technologically, their ecosystem is expected to broaden to include a greater number of individual devices and supplementary infrastructure. This growth is likely to bolster connectivity; however, it could simultaneously render AVs more vulnerable to a plethora of security risks. This development gives rise to critical questions and challenges that demand immediate scholarly attention.

- **Protection of V2X communication:** Ensuring the security of vehicle-to-everything (V2X) communication is critical, as a breach in AVs might have cascading effects on connected smart infrastructure and vice versa. For instance, an attack on an electric vehicle could ripple through to the electricity grid, charging stations, and utility systems. Consequently, future research should prioritize the formulation of strong protective measures and the establishment of secure communication channels.
- **Synchronization of safety and security protocols:** Typically, assessments of vehicle safety and security are performed separately, which leads to the creation of disparate protective measures. However, fostering a seamless synergy between safety and

security protocols within AVs is essential. Therefore, future research must concentrate on analyzing the inter-relations between safety and security measures to ascertain their coordinated efficiency.

- **Engagement with non-automated road participants:** In mixed traffic conditions, AVs need to effectively communicate and cooperate with both automated and non-automated road users, such as traditional vehicles, bicycles, and pedestrians. Gaining insight into and making predictions about human behavior in mixed traffic situations is difficult but vital for ensuring safety. There is an urgent need for research that improves our grasp of the interactions between humans and AVs in these contexts.
- **Safeguarding CAN bus communications:** The Controller area network (CAN) bus, which handles sensor data transmission, is exposed to potential attacks. In the absence of security measures like encryption, vital mission-planning data can be exposed and at risk. Future investigations should focus on strategies for effectively safeguarding CAN bus communications to maintain data integrity and authenticity.
- **Adapting to new attack methods:** As technology keeps advancing, so do the methods used in cyber attacks. Future research needs to stay one step ahead by trying to predict the new ways that attackers might attempt to breach security and by developing strategies to prevent these attacks before they can happen.
- **Formulation of holistic standards and regulations:** The absence of universal standards for the safety and security of AVs presents a considerable obstacle. The creation and enforcement of international norms would supply a uniform framework to steer the development of secure and reliable AV systems, consequently bolstering the overall security stance of AVs.
- **Addressing machine learning weaknesses:** Machine learning, especially deep learning, is a cornerstone of AV technology but is vulnerable to targeted attacks. Future studies should consider the development of solid strategies to shield machine-learning algorithms in AVs from these potential incursions.

9.2. Challenges

The development of autonomous vehicles signifies a transformative potential for the future of both private and public transportation systems. Nevertheless, the realization of this future is contingent upon overcoming numerous obstacles, particularly in the area of security. As this field of research progresses, it becomes increasingly clear that ensuring the secure and reliable operation of AVs is a task of considerable complexity. As discussed in the preceding sections, sensor systems and communication channels, which are integral to the functioning of AVs, are susceptible to an array of cyber attacks. This necessitates substantial advances in the areas of image analysis and processing capacity to consistently and accurately interpret complex driving environments and make optimal decisions in real time.

In addition to these technical challenges, there are also significant societal, legal, and ethical hurdles to be explored. The societal acceptance of AVs lies in public confidence in their safety and reliability, requiring comprehensive and robust safety validation. Furthermore, the regulatory landscape for AVs is still evolving and represents a significant challenge, with requirements varying across countries. Finally, there are also ethical dilemmas to be addressed, relating to the decision-making capabilities of AVs in critical scenarios. Addressing these multifaceted challenges will be a key part of the journey towards a future where autonomous vehicles become a widespread reality.

Ultimately, as the world of transportation is experiencing major changes due to the introduction of autonomous vehicles (AVs), there is a lot of interest in how they could completely change the way we travel. However, as these vehicles continue to develop, especially in terms of how they can understand and react to human emotions, there are many different challenges that emerge. Through our detailed research, we have identified the following key areas that need attention and investigation.

1. **Risk mitigation technologies:** Transitioning from manual to automated driving requires a comprehensive understanding of risk mitigation technologies. In the discussion on risk mitigation requirements and problems, the parameters of object detection, cyber security, and privacy in V2X interactions stand out as significant topics [125].
2. **Real-time decision making:** In order for an autonomous vehicle to be considered competent, it must be able to successfully carry out real-time decision making, which allows it to outperform the skills of a human driver. Technology must continue to advance, especially in the areas of high-speed processing and decision-making algorithms, in order for such achievements to be possible [125].
3. **Garnering public trust:** The level of public trust is a crucial factor that determines the final level of success and broad adoption of autonomous vehicles. This necessitates an amount of technical accuracy that has never been seen before, establishing faith in the autonomous vehicle's capacity to find solutions to problems and ensuring its overall safety [14].
4. **Precision positioning technologies:** The development of technologies that are able to accurately identify the locations of vehicles is necessary for the production of intelligent transportation systems that are both safe and dependable. These systems need to take into account a variety of unknown factors, including the unexpected behaviors of pedestrians, random objects, and different road conditions [14].
5. **Environmental detection:** The ability of an autonomous vehicle to accurately identify its surroundings is essential to the vehicle's ability to navigate successfully. As a result, AV safety relies heavily on the development of technologies that can detect and react appropriately to a variety of settings [14].
6. **Pedestrian detection:** The protection of pedestrians must be given top priority in the design of autonomous vehicles, which calls for detecting systems that are accurate and dependable [14].
7. **Path planning:** The capacity of an autonomous vehicle to plot its own route is a critical factor in determining not just its level of safety but also its level of efficiency. As a result, the creation of technologies that make precise route planning and prediction possible is of critical importance [14].
8. **Motion control:** The successful control of motion is necessary for the safe navigation of AVs. The development of technologies that can precisely regulate the motion of the vehicle, even under unanticipated conditions, is an issue of the highest priority [14].
9. **Vehicular communication technologies:** The field of V2X communications requires the development of reliable vehicular communication technologies, which can enable autonomous cars to connect without any issues with other vehicles and infrastructures [9].
10. **Traffic management:** The increasing number of autonomous vehicles may make traffic congestion worse if it is not controlled in an effective and reliable manner. Innovative methods like policy-based deep reinforcement learning and intelligent routing are able to optimize traffic flow management, which, in turn, helps mitigate congestion [166].

Despite the fact that these challenges appear impossible to overcome, they highlight the considerable future potential for research and innovation in the entire spectrum of autonomous vehicles.

By addressing these difficulties head-on, we can ensure the integration of autonomous vehicles into our transportation networks in a way that is both safe and efficient, leading to a new age of mobility. Researchers can ensure the safe and effective integration of autonomous cars into our transportation networks by continuing to tackle these challenges head-on, ushering in a new era of transportation.

Challenges and Proposed Solutions for Autonomous Vehicle Security

Before delving into the specific challenges and their corresponding solutions, it is important to acknowledge the complex and dynamic nature of security in the autonomous

vehicle landscape. The fusion of advanced technologies such as AI, IoT, and blockchain, while enabling unprecedented levels of automation, also introduces complex security dimensions that demand comprehensive and innovative solutions. These complexities are further compounded by the fact that autonomous vehicles operate in real-time and ever-changing environments, necessitating agile and robust security systems. Therefore, understanding the potential difficulties in implementing fundamental security concepts and supplementary features is of paramount importance, as is the identification of practical solutions to these challenges. Let us explore some of these challenges and their proposed solutions.

Challenge 1—System complexity: The complex network of sensors, advanced algorithms, and interconnected systems inherent in autonomous vehicles introduces substantial complexity to the application of security concepts.

Proposed solution: Incorporating a ‘security by design’ approach, where security measures are fundamentally integrated at the design inception of the system, is critical. Additionally, system compartmentalization could limit potential security breaches by ensuring each component operates independently and is isolated from the others.

Challenge 2—Real-time operation requirements: Given the real-time nature of autonomous vehicles’ operational decisions, the introduction of latency by certain security operations, particularly complex encryption algorithms, can impede smooth functionality.

Proposed solution: The application of lightweight encryption algorithms and hardware-accelerated security operations can help fulfill real-time requirements without compromising security.

Challenge 3—Scalability issues: The exponential growth of data volume exchanged and managed as autonomous vehicles proliferate can strain the system, thereby complicating security maintenance and incident response.

Proposed solution: The implementation of scalable security solutions is essential. Here, distributed ledger technologies such as blockchain can ensure security and privacy in a decentralized and scalable manner.

Challenge 4—Long vehicle lifespan: The typical life cycle of vehicles far outlasts the rapid evolution of cyber threats, posing a unique challenge.

Proposed solution: Over-the-air (OTA) updates can be instrumental in enabling vehicles to continually update their security systems to counter new threats. Ensuring backward compatibility of these updates is a critical aspect of this solution.

Challenge 5—legislation and standards: The accelerated pace of autonomous vehicle technology development often surpasses the existing legislation and security standards.

Proposed solution: A cooperative effort involving vehicle manufacturers, cyber security experts, and policymakers is necessary to establish and regularly update regulations and standards specifically tailored to autonomous vehicles.

Although these challenges are significant, they are not unsolvable as long as there is continual research, innovation, and a concerted effort to collaborate across the numerous industries that are contributing to the development and deployment of autonomous vehicles.

9.3. Open Topics

In order to acquire a more complete understanding of the immense potential and inherent complexities involved in the development of emotionally intelligent autonomous vehicles (EIAVs), the following clarifications may be considered:

- **In-vehicle health monitoring [167]:** An enhanced focus on health monitoring within vehicles could lead to the incorporation of sophisticated biometric and physiological sensors. These could track passenger vital signs, stress levels, and emotional states. EIAVs, equipped with advanced health monitoring systems could adapt their behavior in real time to ensure a safer and more comfortable journey. For example, detecting elevated stress levels could trigger a more conservative driving style or initiate a calming ambient environment.

- **Simulation-based testing and validation [168]:** Enriching simulation-based testing for emotionally intelligent autonomous vehicles (EIAVs) necessitates the introduction of multifaceted emotional scenarios. This incorporation brings a novel layer of complexity to the validation process. For instance, the manner in which an EIAV responds to a passenger experiencing emotional distress becomes a crucial metric of its performance. Similarly, the vehicle's ability to identify and respond appropriately to a passenger's discomfort in heavy traffic or concern about speed forms an essential part of its evaluation. The development of such emotional scenario databases for rigorous testing, followed by a thorough assessment of EIAVs' responses, constitutes a pivotal aspect of their evolution.
- **Underwater Internet of Things (UIoT) [169]:** Gaining higher-level abstractions or insights from the UIoT, EIAVs could incorporate underwater vehicular communication protocols for specific applications, such as underwater rescue or exploration vehicles. The unique challenges and solutions in UIoT communication could provide valuable lessons to enhance V2X (vehicle to everything) communication in EIAVs, even under challenging conditions.
- **Intelligent data processing methods [170]:** To enhance EIAV capabilities, we might integrate artificial intelligence and machine learning techniques to analyze the vast amount of data these vehicles would generate and receive. Emotional data, in particular, can be complex and multimodal, necessitating sophisticated, AI-driven approaches for reliable interpretation and reaction.
- **Autonomous traffic management (ATM) [171]:** Extending the scope of ATM to include affective factors is an intriguing area of research. For instance, traffic congestion, an external factor, invariably impacts the overall mood of a passenger within a vehicle. An advanced EIAV could be designed to intelligently respond to such circumstances. It may proactively select routes less predisposed to causing passenger stress or leverage onboard systems to sustain a tranquil environment, irrespective of the traffic conditions outside. This indicates that future EIAVs must not only be able to navigate efficiently through tangible road networks but also to understand the complex nature of human emotions.

These topics further underscore the groundbreaking potential of EIAVs and the multitude of open-ended research avenues they present. By employing a cross-disciplinary approach and incorporating lessons learned from related disciplines, the emergence of EIAVs as an essential component of our transportation ecosystem becomes more plausible.

