Issues in Information Systems
Volume 24, Issue 3, pp. 271-280, 2023

DOI: https://doi.org/10.48009/3_iis_2023_123

Moving data down the road: a systematic review of information privacy concerns in Internet-of-Vehicles (IoV) literature

Brad Fowler, *Dakota State University, steven.fowler@trojans.dsu.edu*
Omar El-Gayar, *Dakota State University, omar.el-gayar@dsu.edu*

Abstract

Internet-of-Things (IoT) technology reaches far and wide in the modern world. Many consumer products are now capable of connecting to networks in order to manage and move data that is created through their various capabilities. Automobiles are now being manufactured with the ability to connect to wireless networks. This capability allows these vehicles to transmit and receive data to and from their manufacturers. IoT technology implemented in automobiles and their accompanying infrastructure is considered the Internet-of-Vehicles (IoV) technology. The goal of this paper is to better understand the association between privacy concern and IoV through a systematic literature review with suggestions for future research. Through a systematic screening process, 7 articles were identified which studied the relationship between privacy and IoV technologies. All but one article found that privacy concern or perceived risk associated with data privacy was significant in IoV technologies. These findings suggest that privacy may play an important role in users' decisions to adopt and use IoV technology. This article contributes to the growing knowledge of IoV technologies as they emerge in the automobile market.

Keywords: Internet-of-Vehicles, IoV, privacy, security, Internet-of-Things, systematic review

Introduction

The Internet of Things (IoT) technology movement has sought to connect the Internet to as many areas as possible. IoT is a concept that involves adding computing capability to everyday consumer items so that they can make use of network and Internet resources. Some of the common modern IoT devices available to consumers are home security cameras, doorbells, smartwatches, and wearable medical devices(Niknejad et al., 2020). Consumer product manufacturers seem inclined to try to include IoT technology in any product development. This can be witnessed in items that don't seem to have an obvious need for Internet connectivity, such as toasters and refrigerators.

It is not unexpected that auto manufacturers would be inclined to introduce IoT technology in their new car and truck offerings. Many new automobiles come equipped with IoT technology. Transform Insights suggests in the Connected Car Overview, 2020-2030 that there will be 1.8 billion Internet-connected cars in use by 2030 (Arnott, 2022). IoT technology in automobiles allows drivers to lock, unlock, and start their cars through smartphone applications. It also provides rich infotainment options that includes voice assistants and downloadable applications. Bleeding-edge IoT technologies in automobiles are exploring capabilities for vehicle-to-vehicle (V2V) and vehicle-to-other devices (V2X) such as traffic sensors. Other areas associated with this technology are vehicle-to-Internet (V2I), vehicle-to-network (V2N), vehicle-to-infrastructure (V2I), vehicle-to-pedestrian (V2P), and vehicle-to-road (V2R) (Berdigh & El Yassini, 2017; Katsini et al., 2021). Through sensors and programs, IoV cars and trucks can create, store, and send data about various aspects of the vehicle like engine and drivetrain health, vehicle performance, and driver behavior.

With the addition of these IoT technologies to automobiles, concerns arise around the nature and handling of the data created and managed by these vehicles. IoT as a technology can be susceptible to security vulnerabilities that open the door to hacking and data theft. Further, data created through IoT devices are typically shared with and managed by the manufacturer. This raises legitimate concerns over how that data is used and protected. Large organizations are not immune to data breaches. There is also plenty of precedents regarding companies selling data to third parties.

This study seeks to better understand the concept of privacy as it pertains to IoV technology. This is accomplished through a systematic review of the available academic literature. The findings contribute to the overall knowledge of privacy and privacy theory in the area of IoV.

The remainder of this study covers the theoretical background of privacy in IoV and related works, the methodology used to conduct this review, the results of the search for literature, a discussion of the findings, and a conclusion with recommendations for future research.

