Challenges in the Field of Autonomous Vehicles

Subjects: Automation & Control Systems

Contributor: Anushka Biswas , Hwang-Cheng Wang

The term autonomous vehicle (AV) has become ubiquitous in our lives, owing to the extensive research and development that frequently make headlines. Nonetheless, the flourishing of AVs hinges on many factors due to the extremely stringent demands for safety, security, and reliability. Besides lingering technical problems, the complexity of the AV infrastructure makes it vulnerable to security and privacy attacks that can endanger the lives of passengers and commuters. Surpassing traditional centralized security systems, blockchain has emerged as the best solution to provide the much-needed security shield to AVs with its data transparency, immutability, and decentralized approach. Therefore, enriching and enmeshing technologies like AI, edge computing, IoT, 5G and Blockchain into a robust system will lead to the realization of our much-yearned AV dream into reality.

autonomous vehicles | Internet of Things | cyber security | edge intelligence | 5G | blockchain | sensors

1. Introduction

Despite the current accelerated and intensive research into the field of autonomous vehicles (AVs) to bring them to the roads, the field is still riddled with technical [1], legal, and moral challenges. Unless the following obstacles are eliminated or reduced to a considerable extent, it would not be safe or ethical to launch AVs in the market.

2. Infeasible Sensing

For the safe journey of an AV, the sub-task of object detection is one of the most important prerequisites, as it allows the car controller to account for various obstacles while considering possible future trajectories. Sensing the surroundings of the AV heavily depends on the intrinsic properties of the embedded sensors and their quality of perception. **Figure 1** shows the multiple sensors present in an AV to efficiently sense their surroundings. The four main types of sensors are [2]:

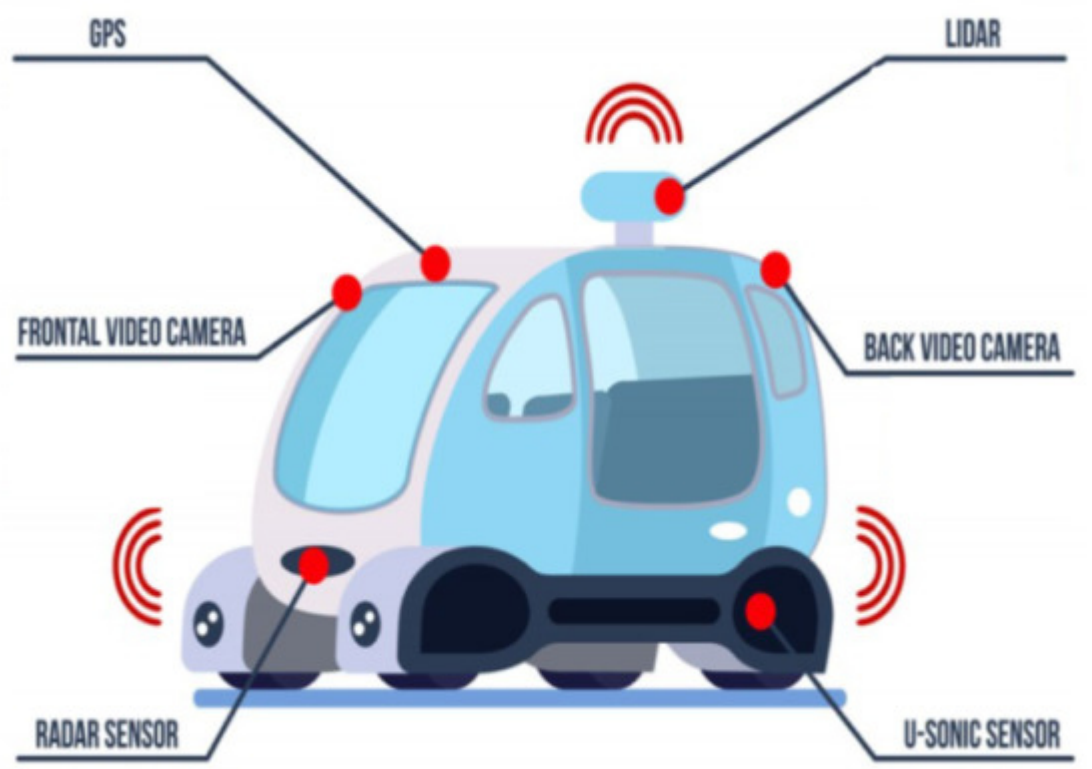

Figure 1. The main set of sensors present in an AV, utilized in sensor fusion.

