OPEN ACCESS Freely available online

Journal of Emerging Trends in Artificial Intelligence

Mini Review Vol. 1, Issue 1, January-December 2026

ChatGPT in the Autonomous Vehicle: What Citizens and Researchers Must Know to Apply?

Mehdi Gheisari[1,6,7,8*], Najmuddin Aamer[2], Yang Liu[3], Christian Fernandez Campusano[4], Abolfazl Mehbodniya[5]

[1]*Institute of Artificial Intelligence, Shaoxing University, Zhejiang, China*
[2]*CSE Department, Navkis College of Engineering, Hassan, Karnataka State, India*
[3]*Department of Computer Science, Swansea University, Swansea, UK*
[4]*Department of Electrical Engineering, Faculty of Engineering, University of Santiago de Chile (USACH), Santiago, Chile*
[5]*Department of Electronics and Communication Engineering, Kuwait College of Science and Technology (KCST), Doha Area, Kuwait*
[6]*Department of computer science and Engineering, Saveetha School of engineering, Saveetha Institute of Medical and Technical Science, Tamil Nadu, India*
[7]*Department of Computer Engineering, Shi.C., Islamic Azad University, Shiraz, Iran*
[8]*Department of R&D, Shenzhen BKD Co LTD, Shenzhen, China*

***Correspondence to:** Mehdi Gheisari[1,6,7,8], [1]Institute of Artificial Intelligence, Shaoxing University, Zhejiang, China; [6]Department of computer science and Engineering, Saveetha School of engineering, Saveetha Institute of Medical and Technical Science, Tamil Nadu, India; [7]Department of Computer Engineering, Shi.C., Islamic Azad University, Shiraz, Iran; [8]Department of R&D, Shenzhen BKD Co LTD, Shenzhen, China, E-mail: mehdi.gheisari61@gmail.com

Received: June 15, 2026; **Manuscript No:** JETA-26-6221; **Editor Assigned:** June 25, 2026; **PreQc No:** JETA-26-6221 (PQ); **Reviewed:** July 02, 2026; **Revised:** July 06, 2026; **Manuscript No:** JETA-26-6221 (R); **Published:** July 17, 2026

Citation: Gheisari M, Aamer N, Liu Y, Campusano CF, Mehbodniya A (2026). ChatGPT in the Autonomous Vehicle: What Citizens and Research-ers Must Know to Apply?. J. Emerg. Trends Artif. Intell. Vol.1 Iss.1, July (2026), pp:1-6.

ABSTRACT

Autonomous Vehicles (AVs) equipped with AI hold transformative potential but raise significant privacy concerns, particularly in their interaction with infrastructure like Road Side Units (RSUs). The ability of AI to hide or leak sensitive information poses risks such as financial loss, compromised privacy, and social inequality. Although recent regulations like the EU AI Act, China's AI governance, and the USA's Executive Order on AI address these issues, they need amendments to specifically cover AV privacy. This research explores these gaps, discusses the risks of using Large Language Models (LLMs) like ChatGPT in AVs, and provides guidelines for safe and responsible AV development.

Keywords: AI ACT; Large Language Models; ChatGPT; Autonomous Vehicles

INTRODUCTION

Recently, the EU approved the AI Act [1]. China implemented Beijing AI governance rules, and the US began studying regulations for AI, including tools like ChatGPT [2]. Despite these efforts, AI in Autonomous Vehicles (AVs) can still hide information, posing risks to both systems and privacy. [3]. IAs we know, in a smart city, AVs are becoming increasingly prevalent on roads due to the growing need for advanced technologies that enhance user experience and improve safety. On the other hand, among multiple LLMs proposed, ChatGPT has gained a strong reputation [4]. Non-technical citizens use AI instead of the technical word of LLMs. To make this paper more readable and understandable for non-technical citizens, we use "AI" instead of LLMs. Its ability to generate coherent and contextually appropriate responses makes it well-suited for use as a virtual assistant or chatbot in the AV ecosystem. However, it can breach privacy and leak private information. Specifically, AVs can collect vast amounts of data from their sensors, cameras, and other devices. This data can include Personally Identifiable Information (PII), such as the driver's location, speed, and driving habits. This data raises significant privacy concerns especially when the AI can hide private information and it could be used to track and monitor individuals without their consent [1-3]. As an example, suppose an important Police AVs' which is carrying prisoners are passing from a road. AI of the AV leaks private information and breaches privacy. Due to this vulnerability, another vehicle hits the police AV and prisoners evaded. Having checked this scenario deeply, it is important for citizens and researchers who are willing to leverage and develop AVs to have a clear understanding of its pros and cons and be aware of what they should do if LLMs of AVs hide information and leak private information without user consent [5].

