Instituto Superior Politécnico Gaya
www.ispgaya.pt
https://doi.org/10.58086/gtcy-wt23

BIBLIOMETRIC STUDY ON THE DEVELOPMENT AND IMPLEMENTATION OF CYBERSECURITY IN AUTONOMOUS VEHICLES

Henrique Teixeira[1]

Mário Lousã[2]

José Morais[3]

Abstract

The main objective was to examine the trajectory of scientific research in this domain, identify the most influential publications related to cybersecurity in autonomous vehicles and pinpoint research opportunities, supported by the PRISMA method. Additionally, the study explores cybersecurity themes in autonomous vehicles, emphasizing the significance of concepts like blockchain, machine learning, and deep learning essential in formulating business strategies. Furthermore, the research identifies influential scientific publications, predominant journals, the most productive countries, and authors with the most publications on cybersecurity in autonomous vehicles. It identifies research opportunities organized into two distinct clusters to provide a comprehensive understanding of the current state of research in this field and offer insights for companies and academics interested in contributing to future advancements in the cybersecurity of autonomous vehicles. The article demonstrates that cybersecurity is a fundamental area for the development and implementation of secure and reliable autonomous vehicles.

Keywords: V2X (vehicles-to-everything) network security; 5G and 6G; mobility security; communication network security; attack prevention.

ESTUDO BIBLIOMÉTRICO SOBRE O DESENVOLVIMENTO E IMPLEMENTAÇÃO DA CIBERSEGURANÇA EM VEÍCULOS AUTÓNOMOS

Resumo

O objetivo principal foi examinar a trajetória da investigação científica neste domínio, identificar as publicações mais influentes relacionadas com a cibersegurança em veículos autónomos e identificar oportunidades de investigação, apoiadas pelo método PRISMA. Além disso, o estudo explora temas de segurança cibernética em veículos autónomos, enfatizando a importância de conceitos como blockchain, aprendizado de máquina e aprendizado profundo, essenciais na formulação de estratégias de negócios. Além disso, a pesquisa identifica publicações científicas influentes, periódicos predominantes, os países mais produtivos e os autores com mais publicações sobre segurança cibernética em veículos autónomos. Identifica oportunidades de investigação organizadas em dois clusters distintos para fornecer uma

[1] ISPGAYA, Instituto Superior Politécnico Gaya, Portugal

[2] CID ISPGAYA; ISPGaya /Instituto Superior Politécnico Gaya, Portuga

[3] CEOSP.PP; ISPGaya /Instituto Superior Politécnico Gaya, Portugal

https://doi.org/10.58086/gtcy-wt23

compreensão abrangente do estado atual da investigação neste campo e oferecer insights para empresas e académicos interessados em contribuir para avanços futuros na segurança cibernética de veículos autónomos. O artigo demonstra que a cibersegurança é uma área fundamental para o desenvolvimento e implementação de veículos autónomos seguros e fiáveis.

Palavras-chave: segurança de rede V2X (veículos para tudo); 5G e 6G; segurança da mobilidade; segurança de redes de comunicação; prevenção de ataques.

Introduction

Technological advances are profoundly redefining the autonomous vehicle landscape, influencing the way we move, and raising essential cybersecurity considerations. As interconnection and automation become integral parts of autonomous vehicles, new challenges and opportunities arise in ensuring cybersecurity (Bathla et al., 2022). The rapid pace of technological advances in the autonomous vehicle landscape raises critical cybersecurity considerations, making them increasingly susceptible to a wide range of cyber threats (Sun et al., 2022). The growing dependence on various autonomous systems and their interaction with intelligent systems in urban traffic infrastructure has further expanded the threat landscape, making cybersecurity a growing concern (Chattopadhyay et al., 2021).

There are several factors that influence the adoption of autonomous vehicles, where efficiency and trust in technologies play essential roles. Acheampong and Cugurullo (2019) state that vehicle efficiency, convenience, driving experience, and trust in autonomous technologies are crucial for the acceptance and adoption of these technologies. By prioritizing cybersecurity in autonomous vehicles, businesses and the automotive industry can strengthen their strategies for responding to cybersecurity threats. The growing presence of digital capabilities through 6G technology requires a robust approach to ensure the continued safety of autonomous vehicles (Algarni & Thayananthan, 2023).

This paper aims to guide future research on crucial elements contributing to the advancement of the cybersecurity concept in autonomous vehicles. Divided into four parts, it reviews the current literature on cybersecurity in this context, presents the methodology used, analyzes the results obtained from bibliometric analysis, and concludes with final considerations. This article is supported by bibliometric analysis, focusing on cybersecurity in autonomous vehicles, and seeks to answer the following four questions:

- RQ1: How has the concept of cybersecurity in autonomous vehicles evolved in academic research over the past 20 years?
- RQ2: What are the most influential scientific publications on cybersecurity in autonomous vehicles?

https://doi.org/10.58086/gtcy-wt23

– RQ3: What are the main authors and papers in scientific publications on cybersecurity in autonomous vehicles?
– RQ4: What are the main focuses of research in the field of cybersecurity in autonomous vehicles?

2. Literature review

2.1. Cybersecurity

Cybersecurity has received significant attention in recent years due to the increasing number of threats and continuous efforts by cybercriminals to overcome security barriers. According to Taherdoost (2022), the process involves protecting sensitive data against unauthorized access, damage, or theft. Sabillon (2018) defines cybersecurity as the protection of information assets, dealing with threats to information processed, stored, and transported by interconnected information systems. Additionally, Sallos et al. (2019) tells us that cybersecurity is increasingly being recognized as a "knowledge problem," emphasizing the need to understand vectors, mechanisms, and trends related to knowledge to address cybersecurity challenges.

As the digital landscape continues to evolve, the importance of cybersecurity in various domains such as health, critical infrastructure, and the automotive industry has become increasingly prominent. Cybersecurity, in the digital era, stands out for its importance and complexity, increased by its interdisciplinary nature. Its areas of application are diverse, from industry to education and health. For example, according to Gordon et al. (2022), cybersecurity is identified as a necessity for the provision of reliable healthcare, especially in the context of robotic surgery. In the automotive industry, according to Wang et al. (2021), there has been an increase in the development of solutions to address increasing incidents of security threats. At the same time, several cybersecurity practices emerged, presenting variations between different industrial areas regarding risks and respective mitigations (Héroux & Fortin, 2020).

2.2. Autonomous vehicles

Autonomous vehicles can transform urban transportation systems, providing safer roads, improving mobility, and enhancing traffic efficiency (Li et al., 2022). According to Qu et al. (2022), autonomous vehicles are equipped with sensors that can perceive environmental information to make informed decisions. For example, lane change is the most common scenario (Wu et al., 2020). In the decision-making process, Guo (2023) states that continuous learning is frequent, incorporating risk awareness and replicating human behaviors to ensure intuitive understanding by other road users.

https://doi.org/10.58086/gtcy-wt23

The implementation of autonomous vehicles raises important considerations in terms of policies, responsibility, and security (Alheeti et al., 2016). According to Nees (2016), there is a need for policies and changes in infrastructure to prepare cities for the integration of autonomous vehicles into existing urban transportation systems. Additionally, Nyholm and Smids (2016) ensure that the security of autonomous vehicles and their communication networks is crucial to preventing intrusions and attacks. Autonomous vehicles, according to Muhammad et al. (2020), have the potential to significantly impact road transportation systems, traffic flow, and user acceptance.