- GNSS/IMU: global navigation satellite system and the inertial measurement unit are used for the localization of the AV. GNSS reports the global position estimate accurately, but its update rate is too slow to match real-time requirements. IMU reports the inertial updates of a body at high frequency (at or higher than 200 Hz) but its accuracy degrades with time. Kalman filtering is used to obtain the best advantages of the two, which gives the vehicle a dead reckoning capability and the ability to gather accurate data for real-time localization [3].

- LiDAR: Light detection and ranging (LiDAR) can be used for scanning, localization, obstacle detection, and accurate depth perception. It works by calculating how long it takes for a beam of light to hit surfaces and bounce back to the laser scanner. The distance is computed using the velocity of light. This approach is known as “time of flight” measurements. The higher the number of layers used in the scanner, the better the perception of the wide range of environmental contours [4]. They generate a "shape" of the surrounding environment in the form of point clouds. Consequently, a particle filter is used to filter out and compare the observed shape against a map of known objects to reduce ambiguity.

- Cameras: Monocular cameras are the most common and widely used sensors in an AV, capturing the 2D RGB images of the surroundings, used for object recognition, tracking, traffic light detection, etc. AVs usually mount between eight and ten cameras, running at approximately 60 Hz and together generating a high amount of data per second. To add depth perception, many systems use double-lens (binocular) cameras called stereo cameras [5]. Both the single lens and the stereo cameras are cheap, allowing them to be used and depended upon extensively.

- RaDAR: RaDAR measures distances, movements, and velocity by sending out Radio waves that reflect back from obstacles and detect short- and long-range depth. Short-range Radars have a range of 20–50 m, whereas long-range radars can extend up to 250 m. Radio waves can penetrate objects and are unaffected by bad weather conditions, unlike LiDAR and cameras. They report the distance of the nearest obstacle and the data generated by them do not require a lot of processing. Hence, they are typically fed as input to the control processor for realizing adaptive cruise control (ACC), blind-spot monitoring (BSM) and predictive emergency braking systems (PEBS) [6].

Table 1 lists the various disadvantages associated with each type of sensor used in AV. Besides those, vehicle computing systems are heavily constrained by memory [7]. Hence, it is not possible to store and run detectors with large volumes of input images which constrain the depth of neural network approaches. There is also the requirement that the entire detection process be fast, which usually leaves no room for image pre-processing to boost detection performance. Maintaining a high level of accuracy with a quick response time is key. One currently used solution is sensor fusion [8], which combines various sensing modalities for perception, such as combining data from LiDAR sensors, radar, sensors atop traffic lights, and sensors in other vehicles. Thus, it improves the accuracy and quality of sensing, in addition to reducing the ambiguities that may come from the use of various sensors. The vehicle positioning and orientation will be calculated by combining data from separate sensors. The fusion of data from different sensors and AI-based intelligent sensing are also extensively discussed in [9]. The types of multi-sensor fusion discussed in various literature [10][11][12] involve camera-radar (CR), camera-LiDAR (CL), and camera-LiDAR-radar (CLR). The paper [13] extensively reviews the sensors used, their pros and cons, and the various sensor fusion technology approaches adopted in AVs.

Table 1. Disadvantages of sensors used in autonomous vehicles.