REVIEW OF LITERATURE

Autonomous vehicles, driven by AI breakthroughs like ChatGPT, have the potential to revolutionize how we travel, making it safer, more efficient, and accessible [6]. With ChatGPT, these vehicles can interact with passengers in a more natural and intuitive way, offering personalized assistance and anticipating users needs, which enhances the overall experience and encourages its acceptance [7]. It also improves safety and decision-making by giving vehicles a better understanding of their surroundings [8-9]. However, we must also address the issues like bias, privacy, and security, and carefully balance the benefits of AI with the need to maintain human judgment to ensure ethical use [4].

As autonomous vehicles (AVs) becoming more widespread, people are getting increasingly concerned about the privacy issues related to their extensive data collection [10]. These vehicles use a wide range of sensors, including cameras and GPS, to gather a lot of personal information about both passengers and their surroundings [11-13]. While many are open to these recent technologies if they bring clear benefits like enhanced safety [14], there's also anxiety about the potential misuse for surveillance or discrimination [10,15]. It is also important to push for stronger privacy protections, such as clear data practices and strict safeguards. Researchers can help by exploring public concerns, developing privacy-friendly technologies, and working with policymakers to ensure that AV data is used ethically and appropriately [13-11]. By working together, researchers can make sure that the advantages of these technologies do not come at the expense of our privacy [14].

AI System Diagram

This section presents a schematic diagram of AI in an autonomous vehicle ecosystem, showcasing the interconnected components that contribute to the improved performance of automated vehicles. Figure 1 illustrates this diagram, which adopts an abstract point of view. To illustrate the system diagram, let's consider another specific example involving an on-board camera. Imagine the mounted camera in AV capturing visual data of people crossing at a crosswalk up ahead. This data is then processed by the "Perception" module, which utilizes computer vision techniques to identify and distinguish the pedestrians as separate objects. The information about the detected individuals is then integrated into the overall representation of the surrounding environment by the "World Model" module. Using this consolidated environmental representation, the "Prediction" module analyzes the data and predicts whether the pedestrians will continue crossing the road or not. Based on these trajectory projections, the "Motion Planning" module plans a safe route for the vehicle, ensuring it stops along a trajectory that accommodates the pedestrians. In the next step, the "Vehicle Control" section translates the planned stop into control signals that activate the corresponding actuators, effectively braking the car to a standstill. As the car stops, the passenger can communicate and ask natural language questions, such as "Why are we stopped here?" The "AV Interaction" module then interprets the inquiry and deduces, for example, that the passenger wants to understand the reason behind the unexpected stop. So, it enhances the environmental representation by indicating the presence of active pedestrians ahead. Finally, the "AV Interaction" module provides the interpreted intent, allowing for a better understanding of the reason for the stoppage. This information can influence future motion-planning actions and decision-making processes.

In an AV system, ChatGPT interacts with the perception, prediction, and motion planning modules to enhance situational awareness, anticipate behaviors, and optimize trajectories. ChatGPT helps interpret sensor data, predict road user actions, and suggest safe routes. To handle conflicting information, data fusion techniques, conflict resolution algorithms, and consensus-building mechanisms are used to integrate and reconcile data from multiple sources, ensuring coherent and informed decision-making. To ensure ChatGPT's responses are free from biases and ethical issues, diverse training data, bias detection algorithms, and clear ethical guidelines are crucial. Continuous monitoring through user feedback, audits, and human oversight helps maintain fairness and transparency. Additionally, establishing feedback loops and ethics committees ensures ongoing alignment with ethical standards.

To minimize the risk of ChatGPT distracting passengers in Autonomous Vehicles (AVs), responses are kept to be contextually appropriate, concise, and primarily voice-based to reduce visual engagement. Interactions made very simple, with guidelines encouraging hands-free use, limited interaction duration, and clear safety reminders. Additionally, an emergency response protocol can help passengers quickly disengage in critical situations, ensuring safety and awareness are maintained.