Background and Related Work

The Tesla automobile manufacturing company has greatly affected how the automobile industry has viewed technology when it comes to automobile design. In fact, many people consider Tesla to be a technology company that makes automobiles rather than an automobile company that heavily uses technology(Crider, 2020). Tesla's cars utilize their connection to the Internet to support many features and capabilities. These technological advances have prompted other automobile manufactures to make technology implementation a priority in their new car designs. IoV is a technological subset of IoT technologies. IoV is a relatively new technology in the field of Information Systems

IoV is a technological subset of IoT technologies. IoV technologies provide vehicles with features that require a network connection. Some of these features include mobile applications, safety, social driving, self-driving, and electric vehicle infrastructure (Sadiku et al., 2018). IoV consists of several network topographies, such as vehicle-to-vehicle (V2V), vehicle-to-road (V2R), vehicle-to-Internet (V2I), and vehicle-to-everything (V2X) (Sadiku et al., 2018) as well as the established variant of V2V called Vehicle Ad-hoc Networks (VANETs) (Yang et al., 2014). The ultimate goal for many IoV technologists is that these vehicle networks provide a robust infrastructure for a functional and safe autonomous vehicle system through vehicular clouds (Gerla et al., 2014).

Information privacy as a construct in information systems research has been defined by Bélanger and Crossler as a combination of data and personal communication privacies. They further define information privacy as "one's ability to control information about themselves"(Bélanger & Crossler, 2011). Users of technology devices should feel a need to protect themselves from losing control of their personal data and digital communications.

Many times, technology users will imply that privacy is a priority in technology-based activities but then contradict these implications with their actions. This contradiction is called the Privacy Paradox (Brown, 2001). Ultimately, users make a risk/reward calculation in the process of determining their privacy concerns. This calculation has been codified into theory with the Privacy Calculus Theory.

Privacy Calculus is used to assess a user's intention to disclose personal information through an evaluation of the perceived benefit that information disclosure provides versus the perceived risk of that disclosure (Culnan & Armstrong, 1999). Uncertainty can also be a factor in privacy concerns. Uncertainty in the technology can stem from incomplete information held by the user (Acquisti et al., 2015). As computer technology advances, users have less understanding of how new technology creates and handles data.

Mitigation opportunities may also have an impact of privacy concerns. Mitigation approaches in IoV can consist of the level to which a user can configure privacy settings in the technology or their own self-efficacy to effect passive and active actions to affect privacy in the usage of the technology (Frik et al., 2019). These privacy factors may have an effect on their willingness to adopt an IoV technology. This study aims to explore the association between IoV and potential privacy concerns (See Figure 1) of the users of IoV technology.

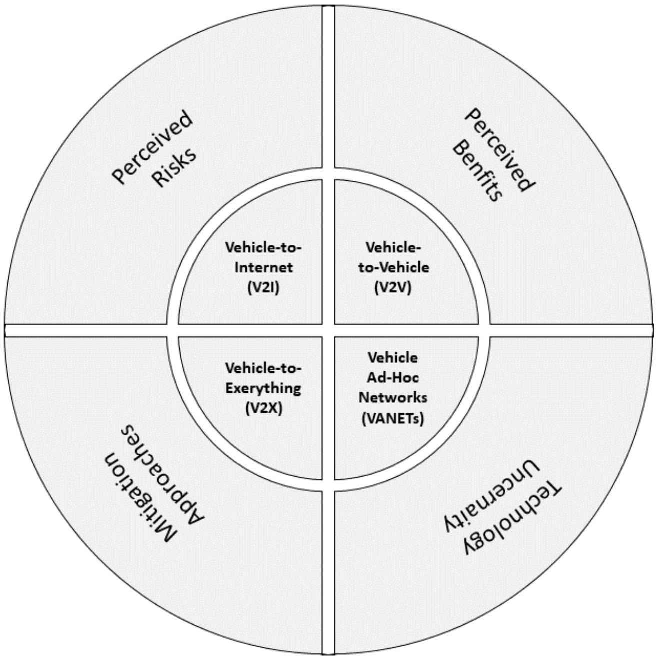

Figure 1: Classification Framework

Methodology

This study was conducted using a systematic literature review. Systematic literature reviews allow researchers to explore a research area with a structured methodology that limits bias in the discovery and reporting of empirical data while also offering replicability (Mariano et al., 2018). This study follows the steps and guidelines established by Kitchenham and Charters for conducting Information Systems and Computer Science systematic literature reviews (Kitchenham & Charters, 2007). These guidelines suggest that systematic literature reviews follow three main activities: planning, conducting, and reporting.