Sensor Type	Disadvantages	Source
GNSS	• The update rate is too slow for the real-time requirements of AV • Cannot work accurately in closed spaces (such as tunnels and crowded city streets) as it requires an unhindered view of the sky • Exposure to and interference from other waves in different radio frequency spectra hampers performance • Receivers may receive multiple signals reflected by surrounding objects (buildings, walls, etc.), introducing unwanted noise (multi-path errors) • Prone to cyberattacks, deliberate jamming, and spoofing	[2][14]
IMU	• Accuracy degrades over time	[2]

Sensor Type	Disadvantages	Source
	• Constantly rounds of small fractions of errors in its measurements (relative to itself), which accumulate over time, leading to significant errors, known as Drift	
LiDAR	• Initial and maintenance costs are very high • Performance degrades significantly in bad weather such as fog, rain, and snow since it uses visible lasers for object detection and distance measurement • It is the most power-hungry sensor, significantly reducing the AV's driving range • External elements and architectural features create occlusions that may lead to partial data collection or inaccurate measurements since it is a line-of-sight technology	[15] [16]
Camera	• Inconsistent performance across different illumination conditions (for example, it can be blinded by strong light) • Performance degrades in bad weather such as snow, rain, and fog • Poor depth perception and low range • Requires high processing power for the large volume of data generated	[17] [18]
RADAR	• Increasing mutual interference among automotive radars leads to inaccurate perception • The generated point cloud after reflection of radio waves gives minimal information about the spatial dimensions of objects	[4][19]

3. Clash between Reliability and Latency

Latency refers to the time for a data packet to be transmitted and processed through multiple intermediate devices and eventually arrive at the destination and be decoded. Besides considering the inference accuracy, we should also pay some attention to another important aspect, namely inference delay. It is obvious that the quality of data and shallow neural networks can significantly hamper the inference accuracy in a pre-trained deep learning model. For the data captured by the sensors on the AV to be reliable and worthy of the decisions based on them, there should be some room for the preprocessing of data to accentuate its quality and hence, allow the vehicle to make correct and ethical decisions at the right moments. However, an additional communication delay is introduced to account for the time taken for data offloading from the mobile devices to a more powerful edge server. Sometimes it may become hampered by the channel dynamics. Nevertheless, the delay introduced by all these vastly

endangers the reliability of autonomous vehicles, since even a delay of a few milliseconds can turn out to be fatal while sensing and deciding how to overcome an obstacle on road, which can even cost the lives of pedestrians and other commuters. Therefore, to achieve a comfortable balance between reliability and incurred latency, it is of utmost importance to cut down the wireless transmission delay between the devices on-board and the edge server.

4. Limited Resources

Unlike the cloud servers which have a large number of powerful graphics processing units (GPUs) and central processing units (CPUs), the edge servers are not as heavily equipped [20] in consideration of the economic benefits and scalability of deployment. For instance, there are a plethora of edge servers that are deployed close to users. As a result, the economic factors of such large-scale deployment automatically come into play. Therefore, an edge server does not need and cannot have as many resources as a cloud server. Thus, they can hardly take a massive number of offloading requests from mobile devices due to constraints in memory, computing, data caching, power resources, limited communication bandwidth, and ultimately, may not be able to process all the tasks fully. If all the data are indiscriminately offloaded to the edge servers, this will lower the processing efficiency and increase the latency of the network.

5. Cyber Security and Privacy

The data acquired by AVs for processing and inferencing are always exposed to a number of security threats due to unauthorized access and weak protection against malicious entities that may jeopardize the private information of the owner. Cybersecurity and privacy are two of the leading bottlenecks hindering the wide deployment of AVs and public acceptance. A survey conducted in 2015 with 5000 respondents across 109 countries [21] revealed people's wariness and concerns regarding the misuse of personal information through the software hacking of vehicles with all levels of automation. The situation had not improved much by 2022, as the main threats had not been eliminated. Cybersecurity is the main liability hazard arising from loopholes in in-vehicle security systems such as fragile connectivity, open channels, insecure bus systems, and the existence of intelligent hackers. The hardware and software systems of an AV can be compromised in the following ways [22]:

- Intelligent hackers can take over the AV and connected vehicles through their wireless networks (Bluetooth, cellular networks, etc.) to sell personal information for financial gains, inflict physical harm or carry out unlawful activities such as drug and human trafficking. This is relatively easier, as demonstrated by a study [23] wherein they took control of the brakes and engines of a Chrysler Jeep by hacking its Internet connection.