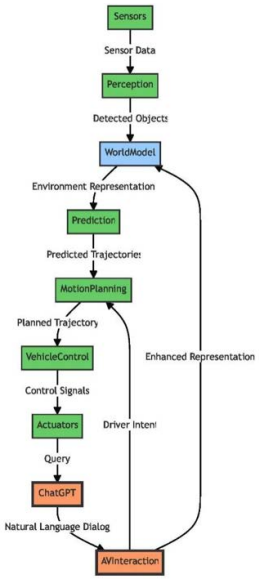

Figure 1: AI in the AV System Diagram

AI Applications in AV

LLMs, referred to as "AI" for simplicity, are well-suited as virtual assistants in autonomous vehicles (AVs) due to their ability to generate human-like responses. AI enhances the passenger experience by enabling voice commands for tasks like adjusting vehicle settings, checking itinerary details, providing

real-time updates on traffic and estimated arrival times, and offering insights into points of interest. Additionally, AI can control various vehicle functions, such as adjusting the temperature or changing the radio station, improving comfort and convenience.

AI also helps passengers understand the AV's actions by explaining maneuvers, like sudden lane changes, which builds trust in the vehicle's decision-making. Furthermore, AI enhances safety by issuing alerts about detected hazards, ensuring passengers are informed and aware of potential risks. In summary, AI as an in-vehicle assistant revolutionizes passenger interactions, boosting satisfaction and convenience. However, AI's ability to collect and possibly leak personal information raises privacy concerns. For instance, during interactions with AI, passengers may unintentionally share sensitive information, which, if not securely managed, could be exploited by malicious actors. AI's connection to other systems could also lead to unintended data disclosures, creating vulnerabilities and potential security risks. In the following sections, we propose solutions to mitigate these privacy risks and enhance AI's safe integration into AVs.

To ensure that ChatGPT's responses are accurate and relevant in real-time driving scenarios for autonomous vehicles (AVs), one should consider these measures: such as use of techniques like differential privacy to protect the sensitive information while allowing meaningful analysis. Implementing algorithms to detect and prevent data manipulation, ensuring information integrity. Strengthening the encryption and access controls to protect data from unauthorized access. Allowing users to manage privacy settings and review or delete their data. Regularly monitoring and audit AI systems to identify and address privacy risks. These steps will improve ChatGPT's effectiveness and ensure responsible AI integration in AVs.

To ensure ChatGPT's reliability in Autonomous Vehicles (AVs), it's crucial to address network connectivity and computational resource issues. Local data caching and preloading can help manage intermittent network problems, while resource monitoring and load balancing ensure adequate computational power. Implementing fault tolerance, such as error recovery and system redundancy, and employing backup systems can maintain continuous operation and reliability even during failures or disruptions.

How Researchers from Different Domains Can Mitigate the Privacy Breaches

As we have found, Autonomous vehicles (AVs) have the potential to revolutionize transportation, offering increased safety, convenience, and efficiency. However, AVs' collection and processing of vast amounts of data raises significant privacy concerns. Information hiding of AI from users, where AI algorithms conceal sensitive data and leaks it without use consent, can lead to fake accidents. So, researchers must address this challenge; it can be divided into several research sub parts. Each one is a challenge which also should be addressed by researchers. In this section, we explain, which points researchers should address to mitigate the privacy breaches in AVs which have happened because of information hiding of AI. So, a numerous key points need more investigation as mentioned below:

Developing privacy-aware AI algorithms:

AI algorithms used in AVs must be designed with privacy in mind. For instance, Differential privacy is a technique that adds carefully calibrated noise to data that can be incorporated into AI algorithms to prevent the identification of sensitive data while still allowing for meaningful statistical analysis. Researchers should develop differential privacy techniques tailored to the unique data collection and processing requirements of AVs.

Implementing data tampering detection mechanisms:

Malicious actors may attempt to manipulate data to conceal privacy breaches or accidents. To prevent this, researchers must develop robust data tampering detection algorithms that can identify and prevent such attempts. These algorithms should be efficient and effective, capable of detecting anomalies in data in real-time as well.

Enhancing data security measures:

Strong encryption and access control mechanisms are essential to protect sensitive data from unauthorized access. Moreover, researchers should develop secure data storage and transmission protocols to prevent data breaches.