9.4. Cyber Security Risks and Safety Concerns of EIAVs

Emotionally intelligent autonomous vehicles (EIAVs) represent an innovative integration of artificial intelligence and machine learning. These vehicles are designed with the capability to understand and adapt to human emotions, thereby promising a transformative shift in the transportation sector. However, alongside the innovative possibilities, they also introduce considerable cyber security risks and safety challenges, which necessitate comprehensive research and strategic intervention. Several crucial points have been identified for the successful deployment of EIAVs:

Cyber security threats:

- **Sensor and communication security:** EIAVs rely heavily on components such as camera sensors, global positioning systems (GPS), and V2X (vehicle-to-everything) communication protocols. These are potential targets for cyber attacks. Therefore, robust protective measures can be instituted to secure these crucial components, as presented in [91].
- **Onboard unit (OBU) security:** The OBU functions as the central processing unit of an autonomous vehicle and can be subjected to cyber exploitations, facing significant threats to the vehicle's safety and functionality. Strengthening the cyber security defenses of the OBU is an essential aspect of protecting EIAVs, as highlighted in [91].

- **Systemic vulnerabilities:** The systemic complexity that is present in EIAVs expands the potential surfaces for cyber attacks. Comprehensive cyber security strategies are essential to ensure that all points of potential intrusion are secured, as described in [172].
- **Interconnected system vulnerabilities:** The interconnected and interoperative nature of systems within EIAVs can introduce unintended security gaps. Early identification and rectification of these vulnerabilities are critical to a robust and secure approach [172].
- **Proprietary system risks:** Proprietary systems or integrated systems that lack optimal interaction with other systems could present additional security challenges. The development and implementation of standardized protocols ensuring seamless interoperability are necessary to alleviate these risks [173].
- **Edge computing concerns:** The incorporation of edge computing and localized nodes in EIAVs can lead to severe privacy and security issues. Addressing these requires a thorough evaluation and subsequent enhancement of existing security protocols, as mentioned in [174].

Safety concerns:

- **Risk mitigation technologies:** To maintain safety standards, concurrent advancements in risk mitigation technologies are indispensable in the progression of autonomous vehicles [125].
- **Object detection and V2X privacy:** The establishment of rigorous safety standards for object detection and V2X privacy is integral to the reliable operation of EIAVs. The formulation of these norms remains a significant area of research [125].
- **Evaluation of autonomous technology:** A comprehensive analysis of the potential benefits and risks of autonomous technology is required for its effective integration into conventional transport systems. This objective evaluation must be coupled with robust risk mitigation strategies [125].
- **Intelligent navigation capabilities:** The ability of EIAVs to intelligently interact with and navigate safely among other road users is fundamental to their operational viability. Enhancing these capabilities forms a crucial part of improving the overall safety of EIAVs [125].

9.4.1. Consequences for People's Lives and the Economy

Autonomous vehicles are becoming increasingly popular, and with their rise comes the need for robust security measures to protect against potential cyber attacks. Security flaws in autonomous vehicles can have significant impacts on people's lives and the economy. Listed below are some ways in which security vulnerabilities in autonomous vehicles could impact people's lives and the economy:

- **Safety:** Security flaws in autonomous vehicles can compromise the safety of passengers and other road users. For example, a hacker could take control of an autonomous vehicle and cause it to crash or drive recklessly [175].
- **Privacy:** Autonomous vehicles collect a lot of data about their passengers, such as their location and driving habits. If these data fall into the wrong hands, they could be used for nefarious purposes [175].
- **Economy:** Autonomous vehicles have the potential to revolutionize the transportation industry, but security flaws could slow down their adoption. If people do not trust autonomous vehicles to be secure, they may be less likely to use them, which could have a negative impact on the economy [175,176].

It is important to note that security flaws in autonomous vehicles are not just theoretical. Researchers have already demonstrated that wireless jamming attacks can impact the fuel efficiency of cooperative adaptive cruise control (CACC) systems [177]. Additionally, there is a lack of effective infrastructure for evaluating security solutions for autonomous vehicles. This means that there is still a lot of work to be done to ensure that autonomous vehicles are secure [178].

In conclusion, security is a crucial aspect of autonomous vehicles, and the potential repercussions of a breach are significant. It is important to continue researching and developing security measures to protect against potential cyber attacks.

9.4.2. Fundamental Security Principles

Fundamental security principles are crucial for protecting the security of autonomous vehicles and the dangers they seek to counteract. Autonomous vehicles rely on complex software and hardware systems to operate [179], and any vulnerabilities in these systems can be exploited by attackers to gain control of the vehicle or cause it to malfunction. This can result in serious safety risks for passengers, other drivers, and pedestrians.

Some of the key security principles that are important for protecting autonomous vehicles include:

- **Safety and Data protection:** Autonomous vehicles generate and process vast amounts of data, including sensor readings, location information, and communication data. Protecting these data from unauthorized access or manipulation is essential to maintain privacy and prevent misuse. Ensuring the security of these systems is vital to prevent unauthorized access or malicious attacks that could compromise the safety of the vehicle and its occupants [179].
- **System integrity:** Autonomous vehicles rely on complex software and hardware systems to operate effectively. By adhering to security principles such as secure coding practices and regular vulnerability assessments, the integrity of these systems can be maintained, reducing the risk of system failures or malfunctions [180].
- **Resilience to attacks:** Autonomous vehicles are potential targets for cyber attacks, which can range from unauthorized access to the vehicle's systems to remote control of its functions. Implementing security principles helps to identify vulnerabilities, establish robust defenses, and develop incident response plans to mitigate the impact of attacks and ensure the vehicle's continued operation [180].
- **Public trust:** Security principles are essential for building and maintaining public trust in autonomous vehicles. By implementing robust security measures, autonomous vehicle manufacturers and operators demonstrate their commitment to protecting the safety and privacy of users [179].
- **Perception security:** Autonomous vehicles heavily rely on perception, such as obstacle detection, traffic sign detection, lane detection, etc. With the power of deep learning algorithms, such perception tasks in autonomous driving systems widely apply deep neural network (DNN)-based models. Recent works have found that DNN models are generally vulnerable to adversarial examples or adversarial attacks. Thus, studying the security of perception in autonomous driving systems under physical-world adversarial attacks is very necessary [181].
- **Data poisoning attack:** The development of connected and autonomous vehicles (CAVs) relies heavily on deep learning technology, which has been widely applied to perform a variety of tasks in CAVs. On the other hand, deep learning faces some security concerns. Data poisoning attacks, as one of the security threats, can compromise deep learning models by injecting poisoned training samples. Therefore, the principles of poisoning attacks are worth studying in order to propose countermeasures [182].
- **Intrusion detection:** Intelligent transportation systems (ITSs), particularly autonomous vehicles (AVs), are susceptible to safety and security concerns that impact in people's lives. The safekeeping of communications and computing constituents of AVs can be threatened using sophisticated hacking techniques, consequently disrupting AVs from operative usage in our daily life routines. In this regard, a multistage intrusion detection framework can be used to identify intrusions from ITSs and produce a low rate of false alarms. The proposed framework can automatically distinguish intrusions in real time [183].

These principles are important for protecting the security of autonomous vehicles and the dangers they seek to counteract. Autonomous vehicles rely on complex software and

hardware systems to operate, and any vulnerabilities in these systems can be exploited by attackers to gain control of the vehicle or cause it to malfunction. By following these fundamental security principles, autonomous vehicle manufacturers can help to protect the security of their vehicles and prevent them from being exploited by attackers.

9.5. Privacy Preservation Techniques in Vehicular Communications

Considering the increasing popularity of vehicular networks, privacy preservation emerges as a vital concern, specifically in transactions between autonomous vehicles and third-party entities, such as traffic management systems. The following methods underscore the key techniques employed to uphold the privacy of information within these interactions:

Encryption: As a foundational method in information security, encryption transforms data into a code to impede unauthorized access. Various algorithms—both symmetric (e.g., AES and DES) and asymmetric (e.g., RSA and ECC)—are employed to safeguard sensitive data [184].

Secure communication protocols: During data transit, the adoption of secure communication protocols is integral. Protocols such as transport layer security (TLS) and Internet protocol security (IPSec) deploy robust encryption and authentication mechanisms to maintain data confidentiality and integrity [185,186].

Anonymization: To protect the identity of individuals or vehicles, anonymization techniques are used. These involve the removal or encryption of personally identifiable information (PII) such as location, image, and license number [187]. For instance, pseudonym systems can be employed where vehicles are allocated pseudonyms, obscuring the traceability of the vehicles' real identity.

Blockchain technology and blockchain smart contract code: The decentralized nature of blockchain technology fortifies data privacy within vehicular networks. It ensures that every data transaction is recorded and authenticated transparently and securely, prohibiting unauthorized alteration or access. In [188], the authors reviewed the applied state-of-the-art formal methods of smart contract specification and verification with the aim of reducing the risk of faults and bug occurrence and avoiding possible resulting costs. However, most approaches fail to reflect the characteristics of the blockchain and user behavior. In, [189], the authors proposed a novel formal modeling approach to verify the execution environment behavior of smart contracts. The authors applied this formalization to a real-world example of a smart contract and analyzed its violations using a statistical model verification technique [189].

Differential Privacy: This methodology allows the public dissemination of information about patterns within a dataset, while safeguarding the individual data points within. In the context of vehicular networks, differential privacy can be leveraged when sharing data with third parties, thereby preventing any possibility of reverse engineering to single out individual vehicles or users.

Homomorphic encryption: This method allows for computations to be conducted on encrypted data without the necessity of decryption. As such, a third-party system could analyze and work with the received data while preserving the privacy of the raw data [190,191].

Federated learning for autonomous vehicle privacy protection: Federated learning is a distributed machine learning technique that allows models to be trained collaboratively without directly sharing the data [192]. Instead of transmitting individual client data to a central server, the central server sends its model to the clients, and each client trains the model with its own data. This approach helps protect the privacy of the data collected by autonomous vehicles while still allowing for model improvement [187,193].

Personalized k anonymity: Personalized k anonymity is a privacy preservation technique that ensures that query contents submitted by users in autonomous vehicles are sufficiently protected. It achieves this by perturbing location information or applying k -

anonymity techniques, which group queries together to provide privacy while maintaining query utility [194].

As part of their functioning, autonomous vehicles need to communicate with various external entities, such as other vehicles (V2V communication), infrastructure (V2I communication), and broader networks (V2N communication). This communication process often involves the transmission of sensitive data, including vehicle location, speed, navigation details, and even potentially sensitive user information. Therefore, ensuring privacy becomes crucial.

Each method described in this subsection—encryption, secure communication protocols, anonymization, blockchain technology, differential privacy, and homomorphic encryption—serves to protect the privacy of data communicated between autonomous vehicles and third-party entities.

Ultimately, while these techniques are not exclusive to autonomous vehicles and can be applied to various domains where secure data transmission is required, they are highly relevant and necessary in the context of autonomous vehicular communications.

9.6. Future Research Directions

The future of cyber security for emotionally intelligent autonomous vehicles (EIAVs) calls for a multidisciplinary approach that embraces advancements in a broad spectrum of technological domains. One such promising proposition arose from Gupta [136], who suggested the incorporation of blockchain technology to reinforce security measures within EIAVs. The unique attributes of blockchain, notably its decentralization and immutability characteristics, have been widely recognized for their potency in securing digital transactions against unauthorized intrusions and manipulations. The decentralized nature of blockchain can act as a potent defense mechanism, distributing data across multiple nodes and thereby significantly reducing the risk of a centralized attack. This approach can effectively prevent single-point-of-failure attacks, providing an extensive and robust type of defense for EIAVs. Furthermore, the built-in integrity of blockchain technology creates an incorruptible digital database of transactions that can be programmed to record virtually anything of value, including sensitive vehicular data. This feature not only offers an added layer of data security but also promotes transparency and traceability, thus fostering trust in the EIAV ecosystem.