Table 1 summarizes the concepts of cybersecurity and autonomous vehicles.

Table 1
Cybersecurity and Autonomous Vehicles Concepts

Concept	Description	Authors
Cybersecurity	Refers to a set of activities and other measures aimed at protecting computers, computer networks, hardware, related devices, software, and the information they contain and communicate, as well as other elements in cyberspace, from attacks, disruptions, or other threats.	Fischer, 2016; Reegård et al., 2019; Veale et al., 2020
Autonomous Vehicles	Refers to vehicles capable of operating and moving without the need for direct human intervention. The autonomy of vehicles can vary at different levels, from driver assistance to complete autonomy, where the vehicle can travel the entire route without requiring human intervention.	Kato et al., 2015; Wachenfeld & Winner, 2016; J. Wang et al., 2020

3. Methodology

Bibliometric analysis is a valuable tool for assessing the impact and influence of scientific production in various areas. It involves, for example, the statistical analysis of published articles and their citations to measure their impact (Baraibar-Diez et al., 2020). However, it is important to note that bibliometric analysis has limitations. It is retrospective in nature, and developments in the literature only become apparent after some time has passed (Coombes, 2023). Bibliometric analysis methods are employed to provide a comprehensive perspective on published scientific articles. This approach is based on processing bibliometric data collected from databases such as Scopus, The Lens, or Web of Science. In recent years, there has been an increase in the application of bibliometric methods in research papers, driven by their reliability and, above all, their effectiveness (Mukherjee et al., 2022).

The methodological foundation of this bibliometric analysis was established using the PRISMA method, which provides a set of guidelines for the preparation of systematic reviews and meta-analyses (Page et al., 2023).

To carry out this study, the database selected was The Lens, a free and accessible data source containing 151.9 million patents and 266.4 million scientific articles and research works in various areas (The Lens, n.d.).

https://doi.org/10.58086/gtcy-wt23

The keywords "cybersecurity" and "autonomous vehicles" were used for the complex boolean search, employing the AND and OR operators between the two expressions to encompass more literature. The analysis focused on the last 20 years, restricting publications to the period between 2004 and 2023. To obtain more specific results for this study, subjects such as "Control and Systems Engineering," "Automotive Engineering," and "Computer Networks and Communications" were selected, along with the study fields "computer science," "engineering," "computer security," "Control (management)," and "Control engineering," resulting in a total of 3028 publications. For the analysis and visualization of the obtained data, VOSviewer version 1.6.19 software and The Lens analysis tool were used.

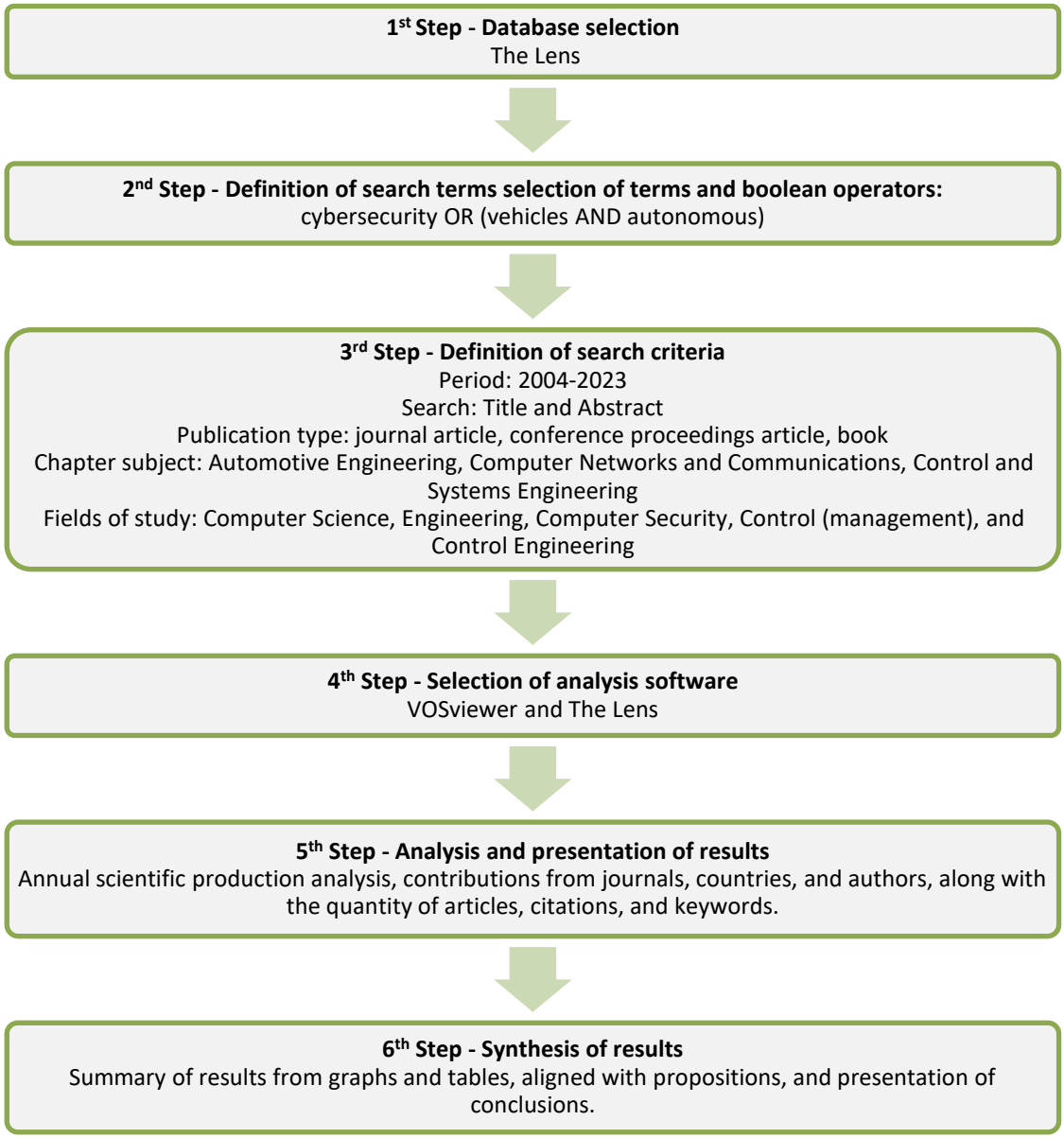
The analysis covers the distribution of publications over the 20 years analyzed, identifying the five types of considered documents: books, conference proceedings, book chapters, journal articles, and conference papers. The top 10 journals contributing the most publications, the top 10 countries with the highest production, the top 10 prominent authors, and the top 10 most cited articles are highlighted. Finally, co-authorship analysis, co-citation analysis, keyword analysis, and cluster analysis of keywords are part of stage five (cf. Figure 1).