This study also incorporates the PRISMA reporting methodology introduced by Liberati, et al. to illustrate the discovery and filtering process for this study (Liberati et al., 2009). Finally, the review of the existent literature will follow a narrative review methodology (Xiao & Watson, 2019). This review methodology was chosen because the goal of this study is to establish the nature of academic research in the area of privacy in the realm of IoV.

Review Planning

This review was conducted using the ABI/INFORM, Academic Search Complete (EBSCOhost), IEEE, ACM Digital Library, and Web of Science academic databases. Each database was searched using the phrases "Internet of Vehicles" AND Privacy OR "Automotive IoT" AND Privacy. Internet of Vehicles and Automotive IoT are two phrases that had been identified as terminology used for this technology. The Boolean expressions AND and OR were used to bind privacy to the technology phrases and broaden the search to include both phrases. Searches were limited to the years 2015-2023. For a study to be considered for review, it must be written in the English language, be peer reviewed, and a full-text version must be available. For an article to be included in the review, it must consider privacy or security in IoV technology.

Review Process

For each database search, the number of results were recorded and the results were scanned for duplicates across the databases. Duplicate studies were removed from consideration. Titles and abstracts were scanned for study relevance. For a study to be selected for further review, it must have addressed some aspect of privacy in regard to IoV. Articles that satisfied the standards were downloaded from the databases. Abstracts for all articles were then subjected to more intense reviews.

The remaining studies were given full-text reviews and were synthesized for the study. For an article to be included in the study, it must use some empirical-based methodology to address the privacy concerns for IoV users. Articles that were excluded were general surveys or reviews of the area of privacy and security of IoV technology as well as design science methodologies that introduce new models, frameworks, taxonomies, and instantiations of systems for improvements to IoV privacy and security.

Results

As illustrated in Figure 2, the search of the selected academic databases identified 781 records that met the search criteria. An additional article was added from another source. Two articles were found to be duplicates and were removed from the results. 779 records were screened in an initial overview of their titles and abstracts. Through this review, 714 records were excluded. The remaining 65 records were then reviewed through a second abstract reading. An additional 39 records were excluded. The remaining 26 articles were given full-text readings.

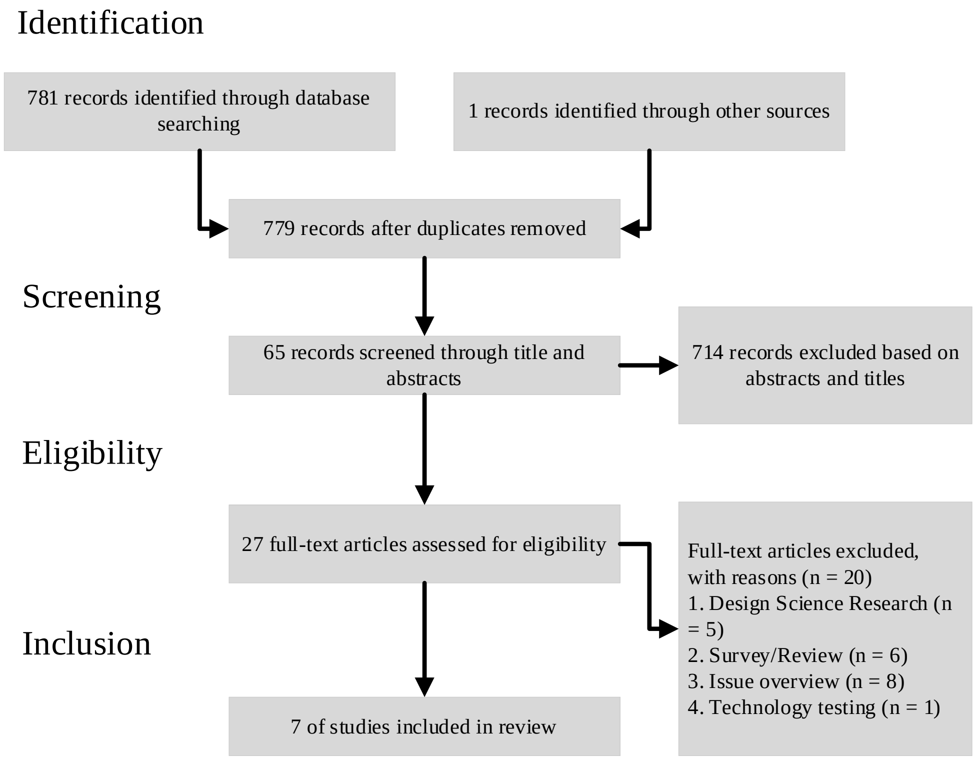
Identification
781 records identified through database searching
1 records identified through other sources
779 records after duplicates removed
Screening
65 records screened through title and abstracts
714 records excluded based on abstracts and titles
Eligibility
27 full-text articles assessed for eligibility
Full-text articles excluded, with reasons (n = 20)
1. Design Science Research (n = 5)
2. Survey/Review (n = 6)
3. Issue overview (n = 8)
4. Technology testing (n = 1)
Inclusion
7 of studies included in review