However, the application of blockchain technology in EIAVs is still in its first steps and presents its own set of challenges and research opportunities. The integration of blockchain with EIAV systems requires extensive exploration to ascertain the optimal approaches for its deployment. This includes but is not limited to determining the type of blockchain (public or private), the consensus protocol, the handling of scalability issues, and the management of privacy concerns. In addition, the unique characteristics of EIAVs, such as the real-time requirement and large-scale data generation, pose new demands for blockchain technology, which calls for further innovations and improvements. Therefore, Gupta's proposal illuminates a pivotal research direction that requires extensive technological exploration, rigorous testing, and continuous optimization to fully harness the potential of blockchain technology to bolster EIAV security [136]. The adoption of proactive cyber security measures, a concept ably advanced in [27], is a necessary complement to this effort. Prioritizing real-time threat detection and responsive algorithms holds great promise to prevent cyber security threats and eliminate them before they develop into severe attacks. Future EIAV research endeavors must resolutely address this aspect, nurturing proactive and preventative cyber security measures.

In [183], an enhanced multistage intrusion detection framework was proposed for autonomous vehicles (AVs) and intelligent transportation systems (ITSs). Recognizing that these systems are susceptible to sophisticated hacking techniques, the researchers introduced a bidirectional long short-term memory (LSTM) architecture that efficiently identifies intrusions in real time. Their integration of a normal state-based mechanism along with deep learning techniques suggests an effective method for managing complex

attack scenarios. This direction, as demonstrated effectively through extensive testing, accentuates the potential of deep learning techniques in augmenting cyber security in AVs and ITSs. He et al. [180] proposed a comprehensive machine-learning-based detection framework for connected and autonomous vehicles (CAVs) to prevent cyber attacks. They proposed a UML (unified modelling language)-based cyber security framework founded on the CAV cyber security principles of the United Kingdom. Their distinctive contribution is the development of a novel CAV communication cyber-attack dataset (CAV-KDD), which is tailored to cyber attacks based on communication. Their findings highlight the importance of machine learning, supported by structured cyber security frameworks, in proactively protecting CAVs against potential cyber threats.

Torre et al. [195] emphasized the importance of securing the integral vehicular technologies of emotionally intelligent autonomous vehicles (EIAVs), including sensing, positioning, and vision systems. As these systems serve as the foundation on which EIAVs operate and interact with their environment, they become prime targets for potential cyber attacks. Consequently, the development of system-specific security methodologies that provide a comprehensive defense is a crucial area for future research. This would entail analyzing the unique security requirements of each component, determining its inherent vulnerabilities, and customizing defensive strategies that are not only reactive but also anticipatory of potential cyber-attack patterns. In addition, these security methodologies would need to be adaptable and scalable to incorporate new technologies and standards, given the accelerated rate of technological advancement. Therefore, future research must incorporate the multifaceted task of designing, validating, and deploying comprehensive security methodologies that can protect these vital vehicular technologies from potential cyber attacks.

The findings of Amara et al. [24] underscore the critical need to comprehend potential attack vectors aimed at autonomous vehicle software and hardware. Due to the intricacy and interconnectedness of these systems, they offer cyber attackers numerous access points of entry. A thorough comprehension of these threats requires a detailed mapping of these potential attack vectors, as well as the identification of their patterns and implications. This would then inform the design of mitigation strategies that effectively mitigate these vulnerabilities. In addition, this comprehension must encompass the consequences of effective cyber attacks, ranging from immediate operational disruptions to long-term effects on user confidence and regulatory compliance. Future research should therefore employ a twofold strategy: constructing a detailed threat landscape particular to autonomous vehicle software and hardware and developing holistic countermeasures that can neutralize threats while ensuring optimal performance. This essential research direction would considerably contribute to the fortification of EIAV systems, thereby facilitating their secure incorporation into our social fabric.

The highly sensitive emotional data involved in EIAVs pose a complex challenge that deserves particular attention. Identifying and implementing optimal strategies to protect these data from potential cyber threats will be crucial. This protective layer may encompass encryption techniques, privacy-preserving computation, and anonymization methods designed exclusively for emotional data. Lastly, considering the novel nature of EIAVs, the development of regulatory frameworks that effectively address their unique cyber security needs without impeding their technological advancement is critical. This endeavor will require a cooperative approach involving researchers, industry stakeholders, and policymakers. Moreover, some additional and potential research directions are presented below:

1. **TinyML in autonomous vehicles for cyber security enhancement and predictive defense:** TinyML appears as a crucial tool in the world of autonomous vehicles (AVs), as first presented in [196], that has the potential to radically alter the structure of the security apparatus. Autonomous cars are often outfitted with a variety of sensors and communication modules, both of which are constantly producing new data. Processing these data centrally or in the cloud might be resource-intensive and, more

importantly, offer a broader attack surface to prospective cyber enemies. The application and capabilities of TinyML may be considered in this aspect. TinyML allows for the localized processing of data by applying lightweight machine learning algorithms directly inside the embedded systems of the vehicle [196]. This ultimately results in a reduction in latency and a significant reduction in the possibility of data breaches occurring during transmission. Additionally, TinyML can be designed to continually monitor the sensor data and network activity inside the car for any anomalies [197]. TinyML has the ability to learn to recognize potentially suspicious patterns that may indicate a cyber assault. These patterns may include an effort to modify sensor readings or control messages. TinyML can learn to recognize these patterns via the use of powerful machine learning models. When an anomaly is discovered, it is possible for it to immediately trigger countermeasures. These countermeasures may include disconnecting the compromised component or contacting a central security system. In addition, since TinyML utilizes such a little amount of power, it is able to maintain its operational state even when the vehicle is not in use, which ensures that the user is always protected. Additionally, the predictive capabilities of TinyML models could be applied to anticipate developing attack vectors, allowing for the creation of proactive security measures. This can be accomplished via the utilization of TinyML's predictive analytics. TinyML's incorporation into autonomous vehicles provides, in essence, an effective method for enhancing cyber security, shortening the reaction times to security events, and ensuring the integrity and resilience of vehicular systems in the face of an ever-evolving environment of cyber threats.

2. **Integration of reinforcement learning, Markov decision processes, and intelligent Rainbow DQN agents in AV cyber security:** The combined power of reinforcement learning (RL), Markov decision processes (MDPs), and intelligent Rainbow DQN agents can serve as a formidable arsenal to enhance the cyber security of autonomous vehicles (AVs). Reinforcement learning, another type of machine learning, can be applied to analyze the patterns and potential vulnerabilities in AV systems by continuously learning from the environment and optimizing responses under different circumstances. Within the framework of Markov decision processes, RL algorithms can be implemented. MDPs evaluate the present state of the system, available actions, transition probabilities, and rewards, enabling RL algorithms to make decisions that maximize some concept of cumulative reward. This is particularly beneficial in the context of cyber security, as the system can learn to make judgments that reduce or prevent incidents related to cyber security. At this point, Rainbow DQN agents incorporate a number of developments in deep Q networks (DQNs) and reinforcement learning. These agents are proficient at managing high-dimensional state spaces, which are typical of AV systems with numerous sensors and intricate networking. This knowledge can be efficiently processed by Rainbow DQN agents, enabling them to make rapid choices based on knowledge. Regarding cyber security, these intelligent agents may be deployed to continuously monitor the in-vehicle networks and data flows. They can detect anomalous patterns or intrusions that may be indicative of cyber attacks or system compromises by gaining knowledge from the data. In addition, through reinforcement learning and its decision-making process, these agents have the ability to predict the likely evolution of an attack, enabling preventative steps to be taken before the attack can have a negative impact. As an example, if an attack pattern is identified, the agent can decide to isolate portions of the vehicle's network, restrict communication with the suspected compromised components, or activate other defense mechanisms. This proactive and learning-based approach facilitated by the synergy of RL, MDPs, and Rainbow DQN agents can substantially increase the resilience and security of autonomous vehicles against complicated and evolving cyber threats.

In conclusion, these outlined future research directions underscore the need for a holistic, comprehensive approach to cyber security within AVs. Achieving a secure future

for emotionally intelligent autonomous vehicles necessitates a concerted effort across multiple disciplines, including cyber security, emotional recognition, AI, and autonomous vehicle development.

9.7. Blockchain Technologies in Autonomous Vehicles: Potential Future Solutions

The potential integration of blockchain technology with autonomous cars is a game-changing step forward for the field of automotive engineering. Blockchain technology, which is a distributed ledger system that has gained recognition for its robust security methods and decentralized design, can revolutionize many aspects of how autonomous cars function. The built-in characteristics of blockchain can be used to improve data security and integrity in a wide variety of ways. Additionally, the cryptographic foundations and consensus algorithms of blockchain may strengthen vehicular communication networks, guaranteeing tamper-resistant data transmission and protecting against harmful intrusions. Integrating blockchain in an era when data are a precious commodity safeguards data integrity and authenticity, establishing trust and dependability in autonomous vehicular ecosystems.

The incomparable capacity of blockchain technology to maintain a digital record of a vehicle's history is a noteworthy application that necessitates special consideration. For instance, blockchain can be utilized to securely record a vehicle's damage history if it is deployed with efficacy. This generates a digital document that exhaustively stores every instance of damage, along with the corresponding restorations and associated information. Utilizing this information in the persistent registry of a blockchain paves the way for a significant reduction in fraud and generates an unprecedented level of transparency and assurance for a diverse group of stakeholders, including vehicle owners, insurance companies, and prospective buyers of used cars. Moreover, it is conceivable that blockchain technology could be utilized effectively to serve as a foundation of truthfulness in the documentation of vehicle mileage. With blockchain's inherently secure structure, an immutable record of a vehicle's mileage can be maintained, effectively identifying odometer modifications. This innovation serves as a sentinel, ensuring an accurate depiction of a vehicle's utilization, thereby imparting a greater degree of transparency and nurturing confidence in transactions related to the vehicle.

When it comes to autonomous vehicles (AVs), blockchain technology opens up an even wider range of possibilities. By integrating blockchain, automobile manufacturers can create a complete and impenetrable library of each vehicle's service history. This record, which is stored on the blockchain, is immune to malicious revisions by unauthorized third parties and can only be updated by organizations with the necessary authority, such as car manufacturers or licensed service providers. This secure service history not only increases the intrinsic worth of the car but also advocates for the vehicle owner's cause by protecting their rights and establishing a culture of precise maintenance standards.

Furthermore, blockchain technology appears as a cutting-edge alternative for greatly streamlining and optimizing the settlement procedure for disputes arising from automobile accidents. In the unfortunate event of an accident involving autonomous cars, blockchain acts as a channel for a fast, impermeable, and transparent data exchange amongst the parties involved. This quick and secure exchange of essential data may speed up insurance claim adjudication procedures, bring disagreements to a solution, and protect car owners' privacy and security. Furthermore, these data may be used to provide insights into accident causation, assisting in the development of improved safety features and practices. In addition, the use of blockchain technology in emotionally intelligent autonomous vehicles (EIAVs) appears as an especially promising area. Blockchain's strict security features and confidentiality promises may be critical in securing the delicate emotional data that EIAVs capture. The preservation of these data is crucial not just for the users' privacy but also for the dependable operation of EIAVs, since they rely on emotional data for successful decision making. By using the blockchain's decentralized and irreversible qualities, the integrity and confidentiality of emotional data can be maintained, supporting progress in the field

of EIAVs while adhering to ethical norms and respecting individual privacy. A variety of advantages incorporating blockchain technology in autonomous cars are illustrated in Figure 6.

Ultimately, the adoption of blockchain technology has the potential to transform the security environment for autonomous cars by building a tiered security architecture that maintains data integrity, promotes transparency, and strengthens privacy guidelines. The use of blockchain is especially important in the case of emotionally intelligent autonomous vehicles, given the delicate nature of the emotional data being handled. Therefore, the need for strong data security measures becomes even more essential. Blockchain technologies provide an intuitive and effective solution to these needs, making its adoption not just a choice but a necessity for the responsible and ethical growth of EIAVs. This leads to a collaborative effort from stakeholders across the spectrum, including academics, technologists, and politicians, to foster an environment favorable to the smooth integration of blockchain technology in the rapidly evolving area of autonomous cars.