Figure 1 presents the methodology used in the research, based on the PRISMA method, consisting of six stages (database selection; definition of search terms and Boolean terms and operators; definition of search criteria; selection of analysis software; analysis and presentation of results; synthesis of results).

https://doi.org/10.58086/gtcy-wt23

Figure 1

Methodology



4. Analysis

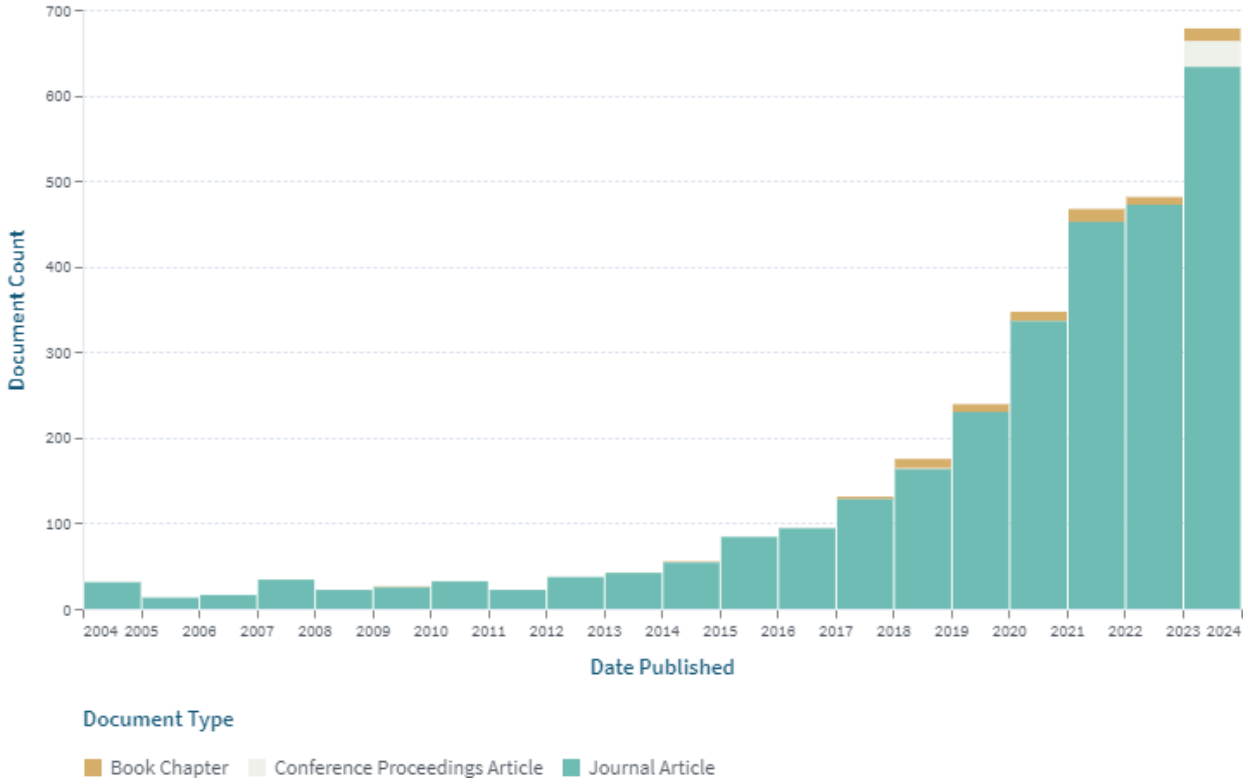
4.1. Evolution of academic research over the last 20 years on the concept of cybersecurity in autonomous vehicles (RQ1)

This study covers a total of 3280 documents over a 20-year period, spanning from 2004 to 2023. Figure 2 illustrates the annual volume of scientific production resulting from the conducted research, considering the elements presented in steps 2 and 3 of Figure 1. Thus, it is possible to observe an increase in annual scientific production on the topic of "Cybersecurity in Autonomous Vehicles". In 2004, 31 documents were published, while in 2023, this number rose to 678, representing a growth of 2187%, with a steady annual increase from 2011 onwards.

https://doi.org/10.58086/gtcy-wt23

Figure 2

Evolution of the number of publications by document type



4.2. Most influential scientific publications on cybersecurity in autonomous vehicles (RQ2)

The results indicate that 3028 documents were published in 110 different journals, with the top 10 representing 82% of the total with 2484 publications (cf. Figure 2 and Table 2). IEEE occupies first place with 909 publications in the areas of engineering, automotive industry, and security.

Table 2

Top 10 Journals by Number of Publications

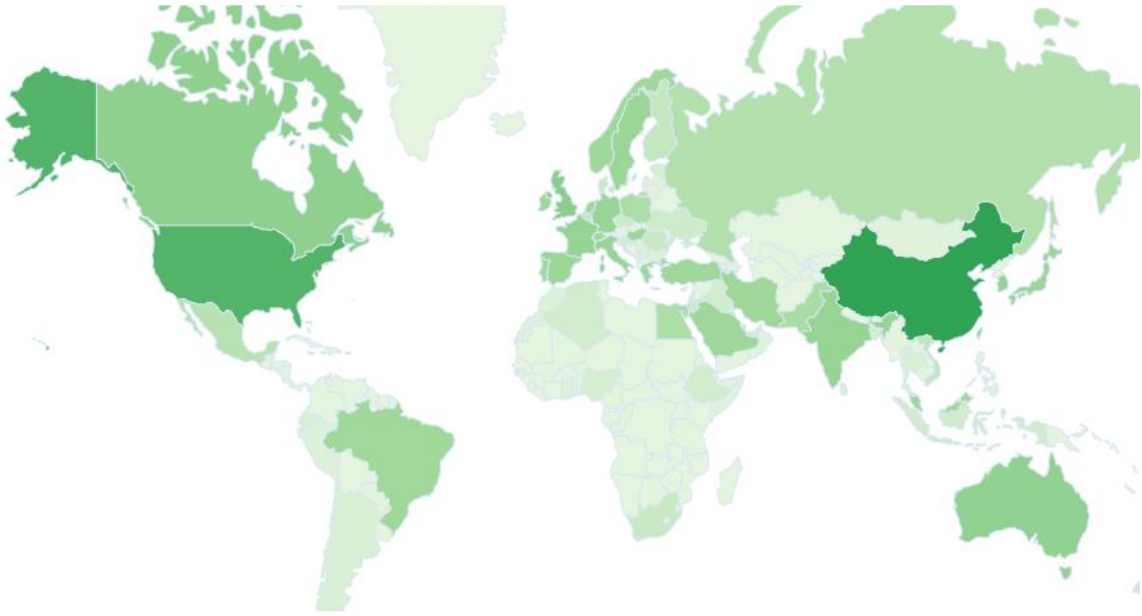
Journal	Fields	Number of publications
Institute of Electrical and Electronics Engineers (IEEE)	Engineering; Automotive Industry; Security.	909
Elsevier BV	Academic and Governmental; Health; Industry.	592
Springer Science and Business Media LLC	Engineering; Medicine; Computing; Mathematics.	221
MDPI AG	Computing; Mathematics; Behavioral Science.	220
Wiley	Computing and Technology; Earth, Spaces, and Environment.	135
Hindawi Limited	Mathematics, Engineering, and Computing; Social Sciences and Education.	94
Informa UK Limited	Science, Technology, and Medicine; Humanities and Social Sciences.	92