Providing user control and transparency:

Users should have clear information about data collection and sharing practices and the ability to control their privacy settings. Due to this fact, researchers should explore different approaches to providing users with granular control over the data collected and shared by their AVs. This may include options to opt out of certain data collection activities, set limits on data sharing, or review and delete their data.

Conducting regular audits and privacy impact assessments:

Regular independent audits and privacy impact assessments should be conducted to identify and address potential privacy risks. Researchers should evaluate the effectiveness of privacy-preserving measures and make necessary adjustments time by time. In other words, regular audits and privacy impact assessments should be conducted to identify and address potential privacy risks.

Advocating for clear regulatory frameworks:

Clear regulatory frameworks that define privacy standards and account-ability for AV manufacturers and operators are essential. Researchers should advocate for developing and enforcing strong privacy regulations and standards. Fostering collaboration and information sharing: Collaboration between researchers, industry stakeholders, and policymakers is crucial to mitigate privacy breaches in AVs. Researchers should share knowledge and best practices, develop common standards, and advocate for clear regulatory frameworks.

Raising public awareness and education:

Educating the public about the importance of privacy in AVs and the potential risks of information hiding is essential.

Researchers should raise awareness about user rights and data collection and sharing responsibilities. By empowering users with knowledge, they can make informed decisions about their privacy.

Formally verifying privacy properties:

Formal verification can provide a high level of assurance that an AI algorithm or system protects user privacy. By proving that, the system satisfies a formal privacy property, researchers can give users confidence that their data will be handled in a privacy-preserving manner.

Formally verifying privacy properties:

Formal verification can provide a high level of assurance that an AI algorithm or system protects user privacy. By proving that, the system satisfies a formal privacy property, researchers can give users confidence that their data will be handled in a privacy-preserving manner.

Investigating homomorphic encryption:

Researchers also need to explore homomorphic encryption in AVs, which allows computations to be performed on encrypted data without first decrypting it. This can be used to protect the privacy of data while AI algorithms are processing it. Considering Secure Multi-party Computation: Moreover, they need to consider Secure multi-party computation which allows multiple parties to compute a function on their inputs without revealing their individual inputs to each other. This can be used to protect the privacy of data when it is being shared between different entities, such as AV manufacturers and insurance companies.

Utilizing Blockchain technology:

Additionally, Blockchain technology can be used to create a secure and tamper-proof record of data transactions. This can be used to track the use of data and ensure that it is not being misused or shared without the consent of the individuals whose data is being processed.

To improve the accuracy of AI responses in critical driving situations for autonomous vehicles (AVs), we can use:

Transfer Learning

Adapt AI models trained on general tasks to specific driving scenarios. For instance, fine-tuning ChatGPT on driving-related datasets helps it provide more relevant responses during critical events.

Active Learning

Continuously refine models by selecting and learning from the most informative real-world driving data. This approach focuses on improving accuracy by addressing challenging scenarios where the AI's responses were previously less effective.

These techniques shall help and ensure that AI in AVs delivers accurate, contextually appropriate information, enhancing safety and reliability. To ensure informed consent and protect passenger privacy in autonomous vehicles (AVs), the following measures can be implemented:

Informed Consent

Provide clear information about data collection practices and obtain explicit consent. Passengers should have control over their privacy settings, including the ability to opt out and manage their data.

Data Anonymization and Encryption

(1) Privacy-Aware AI Design: Use techniques like differential privacy to protect sensitive information during processing.

(2) Homomorphic Encryption: Enable computations on encrypted data to maintain privacy.

(3) Secure Multi-party Computation: Allow secure data processing among multiple entities without revealing individual data.

These measures help ensure passengers' data usage is transparent and their privacy is robustly protected.

To protect autonomous vehicles (AVs) from hacking and manipulation, implementing homomorphic encryption allows computations on encrypted data, ensuring sensitive information remains secure during processing. Additionally, applying differential privacy techniques adds noise to data, safeguarding user anonymity and reducing the risk of privacy breaches. To integrate ChatGPT with Autonomous Vehicle (AV) components, middleware solutions like message brokers and API integration can facilitate smooth communication and data exchange. Service-oriented architectures, such as microservices and event-driven architecture, further enhance integration by enabling modular, real-time interactions between ChatGPT and AV systems, promoting flexibility and responsiveness.

