Cybersecurity in the Automotive Industry: A Systematic Literature Review (SLR).

Ignacio Fernandez de Arroyabe [a b*], Tim Watson [a], and Olga Angelopoulou [a]

[a] *WMG Cyber Security Centre, University of Warwick, Coventry*, UK;

[b] Data Services, Commercial Banking, Lloyds Banking Group, London, UK

[*] nacho.fernandez-de-arroyabe-arranz@warwick.ac.uk
ignacio.fernandez-de-arroyabe@lloydsbanking.com

Cybersecurity in the Automotive Industry: A Systematic Literature Review (SLR).

Abstract

This paper presents a systematic literature review (SLR) on cybersecurity in the automotive industry. Using the R tool Bibliometrix, a total of 537 papers related to cybersecurity and the automotive industry were analysed. First, our paper contributes to academia by showing that research on this topic is grouped into four clusters that correspond to four lines of research: *Automotive Security; Vehicle Engineering; Smart Vehicle; IT Security*. Second, our paper contributes to the literature by highlighting the existing gaps. On the subject of standards and framework, there are gaps in terms of what the security requirements must be for the vehicle. This is very important since, given the heterogeneity of technology that vehicles from different manufacturers have, the cybersecurity requirements are different. Additionally, a gap can also be observed in the literature on the supply chain, which has a very small number of papers. In general, they do not cover or elaborate on the supply chain security, when, from a manufacturing point of view, it is very important to manage an effective cybersecurity strategy for the vehicles. Moreover, our paper also contributes to managers and policy-makers' understanding of cybersecurity. We show that adequate implementation of cybersecurity in the automotive must involve a multidimensional perspective. First, it should be a *multistage model*, ranging from the first stages of design in interconnection with the suppliers to the final stages of use by the customer. Second, it should be a *multi-level model*, as a consequence of the interconnection of the vehicle's control systems. Finally, the model should be *multi-feedback*, structuring the process design as a feedback system, including incident response, diagnosis services and vehicle updates.

Keywords: cybersecurity; automotive industry; systematic literature review; bibliometric analysis, Bibliometrix, R package.

1. Introduction.

The digital transformation, the internet and the connectivity of systems have changed the automotive industry. [1,2] These changes have affected not only the car (and the systems that interact with a vehicle) but also the business model, from the design and production of intelligent vehicles to the maintenance and the after-sales services. [3,4,5] In this context, previous literature has recognised cybersecurity as a key element in this industry (see, for example, [4,6]).

This paper presents a systematic literature review (SLR) on cybersecurity in the automotive industry. Several reasons drive the development of this SLR, focusing on the characteristics and peculiarities of cybersecurity in the automotive industry. First, compared to the classic cybersecurity approach in which cybersecurity focuses exclusively on protecting and controlling information [7], cybersecurity in the automotive industry must cover other relevant aspects. In line with Boyes [8] in their approach for cyber-physical systems, cybersecurity in the automotive industry must include the safety of the vehicle and its occupants, privacy of the data, economic and reputational impact (both to the client and/or the company) and the usability of the vehicle. Second, compared to other cybersecurity approaches in other industries such as IT, cybersecurity in the automotive industry comprises a heterogeneity of integrated components in the vehicle such as ECUs (Electronic Control Unit), actuators, internal networks or connectivity modules. Moreover, related to the heterogeneity of components, there is very little experience and therefore a great level of uncertainty over the type of attacks that can be performed on a vehicle. Third, vehicles are designed and built-in close interaction with suppliers, which means that these must be involved in the secure development of the vehicle throughout the supply chain, both in the components and in the design. [9,10] Last, the evolution of the automotive industry towards more autonomous and interconnected vehicles represents a very important challenge for this industry.