https://doi.org/10.58086/gtcy-wt23

Journal	Fields	Number of publications
Inderscience Publishers	Computer Science and Mathematics; Risk Management, Security, and Emergencies; Science, Engineering, and Technology.	82
Institute of Electrical and Electronics Engineers Inc.	Engineering; Automotive Industry; Security.	81
Emerald	Sustainability; Health; Mathematics.	55

In Figure 4, it shows the most active countries in the production of scientific publications in this area, highlighting China and the United States of America with the highest number of publications.

Figure 4
Scientific Production by Country



Complementing the representation in Figure 4, Table 3 shows the top 10 leading countries in terms of production in research dedicated to the topic of cybersecurity in autonomous vehicles.

Table 3
Top 10 Countries with the greatest number of publications

Country	Number of publications
China	876
USA	611
United Kingdom	188
Canada	148
Australia	143
Republic of Korea	110
France	88
India	86
Germany	80
Italy	74

https://doi.org/10.58086/gtcy-wt23

4.3. Main authors and papers of scientific publications on cybersecurity in autonomous vehicles (RQ3)

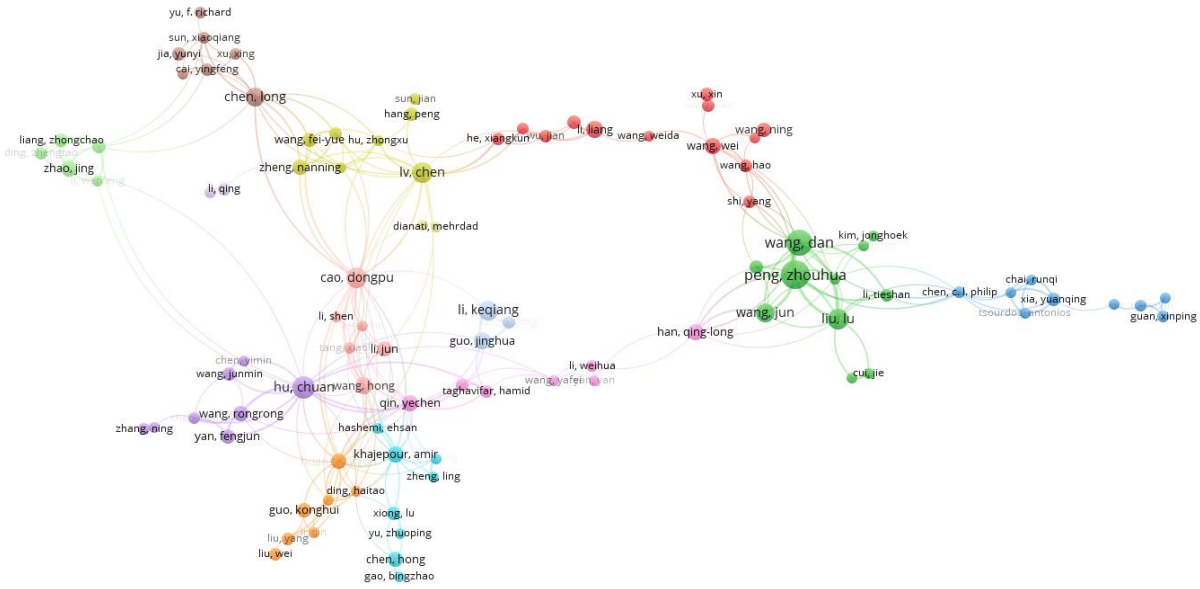
Table 4 highlights the main authors in scientific production, revealing Dan Wang as the most productive author with twenty-six publications. Following, Zhouhua Peng and Chuan Hu appear with twenty-five and eighteen publications, respectively. It is observed that many of the authors presented in Table 4 are from the Asian continent, especially China, indicating their leadership in scientific production in the context of research that addresses the terms “cybersecurity” or “autonomous vehicles”.

Table 4
Number of Published Articles per Author

Authors	Number of publications	Affiliation
Dan Wang	26	Dalian Maritime University, China
Zhouhua Peng	25	Dalian Maritime University, China
Chuan Hu	18	Southeast University, China
Chen Lv	17	Nanyang Technological University, China
Keqiang Li	12	Tsinghua University, China
Amir Khajepour	11	Beijing Institute of Technology, China
Balázs Németh	11	Hungarian Academy of Sciences, Hungary
Bidyadhar Subudhi	10	National Institute of Technology, India
Amr Mohamed	9	University of Ontario Institute of Technology, Canada
António M Pascoal	8	University of Lisbon, Portugal

According to Zupic and Čater (2015), the co-authorship method can reveal patterns of collaboration and productivity among researchers. A total of 173 authors were found in the context of the analysis, each having at least five published documents. Out of these authors, 96 were selected, divided into 14 clusters, with a total of 260 connections. Figure 5 demonstrates the connections among them. The green cluster features the author with the most co-authorships, Zhouhua Peng.

Figure 5
Author Relationships per Document



https://doi.org/10.58086/gtcy-wt23

The articles with the highest number of citations are "Planning and decision-making for autonomous vehicles" (Schwarting et al., 2018), with 538 citations, and "Perception, planning, control, and coordination for autonomous vehicles" (Pendleton et al., 2017), with 403 citations. It is also noted that the most cited paper is the one with the highest average annual citations (107.6).

