International Journal of Research and Development in Engineering Science
ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/
Regular Issue, Vol. 5, Issue.3 (May – June) , 2023 , Pages: 12 - 17
Received: 18 October 2022 ; *Accepted*: 03 May 2023 ; *Published:* 28 May 2023
https://doi.org/10.63328/IJRDES-V5RI3P13
Original Paper : Applied Research – Theoretical Research Paper

Exploring the Perceptions about Public Acceptance, Safety, Privacy, and Cybersecurity of Autonomous Vehicles in Advanvced Transporation Systems

Vishnu Vijayan[1]*, Dilin Dinesh[2] , S. Christopher Ezhil Singh [3], P. Sridharan [4]

Department of Mechanical Engineering, Vimal Jyothi Engineering College, Kannur, Kerala, India – 670632

** Corresponding Author: Vishnu Vijayan ; vishnuvijayan@gmail.com*

Abstract: Concerns regarding cybersecurity, safety, privacy, and public acceptance are raised by the integration of autonomous vehicles (AVs) into sophisticated transportation networks. The purpose of this study is to investigate and evaluate the various perspectives that surround AVs. Evaluating public acceptability entails determining degrees of confidence and concerns about AV technology. The ability of AVs to handle challenging traffic situations while maintaining pedestrian and passenger safety is a safety concern. Concerns about privacy mostly concern how personal information is gathered, used, and safeguarded in AV systems. Implications for cybersecurity also highlight how susceptible antivirus software is to possible hackers or system breaches. This research contributes to a thorough knowledge of the potential and problems associated with the broad adoption of autonomous cars within futuristic transportation ecosystems by looking at these factors.

Keywords: ATS, Autonomous Vehicles, Public Safety, Transportation, Passengers.

1. Introduction

With the introduction of autonomous vehicles, the development of transportation networks is set for a revolutionary change. Driven by advanced technology and artificial intelligence, the widespread adoption of these self-driving cars has the potential to fundamentally alter our perception of transportation infrastructure and mobility. The introduction of autonomous vehicles (AVs) has generated a great deal of attention and discussion because to their technological advances as well as the ways in which they may affect cybersecurity, safety, privacy, and public acceptance in the context of more modern transportation systems. Public acceptability and perception are key factors influencing how well autonomous vehicles are incorporated into society.

The combination of new technologies and human behavior is frequently greeted with both intrigue and trepidation. The public's attitudes, worries, and readiness to accept this revolutionary method of transportation must be fully understood if it is to be widely adopted. The degree to which AV vehicles are adopted and used is greatly influenced by factors like perceived safety, convenience, dependability, and societal trust in AV technology. Safety is an essential component of the discussion around autonomous vehicles. AV enthusiasts highlight that by removing human error a primary contributor to traffic accidents—AVs have the potential to significantly reduce traffic accidents and fatalities. On the other hand, critics and doubters raise concerns about the technology's preparedness, possible weaknesses, and the ethical difficulties associated with making decisions in unanticipated circumstances.

Evaluating autonomous vehicles' technological resilience and promoting trust in their safety features are essential to their mass acceptance. The use of modern technologies in self-driving cars raises important concerns regarding passenger privacy and data security. Discussions about data privacy, surveillance, and possible misuse arise by the gathering and use of personal data, including itinerary details, interests, and habits. When developing and implementing autonomous vehicles, it is crucial to find a balance between the privacy rights of persons and the innovation and convenience of these vehicles. These vehicles' increasing dependence on connected systems and data sharing raises serious concerns about their vulnerability to cyberattacks. The safety and operation of autonomous vehicles is seriously endangered by the possibility of hacking, system breaches, and data manipulation. Ensuring strong cybersecurity measures and

ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/ , IJRDES, Vol. 5, Issue 3, 2023 , https://doi.org/10.63328/IJRDES-V5RI3P13

protecting these systems from cyber threats are essential for maintaining the reliability and dependability of antivirus software. Through an analysis of public attitudes toward safety, privacy, cybersecurity, and acceptance of autonomous vehicles in advanced transportation systems, the present study seeks to reveal the complex factors influencing the direction of this technological revolution. In order to responsibly and safely navigate the transition to automated mobility in the future, it is essential to understand these complex dynamics.