Figure 2: Search and screening methodology

Many of the 18 articles excluded from the full-text review were comprehensive surveys or reviews of the threats or vulnerabilities associated with IoV technologies with suggestions for security solutions. The result of the full-text screening was 7 articles for synthesis.

Publication Statistics

IoV has had a relatively recent boost in popularity. Most automobile manufacturers have pivoted to a position of making the use of technology a premium feature on their products. Because of this, academic research on IoV is relatively new as well. As seen in Figure 3, there was not a multi-article year for IoV until 2021. Only two years had multiple articles published in this area; 2021 and 2022. There were no articles reviewed from 2015, 2017, 2018, and 2023.

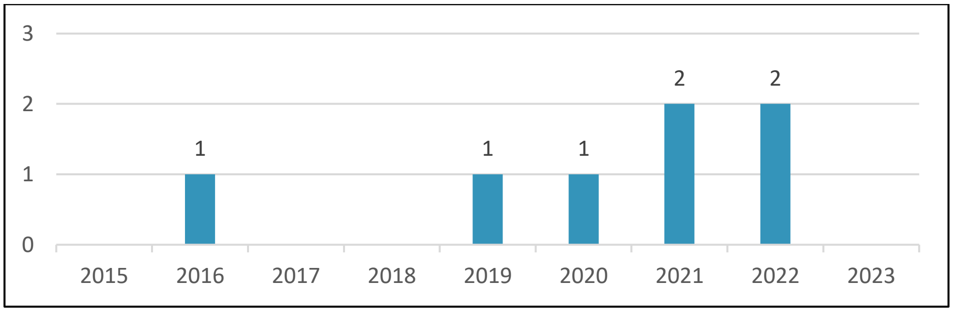

Figure 3: Articles by year

Discussion

This review found 7 articles that associate IoV technology with concerns for users' data privacy and are presented in Table 1. Of the 7 articles, 4 articles used Privacy Concern as the main construct to represent this phenomena (Cichy et al., 2021; Derikx et al., 2016; Milanović et al., 2020; Rohunen & Markkula, 2019), 2 articles used Perceived Risk(Li et al., 2022; Yu & Cai, 2022). Hussain et al. tested a "3-dimension" construct Concern for the Internet of Vehicle Information Privacy (CFIOVIP).

Privacy, as an overall construct, was applied broadly across these studies. Cichy et al.(2021) and Rohunen & Markkula (2019) studied the sharing of driving data.. Yu & Cai looked specifically at the data associated with car infotainment systems (Yu & Cai, 2022). Privacy was specifically addressed in regard to users' attitudes toward the use of IoV data by insurance companies (Derikx et al., 2016; Milanović et al., 2020).