Table 5
Top 10 Most cited papers

Article	Year of publication	Citations	Average*
Chwarting, W., Alonso-Mora, J., & Rus, D. (2018). Planning and decision-making for autonomous vehicles. *Annual Review of Control, Robotics, and Autonomous Systems, 1*(1), 187–210.	2018	538	107.6
Pendleton, S., Andersen, H., Du, X., Shen, X., Meghjani, M., Eng, Y., Rus, D., & Ang, M. (2017). Perception, planning, control, and coordination for autonomous vehicles. *Machines, 5*(1), 6.	2017	403	67.2
Arslan, G., Marden, J. R., & Shamma, J. S. (2007). Autonomous vehicle-target assignment: A game-theoretical formulation. *Journal of Dynamic Systems, Measurement, and Control, 129*(5), 584–596.	2007	374	23.4
Amer, N. H., Zamzuri, H., Hudha, K., & Kadir, Z. A. (2017). Modelling and control strategies in path tracking control for autonomous ground vehicles: A review of state of the art and challenges. *Journal of Intelligent & Robotic Systems, 86*(2), 225–254.	2016	261	37.3
Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. *Journal of Big Data, 7*(1).	2020	235	78.3
Qiao, L., & Zhang, W. (2017). Adaptive non-singular integral terminal sliding mode tracking control for autonomous underwater vehicles. *IET Control Theory and Applications, 11*(8), 1293–1306.	2017	223	37.2
Peng, Z., Wang, D., Li, T., & Han, M. (2020). Output-feedback cooperative formation maneuvering of autonomous surface vehicles with connectivity preservation and collision avoidance. *IEEE Transactions on Cybernetics, 50*(6), 2527–2535.	2019	205	51.3
Faessler, M., Fontana, F., Forster, C., Mueggler, E., Pizzoli, M., & Scaramuzza, D. (2016). Autonomous, vision-based flight and live dense 3D mapping with a quadrotor micro aerial vehicle. *Journal of Field Robotics, 33*(4), 431–450.	2015	193	24.1
Yuan, C., Licht, S., & He, H. (2018). Formation learning control of multiple autonomous underwater vehicles with heterogeneous nonlinear uncertain dynamics. *IEEE Transactions on Cybernetics, 48*(10), 2920–2934.	2017	193	32.2
Bingham, B., Foley, B., Singh, H., Camilli, R., Delaporta, K., Eustice, R., Mallios, A., Mindell, D., Roman, C., & Sakellariou, D. (2010). Robotic tools for deep water archaeology: Surveying an ancient shipwreck with an autonomous underwater vehicle. *Journal of Field Robotics, 27*(6), 702–717.	2010	183	14.1

* The average was calculated based on the interval between the year of publication and the year 2023.

https://doi.org/10.58086/gtcy-wt23

4.4. Main areas of research on cybersecurity in autonomous vehicles (RQ4)

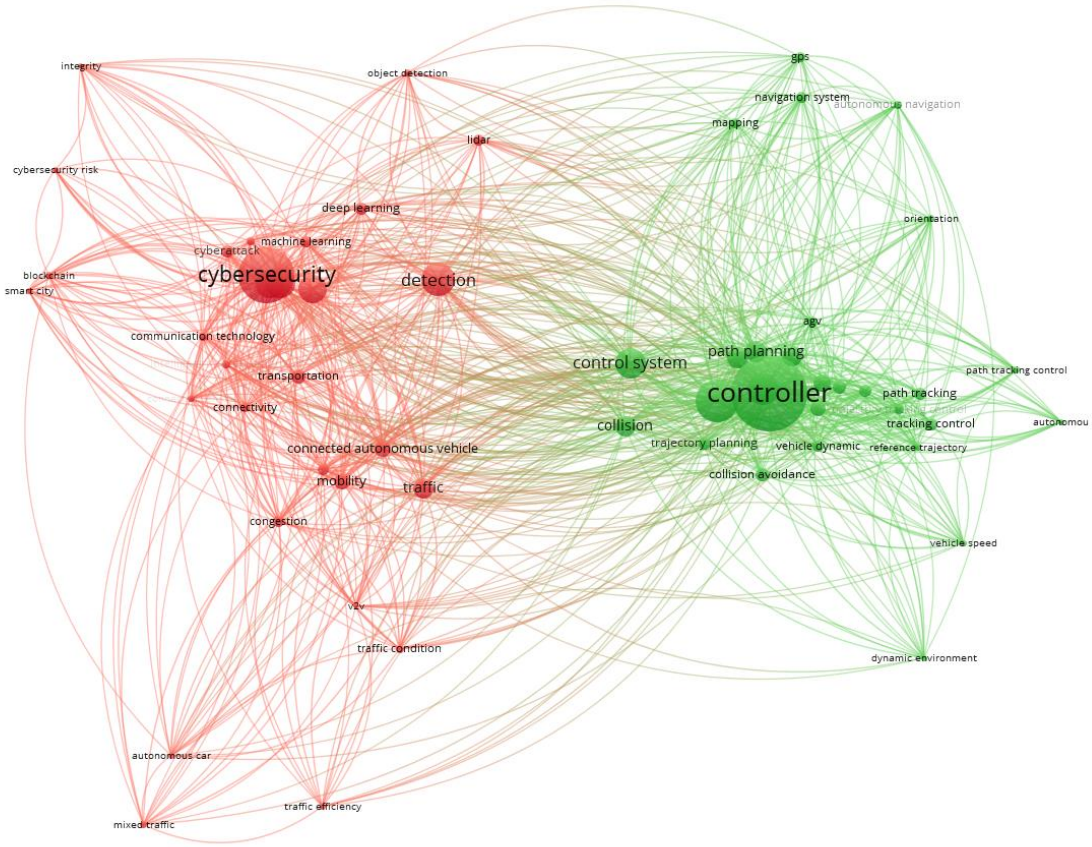
The co-occurrence analysis of the authors' keywords is presented in Figure 6, reflecting the strong connection between cybersecurity and the control system. Keywords with a minimum occurrence of 20 were considered, resulting in a total of 59 keywords distributed across two clusters (cf. Figure 6 and Table 6). The most prominent cluster is the red one, with 30 keywords, where "cybersecurity" is the dominant keyword, recording 323 occurrences. In the green cluster, the keyword "controller" stands out, with 456 occurrences. Table 6 presents the two clusters (red and green) obtained and their respective keywords.

Table 6
Keywords per Cluster

Cluster	Keywords
1 - Red	“Attack”, “autonomous car”, “blockchain”, “cavs”, “communication technology”, “congestion”, “connected autonomous”, “connected vehicle”, “connectivity”, “cyber attack”, cyberattack”, “cybersecurity”, “cybersecurity risk”, deep learning”, “detection”, “integrity”, “inteligente transportation”, “lidar”, “machine learning”, “mixed traffic”, “mobility”, “object detection”, “security”, “smart city”, “threat”, “traffic”, “traffic condition”, “traffic efficiency”, “transportation” e “v2v”.
2 - Green	“agv”, “autonomou”, “autonomous ground vehicle”, “autonomous navigation”, “collision”, “collision avoidance”, “control law”, “control system”, “controller”, “dynamic environment”, “gps”, “mapping”, “navigation system”, “orientation”, “path planning”, “path tracking”, “path tracking control”, “proposed controller”, “reference trajectory”, “tracking”, “tracking control”, “trajectory”, “trajectory planning”, “trajectory tracking”, “trajectory tracking control”, “vehicle model”, “vehicle speed” e “velocity”.

https://doi.org/10.58086/gtcy-wt23

Figure 6
Keyword Co-occurrence Network



4.4.1. Cluster 1 – Red

The cluster presents keywords such as "attack", "detection", "traffic", "mobility", and "connected autonomous vehicle", which are interconnected with the context of this paper, specifically with cybersecurity.