2. Literature Review

Gopindra S. Nair et al. (2021) has discussed how crucial it is for technology companies, automakers, and government organizations to work together in order to thoroughly test autonomous cars (AVs) on public roads. It investigates how the general public views AV safety and identifies factors that influence this perception.

Kareem Othman (2021) discussed the potential benefits of autonomous vehicles (AVs), including improved mobility and reduced energy consumption, emissions, travel time, and vehicle ownership. It highlights the challenges of inadequate laws and regulations and the importance of social acceptance for AVs' success.

Anton Manfreda et al. (2021) explored the millennials' adoption of autonomous vehicles (AVs) within the context of smart cities, where information and communication technology play a crucial role. It investigates factors such as technology adoption, perceived benefits, security, safety, and mobility-related efficiencies as key determinants of AV adoption among millennials.

Artificial intelligence (AI) is transforming the transportation sector, particularly with regard to Intelligent Transportation Systems. Lakshmi Shankar Iyer (2021) reviewed about how governments and corporations have benefited from AI's ability to process massive information, growth in machine learning, IoT, robotics, computer vision, and natural language processing.

Xuan Di et al. (2021) discussed about fundamental assessment of the integration of artificial intelligence (AI) models and methodology in transportation engineering, specifically for autonomous vehicle (AV) control in mixed traffic scenarios. It covers the four stages of AV deployment, with a focus on phases involving both human-driven and autonomous vehicles.

Ali Alsalman et al. (2021) discussed the rapidly changing AV scene and the anticipated switch to electric vehicles (EVs). The current state of EVs is examined, along with the availability of charging stations, how long it takes to charge them, and their range.

Yunpeng Wang et al. (2020) addressed challenges such as spatiotemporal constraints at unsignalized intersections, multi-objective trajectory optimization, and diverse decision-making behaviours of CAVs. The approach includes conflict resolution at intersections, optimizing trajectories for safety, energy efficiency, and ride comfort, and a composite route planning strategy accommodating heterogeneous CAV decision-making.

Josue Ortega et al. (2020) studied the overtaking manoeuvres by Autonomous Vehicles (AVs) on the road, a challenging task involving acceleration, deceleration, and lane changes. The study utilizes simulation software, Pre-Scan, Adaptive Cruise Control (ACC) and Technology Independent Sensors (TIS) to simulate AVs' overtaking in an urban environment.

Santhanakrishnan Narayanan et al. (2020) work addressed the growing interest in Shared Autonomous Vehicles (SAVs) and offers a comprehensive overview of the field. It focuses on reviewing the anticipated impacts of SAVs across seven categories: Traffic & Safety, Travel behaviour, Economy, Transport supply, Land-use, Environment, and Governance.

Connected and Autonomous Vehicles (CAVs) have the potential to transform urban mobility but face significant privacy and cybersecurity challenges. Na Liu et al. (2020) examined user acceptance in the context of CAVs. Key themes include awareness, education for users and vendors, safety, responsibility, legislation, and trust.

Dasom Lee et al. (2020) examined the safety and liability issues surrounding connected and automated vehicles (CAVs) in the context of evolving regulations and road traffic rules. It focuses on the rules for on-road testing in Australia, the United States, and Germany, as well as government policies in Victoria, Australia, and California, the United States.

Jing et al (2020) explored factors influencing public acceptance of autonomous vehicles (AVs), a critical aspect for their adoption. Seven factors, including perceived ease of use, attitude, social norm, trust, perceived usefulness, perceived risk, and compatibility, were identified, with behavioral theories supporting their significance.

Pranav Kumar Singh et al. (2019) provided a comprehensive survey of vehicular communication, a critical area of research with applications in safety, infotainment, mobility, and the environment. It covers the latest advancements and future research directions in this field. The article discusses architecture,

ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/ , IJRDES, Vol. 5, Issue 3, 2023 , https://doi.org/10.63328/IJRDES-V5RI3P13

applications, emerging radio access technologies, standardization, and project activities in vehicular communication.