Both studies found that privacy was a significant factor in whether or not to allow insurance companies to use IoV data. Li et al. used technology uncertainty as a construct in their study. This may not have been a clear measurement of privacy concerns since they included autonomous technology in the study. All of the studies reviewed used a relatively limited geographical demographic for their sample populations. 2 studies focused on Chinese drivers (Li et al., 2022; Yu & Cai, 2022), 1 study focused on German drivers (Cichy et al., 2021), and 1 study focused on Dutch drivers (Derikx et al., 2016). Ultimately, only one study failed to find privacy concerns or perceived risk to be significant (Li et al., 2022).

Cichy et al. designed a mixed methods approach using interviews, a survey and a field experiment to study privacy concerns in connected cars. They found that subjects that believe that they own their driving data were less willing to share it unless they were adequately compensated for it (Cichy et al., 2021). Similarly, Derikx et al. found that drivers are inclined to maintain traditional auto insurance coverage as opposed to usage-based plans unless there is some form of financial compensation (Derikx et al., 2016). Milanović et al. found that even though auto consumers find insurance companies to be reliable, they are not trusting of telematic technology (Milanović et al., 2020). Hussain et al. did an exploratory analysis of factors associated with behavioral intentions and found that their 3-demension construct measuring IoV information privacy was valid(Hussain et al., 2021). Li et al. found that Technology Acceptance Model (TAM) based constructs positively affected users willingness to adopt connected and autonomous vehicles but perceived risk did not positively influence adoption (Li et al., 2022).

Although literature suggests a variety of classifications of IoV technology, the studies identified in this review focused mainly on the V2I architecture (Cichy et al., 2021; Derikx et al., 2016; Milanović et al., 2020; Rohunen & Markkula, 2019). It is possible that privacy concerns by the general IoV user are more likely to be associated with a connection between the vehicle and the Internet as opposed to the vehicle and infrastructure or other vehicles.

Two studies used IoV terminology that was not found in other research studies (Li et al., 2022; Yu & Cai, 2022). These terminologies included Connected and Autonomous Vehicles (CAVs) and Intelligent Connected Vehicles (ICVs). Rohunen and Markkula conducted qualitative research to better understand users' privacy concerns with mobile data sharing. They found that users do have privacy concerns but, ultimately, are not concerned about their privacy with mobile data sharing to a large extent. They also found that users' privacy concerns may change during use and the benefits associated with privacy calculus are driven by altruistic motives(Rohunen & Markkula, 2019). Yu and Cai studied infotainment device based automobile connections and found that privacy constructs such as perceived security risk and perceived privacy risk affect users' behavioral intention (Yu & Cai, 2022).

Table 1: Summary of studies

Study	Year	Privacy Constructs	IoV Type	Theoretical Model(s)	Context	Participants	Sample Size	Limitations	Findings
Cichy et al.	2021	Privacy Concerns	V2I	Created from Previous Qualitative Study	Effect of privacy concerns on willingness to share driving data	German car drivers	333	Common method bias, limited ability to measure moderating effects, single geographic demographic	Significant
Derikx et al.	2016	Privacy Concerns	V2I	Experiment - No model	Whether privacy concerns can be quelled through financial compensation in auto insurance telematics	Dutch car drivers	60	Limited demographic (education, age)	Significant
Hussain et al.	2021	Concern For Internet of Vehicle Information Privacy (CFIOVIP)	VANETs	CFIOVIP	Exploratory analysis of measurement tool for privacy concern in IoV	College students	357	Limited demographic (education, age)	Valid Model
Li et al.	2022	Technological Uncertainty, Perceived Risk	Connected and Autonomous Vehicles (CAV)	TAM, UTAUT2, Perceived Risk Theory	Better understand factors in the adoption of connected and autonomous vehicles	Chinese car drivers	362	Limited factors, single geographic demographic	Not Significant
Milanovic et al	2020	Privacy Concerns	V2I	UTAUT	Privacy concerns as a factor in adoption of auto insurance telematic devices	Various demographic groups	502	Single geographic demographic, Limited mediating variables, cross-sectional	Significant
Rohunen & Markkula	2019	Privacy Concerns (Qualitative)	V2I	None	Better understand the privacy concerns associated with mobility data collection	Mobility service system users	18 Interviews, 62 Surveys	No theoretical foundation	NA
Yu & Cai	2022	Perceived Privacy Risk	Intelligent Connected Vehicles (ICV)	TPB, TRA	How the use of connected car infotainment system's perceived risk affects user trust, attitude, and behavioral intent	Chinese car drivers	500	Limited geographic demographic, Limited demographic (internet users), limited experience with connected vehicles	Significant