According to Craigen et al. (2014), cybersecurity encompasses a wide range of tools, policies, concepts, and technologies aimed at protecting individuals, organizations, and governments from online threats. For Da Veiga (2016), cybersecurity is essential to protecting intelligent resources in cyberspace. Matheu et al. (2020) argue that cybersecurity involves the use of various technologies and protocols to connect physical devices to online infrastructure, especially in scenarios such as the Internet of Things. In this context, Karagiannis et al. (2022) state that the National Institute of Standards and Technology launched the National Initiative for Cybersecurity Education with the aim of providing a systematic framework for education and learning in cybersecurity and establishing concepts and practices adopted by professionals. According to Gcaza and von Solms (2017), the notion of cybersecurity is also linked to the urgency of safeguarding multiple resources simultaneously against a variety of cyber threats, influencing cybersecurity strategies and culture.

https://doi.org/10.58086/gtcy-wt23

To address cybersecurity concerns in connected Autonomous Vehicles (AVs), it is crucial to consider potential attacks, detection methods, traffic management, and the impact on mobility. For Liu et al. (2022), AVs are susceptible to various attacks, posing serious security risks. Detection of attacks in AVs can be achieved through advanced technologies such as blockchain or Bayesian attack graphs (Fu et al., 2022; Queralta et al., 2020). These technologies enhance autonomy and provide real-time data for precise location and environment updates, thus improving the detection of potential cyber threats. AVs have the potential to mitigate traffic congestion, increase road safety, and reduce fuel consumption and emissions (Montanaro et al., 2019). However, Martin-Gasulla et al. (2019) state that the initial incorporation of AVs with low penetration rates may result in more limited traffic capabilities. It is essential to develop comprehensive traffic analysis methods and traffic management strategies to ensure the gradual introduction of AVs into existing traffic systems (Zhou et al., 2022). Additionally, the connectivity of AVs, from vehicle to vehicle and infrastructure to vehicle, can significantly improve traffic management and safety by collecting information from nearby vehicles and infrastructures, enhancing their perception capabilities and decision-making processes (Yamazato, 2017).

4.4.2. Cluster 2 – Green

The cluster presents keywords such as "controller", "control system", "collision", "trajectory", "tracking", "path planning", and "autonomous ground vehicle" which are interconnected with the context of this article, specifically with autonomous vehicles.

The development of controllers for autonomous vehicles has increasingly improved their collision prevention capabilities (Tiwari et al., 2021). These controllers are essential to enable autonomous vehicles to navigate complex traffic scenarios and avoid collisions with other vehicles and obstacles (Lin et al., 2020). According to Matous et al. (2021), the development of collision prevention systems for autonomous vehicles has been a key area of development, aiming to provide these vehicles with the ability to react to sudden changes in their environment and avoid potential collisions. Additionally, Lin et al. (2020) highlights the importance of integrating trajectory replanning and vehicle-to-vehicle information interaction in collision prevention control systems. For Guo, J. et al. (2018), an adaptive trajectory control approach based on neural networks was proposed for autonomous vehicle collision prevention control systems, demonstrating stability using Lyapunov theory.

However, Evtukov et al. (2018) argue that attention should be focused on addressing cybersecurity vulnerabilities to prevent external interference with the control unit of an autonomous vehicle. The complexity of data and traffic behaviors in autonomous vehicle networks may enable various types of attacks (Aldhyani & Alkahtani, 2022). To address these challenges, Vitale et al. (2021) propose the

https://doi.org/10.58086/gtcy-wt23

development of methodologies to assess the vulnerabilities and impacts of potential cyberattacks on autonomous vehicles.

5. Results

Scientific interest in the field of cybersecurity in autonomous vehicles has been growing over the past 20 years, from 2004 to 2023. In 2004, there were 31 publications, which increased to 678 publications in 2023, representing a growth of 2187%. The year 2012 marked an annual growth of 168%, after which scientific production maintained an upward trend. The significance of cybersecurity in autonomous vehicles has been reinforced due to the emerging availability of technologies such as blockchain, machine learning, and deep learning, as well as the use of technologies like 5G and 6G, making vehicles increasingly interconnected with each other and their environmental context.

Bibliometric analysis revealed that China, the United States, the United Kingdom, and Canada are the most active in producing scientific publications on the topic. This analysis aligns with the level of investment and prioritization of research and development in the area that these countries demonstrate, such as the creation of regulatory policies as indicated using keywords like "guidance law," "regulation," or "law".

Consumer perspectives play a crucial role in the widespread acceptance and adoption of autonomous vehicles. Trust in security, along with other aspects such as reliability and user experience, will significantly influence consumers' willingness to adopt autonomous vehicles. Keywords such as "control design," "awareness," and "cybersecurity awareness" represent the importance in their regard.

By analyzing existing literature, the article provides a comprehensive perspective on the current state, highlighting key themes, trends, and identified security gaps, such as the use of artificial intelligence and environmental connectivity, contributing to reinforcing the need for research by academics and investment by companies.

Aspects such as cybersecurity, reliability, and regulation were identified as key areas. Thus, automotive companies can benefit from this analysis, which identified fundamental elements to be addressed in the cybersecurity of autonomous vehicles.

6. Limitations and future research

As in any study, the present research has some limitations that need to be recognized but may represent a starting point for future work. The results obtained reflect the choices made in steps one to three (Figure

https://doi.org/10.58086/gtcy-wt23

1), as described in the methodology section. This includes the selection of the database and the keywords used in the search. Therefore, these decisions represent an inherent limitation of the paper.

For future research, it would be relevant to explore the contributions that technology can provide to boost cybersecurity in autonomous vehicles. The results suggest conducting a study that investigates the relationship between vehicle-to-vehicle and environmental communication and their predictive capabilities.

7. Conclusions

Cybersecurity is a fundamental challenge for the development and implementation of safe and reliable autonomous vehicles. Challenges include the vulnerability of control systems, the possibility of cyber-attacks, and the lack of specific regulations. The development of new security technologies, cooperation between industry and researchers, and collaboration between education and public awareness are opportunities for development.