These peculiarities in the automotive industry have meant that cybersecurity is approached from multiple angles, not only from the classic IT, but also from safety, security, or industrial point of view, which considers the relationship with the supply chain, and even from a regulatory perspective, which seeks the application of standards. [11,12,13,14] That is, research from the IT area, which extrapolates cybersecurity solutions to the automotive industry; [5,11,15,16] from the perspective of IoT, which considers the vehicle as an element (device) of the Smart City; [17,18,19,20,21] and finally, works from the perspective of engineering and manufacturing, which consider automotive cybersecurity as a process in the automotive supply chain. [1,22] This has generated a diverse body

of literature with inconclusive results, which does not provide an adequate perspective and framework both for research and for the implementation of cybersecurity in the automotive sector.

2. Methodology and data

For conducting the SLR, this study employs a bibliometric analysis. Bibliometric analysis has been used extensively in various disciplines to analyse bibliometric metadata. [23,24,25,26,27] The bibliometric analysis employs a quantitative approach to describe, evaluate, and monitor the published research. [27] It provides a static, transparent, and systematic picture of the research. It is a structural analysis which can help to infer the pattern over time of the themes researched, identify changes, and detect the most prolific institutions, authors, and countries in a particular area of research. [26,28]

For the development of the SLR of cybersecurity in the automotive industry, we follow the approach from Kitchenham [29], Brereton et al. [30], Denyer and Tranfield [31], Cheah [12], and Hou and Wang [32]. Figure 1 highlights some of the steps of the process followed in this SLR.

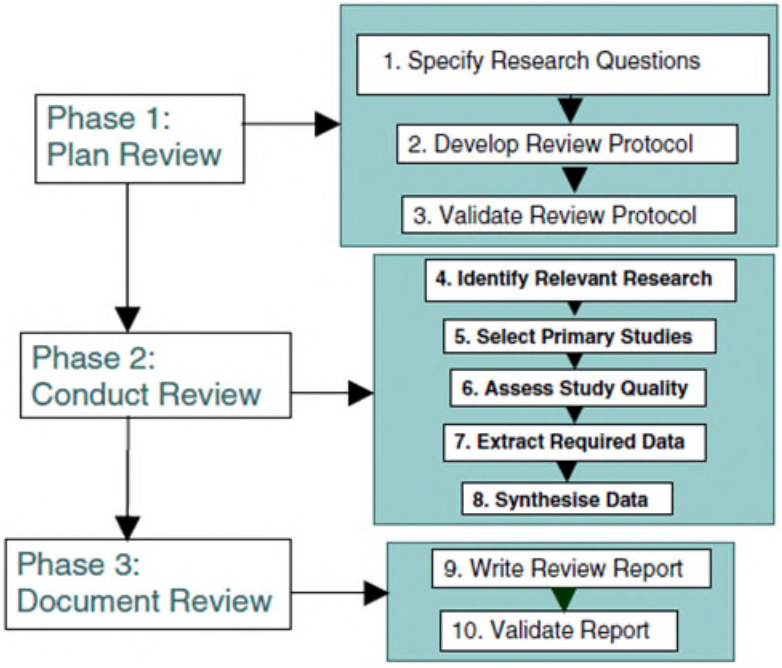


Figure 1. Systematic literature review process [30]

To achieve the research objectives and analyse the metadata of the relevant research documents were analysed using the open-source analytical R package Bibliometrix. [28] Bibliometrix permits to infer the pattern over time, themes researched, identify shifts, and to detect the most prolific institutions, authors, and countries in a particular area of research, [28] using co-citation, bibliographic coupling, strategic mapping, and co-occurrences analysis.