Conclusion and Future Research

IoV is becoming a significant component of modern features in new automobiles. Manufacturers will continue to add features to their automotive products that use network connections as integral parts of their functionality. Like other IoT technologies, IoV has the potential to collect sensitive personal data such as locations and driving habits. This paper sought to explore the established literature that examines the relationships between IoV technologies and privacy concerns that users may have.

The findings of the reviewed articles for this study suggest that privacy is a significant concern for the use of IoV technology. Further, given the relative immaturity of the IoV area, more research is needed to fully understand the role that privacy plays in the adoption and continued use of this technology. This study contributes to the continuing development of knowledge of privacy concern in the area of IoV by identifying and synthesizing the research available to date.

Within the area of IoV literature, there are a lack of studies that address adoption and use of IoV that employ established Information Systems theory. Future research should venture to test privacy constructs as they are related to IoV technology through established Information Systems adoption theories such as Technology Acceptance Model (TAM) or Unified Theory of Acceptance and Usage of Technology (UTAUT) while also incorporating established privacy theories such as the Privacy Paradox or Privacy Calculus.

Further, we did not find any studies that examine North American or South American drivers in their sample population. This may be significant given the percentage of drivers in the total population who reside in these areas. Also, many of the IoV technologies have been developed and implemented by North American companies and, thus, North American drivers may have been exposed to this technology longer than other demographics. Future research should strive to understand the attitudes of North American and South American car buyers in regard to IoV features available in new vehicles.

IoV is a relatively new area of IoT computer technology. This area is not yet mature and could benefit from an effort to standardize the terminology associated with the technology. V2V, V2I, V2R, and VANETS are all acronyms that sometimes overlap. Standardization would benefit future research efforts in this field. Automotive IoT was identified early in the research process for this study to represent this area of technology. It was not found to be a significant term in any studies screened or reviewed for this study.

Future research should seek to establish a common vernacular for the IoV field. Further, the types of vehicles associated with studies tend to be undefined. A taxonomy should be developed that identifies all types of vehicles that employ IoV technologies.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514. https://doi.org/10.1126/science.aaa1465

Arnott, M. (2022, June 30). *Connected cars will hit 2.5 billion connections in 2030, driving cellular IoT and 5G adoption*. https://transformainsights.com/blog/connected-cars-cellular-iot-5g

Bélanger & Crossler. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly*, *35*(4), 1017. https://doi.org/10.2307/41409971

Berdigh, A., & El Yassini, K. (2017). Connected car overview: Solutions, challenges and opportunities. *Proceedings of the 1st International Conference on Internet of Things and Machine Learning*, 1–7. https://doi.org/10.1145/3109761.3158382

Brown, B. (2001). *Studying the internet experience*. 24.

Cichy, P., Salge, T. O., & Kohli, R. (2021). Privacy Concerns and Data Sharing in the Internet of Things: Mixed Methods Evidence from Connected Cars. *MIS Quarterly*, *45*(4), 1863–1892. https://doi.org/10.25300/MISQ/2021/14165

Crider, J. (2020, February 6). *Tesla Is A Tech Company—Here's Why—CleanTechnica*. CleanTechnica. https://cleantechnica.com/2020/02/06/tesla-is-a-tech-company-heres-why/

Culnan, M. J., & Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science*, *10*(1), 104–115. https://doi.org/10.1287/orsc.10.1.104

Derikx, S., de Reuver, M., & Kroesen, M. (2016). Can privacy concerns for insurance of connected cars be compensated? *Electronic Markets*, *26*(1), 73–81. https://doi.org/10.1007/s12525-015-0211-0

Frik, A., Nurgalieva, L., Bernd, J., Lee, J., Schaub, F., & Egelman, S. (2019). Privacy and security threat models and mitigation strategies of older adults. *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, 21–40.