Bibliographic references

Acheampong, R. A., & Cugurullo, F. (2019). 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*, *62*, 349–375. https://doi.org/10.1016/J.TRF.2019.01.009

Aldhyani, T. H. H., & Alkahtani, H. (2022). Attacks to Automatous Vehicles: A Deep Learning Algorithm for Cybersecurity. *Sensors 2022, Vol. 22, Page 360*, *22*(1), 360. https://doi.org/10.3390/S22010360

Algarni, A. M., & Thayananthan, V. (2023). Autonomous Vehicles With a 6G-Based Intelligent Cybersecurity Model. *IEEE Access*, *11*, 15284–15296. https://doi.org/10.1109/ACCESS.2023.3244883

Alheeti, K. M. A., Gruebler, A., & McDonald-Maier, K. (2016). Intelligent Intrusion Detection of Grey Hole and Rushing Attacks in Self-Driving Vehicular Networks. *Computers 2016, Vol. 5, Page 16*, *5*(3), 16. https://doi.org/10.3390/COMPUTERS5030016

Baraibar-Diez, E., Luna, M., Odriozola, M. D., & Llorente, I. (2020). Mapping Social Impact: A Bibliometric Analysis. *Sustainability 2020, 12*(22), 9389. https://doi.org/10.3390/SU12229389

Bathla, G., Bhadane, K., Singh, R. K., Kumar, R., Aluvalu, R., Krishnamurthi, R., Kumar, A., Thakur, R. N., & Basheer, S. (2022). Autonomous Vehicles and Intelligent Automation: Applications, Challenges, and Opportunities. *Mobile Information Systems*, *2022*. https://doi.org/10.1155/2022/7632892

Chattopadhyay, A., Lam, K. Y., & Tavva, Y. (2021). Autonomous Vehicle: Security by Design. *IEEE Transactions on Intelligent Transportation Systems*, *22*(11), 7015–7029. https://doi.org/10.1109/TITS.2020.3000797

Coombes, P. (2023). A review of business model research: what next for industrial marketing scholarship? *Journal of Business and Industrial Marketing*, *38*(3), 520–532. https://doi.org/10.1108/JBIM-06-2021-0296

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21. https://doi.org/10.22215/TIMREVIEW/835

Da Veiga, A. (2016). A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. *Proceedings of 2016 SAI Computing Conference, SAI 2016*, 1006–1015. https://doi.org/10.1109/SAI.2016.7556102

Evtukov, S., Golov, E., & Sazonova, T. (2018). Prospects of scientific research in the field of active and passive safety of vehicles. *MATEC Web of Conferences*, *239*, 04018. https://doi.org/10.1051/MATECCONF/201823904018

Fischer, E. A. (2016). *Cybersecurity Issues and Challenges: In Brief*. www.crs.gov

Fu, Y., Wang, C., Wang, F., S., L., Du, Z., & Cao, Z. (2022). An intelligent method for building attack paths based on Bayesian attack graphs. *Https://Doi.Org/10.1117/12.2653480*, *12474*, 264–268. https://doi.org/10.1117/12.2653480

Gcaza, N., & von Solms, R. (2017). Cybersecurity culture: An ill-defined problem. *IFIP Advances in Information and Communication Technology*, *503*, 98–109. https://doi.org/10.1007/978-3-319-58553-6_9

Gordon, W. J., Ikoma, N., Lyu, H., Jackson, G. P., & Landman, A. (2022). Protecting procedural care—cybersecurity considerations for robotic surgery. *Npj Digital Medicine 2022 5:1*, *5*(1), 1–3. https://doi.org/10.1038/s41746-022-00693-8

Guo, J., Luo, Y., & Li, K. (2018). Adaptive coordinated collision avoidance control of autonomous ground vehicles. *Proceedings of the Institution of Mechanical Engineers. Part I: Journal of Systems and Control Engineering*, *232*(9), 1120–1133. https://doi.org/10.1177/0959651818774991

Guo, S. (2023). Automatic driving model based on machine learning agents. *In Fifth International Conference on Computer Information Science and Artificial Intelligence (CISAI 2022)* (Vol. 12566, pp. 859-864). SPIE. https://doi.org/10.1117/12.2667914

Héroux, S., & Fortin, A. (2020). Cybersecurity Disclosure by the Companies on the S&P/TSX 60 Index. *Accounting Perspectives*, *19*(2), 73–100. https://doi.org/10.1111/1911-3838.12220

Karagiannis, S., Magkos, E., Karavaras, E., Karnavas, A., Nikiforos, M. N., & Ntantogian, C. (2022). *Towards NICE-by-Design Cybersecurity Learning Environments: A Cyber Range for SOC Teams*. https://doi.org/10.21203/RS.3.RS-1902186/V1

Kato, S., Takeuchi, E., Ishiguro, Y., Ninomiya, Y., Takeda, K., & Hamada, T. (2015). An open approach to autonomous vehicles. *IEEE Micro*, *35*(6), 60–68. https://doi.org/10.1109/MM.2015.133

Li, G., Yang, Y., Li, S., Qu, X., Lyu, N., & Li, S. E. (2022). Decision making of autonomous vehicles in lane change scenarios: Deep reinforcement learning approaches with risk awareness. *Transportation Research Part C: Emerging Technologies*, *134*, 103452. https://doi.org/10.1016/J.TRC.2021.103452

Lin, F., Wang, K., Zhao, Y., & Wang, S. (2020). Integrated Avoid Collision Control of Autonomous Vehicle Based on Trajectory Re-Planning and V2V Information Interaction. *Sensors 2020, Vol. 20, Page 1079*, *20*(4), 1079. https://doi.org/10.3390/S20041079

Liu, Y., Yang, X., Li, M., Wu, M., Sun, C., & Zhou, S. (2022). On the Criteria for Cybersecurity and Risk Assessment Based on ISO/SAE 21434 for the Application of Autonomous Vehicle. *Proceedings of the 2022 International Conference on Computer Science, Information Engineering and Digital Economy (CSIEDE 2022)*, *103*, 134–143. https://doi.org/10.2991/978-94-6463-108-1_16

Martin-Gasulla, M., Sukennik, P., & Lohmiller, J. (2019). Investigation of the Impact on Throughput of Connected Autonomous Vehicles with Headway Based on the Leading Vehicle Type. *Transportation Research Record*, *2673*(5), 617–626. https://doi.org/10.1177/0361198119839989

Matheu, S. N., Hernández-Ramos, J. L., Skarmeta, A. F., & Baldini, G. (2020). A Survey of Cybersecurity Certification for the Internet of Things. *ACM Computing Surveys (CSUR)*, *53*(6), 115. https://doi.org/10.1145/3410160

Matous, J., Basso, E. A., Thyri, E. H., & Pettersen, K. Y. (2021). Unifying Reactive Collision Avoidance and Control Allocation for Multi-Vehicle Systems. *CCTA 2021 - 5th IEEE Conference on Control Technology and Applications*, 76–81. https://doi.org/10.1109/CCTA48906.2021.9658918

Montanaro, U., Dixit, S., Fallah, S., Dianati, M., Stevens, A., Oxtoby, D., & Mouzakitis, A. (2019). Towards connected autonomous driving: review of use-cases. *Vehicle System Dynamics*, *57*(6), 779–814. https://doi.org/10.1080/00423114.2018.1492142

Muhammad, T., Kashmiri, F. A., Naeem, H., Qi, X., Chia-Chun, H., & Lu, H. (2020). Simulation Study of Autonomous Vehicles' Effect on Traffic Flow Characteristics including Autonomous Buses. *Journal of Advanced Transportation*, *2020*. https://doi.org/10.1155/2020/4318652