This article looks into the Internet of Vehicles (IoV), which enhances transportation systems by fusing Vehicle Ad-Hoc Networks (VANETs) and the Internet of Things (IoT). Surbhi Sharma et al. (2019) investigated IoV applications, evaluates IoV and VANETs, and highlights security issues in IoT systems. The paper discusses existing security solutions and their shortcomings while covering security requirements, difficulties, and threats in IoV.

David Elliott et al. (2019) addressed key aspects of Connected and Automated Vehicles (CAVs) research. It covers inter-CAV communications, security, intersection control, collision avoidance, and pedestrian detection.

Muhammad Arif et al. (2019) discussed the evolution of Intelligent Transportation Systems (ITS) into data-driven ITS, focusing on Vehicular Ad hoc Networks (VANETs). VANETs, a subset of mobile ad hoc networks, involve smart vehicles, roadside units (RSUs), and onboard units (OBUs) communicating via unreliable wireless connections.

Ransford A. Acheampong et al. (2019) study examined the essential problem of public acceptability of autonomous vehicles (AVs) and the factors influencing people's choices to use AVs for private, shared, and public transportation. The study develops four conceptual frameworks that take into account latent behavioural aspects such perceived benefits, ease of use, phobias, subjective norms, and environmental attitudes as well as socio-demographic data.

Ying He et al. (2019) addressed the security challenges in Cognitive Radio Vehicular Ad Hoc Networks (CR-VANETs) by proposing a unified trust management framework. It identifies a new attack called Joint Spectrum Sensing and Data Transmission (JSSDT) attack, which involves fake sensing data and dropped packets.

Platoon safety and communication integrity may be compromised by malicious attacks such as message spoofing, denial of service assaults, burst transmission, and message falsification. Alberto Petrillo et al. (2018) suggested a collaborative control approach to improve platoon defence against these dangers, which is supported by analytical and experimental techniques.

Margarita Martínez-Díaz et al. (2018) discussed technical difficulties, traffic control, and moral and ethical issues in autonomous driving. Even though the development of AVs has advanced significantly, obstacles must still be detected at high speeds, cooperative vehicle behaviour must be addressed, and legal concerns like liability and privacy must be addressed.

Alberto Petrillo et al. (2018) discussed the difficulty of creating secure automated platooning systems that rely on wireless communication and dispersed control systems. It introduces a brand-new distributed adaptive collaborative control approach that makes use of data from linked cars to achieve leader synchronization.

Alessandro Salvi et al. (2017) decentralized consensus technique for platooning non-identical vehicles with diverse communication delays across time is presented. Drivetrain dynamics are modelled in the control protocol as third-order linear systems with state feedback. By calculating the delay margin and decay rate, it sets the required and sufficient conditions for convergence and exponential stability.

Hamssa Hasrouny et al. (2017) thoroughly discussed the security concerns of vehicular ad hoc networks (VANETs). It begins by giving a thorough overview of the VANET security characteristics, difficulties, and needs while highlighting the necessity of a secure VANET architecture. Second, it offers a brand-new taxonomy of different VANET threats and the solutions that go with them. Finally, the article contrasts various strategies using standards for security in VANETs.

Mohamed Nidhal Mejri et al. (2014) evaluated the privacy and security issues that are particular to these networks and provide a summary of their communication architecture. The study classifies current security concerns in VANETs and looks at cryptographic solutions put forth to address these issues.

The application of classification methods for intrusion detection in Mobile Ad-hoc Networks (MANETs) is examined by Aikaterini Mitrokotsa et al. (2013) in this research. Five supervised classification algorithms are evaluated in the study while taking into account a range of traffic patterns, mobility patterns, and attack scenarios.

3. Experimental Procedure

The Clearly state the objectives of the study, such as gaining an understanding of the public's attitudes and concerns regarding autonomous vehicles (AVs).

Select a representative and varied sample of respondents from a range of demographic groups (e.g., age, gender, geography, etc.).