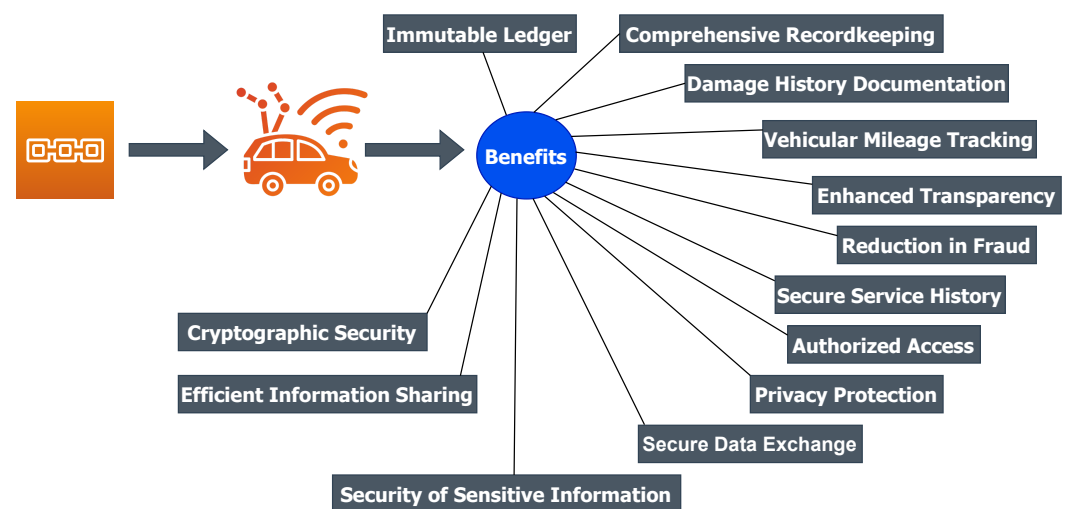


Figure 6. Benefits and potential future solutions of AVs.

10. Conclusions

This article explores the ecosystem of autonomous vehicle technology, a field that is swiftly advancing and reshaping the transportation landscape due to recent innovations. Despite the immense potential of these innovations, their widespread adoption faces major difficulties. The dual concerns of cyber security and safety stand out as pivotal elements that necessitate a thorough investigation and proactive countermeasures. Our investigation demonstrates both the fundamental principles underpinning AV technology and the complicated information security dynamics behind their secure operation. We provided a comprehensive overview of potential cyber security attacks, with a particular emphasis on the emerging and unmitigated threat posed by machine learning (ML) attacks on deep neural networks (DNNs).

The major threat presented under various cyber threats is a growing field of autonomous vehicle (AV) research that has attracted considerable academic interest and scholarly research. The lack of effective countermeasures to machine learning (ML) attacks on deep neural networks (DNNs) is a critical deficiency in our defensive mechanisms against the ever-evolving cyber security threats aimed at AVs. Unquestionably, the resilience and impregnability of AVs against such intrusions will be crucial in determining their future growth and gaining wider societal approval. Identifying, categorizing, and comprehending these prospective assaults is an additional crucial aspect of our work. We have classified these threats based on the principles of data availability, authenticity, integrity, and confidentiality, providing a comprehensive analysis of the threats currently confronting the AV industry. In addition to demonstrating the current status of the threat

landscape, this classification uncovers the gaps in existing defense strategies, thereby spotlighting crucial research and mitigation areas. For each type of attack, we determined its status in terms of mitigation: fully mitigated for threats that have been completely neutralized by existing countermeasures, partially mitigated for threats that remain viable under certain circumstances, and uncovered for threats that require additional research or for which existing solutions have proven insufficient. The aforementioned findings demonstrate the urgent need for enhanced security measures in the AV technology industry. Given the potentially catastrophic effects of security flaws in these systems, ensuring their safety is not merely a recommendation but an absolute necessity.

Therefore, future research must concentrate on the development and implementation of resilient encryption protocols, the remediation of fundamental vulnerabilities, and the design of inventive countermeasures that can adapt to an ever-changing threat landscape. As we stand on the edge of a new era in which autonomous vehicles could transform our transportation systems, it is crucial that we maintain a proactive stance regarding the cyber security risks and safety challenges that accompany this technological revolution. By establishing a robust and secure operational environment for unmanned autonomous vehicles, we can not only ensure their operational effectiveness but also inspire public confidence in their deployment. Nonetheless, it is crucial to remember that this attempt is a process, not a destination. As the threat environment evolves, our defensive strategies must also evolve. By maintaining alertness, conducting sustained research, and collaborating across disciplines, we can effectively navigate this complex environment and safeguard the promising future of autonomous vehicles from the cyber security threats they face.

Author Contributions: A.G., A.K., L.T., C.K., P.K., N.S., G.K., and D.T., conceived of the idea, designed and constructed the review article, analyzed the applications of autonomous vehicles, drafted the initial manuscript, and revised the final manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

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

Abbreviations

The following abbreviations are used in this manuscript:

AV	Autonomous vehicle
EIAV	Emotionally intelligent autonomous vehicle
LiDAR	Light imaging detection and ranging
GPS	Global positioning system
FAV	Fully autonomous vehicle
ECU	Engine control unit
CAN	Controller area network
CIA	Confidentiality, integrity, and availability
NHTSA	National Highway Traffic Safety Administration
DOA	Direction of arrival
IMU	Inertial measurement unit
V2V	Vehicle to vehicle
V2I	Vehicle to infrastructure
VANET	Vehicular ad hoc network
ABAKA	Anonymous batch authentication and key agreement
CMAF	Cooperative message authentication protocol
DoS	Denial of service
DDoS	Distributed denial of service
SPECS	Secure and privacy-enhancing communications scheme
IBV	Identity-based batch verification
RSU	Roadside unit
TA	Trusted authority
P2V	Pedestrian to vehicle

V2P	Vehicle to pedestrian
OBD	Onboard diagnostic
OEM	Original equipment manufacturer
DNN	Deep neural network
CNN	Convolutional neural network
FGSM	Fast gradient sign method
JSMA	Jacobian saliency-based adversarial attack
AEV	Autonomous electric vehicle
AUV	Autonomous underwater vehicle
AGV	Autonomous guided vehicle
AAeV	Autonomous aerial electric vehicle
OTA	Over the air
AVSN	Blockchain-enabled autonomous vehicular social network
CAV	Connected autonomous vehicle
UAV	Unmanned aerial vehicle
BCC	Blockchain-based collaborative crowd sensing
AVN	Autonomous vehicular network
UIoT	Underwater Internet of Things
CACC	Cooperative adaptive cruise control

References

- Guizzo, E. How Google's Self-Driving Car Works. IEEE Spectrum Online. Available online: <https://spectrum.ieee.org/how-google-self-driving-car-works> (accessed on 23 July 2023).
- Stiller, C.; Ziegler, J. 3D perception and planning for self-driving and cooperative automobiles. In Proceedings of the International Multi-Conference on Systems, Signals & Devices, Chemnitz, Germany, 20–23 March 2012; pp. 1–7.
- Levinson, J.; Askeland, J.; Becker, J.; Dolson, J.; Held, D.; Kammel, S.; Kolter, J.Z.; Langer, D.; Pink, O.; Pratt, V.; et al. Towards fully autonomous driving: Systems and algorithms. In Proceedings of the 2011 IEEE Intelligent Vehicles Symposium (IV), Baden-Baden, Germany, 5–9 June 2011; pp. 163–168. [\[CrossRef\]](#)
- Petit, J.; Shladover, S.E. Potential Cyberattacks on Automated Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2015**, *16*, 546–556. [\[CrossRef\]](#)
- Jawhar, I.; Mohamed, N.; Wsmani, H. An Overview of Inter-Vehicular Communication Systems, Protocols and Middleware. *J. Netw.* **2013**, *8*, 12. [\[CrossRef\]](#)
- Petit, J.; Feiri, M.; Kargl, F. Revisiting attacker model for smart vehicles. In Proceedings of the IEEE 6th International Symposium on Wireless Vehicular Communications (WiVeC 2014), Vancouver, BC, Canada, 14–15 September 2014; pp. 1–5.
- 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 2014, Monterey, CA, USA, 5–8 May 2014; pp. 262–269.
- Uma, M.; Ganapathi, P. A survey on various cyber attacks and their classification. *Int. J. Netw. Secur.* **2013**, *15*, 390–396.
- 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. [\[CrossRef\]](#) [\[PubMed\]](#)
- 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. [\[CrossRef\]](#)
- Rasouli, A.; Tsotsos, J.K. Autonomous vehicles that interact with pedestrians: A survey of theory and practice. *IEEE Trans. Intell. Transp. Syst.* **2019**, *21*, 900–918. [\[CrossRef\]](#)
- 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. [\[CrossRef\]](#)
- Schwarting, W.; Alonso-Mora, J.; Rus, D. Planning and decision-making for autonomous vehicles. *Annu. Rev. Control. Robot. Auton. Syst.* **2018**, *1*, 187–210. [\[CrossRef\]](#)
- 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. [\[CrossRef\]](#)
- Vargas, J.; Alsweiss, S.; Toker, O.; Razdan, R.; Santos, J. An Overview of Autonomous Vehicles Sensors and Their Vulnerability to Weather Conditions. *Sensors* **2021**, *21*, 5397. [\[CrossRef\]](#)
- Tian, Y.; Pei, K.; Jana, S.; Ray, B. DeepTest: Automated Testing of Deep-Neural-Network-Driven Autonomous Cars. In Proceedings of the 40th International Conference on Software Engineering, ICSE '18, Gothenburg, Sweden, 27 May–3 June 2018; pp. 303–314. [\[CrossRef\]](#)
- Jing, P.; Xu, G.; Chen, Y.; Shi, Y.; Zhan, F. The Determinants behind the Acceptance of Autonomous Vehicles: A Systematic Review. *Sustainability* **2020**, *12*, 1719. [\[CrossRef\]](#)
- NHTSA. Automated Vehicles for Safety. Available online: www.nhtsa.gov/technology-innovation/automated-vehicles-safety (accessed on 23 July 2023).
- Salovey, P.; Mayer, J.D. Emotional intelligence. *Imagin. Cogn. Personal.* **1990**, *9*, 185–211. [\[CrossRef\]](#)