Mukherjee, D., Lim, W. M., Kumar, S., & Donthu, N. (2022). Guidelines for advancing theory and practice through bibliometric research. *Journal of Business Research*, *148*, 101–115. https://doi.org/10.1016/J.JBUSRES.2022.04.042

Nees, M. A. (2016). Acceptance of Self-driving Cars: An examination of idealized versus realistic portrayals with a self-driving car acceptance scale. In *Proceedings of the human factors and ergonomics society annual meeting 60*(1), pp. 1449-1453. Sage CA: Los Angeles, CA: SAGE Publications. https://doi.org/10.1177/1541931213601332

Nyholm, S., & Smids, J. (2016). The Ethics of Accident-Algorithms for Self-Driving Cars: an Applied Trolley Problem? *Ethical Theory and Moral Practice*, *19*(5), 1275–1289. https://doi.org/10.1007/S10677-016-9745-2/METRICS

Page, M. J., Moher, D., Bossuyt, P., Boutron, I., Hoffmann, T., mulrow, cindy, Shamseer, L., Tetzlaff, J., Akl, E., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J., Hróbjartsson, A., Lalu, M., Li, T., Loder, E., Mayo-Wilson, E., McDonald, S., … McKenzie, J. (2023). *PRISMA 2020 explanation and elaboration: updated guidance and exemplars for reporting systematic reviews*. https://doi.org/10.31222/OSF.IO/GWDHK

Pendleton, S. D., Andersen, H., Du, X., Shen, X., Meghjani, M., Eng, Y. H., Rus, D., & Ang, M. H. (2017). Perception, Planning, Control, and Coordination for Autonomous Vehicles. *Machines 2017, Vol. 5, Page 6*, *5*(1), 6. https://doi.org/10.3390/MACHINES5010006

Qu, D., Zhang, K., Song, H., Wang, T., & Dai, S. (2022). Analysis of Lane-Changing Decision-Making Behavior of Autonomous Vehicles Based on Molecular Dynamics. *Sensors 2022, Vol. 22, Page 7748*, *22*(20), 7748. https://doi.org/10.3390/S22207748

Queralta, J. P., Qingqing, L., Zou, Z., & Westerlund, T. (2020). Enhancing Autonomy with Blockchain and Multi-Access Edge Computing in Distributed Robotic Systems. *2020 5th International Conference on Fog and Mobile Edge Computing, FMEC 2020*, 180–187. https://doi.org/10.1109/FMEC49853.2020.9144809

Reegård, K., Blackett, C., & Katta, V. (2019). *The Concept of Cybersecurity Culture*. In 29th European Safety and Reliability Conference, pp. 4036-4043. https://doi.org/10.3850/978-981-11-2724-3_0761-cd

Sabillon, R. (2018). A Practical Model to Perform Comprehensive Cybersecurity Audits. *Enfoque UTE*, *9*(1), 127–137. https://doi.org/10.29019/ENFOQUEUTE.V9N1.214

Sallos, M. P., Garcia-Perez, A., Bedford, D., & Orlando, B. (2019). Strategy and organisational cybersecurity: a knowledge-problem perspective. *Journal of Intellectual Capital*, *20*(4), 581–597. https://doi.org/10.1108/JIC-03-2019-0041/FULL/XML

Schwarting, W., Alonso-Mora, J., & Rus, D. (2018). Planning and Decision-Making for Autonomous Vehicles. *Https://Doi.Org/10.1146/Annurev-Control-060117-105157*, *1*, 187–210. https://doi.org/10.1146/ANNUREV-CONTROL-060117-105157

Sun, X., Yu, F. R., & Zhang, P. (2022). A Survey on Cyber-Security of Connected and Autonomous Vehicles (CAVs). *IEEE Transactions on Intelligent Transportation Systems*, *23*(7), 6240–6259. https://doi.org/10.1109/TITS.2021.3085297

Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. *Electronics 2022, Vol. 11, Page 2181*, *11*(14), 2181. https://doi.org/10.3390/ELECTRONICS11142181

The Lens. (n.d.). *The Lens - Free & Open Patent and Scholarly Search*. Retrieved December 31, 2023, from https://www.lens.org/

Tiwari, T., Agarwal, S., & Etar, A. (2021). Controller design for autonomous vehicle. *Proceedings of the 2021 1st International Conference on Advances in Electrical, Computing, Communications and Sustainable Technologies, ICAECT 2021*. https://doi.org/10.1109/ICAECT49130.2021.9392498

Veale, M., Fundação, I. B., & Vargas, G. (2020). *Standard-Nutzungsbedingungen: Cybersecurity*. https://doi.org/10.14763/2020.4.1533

Vitale, C., Piperigkos, N., Laoudias, C., Ellinas, G., Casademont, J., Escrig, J., Kloukiniotis, A., Lalos, A. S., Moustakas, K., Diaz Rodriguez, R., Baños, D., Roqueta Crusats, G., Kapsalas, P., Hofmann, K. P., & Khodashenas, P. S. (2021). CARAMEL: results on a secure architecture for connected and autonomous vehicles detecting GPS spoofing attacks. *Eurasip Journal on Wireless Communications and Networking*, *2021*(1), 1–28. https://doi.org/10.1186/s13638-021-01971-x

Wachenfeld, W., & Winner, H. (2016). The release of autonomous vehicles. *Autonomous Driving: Technical, Legal and Social Aspects*, 425–449. https://doi.org/10.1007/978-3-662-48847-8_21

Wang, J., Zhang, L., Huang, Y., & Zhao, J. (2020). Safety of Autonomous Vehicles. *Journal of Advanced Transportation*, 2020, 1-13. https://doi.org/10.1155/2020/8867757

Wang, Y., Wang, Y., Qin, H., Ji, H., Zhang, Y., & Wang, J. (2021). A Systematic Risk Assessment Framework of Automotive Cybersecurity. *Automotive Innovation*, *4*(3), 253–261. https://doi.org/10.1007/S42154-021-00140-6

Wu, X., Qiao, B., & Su, C. (2020). Trajectory Planning with Time-Variant Safety Margin for Autonomous Vehicle Lane Change. *Applied Sciences, 10*(5), 1626. https://doi.org/10.3390/APP10051626

Yamazato, T. (2017). V2X communications with an image sensor. *Journal of Communications and Information Networks 2017 2:4*, *2*(4), 65–74. https://doi.org/10.1007/S41650-017-0044-4

Zhou, J., Shen, Z., Wang, X., & Wang, L. (2022). *Unsignalized Intersection Management Strategy for Mixed Autonomy Traffic Streams*. arXiv preprint arXiv:2204.03499. https://doi.org/10.48550/arXiv.2204.03499

Zupic, I., & Čater, T. (2015). Bibliometric Methods in Management and Organization. *Organizational Research Methods*, *18*(3), 429–472. https://doi.org/10.1177/1094428114562629