To evaluate ChatGPT's performance in real-time Autonomous Vehicle (AV) scenarios, key metrics like response time, accuracy rate, latency, and conversational coherence are critical for ensuring its reliability and effectiveness. Ensuring consistent accuracy and robustness involves strategies such as data augmentation, continuous training, adaptive learning, and regular performance monitoring. In an unexpected obstacle scenario, ChatGPT can assist Autonomous Vehicles (AVs) by providing real-time recommendations, such as suggesting alternative routes or actions based on sensor data. This enhances situational awareness and helps validate decisions, ensuring safer navigation in challenging situations. In complex urban environments, ChatGPT enhances Autonomous Vehicles (AVs) by providing real-time responses and insights based on dynamic traffic data. It analyzes sensor inputs to suggest route adjustments and alternative paths, ensuring safe navigation through unexpected events. Through continuous learning, ChatGPT adapts its responses, improving its ability to handle diverse and evolving urban traffic conditions. This is out of the scope of this work and shall be considered in future work.

What Non-Technical Citizens can do to mitigate the Risk

Citizens who are non-technical can follow some practical steps to mitigate potential risks of privacy-preservation issues. Citizens can: Raise concerns directly with elected leaders by speaking during public comment periods at local government

meetings. This allows residents to explain specific worries about AV testing plans and privacy-preservation breaches that happened due to information hiding and how proposals may impact traffic, infrastructure or neighborhood safety. In other words, giving context helps leaders make informed policy decisions. Writing to representatives provides another way for in-put. Correspondence can outline reasonable qualms, such as limitations- privacy breaches due to sensitive information hiding- not yet addressed in pilots. Suggesting restrictions, speed limits or awareness efforts offers solutions to improve safety via preventing privacy breaches. Including well-thought-out policy suggestions demonstrates engaged participation in the process.

Organize educational workshops to inform neighbors about technology abilities and limitations. With expert collaboration, workshops clarify capabilities and risks to dispel misconceptions. These also create a forum for building consensus on positions through respectful discussions. Being a volunteer for oversight boards and panels which allows close observation of testing procedures, including privacy breach. Safety professionals value extra viewpoints on protocols to spot potential issues and ensure safeguards. Concerned residents in advisory roles can confirm well-performed tests minimize hazards like information leakage and privacy breach as technologies progress. Inform the public about consumer rights regarding AV safety and where to report issues. Documenting safety including information leakage and privacy breach problems through appropriate channels provides regulators data to resolve issues proactively. Knowledge of options to facilitate responses empowers people.

Submit transparency requests for testing details especially information leakage and safety documentation which increases openness. In this case, citizens can understand evaluation methods, incident reporting and AI oversight which allows for informed scrutiny and boosting performance via providing safety. Support “right to repair” legislation enables third party evaluations and adding another layer of accountability forging to safety. In other words, with rising complexity, repair data access guarantees quality and safety. Advocate practical standards like limiting ranges, brake-oil amount or remote assistance, preventing information leakage and premature autonomy. Moreover, they can strict guidelines phasing skills through extensive validation which are safer than unrestrained deployment. Demand reasonable licensing reflecting validation metrics like brake-oil duration tested of the important corresponding AV. Mapping completeness and risk minimization especially privacy-preservation shows measured backing for growth. Push companies to disclose failure monitoring and prevention willingly demonstrates prioritizing transparency like information leakage of an important AV. In this way, they can comprehend issue identification like privacy breach and resolution, maintains responsible progress and trust as good community associates.

CONCLUSION

The recent actions taken by Europe, USA and China in regards to AI, demonstrate the growing awareness and concern about the potential risks and ethical implications of AI. These regulations and rules are guidelines for promoting transparency and accountability in AI development and use. Through investigation, we have found that they need to cover the above-mentioned topics so that citizens and researchers can use them as a starting point for addressing privacy breaches caused by AI in AVs when it hides sensiti ve information and can work towards implementing similar measures in other regions. The above-mentioned challenges need to be addressed by researchers and citizens. If the acts cover the above-mentioned topics, then, through collaborating sharing knowledge and resources, countries and organizations can create a global and comprehensive standard for responsible and ethical AI use. This not only protects individuals’ and AVs’ privacy, but also promotes trust and confidence in AI technology, which is crucial for its continued advancement and integration into our daily lives. Additionally, by considering the different approaches taken by North America, Europe and China, citizens and researchers can obtain valuable insights and perspectives on how to effectively address the above-mentioned issues from different perspectives. Ultimately, it is through collective efforts and a global mindset that we can mitigate risks and promote the responsible use of AI in autonomous vehicles.