- GNSS data can be remotely manipulated to create confusion or critically endanger passenger safety. This can be achieved by injecting fake messages or spoofing GNSS [24].

- Physical attacks on sensors include the use of bright lights to blind cameras, and creating interference using ultrasound or radio waves to distract other sensors from correctly perceiving obstacles. Such situations may even lead to fatal accidents. Other onboard hardware may be tampered with leading to privacy breaches.

- The attacker may even intercept messages in intra-vehicle and inter-vehicle communication (V2V and V2I) and gravely endanger the safety and privacy of the owners and other AVs.

Cyberattacks [25][26] can lead to functional safety issues and can easily lead to privacy and/or identity theft, even costing someone's life, if the attacker deliberately changes the direction and takes full control over the actions of the AV. This has prompted companies and governments to take precautionary steps. Various software may be installed to detect malfunction or the presence of hackers, with frequent software updates and changing security architectures. Governments in the US, China, EU, and Singapore have enacted new legislation to address privacy and cybersecurity risks along with the adoption of a control-oriented strategy. Stronger laws and better software can go a long way in tackling these issues.

6. Legal Issues

As autonomous vehicles gradually take over driving control, the law must alter its code and implementation. Worldwide regulations exist to provide the safest and the most secure travel experience to people. Therefore, autonomous vehicles must prove that they conform to the desired safety standard. Current research in the US and Europe is working on this [27][28]. Legal challenges are one of the most critical issues concerning AVs, covering myriad public policies, traffic codes, technical standards of conventional vehicles, and tort law [29]. The use of the term "autonomous" in the case of vehicles has sometimes been misconstrued by the law because "autonomy" has broader philosophical connotations, unlike the technical one, which simply means that it can work independently of human intervention while driving [30]. The Convention of Road Traffic of many countries still mandatorily requires the presence of a driver who shall, at times, be able to take control of the vehicle. This provides a legal framework for semi-autonomous vehicles, but the fully autonomous ones are still off the hook, for which they need to prove that they are either safer than or as safe as their predecessors.

7. Moral and Ethical Issues

When faced with unexpected traffic situations that require complex decision making within split seconds, human drivers are not expected to react optimally and may be excused for making wrong decisions. However, for AVs, which are capable of analyzing the potential outcomes of various options and taking actions accordingly within milli-seconds, wrongful decision making then becomes part of extensive debate and legislation. The AV must conform to the expected moral norms, which differ from person to person. For instance, personality traits determine whether the driver would like to endanger their own life to save others [31]. It was found in a study [32] that participants programming an AV tend to more readily endanger car occupants than pedestrians compared to participants driving in a simulator. There is growing evidence of discrepancies between moral judgments (what they would do in moral dilemmas) and moral action (what they would actually do) [33][34]. What is considered ethical for human drivers may not be so for self-driving cars, and the evaluation of morality may vary based on the perspective of the way that the situation has been presented. Would it be acceptable that, because of AVs, fewer

people are harmed, but pedestrians become the ones more likely to be harmed than vehicle passengers? Thus, the introduction of AVs may put different groups at risk compared to the current situation.