Obtain informed consent from each participant by explaining the study's objectives.

ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/ , IJRDES, Vol. 5, Issue 3, 2023 , https://doi.org/10.63328/IJRDES-V5RI3P13

Create a thorough survey that covers a range of AV-related topics, including public acceptance, safety, privacy, and cybersecurity.

To find and fix any uncertain sections or problems, conduct a small-group pilot test of the survey.
Conduct focus groups, interviews, or surveys for the chosen individuals to distribute the questionnaire.

Determine trends, concerns, and attitudes towards AVs through a quantitative and qualitative analysis of the data that has been collected.

Asking questions on observed hazards, potential benefits, and trust in AV technology could assist researchers evaluate participants' views on AV safety.

Asking questions regarding the data gathering, sharing, and surveillance associated with AVs can help evaluate participants' privacy concerns.

Find out how much the participants understand about the potential cybersecurity risks in AVs and what they think about the corresponding security measures.

Analyse responses related to the willingness to use AVs and the factors influencing this acceptance in order to assess the general level of public acceptability of AVs.

Analyse the quantitative data using statistical software and techniques, such as regression modelling, correlation analysis, and descriptive statistics.

To find out more about the viewpoints of participants, conduct a thematic analysis of qualitative data collected through focus groups, interviews, and open-ended questions.

Analyse the data and make judgments regarding cybersecurity awareness, privacy concerns, security concerns, and public perceptions of AVs.

Create a thorough report with the findings and observations, along with ideas for researchers, industry stakeholders, and policymakers.

Make sure that all ethical guidelines are followed during the study, keeping participant anonymity and privacy into consideration.

To promote AV technology and public awareness, distribute the research findings through reports, presentations, and academic publications.

4. Result and Discussion

The study focuses at how the public feels about autonomous vehicles (AVs) within modern transportation networks, having a focus on cybersecurity, safety, acceptance, and privacy. The results show varying levels of acceptance, with concerns about safety having a major impact on public opinion.

Concerns about cybersecurity and privacy also have an impact on public opinion, which highlights how important it is that these issues be taken into account while developing new security software. These findings show that in order to increase public trust in AV technology, extensive education and awareness initiatives are necessary. Collaboration between parties is crucial for the creation of efficient cybersecurity safeguards and guaranteeing that AVs adhere to privacy and safety regulations.

Some of the applications of this study are given below.

- Create educational initiatives and public awareness campaigns to educate people about the advantages and safety features of autonomous vehicles.
- To give consumers peace of mind that their personal information is safe, autonomous car systems should incorporate cutting-edge privacy protection measures.
- Provide AV operators and manufacturers with training programs to improve their cybersecurity knowledge and safeguard against possible cyberattacks.
- To gain the trust of prospective AV users, implement transparency measures including providing safety data and cybersecurity procedures.
- Work alongside governments to create thorough legislative frameworks that cover cybersecurity, privacy, and safety requirements for self-driving cars.

5. Conclusion

Concerning cybersecurity, the employment of autonomous vehicles (AVs) in cutting-edge transportation networks is a possibility. The study's findings and observations shed light on the various advantages and challenges associated with the adoption of AV. It is evident that a key factor in assessing AV viability is public approval. When creating strategies for the deployment of AV, it is imperative to comprehend and effectively handle public opinions, concerns, and expectations. Building confidence among producers, policymakers, and the public requires education, awareness-raising, and effective channels of communication. Safety is the top focus. Autonomous vehicles (AVs) possess the capacity to

ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/ , IJRDES, Vol. 5, Issue 3, 2023 , https://doi.org/10.63328/IJRDES-V5RI3P13

considerably reduce accidents; nevertheless, prior to realizing these safety benefits, it is imperative to surmount technological obstacles, provide dependable cybersecurity, and establish accountability structures. Another complex issue is privacy, given the massive volume of data generated by AVs. Finding the ideal balance between privacy protection and the advantages of data-driven services requires rigorous planning and regulation.