20. Ribeiro, M.A.; Gursay, D.; Chi, O.H. Customer acceptance of autonomous vehicles in travel and tourism. *J. Travel Res.* **2022**, *61*, 620–636. [\[CrossRef\]](#)
21. Li, J.; Holländer, K.; Butz, A. Introducing automated driving to the generation 50+. In Proceedings of the 11th International Conference on Automotive User Interfaces and Interactive Vehicular Applications: Adjunct Proceedings, Utrecht, The Netherlands, 21–25 September 2019; pp. 375–380.
22. Hengstler, M.; Enkel, E.; Duelli, S. Applied artificial intelligence and trust—The case of autonomous vehicles and medical assistance devices. *Technol. Forecast. Soc. Chang.* **2016**, *105*, 105–120. [\[CrossRef\]](#)
23. Sun, X.; Li, J.; Tang, P.; Zhou, S.; Peng, X.; Li, H.N.; Wang, Q. Exploring personalised autonomous vehicles to influence user trust. *Cogn. Comput.* **2020**, *12*, 1170–1186. [\[CrossRef\]](#)
24. Amara, D.K.; Chebrolu, N.R.; R, V.; Kp, S. A Brief Survey on Autonomous Vehicle Possible Attacks, Exploits and Vulnerabilities. *arXiv* **2018**, arXiv:1810.04144.
25. Hu, H.; Wei, N. A study of GPS jamming and anti-jamming. In Proceedings of the 2009 2nd International Conference on Power Electronics and Intelligent Transportation System (PEITS), Shenzhen, China, 19–20 December 2009; pp. 388–391.
26. Ahmad, M.; Akhtar, M.U. Impact and Detection of GPS Spoofing and Countermeasures against Spoofing. In Proceedings of the 2nd International Conference on Computing, Mathematics and Engineering Technologies–iCoMET, Sukkur, Pakistan, 30–31 January 2019.
27. Parkinson, S.; Ward, P.; Wilson, K.; Miller, J. Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 2898–2915. [\[CrossRef\]](#)
28. O'Hanlon, B.W.; Psiaki, M.; Bhatti, J.A.; Shepard, D.P.; Humphreys, T.E. Real-Time GPS Spoofing Detection via Correlation of Encrypted Signals. *Navig.-J. Inst. Navig.* **2013**, *60*, 267–278. [\[CrossRef\]](#)
29. Yang, Q.; Zhang, Y.; Tang, C.; Lian, J. A Combined Antijamming and Antispoofing Algorithm for GPS Arrays. *Int. J. Antennas Propag.* **2019**, *2019*, 8012569. [\[CrossRef\]](#)
30. Nayegandhi, A. Lidar Technology Overview. In Proceedings of the US Geological Survey, St. Petersburg, FL, USA, 12 April 2019; pp. 1–9.
31. Petit, J.; Stottelaar, B.; Feirii, M. Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR. *Black Hat Eur.* **2015**, *11*, 995.
32. 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.
33. Changalvala, R.; Malik, H. LiDAR Data Integrity Verification for Autonomous Vehicle. *IEEE Access* **2019**, *18*, 7. [\[CrossRef\]](#)
34. Bahirat, K.; Prabhakaran, B. A study on lidar data forensics. In Proceedings of the 2017 IEEE International Conference on Multimedia and Expo (ICME), Hong Kong, China, 10–14 July 2017; pp. 679–684.
35. Hallyburton, R.S.; Pajic, M. Securing Autonomous Vehicles Under Partial-Information Cyber Attacks on LiDAR Data. *arXiv* **2023**, arXiv:2303.03470.
36. Bhupathiraju, S.H.V.; Sheldon, J.; Bauer, L.A.; Bindschaedler, V.; Sugawara, T.; Rampazzi, S. EMI-LiDAR: Uncovering Vulnerabilities of LiDAR Sensors in Autonomous Driving Setting Using Electromagnetic Interference. In Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Guildford, UK, 29 May–1 June 2023; pp. 329–340. [\[CrossRef\]](#)
37. Cao, Y.; Xiao, C.; Yang, D.; Fang, J.; Yang, R.; Liu, M.; Li, B. Adversarial objects against lidar-based autonomous driving systems. *arXiv* **2019**, arXiv:1907.05418.
38. Haddrell, M.; Martin, K.M. Towards an Autonomous Vehicle Enabled Society: Cyber Attacks and Countermeasures. 2016. Available online: <http://book.itep.ru/depositary/pilotless/RH-2016-autonomous-cars-Michael-Haddrell.pdf> (accessed on 23 July 2023).
39. Amoozadeh, M.; Raghuramu, A.; nee Chuah, C.; Ghosal, D.; Zhang, H.M.; Rowe, J.; Levitt, K. Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. *IEEE Commun. Mag.* **2015**, *53*, 126–132. [\[CrossRef\]](#)
40. Cheng, H.Y.; Jeng, B.S.; Tseng, P.T.; Fan, K.C. Lane Detection with Moving Vehicles in the Traffic Scenes. *IEEE Trans. Intell. Transp. Syst.* **2006**, *7*, 571–582. [\[CrossRef\]](#)
41. Bahlmann, C.; Zhu, Y.; Ramesh, V.; Pellkofer, M.; Koehler, T. A system for traffic sign detection, tracking, and recognition using color, shape, and motion information. In Proceedings of the IEEE Proceedings, Intelligent Vehicles Symposium, Las Vegas, NV, USA, 6–8 June 2005; pp. 255–260.
42. Eum, S.; Jung, H.G. Enhancing Light Blob Detection for Intelligent Headlight Control Using Lane Detection. *IEEE Trans. Intell. Transp. Syst.* **2013**, *14*, 255–260. [\[CrossRef\]](#)
43. Gomes, L. Hidden Obstacles for Google's Self-Driving Cars. Available online: www.technologyreview.com/s/530276/hidden-obstacles-for-googles-self-driving-cars/ (accessed on 23 July 2023).
44. 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 I2010 IEEE Symposium on Security and Privacy, Berkeley/Oakland, CA, USA, 16–19 May 2010; pp. 447–462.
45. Joo, J.; Park, M.C.; Han, D.S.; Pejovic, V. Deep learning-based channel prediction in realistic vehicular communications. *IEEE Access* **2019**, *7*, 27846–27858. [\[CrossRef\]](#)

46. Mehdizadeh, A.; Cai, M.; Hu, Q.; Alamdar Yazdi, M.A.; Mohabbati-Kalejahi, N.; Vinel, A.; Rigdon, S.E.; Davis, K.C.; Megahed, F.M. A Review of Data Analytic Applications in Road Traffic Safety. Part 1: Descriptive and Predictive Modeling. *Sensors* **2020**, *20*, 1107. [CrossRef]
47. Zahedi, F.; Farzaneh, N. An evolutionary game theory-based security model in vehicular ad hoc networks. *Int. J. Commun. Syst.* **2020**, *33*, e4290. [CrossRef]
48. Tesei, A.; Luise, M.; Pagano, P.; Ferreira, J. Secure Multi-access Edge Computing Assisted Maneuver Control for Autonomous Vehicles. In Proceedings of the 2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring), Helsinki, Finland, 25–28 April 2021; pp. 1–6. [CrossRef]
49. Shrivastava, D.; Pandey, A. A Study of Sybil and Temporal Attacks in Vehicular Ad-Hoc Networks: Types, Challenges, and Impacts. *Int. J. Comput. Appl. Technol. Res.* **2014**, *3*, 284–291. [CrossRef]
50. Huang, J.L.; Yeh, L.Y.; Chien, H.Y. ABAKA: An Anonymous Batch Authenticated and Key Agreement Scheme for Value-Added Services in Vehicular Ad Hoc Networks. *IEEE Trans. Veh. Technol.* **2011**, *60*, 248–262. [CrossRef]
51. Chen, C.; Wang, X.; Han, W.; Zang, B. A Robust Detection of the Sybil Attack in Urban VANETs. In Proceedings of the 2009 29th IEEE International Conference on Distributed Computing Systems Workshops, Montreal, QC, Canada, 22–26 June 2009; pp. 270–276.
52. Hao, Y.; Tang, J.; Cheng, Y. Cooperative Sybil Attack Detection for Position Based Applications in Privacy Preserved VANETs. In Proceedings of the 2011 IEEE Global Telecommunications Conference-GLOBECOM 2011, Houston, TX, USA, 5–9 December 2011; pp. 1–5.
53. Hao, Y.; Cheng, Y.; Zhou, C.; Song, W. A Distributed Key Management Framework with Cooperative Message Authentication in VANETs. *IEEE J. Sel. Areas Commun.* **2011**, *29*, 616–629. [CrossRef]
54. Zhou, T.; Choudhury, R.R.; Ning, P.; Chakrabarty, K. P2DAP—Sybil Attacks Detection in Vehicular Ad Hoc Networks. *IEEE J. Sel. Areas Commun.* **2011**, *29*, 582–594. [CrossRef]
55. Triki, B.; Rekhis, S.; Chammem, M.; Boudriga, N. A privacy preserving solution for the protection against sybil attacks in vehicular ad hoc networks. In Proceedings of the 6th Joint IFIP Wireless and Mobile Networking Conference (WMNC), Dubai, United Arab Emirates, 23–25 April 2013; pp. 1–8.
56. Grover, J.; Laxmi, V.; Gaur, M.S. Sybil attack detection in VANET using neighbouring vehicles. *Int. J. Secur. Netw.* **2014**, *9*, 222–233. [CrossRef]
57. Pathre, A.; Agrawal, C.; Jain, A. Identification of malicious vehicle in vanet environment from ddos attack. *J. Glob. Res. Comput. Sci.* **2013**, *4*, 1–5.
58. Pathre, A.; Agrawal, C.; Jain, A. A novel defense scheme against DDOS attack in VANET. In Proceedings of the 2013 Tenth International Conference on Wireless and Optical Communications Networks (WOCN), Bhopal, India, 26–28 July 2013; pp. 1–5.
59. Malla, A.M.; Sahu, R.K. Security Attacks with an Effective Solution for DOS Attacks in VANET. *Int. J. Comput. Appl.* **2013**, *66*, 975–8887.
60. He, L.; Zhu, W.T. Mitigating DoS attacks against signature-based authentication in VANETs. In Proceedings of the 2012 IEEE International Conference on Computer Science and Automation Engineering (CSAE), Zhangjiajie, China, 25–27 May 2012; pp. 261–265.
61. Verma, K.; Hasbullah, H.; Kumar, A. Prevention of DoS attacks in VANET. *Wirel. Pers. Commun.* **2013**, *73*, 95–126. [CrossRef]
62. Safi, S.M.; Movaghar, A.; Mohammadzadeh, M. A novel approach for avoiding wormhole attacks in VANET. In Proceedings of the 2009 First Asian Himalayas International Conference on Internet, Kathmandu, Nepal, 28–30 October 2009; pp. 1–6.
63. Zhang, C.; Lu, R.; Lin, X.; Ho, P.; Shen, X. An Efficient Identity-Based Batch Verification Scheme for Vehicular Sensor Networks. In Proceedings of the IEEE INFOCOM 2008-The 27th Conference on Computer Communications, Phoenix, AZ, USA; 2008; pp. 246–250.
64. Chim, T.W.; Yiu, S.; Hui, L.C.K.; Li, V.O.K. SPECS: Secure and privacy enhancing communications schemes for VANETs. *Ad Hoc Netw.* **2011**, *9*, 189–203. [CrossRef]
65. Kim, T.; Studer, A.; Dubey, R. VANET alert endorsement using multi-source filters. In Proceedings of the Seventh International Workshop on Vehicular Ad Hoc Networks, VANET 2010, Chicago, IL, USA, 24 September 2010.
66. Lin, X.; Sun, X.; Ho, P.H.; Shen, X. GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications. *IEEE Trans. Veh. Technol.* **2007**, *56*, 3442–3456.
67. Papadimitratos, P.; Buttyan, L.; Hubaux, J.P.; Kargl, F.; Kung, A.; Raya, M. Architecture for Secure and Private Vehicular Communications. In Proceedings of the 2007 7th International Conference on ITS Telecommunications, Sophia Antipolis, France, 6–8 June 2007; pp. 1–6.
68. Hussein, A.; García, F.; Armingol, J.M.; Olaverri-Monreal, C. P2V and V2P communication for Pedestrian warning on the basis of Autonomous Vehicles. In Proceedings of the 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), Rio de Janeiro, Brazil, 1–4 November 2016; pp. 2034–2039.
69. Can Driverless Vehicles Be Hacked? Available online: <https://www.hlmlawfirm.com/blog/can-driverless-vehicles-be-hacked/> (accessed on 19 July 2023).
70. HackerNoon. Available online: <https://hackernoon.com/how-to-hack-self-driving-cars-vulnerabilities-in-autonomous-vehicles-jh3r37cz> (accessed on 19 July 2023).