References

1. Yang, B.; Cao, X.; Xiong, K.; Yuen, C.; Guan, Y.L.; Leng, S.; Qian, L.; Han, Z. Edge intelligence for autonomous driving in 6G wireless system: Design challenges and solutions. IEEE Wirel. Commun. 2021, 28, 40–47.
2. Liu, S.; Liu, L.; Tang, J.; Yu, B.; Wang, Y.; Shi, W. Edge computing for autonomous driving: Opportunities and challenges. Proc. IEEE 2019, 107, 1697–1716.
3. Huang, S.; Dissanayake, G. Convergence and consistency analysis for extended Kalman filter based SLAM. IEEE Trans. Robot. 2007, 23, 1036–1049.
4. Zhu, L. Analyze the Advantages and Disadvantages of Different Sensors for Autonomous Vehicles. In Proceedings of the 2022 7th International Conference on Social Sciences and Economic Development (ICSSED 2022), Wuhan, China, 25–27 March 2022; Atlantis Press: Dordrecht, The Netherlands; pp. 1020–1024.
5. Cudrano, P.; Mentasti, S.; Matteucci, M.; Bersani, M.; Arrigoni, S.; Cheli, F. Advances in centerline estimation for autonomous lateral control. In Proceedings of the 2020 IEEE Intelligent Vehicles Symposium (IV), Las Vegas, NV, USA, 9 October–13 November 2020; pp. 1415–1422.
6. Ivanov, A.; Shadrin, S.; Kristalniy, S.; Popov, N. Possible scenarios of autonomous vehicles' testing in Russia. In Proceedings of the IOP Conference Series: Materials Science and Engineering, Wuhan, China, 10–12 October 2019; IOP Publishing: Bristol, UK; Volume 534, pp. 1–7.
7. Lewis, G. Object Detection for Autonomous Vehicles. 2014. Available online: https://web.stanford.edu/class/cs231a/prev_projects_2016/object-detection-autonomous.pdf (accessed on 28 September 2022).
8. Kocić, J.; Jovičić, N.; Drndarević, V. Sensors and sensor fusion in autonomous vehicles. In Proceedings of the 2018 26th Telecommunications Forum (TELFOR), Belgrade, Serbia, 20–21 November 2018; pp. 420–425.
9. Sharma, A.; Sharma, V.; Jaiswal, M.; Wang, H.C.; Jayakody, D.N.K.; Basnayaka, C.M.W.; Muthanna, A. Recent Trends in AI-Based Intelligent Sensing. Electronics 2022, 11, 1661.
10. Pollach, M.; Schiegg, F.; Knoll, A. Low latency and low-level sensor fusion for automotive use-cases. In Proceedings of the 2020 IEEE International Conference on Robotics and Automation (ICRA), Paris, France, 31 May–31 August 2020; pp. 6780–6786.