Critical for the final foundation is cybersecurity. AVs are susceptible to assaults because of their connectivity, thus robust security measures are necessary to protect users and the system of transportation. Stakeholder cooperation, ongoing research, and adaptable security frameworks are crucial in this context. In conclusion, the effectiveness of AVs in current transportation systems depends on addressing public concerns, enhancing safety procedures, safeguarding personal data, and enhancing cybersecurity. Governments, business, academia, and the general public must work together to develop a cooperative, multidisciplinary strategy in order to overcome these challenges and realize the revolutionary potential of autonomous vehicles.

References

[1]. Lakshmi Shankar Iyer, AI enabled applications towards intelligent transportation, Transportation Engineering, Volume 5, 2021, https://doi.org/10.1016/j.treng.2021.100083.

[2]. Kareem Othman, Public acceptance and perception of autonomous vehicles: a comprehensive review, AI and Ethics, Volume 1, 2021, https://doi.org/10.1007/s43681-021-00041-8.

[3]. Xuan Di, Rongye Shi, A survey on autonomous vehicle control in the era of mixed-autonomy: From physics-based to AI-guided driving policy learning, Transportation Research Part C: Emerging Technologies, Volume 125, 2021, https://doi.org/10.1016/j.trc.2021.103008.

[4]. Gopindra S. Nair, Chandra R. Bhat, Sharing the road with autonomous vehicles: Perceived safety and regulatory preferences, Transportation Research Part C: Emerging Technologies, Volume 122, 2021 https://doi.org/10.1016/j.trc.2020.102885.

[5]. Josue Ortega, Henrietta Lengyel, Zsolt Szalay, Overtaking maneuver scenario building for autonomous vehicles with PreScan software, Transportation Engineering, Volume 2, 2020 , https://doi.org/10.1016/j.treng.2020.100029.

[6]. 6. Na Liu, Alexandros Nikitas, Simon Parkinson, Exploring expert perceptions about the cyber security and privacy of Connected and Autonomous Vehicles: A thematic analysis approach, Transportation Research Part F: Traffic Psychology and Behaviour, Volume 75, 2020, https://doi.org/10.1016/j.trf.2020.09.019.

[7]. Dasom Lee, David J. Hess, Regulations for on-road testing of connected and automated vehicles: Assessing the potential for global safety harmonization, Transportation Research Part A: Policy and Practice, Volume 136, 2020, Pages 85-98, https://doi.org/10.1016/j.tra.2020.03.026.

[8]. Jing, Peng and Xu, Gang and Chen, Yuexia and Shi, Yuji and Zhan, Fengping, The determinants behind the acceptance of autonomous vehicles: A systematic review, Sustainability, Volume 12 ,2020, pages 17-19, https://doi:10.3390/su12051719.

[9]. Ali Alsalman, Lateef N. Assi, Shabnam Ghotbi, SeyedAli Ghahari, Ali Shubbar, Users, planners, and governments perspectives: A public survey on autonomous vehicles future advancements, Transportation Engineering, Volume 3, 2021, https://doi.org/10.1016/j.treng.2020.100044.

[10]. Yunpeng Wang, Pinlong Cai, Guangquan Lu, Cooperative autonomous traffic organization method for connected automated vehicles in multi intersection road networks, Transportation Research Part C: Emerging Technologies, Volume 111, 2020, Pages 458-476, https://doi.org/10.1016/j.trc.2019.12.018.

[11]. Pranav Kumar Singh, Sunit Kumar Nandi, Sukumar Nandi, A tutorial survey on vehicular communication state of the art, and future research directions, Vehicular Communications, Volume 18, 2019, https://doi.org/10.1016/j.vehcom.2019.100164.

[12]. Surbhi Sharma, Baijnath Kaushik, A survey on internet of vehicles: Applications, security issues & solutions, Vehicular Communications, Volume 20, 2019, https://doi.org/10.1016/j.vehcom.2019.100182.

[13]. Santhanakrishnan Narayanan, Emmanouil Chaniotakis, Constantinos Antoniou, Shared autonomous vehicle services: A comprehensive review, Transportation Research Part C: Emerging Technologies, Volume 111, 2020, Pages 255-293, https://doi.org/10.1016/j.trc.2019.12.008.