71. Algarni, A.; Thayanathan, V. Autonomous Vehicles: The Cybersecurity Vulnerabilities and Countermeasures for Big Data Communication. *Symmetry* **2022**, *14*, 2494. [\[CrossRef\]](#)
72. Kumar, K.N.; Vishnu, C.; Mitra, R.; Mohan, C.K. Black-box adversarial attacks in autonomous vehicle technology. In Proceedings of the 2020 IEEE Applied Imagery Pattern Recognition Workshop (AIPR), Washington, DC, USA, 13–15 October 2020; pp. 1–7.
73. Santa, J.; Bernal-Escobedo, L.; Sanchez-Iborra, R. On-board unit to connect personal mobility vehicles to the IoT. *Procedia Comput. Sci.* **2020**, *175*, 173–180. [\[CrossRef\]](#)
74. Chang, X.; Li, H.; Rong, J.; Huang, Z.; Chen, X.; Zhang, Y. Effects of on-board unit on driving behavior in connected vehicle traffic flow. *J. Adv. Transp.* **2019**, *2019*, 1–12. [\[CrossRef\]](#)
75. Zhang, B.; Wang, X.; Xie, R.; Li, C.; Zhang, H.; Jiang, F. A reputation mechanism based Deep Reinforcement Learning and blockchain to suppress selfish node attack motivation in Vehicular Ad-Hoc Network. *Future Gener. Comput. Syst.* **2023**, *139*, 17–28. [\[CrossRef\]](#)
76. Karmakar, G.; Chowdhury, A.; Das, R.; Kamruzzaman, J.; Islam, S. Assessing trust level of a driverless car using deep learning. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 4457–4466. [\[CrossRef\]](#)
77. Zhang, Y.; Ge, B.; Li, X.; Shi, B.; Li, B. Controlling a Car Through OBD Injection. In Proceedings of the 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud), Beijing, China, 25–27 June 2016; pp. 26–29.
78. Yan, W. A two-year survey on security challenges in automotive threat landscape. In Proceedings of the 2015 International Conference on Connected Vehicles and Expo (ICCVE), Shenzhen, China, 19–23 October 2015; pp. 185–189.
79. Yadav, A.; Bose, G.; Bhang, R.; Kapoor, K. Security, Vulnerability and Protection of Vehicular On-board Diagnostics. *Int. J. Secur. Its Appl.* **2016**, *10*, 405–422. [\[CrossRef\]](#)
80. Oka, D.K.; Larson, U.E. Conducting Forensic Investigations of Cyber Attacks on Automobile In-Vehicle Networks. *Int. J. Digit. Crime Forensics* **2009**, *2*, 28–41.
81. Vallance, C. Car Hack Uses Digital-Radio Broadcasts to Seize Control. 22 July 2015. Available online: www.bbc.com/news/technology-33622298 (accessed on 23 July 2023).
82. Checkoway, S.; McCoy, D.; Kantor, B.; Anderson, D.; Shacham, H.; Savage, S.; Koscher, K.; Czeskis, A.; Roesner, F.; Kohno, T. Comprehensive experimental analyses of automotive attack surfaces. In Proceedings of the 20th USENIX Conference on Security, San Francisco, CA, USA, 8–12 August 2011.
83. Luo, F.; Hou, S. *Security Mechanisms Design of Automotive Gateway Firewall*; Technical Report; SAE Technical Paper; SAE: Warrendale, PA, USA, 2019.
84. Zhang, H.; Meng, X.; Zhang, X.; Liu, Z. CANsec: A Practical in-Vehicle Controller Area Network Security Evaluation Tool. *Sensors* **2020**, *20*, 4900. [\[CrossRef\]](#) [\[PubMed\]](#)
85. Duan, X.; Yan, H.; Tian, D.; Zhou, J.; Su, J.; Hao, W. In-Vehicle CAN Bus Tampering Attacks Detection for Connected and Autonomous Vehicles Using an Improved Isolation Forest Method. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 2122–2134. [\[CrossRef\]](#)
86. Hoque, M.A.; Hossain, M.; Hasan, R. BenchAV: A Security Benchmarking Framework for Autonomous Driving. In Proceedings of the 2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 8–11 January 2022; pp. 729–730. [\[CrossRef\]](#)
87. Brocklehurst, C.; Radenkovic, M. Resistance to Cybersecurity Attacks in a Novel Network for Autonomous Vehicles. *J. Sens. Actuator Netw.* **2022**, *11*, 35. [\[CrossRef\]](#)
88. Qurashi, J.M.; Ikram, M.J.; Jambi, K.; Eassa, F.E.; Khemakhem, M. Autonomous Vehicles: Security Challenges and Game theory-based Countermeasures. In Proceedings of the 2023 1st International Conference on Advanced Innovations in Smart Cities (ICAISC), Jeddah, Saudi Arabia, 23–25 January 2023; pp. 1–6. [\[CrossRef\]](#)
89. Yadav, N.; Ansar, S.A.; Chaurasia, P.K. Review of Attacks on Connected and Autonomous Vehicles (CAV) and their Existing Solutions. In Proceedings of the 2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 13–14 October 2022; pp. 1–6. [\[CrossRef\]](#)
90. Goyal, S.B. Autonomous Vehicles: Improving Cyber Security. *Int. J. Adv. Res. Technol. Innov.* **2022**, *4*, 118–126.
91. Kamal, M.; Kyrkou, C.; Piperigkos, N.; Papandreou, A.; Kloukinotis, A.; Casademont, J.; Mateu, N.P.; Castillo, D.B.; Rodriguez, R.D.; Durante, N.G.; et al. A Comprehensive Solution for Securing Connected and Autonomous Vehicles. In Proceedings of the 2022 Design, Automation & Test in Europe Conference & Exhibition (DATE), Antwerp, Belgium, 14–23 March 2022; pp. 790–795. [\[CrossRef\]](#)
92. Kennedy, C. New Threats to Vehicle Safety: How Cybersecurity Policy Will Shape the Future of Autonomous Vehicles. *Mich. Telecommun. Technol. Law Rev.* **2017**, *23*, 343–356.
93. Wang, Z.; Wei, H.; Wang, J.; Zeng, X.; Chang, Y. Security Issues and Solutions for Connected and Autonomous Vehicles in a Sustainable City: A Survey. *Sustainability* **2022**, *14*, 12409. [\[CrossRef\]](#)
94. Shangguan, L.; Chour, K.; Ko, W.H.; Kim, J.; Kamath, G.K.; Satchidanandan, B.; Gopalswamy, S.; Kumar, P.R. Dynamic Watermarking for Cybersecurity of Autonomous Vehicles. *IEEE Trans. Ind. Electron.* **2023**, *70*, 11735–11743. [\[CrossRef\]](#)
95. Szegedy, C.; Zaremba, W.; Sutskever, I.; Bruna, J.; Erhan, D.; Goodfellow, I.; Fergus, R. Intriguing properties of neural networks. *arXiv* **2014**, arXiv:1312.6199
96. Goodfellow, I.; Shlens, J.; Szegedy, C. Explaining and Harnessing Adversarial Examples. *arXiv* **2014**, arXiv:1412.6572.
97. Kurakin, A.; Goodfellow, I.J.; Bengio, S. Adversarial examples in the physical world. In *Artificial Intelligence Safety and Security*; Chapman and Hall/CRC: London, UK, 2018; pp. 99–112.

98. Engstrom, L.; Tsipras, D.; Schmidt, L.; Madry, A. A Rotation and a Translation Suffice: Fooling CNNs with Simple Transformations. In Proceedings of the ICLR 2019 Conference Blind Submission, New Orleans, LA, USA, 6–9 May 2019.
99. Pei, K.; Cao, Y.; Yang, J.; Jana, S. Towards Practical Verification of Machine Learning: The Case of Computer Vision Systems. *arXiv* **2017**, arXiv:1712.01785.
100. Liu, Y.; Ma, S.; Aafer, Y.; Lee, W.C. Trojaning Attack on Neural Networks. In Proceedings of the Network and Distributed System Security Symposium, Diego, CA, USA, 18–21 February 2018.
101. Papernot, N.; McDaniel, P.; Jha, S.; Fredrikson, M. The Limitations of Deep Learning in Adversarial Settings. In Proceedings of the 1st IEEE European Symposium on Security & Privacy, Saarbrücken, Germany, 21–24 March 2016.
102. Papernot, N.; McDaniel, P.; Goodfellow, I.; Jha, S.; Celik, Z.B.; Swami, A. Practical Black-Box Attacks against Machine Learning. In Proceedings of the 2017 ACM Asia Conference on Computer and Communications Security, Abu Dhabi, United Arab Emirates, 2–6 April 2017.
103. Carlini, N.; Wagner, D. Towards Evaluating the Robustness of Neural Networks. In Proceedings of the 2017 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2017; pp. 39–57.
104. Carlini, N.; Wagner, D. Adversarial Examples Are Not Easily Detected: Bypassing Ten Detection Methods. In Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security, Dallas, TX, USA, 3 November 2017; pp. 3–14.
105. Brown, T.B.; Mané, D.; Roy, A.; Abadi, M.; Gilmer, J. Adversarial patch. *arXiv* **2017**, arXiv:1712.09665.
106. Su, J.; Vargas, D.V.; Kouichir, S. One pixel attack for fooling deep neural networks. *IEEE Trans. Evol. Comput.* **2017**, *23*, 828–841. [[CrossRef](#)]
107. Fényes, D.; Németh, B.; Gáspár, P. Design of LPV control for autonomous vehicles using the contributions of big data analysis. *Int. J. Control* **2022**, *95*, 1802–1813. [[CrossRef](#)]
108. Familsamavati, S.; Yari, P.; Salehian, S.; Salehian, R.; Abbasi, M.; Khosravi, M.R. The Role of Big Data and Smart Technologies in Autonomous Vehicles. In Proceedings of the 5th International Conference on Future Networks & Distributed Systems, ICFNDS 2021, New York, NY, USA, 15–16 December 2021; pp. 641–646. [[CrossRef](#)]
109. Yoo, A.; Shin, S.; Lee, J.; Moon, C. Implementation of a Sensor Big Data Processing System for Autonomous Vehicles in the C-ITS Environment. *Appl. Sci.* **2020**, *10*, 7858. [[CrossRef](#)]
110. Karras, A.; Karras, C.; Schizas, N.; Avlonitis, M.; Sioutas, S. AutoML with Bayesian Optimizations for Big Data Management. *Information* **2023**, *14*, 223. [[CrossRef](#)]
111. Karras, C.; Karras, A.; Giotopoulos, K.C.; Avlonitis, M.; Sioutas, S. Consensus Big Data Clustering for Bayesian Mixture Models. *Algorithms* **2023**, *16*, 245. [[CrossRef](#)]
112. Karras, C.; Karras, A.; Tsoilis, D.; Giotopoulos, K.C.; Sioutas, S. Distributed Gibbs Sampling and LDA Modelling for Large Scale Big Data Management on PySpark. In Proceedings of the 2022 7th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), Ioannina, Greece, 23–25 September 2022; pp. 1–8. [[CrossRef](#)]
113. Samoladas, D.; Karras, C.; Karras, A.; Theodorakopoulos, L.; Sioutas, S. Tree Data Structures and Efficient Indexing Techniques for Big Data Management: A Comprehensive Study. In Proceedings of the 26th Pan-Hellenic Conference on Informatics, PCI '22, Athens, Greece, 25–27 November 2022; pp. 123–132. [[CrossRef](#)]
114. Nguyen, H.; Nguyen, T.; Leppänen, T.; Partala, J.; Pirttikangas, S. Situation awareness for autonomous vehicles using blockchain-based service cooperation. In *Proceedings of the International Conference on Advanced Information Systems Engineering*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 501–516.
115. Kianersi, D.; Uppalapati, S.; Bansal, A.; Straub, J. Evaluation of a Reputation Management Technique for Autonomous Vehicles. *Future Internet* **2022**, *14*, 31. [[CrossRef](#)]
116. Baza, M.; Nabil, M.; Lasla, N.; Fidan, K.; Mahmoud, M.; Abdallah, M. Blockchain-based firmware update scheme tailored for autonomous vehicles. In Proceedings of the 2019 IEEE Wireless Communications and Networking Conference (WCNC), Marrakesh, Morocco, 15–18 April 2019; pp. 1–7.
117. Oham, C.; Kanhere, S.S.; Jurdak, R.; Jha, S. A blockchain based liability attribution framework for autonomous vehicles. *arXiv* **2018**, arXiv:1802.05050.
118. Shivers, R.M. Toward a Secure and Decentralized Blockchain-Based Ride-Hailing Platform for Autonomous Vehicles. PhD Thesis, Tennessee Technological University, Cookeville, TN, USA, 2019.
119. Mollah, M.B.; Zhao, J.; Niyato, D.; Guan, Y.L.; Yuen, C.; Sun, S.; Lam, K.Y.; Koh, L.H. Blockchain for the internet of vehicles towards intelligent transportation systems: A survey. *IEEE Internet Things J.* **2020**, *8*, 4157–4185. [[CrossRef](#)]
120. Karras, A.; Karras, C.; Drakopoulos, G.; Tsoilis, D.; Mylonas, P.; Sioutas, S. SAF: A Peer to Peer IoT LoRa System for Smart Supply Chain in Agriculture. In *Artificial Intelligence Applications and Innovations*; Maglogiannis, I., Iliadis, L., Macintyre, J., Cortez, P., Eds.; Springer: Cham, Switzerland, 2022; pp. 41–50.
121. Kamble, N.; Gala, R.; Vijayaraghavan, R.; Shukla, E.; Patel, D. Using Blockchain in Autonomous Vehicles. In *Artificial Intelligence and Blockchain for Future Cybersecurity Applications*; Maleh, Y., Baddi, Y., Alazab, M., Tawalbeh, L., Romdhani, I., Eds.; Springer International Publishing: Cham, Switzerland, 2021; pp. 285–305. [[CrossRef](#)]
122. Show, A.K.; Kumar, A.; Singhal, A.; Gayathri, N.; Vengatesan, K. Future blockchain technology for autonomous applications/ autonomous vehicle. In *Opportunities and Challenges for Blockchain Technology in Autonomous Vehicles*; IGI Global: Hershey, PA, USA, 2021; pp. 165–177.