The study was carried out as follows. First, we retrieved all those existing papers in the topic of interest from the Web of Science (WoS) and SCOPUS databases, since Bibliometrix only accepts these two databases as input. The search query was run in September 2021 using the following search combinations:

‘‘Smart Vehicle* OR Automotive* AND Security*”

‘‘Cyber Security* AND Automotive* AND Challenge*”

‘‘Smart Vehicle* OR Automotive* AND Security* AND Challenge*”

‘‘Cyber Security* AND Automotive* OR Smart Vehicle* AND Communication*”

‘‘Cyber Security* AND Requirements * AND Automotive*”

‘‘Smart Vehicle* OR Automotive* AND Security* AND Standard*”

‘‘Smart Vehicle* OR Automotive* AND Security* AND Connected Car*”

‘‘Smart Vehicle* OR Automotive* AND Security* AND Attacks*”

‘‘Smart Vehicle* OR Automotive* AND IoT* OR IIoT* AND Security*”

‘‘Smart Vehicle* OR Automotive* AND VANET* AND Security*”

‘‘Smart Vehicle* OR Automotive* AND Smart City* AND Security*”

‘‘Smart Vehicle* OR Automotive* AND Vulnerabilities*”

‘‘Smart Vehicle* OR Automotive* AND Supply Chain* AND Security*”

‘‘VANET* OR Vehicle-ad-hoc-Network* AND Security*”

For example, the search command for the Web Of Science (WoS) was as follows:

TS=(("cyber secur" OR cybersec*) AND (automo* OR vanet))*

Where ‘*TS*’ stands for Topic; ‘*’ is used to retrieve words with variant zero to many characters (for example: automo* will include automotive, automobile, etc.); ‘*OR*’ used to find all records containing any of the terms; ‘*AND*’ used to find records containing all terms.

While, in the search command for SCOPUS looked like this:

TITLE (cyber AND security AND (automotive OR vehicle OR vanet OR (smart AND vehicle))) OR KEY (cyber AND security AND (automotive OR vehicle OR vanet OR (smart AND vehicle)))

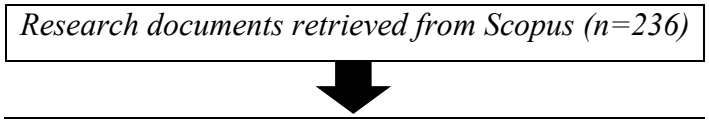
Where '*TITLE*' stands for the title of the manuscript and '*KEY'* stands for a keyword; '*OR*' is used to find all records containing any of the terms; '*AND*' is used to find records containing all terms.

Second, the results from the searches were filtered (language written, subject areas, etc.). The period was left open in order to analyse the behaviour of the theme throughout the history of the database. The types of documents found in the search were mainly published in *journals, conferences and proceedings, books, norms and standards*. To guarantee that our SLR did not miss any important material, secondary searches were conducted based on references, key journals and conferences found in the primary studies.

Moreover, following Kitchenham [29], to maintain the quality of the research, the selection of material for the SLR was subject to a set of exclusion criteria:

- Informal literature surveys (no defined research questions; no defined search process; no defined data extraction process).
- Duplicate reports of the same study (when several reports of a study exist in different journals the most complete version of the study was included in the review).
- Opinion pieces or viewpoints or purely anecdotal.
- Works describing software or technical solutions.

Furthermore, the content was revised, to especially discard those with a highly technical or mathematical component. A total of 326 items in WoS (Web of Science), and 236 from Scopus fulfilled the criteria and were included for further analysis. We combined the results from the two databases and excluded 25 duplicates for the next step, which resulted in a total of 537 unique documents. Furthermore, the titles, abstracts, and keywords of the selected articles have been manually reviewed, and those sources which were not in the field of research have been removed. The result was 517 publications, 193 were *proceedings;* 187 were *journal articles*; 125 were *conference papers*; 8 were *books (or book chapters),* and 4 were *working papers* (see Figure 2).



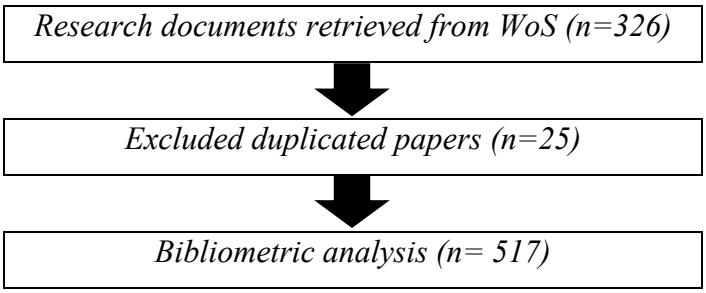


Figure. 2. Step-wise details of the data retrieval process.