Gerla, M., Lee, E.-K., Pau, G., & Lee, U. (2014). Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds. *2014 IEEE World Forum on Internet of Things (WF-IoT)*, 241–246. https://doi.org/10.1109/WF-IoT.2014.6803166

Hussain, H. I., Kamarudin, F., Mohd-Sanusi, Z., Shuhidan, S. M., Saad Al-Dhubaibi, A. A., & Ahmad Razimi, M. S. (2021). Governance in the Internet of Vehicles (IoV) Context: Examination of Information Privacy, Transport Anxiety, Intention, and Usage. *Journal of Advanced Transportation*, *2021*, 1–10. https://doi.org/10.1155/2021/5563260

Katsini, C., Raptis, G. E., Alexakos, C., & Serpanos, D. (2021). FoRePlan: Supporting Digital Forensics Readiness Planning for Internet of Vehicles. *25th Pan-Hellenic Conference on Informatics*, 369–374. https://doi.org/10.1145/3503823.3503891

Kitchenham, B., & Charters, S. (2007). *Guidelines for performing Systematic Literature Reviews in Software Engineering*.

Li, G., Liang, Y., Wang, H., Chen, J., & Chang, X. (2022). Factors Influencing Users' Willingness to Adopt Connected and Autonomous Vehicles: Net and Configurational Effects Analysis Using PLS-SEM and FsQCA. *Journal of Advanced Transportation*, *2022*, 1–23. https://doi.org/10.1155/2022/7489897

Liberati, A., Altman, D. G., Tetzlaff, J., Mulrow, C., Gøtzsche, P. C., Ioannidis, J. P. A., Clarke, M., Devereaux, P. J., Kleijnen, J., & Moher, D. (2009). *The PRISMA Statement for Reporting Systematic Reviews and Meta-Analyses of Studies That Evaluate Health Care Interventions: Explanation and Elaboration*. 30.

Mariano, D. C. B., Leite, C., Santos, L. H. S., & de Melo-Minardi, R. C. (2018). A guide to performing systematic literature reviews in bioinformatics. *AsXiv Preprint ArXiv*.

Milanović, N., Milosavljević, M., Benković, S., Starčević, D., & Spasenić, Ž. (2020). An Acceptance Approach for Novel Technologies in Car Insurance. *Sustainability*, *12*(24), 10331. https://doi.org/10.3390/su122410331

Niknejad, N., Hussin, A. R. C., Ghani, I., & Ganjouei, F. A. (2020). A confirmatory factor analysis of the behavioral intention to use smart wellness wearables in Malaysia. *Universal Access in the Information Society*, *19*(3), 633–653. https://doi.org/10.1007/s10209-019-00663-0

Rohunen, A., & Markkula, J. (2019). On the road – listening to data subjects' personal mobility data privacy concerns. *Behaviour & Information Technology*, *38*(5), 486–502. https://doi.org/10.1080/0144929X.2018.1540658

Sadiku, M. N. O., Tembely, M., & Musa, S. M. (2018). INTERNET OF VEHICLES: AN INTRODUCTION. *International Journal of Advanced Research in Computer Science and Software Engineering*, *8*(1), 11. https://doi.org/10.23956/ijarcsse.v8i1.512

Xiao, Y., & Watson, M. (2019). Guidance on Conducting a Systematic Literature Review. *Journal of Planning Education and Research*, *39*(1), 93–112. https://doi.org/10.1177/0739456X17723971

Yang, F., Wang, S., Li, J., Liu, Z., & Sun, Q. (2014). An overview of Internet of Vehicles. *China Communications*, *11*(10), 1–15. https://doi.org/10.1109/CC.2014.6969789

Yu, Z., & Cai, K. (2022). Perceived Risks toward In-Vehicle Infotainment Data Services on Intelligent Connected Vehicles. *Systems*, *10*(5), 162. https://doi.org/10.3390/systems10050162