FUTURE WORK

Considering alternative architectural designs and ensemble methods could really boost the current system. It's important to explore areas like privacy-aware AI, better data tampering detection, and stronger data security. By also focusing on giving users more control, supporting clear regulations, and encouraging collaborative research, we can make the system more reliable and secure for everyone. To broaden the study's scope to include different Autonomous Vehicle (AV) domains, we can look into various sectors like delivery services and emergency vehicles, analyze specific datasets, and test privacy measures in real-world situations. Collaborating across domains and bringing in expertise from different fields can be crucial in tackling privacy challenges and creating strong solutions for various AV applications.

DATA AVAILABILITY

This paper opens the eye of researchers and citizens how to mitigate the AI issue (matter Arising). So no data is available.

AI Use Statement

During the preparation of this work the author(s) used Aval AI in order to improve english. No AI tools were used for data analysis, interpretation, or generation of scientific content. After using this tool / service, the author(s) reviewed and edited the content as needed and take(s) full responsibility for the content of the published article.

FUNDING

No available funding

REFERENCES

1. Gibney E. What the EU's tough AI law means for research and ChatGPT. Nature. 2024;626(8001):938-9.
2. Chu C, Zhmoginov A, Sandler M. Cyclegan, a master of steganography. arXiv preprint arXiv:1712.02950. 2017 Dec 8.
3. Hutson M. Two-faced AI language models learn to hide deception. Nature. 2024.
4. Abrams SS. (R) evolutions of Thought: Artificial Intelligence and Education Futures. Teachers College Record. 2023;125(11-12):41-8.
5. Du H, Teng S, Chen H, Ma J, Wang X, et al. Retracted: Chat With ChatGPT on Intelligent Vehicles: An IEEE TIV Perspective. IEEE Transactions on Intelligent Vehicles. 2023;8(3):2020-6.
6. Stappen L, Dillmann J, Striegel S, Vögel HJ, Flores-Herr N,et al. Integrating generative artificial intelligence in intelligent vehicle systems. In2023 IEEE 26th International Conference on Intelligent Transportation Systems (ITSC) 2023 Sep 24 (pp. 5790-5797). IEEE.
7. Madaan A, Zhou S, Alon U, Yang Y, Neubig G. Language models of code are few-shot commonsense learners. InProceedings of the 2022 Conference on Empirical Methods in Natural Language Processing (pp. 1384-1403).
8. Opara Emmanuel Chinonso, Adalikwu Mfon-Ette Theresa, Tolorunleke Caroline Aduke (2023). ChatGPT for Teaching, Learning and Research: Prospects and Challenges. Glob Acad J Humanit Soc Sci. 2023;5.
9. Deng J, Lin Y. The benefits and challenges of ChatGPT: An overview. Benefits. 2023;2(2):2022.
10. Chowdhary S, Kawakami A, Gray ML, Suh J, Olteanu A, et al. Can workers meaningfully consent to workplace wellbeing technologies?. InProceedings of the 2023 ACM conference on fairness, accountability, and transparency 2023 Jun 12 (pp. 569-582).
11. Khan SM, Salek MS, Harris V, Comert G, Morris EA, et al. Autonomous Vehicles for All?. Journal on Autonomous Transportation Systems. 2024;1(1):1-8.
12. Li T, Lin L, Choi M, Fu K, Gong S, et al. Youtube av 50k: an annotated corpus for comments in autonomous vehicles. In2018 International Joint Symposium on Artificial Intelligence and Natural Language Processing (iSAI-NLP) 2018 Nov 15 (pp. 1-5). IEEE.
13. Lim HS, Taeihagh A. Autonomous vehicles for smart and sustainable cities: An in-depth exploration of privacy and cybersecurity implications. Energies. 201;11(5):1062.
14. Lopresti D, Shekhar S. A national research agenda for intelligent infrastructure: 2021 Update. arXiv preprint arXiv:2101.01671. 2021 Jan 5.
15. Othman K. Public acceptance and perception of autonomous vehicles: a comprehensive review. AI and Ethics. 2021;1(3):355-87.