123. Pedrosa, A.R.; Pau, G. ChargetUp: On Blockchain-Based Technologies for Autonomous Vehicles. In Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, CryBlock'18, New York, NY, USA, 15 June 2018; pp. 87–92. [\[CrossRef\]](#)
124. Jain, S.; Ahuja, N.J.; Srikanth, P.; Bhadane, K.V.; Nagaiah, B.; Kumar, A.; Konstantinou, C. Blockchain and Autonomous Vehicles: Recent Advances and Future Directions. *IEEE Access* **2021**, *9*, 130264–130328. [\[CrossRef\]](#)
125. Bathla, G.; Bhadane, K.V.; Singh, R.K.; Kumar, R.; Aluvalu, D.R.; Krishnamurthi, R.; Kumar, A.; Thakur, R.N.; Basheer, S. Autonomous Vehicles and Intelligent Automation: Applications, Challenges, and Opportunities. *Mob. Inf. Syst.* **2022**, *2022*, 7632892. [\[CrossRef\]](#)
126. Yeasmin, S.; Haque, A. A Multi-Factor Authenticated Blockchain-Based OTA Update Framework for Connected Autonomous Vehicles. In Proceedings of the 2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall), Norman, OK, USA, 27–30 September 2021; pp. 1–6. [\[CrossRef\]](#)
127. Narbayeva, S.; Bakibayev, T.; Abeshev, K.; Makarova, I.; Shubenkova, K.; Pashkevich, A. Blockchain technology on the way of autonomous vehicles development. *Transp. Res. Procedia* **2020**, *44*, 168–175. [\[CrossRef\]](#)
128. Wang, Y.; Su, Z.; Zhang, K.; Benslimane, A. Challenges and Solutions in Autonomous Driving: A Blockchain Approach. *IEEE Netw.* **2020**, *34*, 218–226. [\[CrossRef\]](#)
129. Alladi, T.; Chamola, V.; Sahu, N.; Guizani, M. Applications of blockchain in unmanned aerial vehicles: A review. *Veh. Commun.* **2020**, *23*, 100249. [. : 10.1016/j.vehcom.2020.100249. \[CrossRef\]](#)
130. Hui, Y.; Huang, Y.; Su, Z.; Luan, T.H.; Cheng, N.; Xiao, X.; Ding, G. BCC: Blockchain-Based Collaborative Crowdsensing in Autonomous Vehicular Networks. *IEEE Internet Things J.* **2022**, *9*, 4518–4532. [\[CrossRef\]](#)
131. Bendiab, G.; Hameurlaine, A.; Germanos, G.; Kolokotronis, N.; Shiaeles, S. Autonomous Vehicles Security: Challenges and Solutions Using Blockchain and Artificial Intelligence. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 3614–3637. [\[CrossRef\]](#)
132. Aloqaily, M.; Hussain, R.; Khalaf, D.; Slehat, D.; Oracevic, A. On the Role of Futuristic Technologies in Securing UAV-Supported Autonomous Vehicles. *IEEE Consum. Electron. Mag.* **2022**, *11*, 93–105. [\[CrossRef\]](#)
133. Jha, S.; Jha, N.; Prashar, D.; Ahmad, S.; Alouffi, B.; Alharbi, A. Integrated IoT-Based Secure and Efficient Key Management Framework Using Hashgraphs for Autonomous Vehicles to Ensure Road Safety. *Sensors* **2022**, *22*, 2529. [\[CrossRef\]](#) [\[PubMed\]](#)
134. Kuzmin, A.; Znak, E. Blockchain-base structures for a secure and operate network of semi-autonomous Unmanned Aerial Vehicles. In Proceedings of the 2018 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), Singapore, 31 July 2018–2 August 2018; pp. 32–37. [\[CrossRef\]](#)
135. Rajendar, S.; Thangavel, U.; Devendran, S.; Selvi, V.; Muthumanickam, S.S. Blockchain for Securing Autonomous Vehicles. In Proceedings of the 2023 Second International Conference on Electronics and Renewable Systems (ICEARS), Tamil Nadu, India, 2–4 March 2023; pp. 713–717. [\[CrossRef\]](#)
136. Gupta, R.; Tanwar, S.; Kumar, N.; Tyagi, S. Blockchainbased security attack resilience schemes for autonomous vehicles in industry 4.0: A systematic review. *Comput. Electr. Eng.* **2020**, *86*, 106717. [\[CrossRef\]](#)
137. Reyna, A.; Martín, C.; Chen, J.; Soler, E.; Díaz, M. On blockchain and its integration with IoT. Challenges and opportunities. *Future Gener. Comput. Syst.* **2018**, *88*, 173–190. [. : 10.1016/j.future.2018.05.046. \[CrossRef\]](#)
138. Jabbar, R.; Dhib, E.; Said, A.B.; Krichen, M.; Fetais, N.; Zaidan, E.; Barkaoui, K. Blockchain Technology for Intelligent Transportation Systems: A Systematic Literature Review. *IEEE Access* **2022**, *10*, 20995–21031. [\[CrossRef\]](#)
139. Jiang, T.; Fang, H.; Wang, H. Blockchain-based internet of vehicles: Distributed network architecture and performance analysis. *IEEE Internet Things J.* **2018**, *6*, 4640–4649. [\[CrossRef\]](#)
140. Zhang, X.; Chen, X. Data security sharing and storage based on a consortium blockchain in a vehicular ad hoc network. *Ieee Access* **2019**, *7*, 58241–58254. [\[CrossRef\]](#)
141. Singh, S.K.; Park, J.H.; Sharma, P.K.; Pan, Y. BIIoVT: Blockchain-based secure storage architecture for intelligent internet of vehicular things. *IEEE Consum. Electron. Mag.* **2021**, *11*, 75–82. [\[CrossRef\]](#)
142. Yin, Y.; Li, Y.; Ye, B.; Liang, T.; Li, Y. A blockchain-based incremental update supported data storage system for intelligent vehicles. *IEEE Trans. Veh. Technol.* **2021**, *70*, 4880–4893. [\[CrossRef\]](#)
143. Kakkar, R.; Gupta, R.; Agrawal, S.; Tanwar, S.; Sharma, R. Blockchain-based secure and trusted data sharing scheme for autonomous vehicle underlying 5G. *J. Inf. Secur. Appl.* **2022**, *67*, 103179. [\[CrossRef\]](#)
144. Nair, M.M.; Tyagi, A.K. Preserving privacy using blockchain technology in autonomous vehicles. In *Proceedings of the International Conference on Network Security and Blockchain Technology*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 237–248.
145. Singh, M.; Kim, S. Introduce reward-based intelligent vehicles communication using blockchain. In Proceedings of the 2017 International SoC Design Conference (ISOCC), Seoul, Republic of Korea, 5–8 November 2017; pp. 15–16.
146. Rowan, S.; Clear, M.; Gerla, M.; Huggard, M.; Goldrick, C.M. Securing vehicle to vehicle communications using blockchain through visible light and acoustic side-channels. *arXiv* **2017**, arXiv:1704.02553.
147. Yang, Z.; Yang, K.; Lei, L.; Zheng, K.; Leung, V.C. Blockchain-based decentralized trust management in vehicular networks. *IEEE Internet Things J.* **2018**, *6*, 1495–1505. [\[CrossRef\]](#)
148. Mitra, S.; Bose, S.; Gupta, S.S.; Chattopadhyay, A. Secure and tamper-resilient distributed ledger for data aggregation in autonomous vehicles. In Proceedings of the 2018 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), Chengdu, China, 26–30 October 2018; pp. 548–551.