[14]. Anton Manfreda, Klara Ljubi, Aleš Groznik, Autonomous vehicles in the smart city era: An empirical study of adoption factors important for millennials, International Journal of Information Management, Volume 58, 2021, https://doi.org/10.1016/j.ijinfomgt.2019.102050.

[15]. David Elliott, Walter Keen, Lei Miao, Recent advances in connected and automated vehicles, Journal of Traffic and Transportation Engineering (English Edition), Volume 6, Issue 2, 2019, Pages 109-131, https://doi.org/10.1016/j.jtte.2018.09.005.

[16]. Muhammad Arif, Guojun Wang, Md Zakirul Alam Bhuiyan, Tian Wang, Jianer Chen, A survey on security attacks in VANETs: Communication, applications and challenges,

ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/ , IJRDES, Vol. 5, Issue 3, 2023 , https://doi.org/10.63328/IJRDES-V5RI3P13

Vehicular Communications, Volume 19, 2019, https://doi.org/10.1016/j.vehcom.2019.100179.

[17]. Ransford A. Acheampong, Federico Cugurullo, Capturing the behavioural determinants behind the adoption of autonomous vehicles: Conceptual frameworks and measurement models to predict public transport, sharing and ownership trends of self-driving cars, Transportation Research Part F: Traffic Psychology and Behaviour, Volume 62, 2019, Pages 349-375, https://doi.org/10.1016/j.trf.2019.01.009.

[18]. Alberto Petrillo, Antonio Pescapé, Stefania Santini, A collaborative approach for improving the security of vehicular scenarios: The case of platooning, Computer Communications, Volume 122, 2018, Pages 59-75, https://doi.org/10.1016/j.comcom.2018.03.014.

[19]. Ying He, F. Richard Yu, Zhexiong Wei, Victor Leung, Trust management for secure cognitive radio vehicular ad hoc networks, Ad Hoc Networks, Volume 86, 2019, Pages 154-165, https://doi.org/10.1016/j.adhoc.2018.11.006.

[20]. Margarita Martínez-Díaz, Francesc Soriguera, Autonomous vehicles: theoretical and practical challenges, Transportation Research Procedia, Volume 33, 2018, Pages 275-282, https://doi.org/10.1016/j.trpro.2018.10.103.

[21]. Alessandro Salvi, Stefania Santini, Antonio Saverio Valente, Design, analysis and performance evaluation of a third order distributed protocol for platooning in the presence of time-varying delays and switching topologies, Transportation Research Part C: Emerging Technologies, Volume 80, 2017, Pages 360-383, https://doi.org/10.1016/j.trc.2017.04.013.

[22]. Alberto Petrillo, Alessandro Salvi, Stefania Santini, Antonio Saverio Valente, Adaptive multi-agents synchronization for collaborative driving of autonomous vehicles with multiple communication delays, Transportation Research Part C: Emerging Technologies, Volume 86, 2018, Pages 372-392, https://doi.org/10.1016/j.trc.2017.11.009.

[23]. Hamssa Hasrouny, Abed Ellatif Samhat, Carole Bassil, Anis Laouiti, VANet security challenges and solutions: A survey, Vehicular Communications, Volume 7, 2017, Pages 7-20, https://doi.org/10.1016/j.vehcom.2017.01.002.

[24]. Mohamed Nidhal Mejri, Jalel Ben-Othman, Mohamed Hamdi, Survey on VANET security challenges and possible cryptographic solutions, Vehicular Communications, Volume 1, Issue 2, 2014, Pages 53-66, https://doi.org/10.1016/j.vehcom.2014.05.001.

[25]. Aikaterini Mitrokotsa, Christos Dimitrakakis, Intrusion detection in MANET using classification algorithms: The effects of cost and model selection, Ad Hoc Networks, Volume 11, Issue 1, 2013, Pages 226-237, https://doi.org/10.1016/j.adhoc.2012.05.006.