11. Gu, S.; Zhang, Y.; Yang, J.; Alvarez, J.M.; Kong, H. Two-view fusion based convolutional neural network for urban road detection. In Proceedings of the 2019 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), Macau, China, 3–8 November 2019; pp. 6144–6149.
12. Nobis, F.; Geisslinger, M.; Weber, M.; Betz, J.; Lienkamp, M. A deep learning-based radar and camera sensor fusion architecture for object detection. In Proceedings of the 2019 Sensor Data Fusion: Trends, Solutions, Applications (SDF), Bonn, Germany, 15–17 October 2019; pp. 1–7.
13. Yeong, D.J.; Velasco-Hernandez, G.; Barry, J.; Walsh, J. Sensor and sensor fusion technology in autonomous vehicles: A review. Sensors 2021, 21, 2140.
14. Čaušević, S.; Šimić, E.; Kalem, A.; Selimović, A. GNSS Limitations During Position Determination and Receiver Rerformance Testing Using Android Mobile Application. TEM J. 2020, 9, 129–135.
15. Wood, R.L.; Mohammadi, M.E. LiDAR scanning with supplementary UAV captured images for structural inspections. In Proceedings of the International LiDAR Mapping Forum 2015, Denver, CO, USA, 23–25 February 2015.
16. Beland, M.; Parker, G.; Sparrow, B.; Harding, D.; Chasmer, L.; Phinn, S.; Antonarakis, A.; Strahler, A. On promoting the use of lidar systems in forest ecosystem research. For. Ecol. Manag. 2019, 450, 117484.
17. Campbell, S.; O'Mahony, N.; Krpalcova, L.; Riordan, D.; Walsh, J.; Murphy, A.; Ryan, C. Sensor technology in autonomous vehicles: A review. In Proceedings of the 2018 29th Irish Signals and Systems Conference (ISSC), Belfast, UK, 21–22 June 2018; pp. 1–4.
18. Thakur, R. Infrared sensors for autonomous vehicles. Recent Dev. Optoelectron. Devices 2018, 84.
19. Prochowski, L.; Szwajkowski, P.; Ziubiński, M. Research scenarios of autonomous vehicles, the sensors and measurement systems used in experiments. Sensors 2022, 22, 6586.
20. Shah-Mansouri, H.; Wong, V.W. Hierarchical fog-cloud computing for IoT systems: A computation offloading game. IEEE Internet Things J. 2018, 5, 3246–3257.
21. Kyriakidis, M.; Happee, R.; de Winter, J.C. Public opinion on automated driving: Results of an international questionnaire among 5000 respondents. Transp. Res. Part F Traffic Psychol. Behav. 2015, 32, 127–140.
22. Taeihagh, A.; Lim, H.S.M. Governing autonomous vehicles: Emerging responses for safety, liability, privacy, cybersecurity, and industry risks. Transp. Rev. 2019, 39, 103–128.
23. Schellekens, M. Car hacking: Navigating the regulatory landscape. Comput. Law Secur. Rev. 2016, 32, 307–315.
24. Bagloee, S.A.; Tavana, M.; Asadi, M.; Oliver, T. Autonomous vehicles: Challenges, opportunities, and future implications for transportation policies. J. Mod. Transp. 2016, 24, 284–303.

25. Kim, S.; Shrestha, R. Security and Privacy in Intelligent Autonomous Vehicles. In Automotive Cyber Security; Springer: Berlin/Heidelberg, Germany, 2020; pp. 35–66.
26. Kim, S.; Shrestha, R. In-vehicle communication and cyber security. In Automotive Cyber Security; Springer: Berlin/Heidelberg, Germany, 2020; pp. 67–96.
27. Anderson, J.M.; Kalra, N.; Wachs, M. Liability and Regulation of Autonomous Vehicle Technologies; RAND Corporation: Berkeley, CA, USA, 2009; Available online: http://www.rand.org/pubs/external_publications/EP20090427.html (accessed on 28 September 2022).
28. Gurney, J.K. Sue my car not me: Products liability and accidents involving autonomous vehicles. J. Law Technol. Policy 2013, 2013, 247–277.
29. Barabás, I.; Todoruţ, A.; Cordoş, N.; Molea, A. Current challenges in autonomous driving. In Proceedings of the IOP Conference Series: Materials Science and Engineering, Birmingham, UK, 13–15 October 2017; IOP Publishing: Bristol, UK, 2017; Volume 252, p. 012096.
30. Ilková, V.; Ilka, A. Legal aspects of autonomous vehicles—an overview. In Proceedings of the 2017 21st international conference on process control (PC), Štrbské Pleso, Slovakia, 6–9 June 2017; pp. 428–433.
31. Ju, U.; Kang, J.; Wallraven, C. To brake or not to brake? Personality traits predict decision-making in an accident situation. Front. Psychol. 2019, 10, 134.
32. Luzuriaga, M.; Heras, A.; Kunze, O. Hurting others vs. hurting myself, a dilemma for our autonomous vehicle. Rev. Behav. Econ. 2020, 7, 1–30.
33. Francis, K.B.; Howard, C.; Howard, I.S.; Gummerum, M.; Ganis, G.; Anderson, G.; Terbeck, S. Virtual morality: Transitioning from moral judgment to moral action? PloS ONE 2016, 11, e0164374.
34. FeldmanHall, O.; Mobbs, D.; Evans, D.; Hiscox, L.; Navrady, L.; Dalgleish, T. What we say and what we do: The relationship between real and hypothetical moral choices. Cognition 2012, 123, 434–441.