149. 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. [\[CrossRef\]](#)
150. Oham, C.; Michelin, R.A.; Jurdak, R.; Kanhere, S.S.; Jha, S. B-FERL: Blockchain based framework for securing smart vehicles. *Inf. Process. Manag.* **2021**, *58*, 102426. [\[CrossRef\]](#)
151. Reebadiya, D.; Rathod, T.; Gupta, R.; Tanwar, S.; Kumar, N. Blockchain-based secure and intelligent sensing scheme for autonomous vehicles activity tracking beyond 5g networks. *Peer- Netw. Appl.* **2021**, *14*, 2757–2774. [\[CrossRef\]](#)
152. Wang, J.; Liu, Y.; Niu, S.; Song, H. Lightweight blockchain assisted secure routing of swarm UAS networking. *Comput. Commun.* **2021**, *165*, 131–140. [\[CrossRef\]](#)
153. Kamal, M.; Srivastava, G.; Tariq, M. Blockchain-based lightweight and secured v2v communication in the internet of vehicles. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 3997–4004. [\[CrossRef\]](#)
154. Ali, A.; Iqbal, M.M.; Jabbar, S.; Asghar, M.N.; Raza, U.; Al-Turjman, F. VABLOCK: A blockchain-based secure communication in V2V network using icn network support technology. *Microprocess. Microsyst.* **2022**, *93*, 104569. [\[CrossRef\]](#)
155. Cebe, M.; Erdin, E.; Akkaya, K.; Aksu, H.; Uluagac, S. Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles. *IEEE Commun. Mag.* **2018**, *56*, 50–57. [\[CrossRef\]](#)
156. Alphand, O.; Amoretti, M.; Claeys, T.; Dall'Asta, S.; Duda, A.; Ferrari, G.; Rousseau, F.; Tourancheau, B.; Veltri, L.; Zanichelli, F. IoTChain: A blockchain security architecture for the Internet of Things. In Proceedings of the 2018 IEEE Wireless Communications and Networking Conference (WCNC), Barcelona, Spain, 15–18 April 2018; pp. 1–6.
157. Li, C.; Palanisamy, B. Privacy in internet of things: From principles to technologies. *IEEE Internet Things J.* **2018**, *6*, 488–505. [\[CrossRef\]](#)
158. Davi, L.; Hatebur, D.; Heisel, M.; Wirtz, R. Combining safety and security in autonomous cars using blockchain technologies. In Proceedings of the Computer Safety, Reliability, and Security: SAFECOMP 2019 Workshops, ASSURE, DECSoS, SASSUR, STRIVE, and WAISE, Turku, Finland, 10 September 2019; Proceedings 38; Springer: Berlin/Heidelberg, Germany, 2019; pp. 223–234.
159. Rathore, H.; Samant, A.; Jadliwala, M. TangleCV: A distributed ledger technique for secure message sharing in connected vehicles. *ACM Trans. Cyber-Phys. Syst.* **2020**, *5*, 1–25. [\[CrossRef\]](#)
160. Li, M.; Chen, Y.; Lal, C.; Conti, M.; Alazab, M.; Hu, D. Eunomia: Anonymous and secure vehicular digital forensics based on blockchain. *IEEE Trans. Dependable Secur. Comput.* **2021**, *20*, 225–241. [\[CrossRef\]](#)
161. Yao, Q.; Li, T.; Yan, C.; Deng, Z. Accident responsibility identification model for Internet of Vehicles based on lightweight blockchain. *Comput. Intell.* **2023**, *39*, 58–81. [\[CrossRef\]](#)
162. Kang, J.; Xiong, Z.; Niyato, D.; Ye, D.; Kim, D.I.; Zhao, J. Toward secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract theory. *IEEE Trans. Veh. Technol.* **2019**, *68*, 2906–2920. [\[CrossRef\]](#)
163. Abbes, S.; Rekhis, S. A blockchain-based solution for reputation management in IoV. In Proceedings of the 2021 International Wireless Communications and Mobile Computing (IWCMC), Harbin City, China, 28 June–2 July 2021; pp. 1129–1134.
164. Feng, L.; Yang, Z.; Guo, S.; Qiu, X.; Li, W.; Yu, P. Two-Layered Blockchain Architecture for Federated Learning Over the Mobile Edge Network. *IEEE Netw.* **2022**, *36*, 45–51. [\[CrossRef\]](#)
165. Bhattacharya, P.; Shukla, A.; Tanwar, S.; Kumar, N.; Sharma, R. 6Blocks: 6G-enabled trust management scheme for decentralized autonomous vehicles. *Comput. Commun.* **2022**, *191*, 53–68. [\[CrossRef\]](#)
166. Mushtaq, A.; Haq, I.; Sarwar, M.A.; Khan, A.; Shafiq, O. Traffic Management of Autonomous Vehicles using Policy Based Deep Reinforcement Learning and Intelligent Routing. *arXiv* **2022**, arXiv:2206.14608.
167. Elayan, H.; Aloqaily, M.; Salameh, H.B.; Guizani, M. Intelligent Cooperative Health Emergency Response System in Autonomous Vehicles. In Proceedings of the 2021 IEEE 46th Conference on Local Computer Networks (LCN), Edmonton, AB, Canada, 4–7 October 2021; pp. 293–298. [\[CrossRef\]](#)
168. Kusari, A.; Li, P.; Yang, H.; Punshi, N.; Rasulis, M.; Bogard, S.; LeBlanc, D.J. Enhancing SUMO simulator for simulation based testing and validation of autonomous vehicles. In Proceedings of the 2022 IEEE Intelligent Vehicles Symposium (IV), Aachen, Germany, 5–9 June 2022; pp. 829–835. [\[CrossRef\]](#)
169. Qiu, T.; Zhao, Z.; Zhang, T.; Chen, C.; Chen, C.L.P. Underwater Internet of Things in Smart Ocean: System Architecture and Open Issues. *IEEE Trans. Ind. Inform.* **2020**, *16*, 4297–4307. [\[CrossRef\]](#)
170. Ganin, D.V.; Gladkikh, A.A.; Dementiev, V.; Kutuzov, V. Intelligent data processing methods in sensor networks of mobile and autonomous objects. *IOP Conf. Ser. Earth Environ. Sci.* **2021**, *857*, 012001. [\[CrossRef\]](#)
171. El Hamdani, S.; Benamar, N. Autonomous Traffic Management: Open Issues and New Directions. In Proceedings of the 2018 International Conference on Selected Topics in Mobile and Wireless Networking (MoWNeT), Tangier, Morocco, 20–22 June 2018; pp. 1–5. [\[CrossRef\]](#)
172. Axelrod, C.W. Cybersecurity in the age of autonomous vehicles, intelligent traffic controls and pervasive transportation networks. In Proceedings of the 2017 IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, NY, USA, 5 May 2017; pp. 1–6. [\[CrossRef\]](#)
173. Axelrod, C.W. Cybersecurity challenges of systems-of-systems for fully-autonomous road vehicles. In Proceedings of the 2017 13th International Conference and Expo on Emerging Technologies for a Smarter World (CEWIT), Stony Brook, NY, USA, 7–8 November 2017; pp. 1–6. [\[CrossRef\]](#)
174. Sharma, P.K.; Vohra, D.; Rathore, S. Security and Privacy in V2X Communications: How Can Collaborative Learning Improve Cybersecurity? *IEEE Netw.* **2022**, *36*, 32–39. [\[CrossRef\]](#)

175. Ahmed, M.; Iqbal, R.; Amin, S.; Alhabshneh, O.; Garba, A. Autonomous Vehicle and its Adoption: Challenges, Opportunities, and Future Implications. In Proceedings of the 2022 International Conference on Emerging Trends in Computing and Engineering Applications (ETCEA), Karak, Jordan, 23–24 November 2022; pp. 1–6. [\[CrossRef\]](#)
176. Stinson, M.; Zou, B.; Briones, D.; Manjarrez, A.; Mohammadian, A.K. Vehicle ownership models for a sharing economy with autonomous vehicle considerations. *Transp. Lett.* **2021**, *15*, 1–17. [\[CrossRef\]](#)
177. Taylor, C.R.; Carter, J.M.; Huff, S.; Nafziger, E.; Rios-Torres, J.; Zhang, B.; Turcotte, J. Evaluating Efficiency and Security of Connected and Autonomous Vehicle Applications. In Proceedings of the 2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 8–11 January 2022; pp. 236–239. [\[CrossRef\]](#)
178. Boddupalli, S.; Chamarithi, V.S.G.; Lin, C.W.; Ray, S. CAVELIER: Automated Security Evaluation for Connected Autonomous Vehicle Applications. In Proceedings of the 2022 IEEE 25th International Conference on Intelligent Transportation Systems (ITSC), Macau, China, 8–12 October 2022; pp. 4335–4340. [\[CrossRef\]](#)
179. Kaasen, A.D.; Grov, G.; Mancini, F.; Baksaas, M. Towards data-driven autonomous cyber defence for military unmanned vehicles-threats & attacks. In Proceedings of the MILCOM 2022-2022 IEEE Military Communications Conference (MILCOM), Rockville, MD, USA, 28 November 2022–2 December 2022; pp. 861–866. [\[CrossRef\]](#)
180. He, Q.; Meng, X.; Qu, R.; Xi, R. Machine Learning-Based Detection for Cyber Security Attacks on Connected and Autonomous Vehicles. *Mathematics* **2020**, *8*, 1311. [\[CrossRef\]](#)
181. Security of the Perception in Autonomous Driving under Physical-World Adversarial Attacks. 2022. Available online: <https://bpb-us-w2.wpmucdn.com/wp.ovptl.uci.edu/dist/e/3/files/2022/10/ICS-1.pdf> (accessed on 23 July 2023).
182. Cui, C.; Du, H.; Jia, Z.; He, Y.; Yang, Y.; Jin, M. Data Poisoning Attack Using Hybrid Particle Swarm Optimization in Connected and Autonomous Vehicles. In Proceedings of the 2022 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE), Gold Coast, Australia, 18–20 December 2022; pp. 1–5. [\[CrossRef\]](#)
183. Khan, I.A.; Moustafa, N.; Pi, D.; Haider, W.; Li, B.; Jolfaei, A. An Enhanced Multi-Stage Deep Learning Framework for Detecting Malicious Activities From Autonomous Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 25469–25478. [\[CrossRef\]](#)
184. Mishra, A.; Cha, J.; Kim, S.; Privacy-preserved in-cabin monitoring system for autonomous vehicles. *Comput. Intell. Neurosci.* **2022**, *2022*, 5389359. [\[CrossRef\]](#)
185. Jarouf, A.; Meskin, N.; Al-Kuwari, S.; Shakerpour, M.; Cassanderas, C.G. Security analysis of merging control for connected and automated vehicles. In Proceedings of the 2022 IEEE Intelligent Vehicles Symposium (IV), Aachen, Germany, 4–9 June 2022; pp. 1739–1744.
186. Brubaker, C.; Jana, S.; Ray, B.; Khurshid, S.; Shmatikov, V. Using Frankencerts for Automated Adversarial Testing of Certificate Validation in SSL/TLS Implementations. In Proceedings of the 2014 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 18–21 May 2014; pp. 114–129. [\[CrossRef\]](#)
187. Kim, J.S. Design of Federated Learning Engagement Method for Autonomous Vehicle Privacy Protection. In Proceedings of the 2022 Joint 12th International Conference on Soft Computing and Intelligent Systems and 23rd International Symposium on Advanced Intelligent Systems (SCIS&ISIS), Ise, Japan, 29 November 2022–2 December 2022; pp. 1–2. [\[CrossRef\]](#)
188. Krichen, M.; Lahami, M.; Al-Haija, Q.A. Formal Methods for the Verification of Smart Contracts: A Review. In Proceedings of the 2022 15th International Conference on Security of Information and Networks (SIN), Sousse, Tunisia, 11–13 November 2022; pp. 1–8. [\[CrossRef\]](#)
189. Abdellatif, T.; Brousmiche, K.L. Formal Verification of Smart Contracts Based on Users and Blockchain Behaviors Models. In Proceedings of the 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 26–28 February 2018; pp. 1–5. [\[CrossRef\]](#)
190. Cheon, J.H.; Han, K.; Hong, S.M.; Kim, H.J.; Kim, J.; Kim, S.; Seo, H.; Shim, H.; Song, Y. Toward a secure drone system: Flying with real-time homomorphic authenticated encryption. *IEEE Access* **2018**, *6*, 24325–24339. [\[CrossRef\]](#)
191. Sultan, A.; Tahir, S.; Tahir, H.; Anwer, T.; Khan, F.; Rajarajan, M.; Rana, O. A novel image-based homomorphic approach for preserving the privacy of autonomous vehicles connected to the cloud. *IEEE Trans. Intell. Transp. Syst.* **2022**, *24*, 1936–1948. [\[CrossRef\]](#)
192. Karras, A.; Karras, C.; Giotopoulos, K.C.; Tsoilis, D.; Oikonomou, K.; Sioutas, S. Peer to Peer Federated Learning: Towards Decentralized Machine Learning on Edge Devices. In Proceedings of the 2022 7th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), Ioannina, Greece, 23–25 September 2022; pp. 1–9. [\[CrossRef\]](#)
193. Karras, A.; Karras, C.; Giotopoulos, K.C.; Tsoilis, D.; Oikonomou, K.; Sioutas, S. Federated Edge Intelligence and Edge Caching Mechanisms. *Information* **2023**, *14*, 414. [\[CrossRef\]](#)
194. Wang, J.; Cai, Z.; Yu, J. Achieving Personalized k -Anonymity-Based Content Privacy for Autonomous Vehicles in CPS. *IEEE Trans. Ind. Inform.* **2020**, *16*, 4242–4251. [\[CrossRef\]](#)
195. Torre, G.D.L.; Rad, P.; Choo, K.K.R. Driverless vehicle security: Challenges and future research opportunities. *Future Gener. Comput. Syst.* **2020**, *108*, 1092–1111. [\[CrossRef\]](#)

196. Schizas, N.; Karras, A.; Karras, C.; Sioutas, S. TinyML for Ultra-Low Power AI and Large Scale IoT Deployments: A Systematic Review. *Future Internet* **2022**, *14*, 363. [[CrossRef](#)]
197. Antonini, M.; Pincheira, M.; Vecchio, M.; Antonelli, F. An Adaptable and Unsupervised TinyML Anomaly Detection System for Extreme Industrial Environments. *Sensors* **2023**, *23*, 2344. [[CrossRef](#)] [[PubMed](#)]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.