Third, these search results were exported, both databases allow generating an exportable file where important information of the search result, such as the source of the publications, the name of the authors, affiliations, references, DOI numbers, and type of publication, abstract or keywords, is stored.

Fourth, the exportable files were uploaded to R for the bibliometric analysis. For this study, the tool used was Bibliometrix with the Biblioshiny package, [28] which creates relations between the metadata of the research materials obtained from the results, to provide information on research groups, main researchers, and related topics, among others.

For the analysis, the Bibliometrix R package, permits three different types of bibliometric analysis: *descriptive, relational and prospective.* [26, 28] The descriptive analysis provides information on the level of development in the different fields, comparing institutions, publishers, and countries, in different periods. The relational analysis looks at the cognitive structure of the research topics, the new themes or topics and the patterns. Finally, the prospective analysis assesses the impact of academic publications and compares the contributions between investigations, permitting to forecast the future research themes and topics.

3. Analysis and Findings

3.1. Descriptive Analysis.

Figure 3 shows the annual distribution of papers, with most of the material published since 2016. The timeline of publication of the papers, it being given by the Annual Scientific Production, see Figure 3, as it can be shown that the dataset is mostly, by recently published research material, between 2016 and 2021, but extends to relevant research material that covers from 2006 to 2022. This shows that research in this field is incipient. This is in line with findings from Contreras-

Castillo et al. [15] and Kennedy [33], who point out that for example the electric vehicle, IoT, or autonomous vehicles, are new fields of research. Moreover, this is corroborated by Contreras-Castillo et al. [15], and Haas and Möller [16], who note that within IT security, interest in cybersecurity in industrial environments has only take place in the recent years. Finally, the increase in electric cars has fostered automobile companies to include hardware and software in the design and engineering of vehicles to implement levels of cybersecurity in automobiles.[1,6]

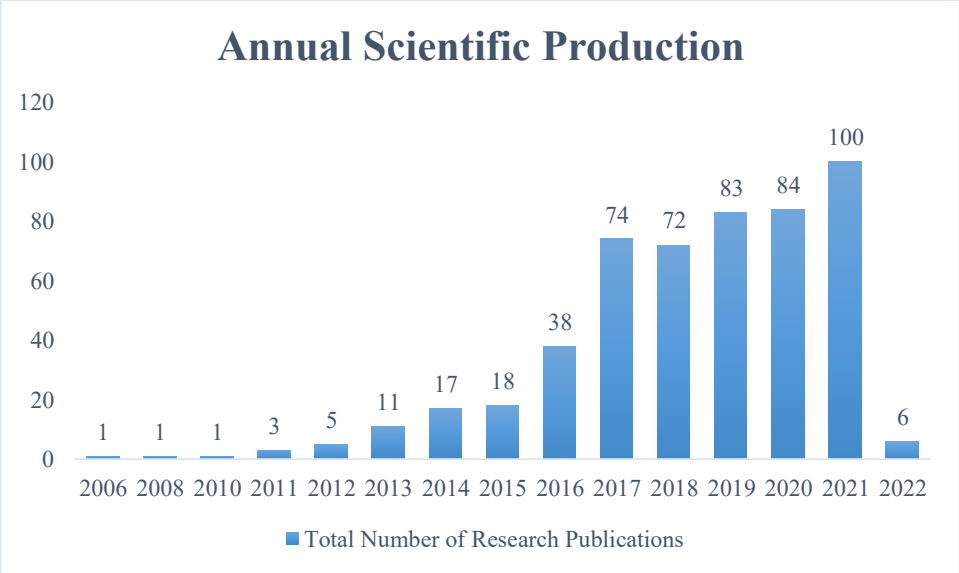


Figure 3. Scientific production by year

Regarding the geographical distribution of papers, Figure 4 show that most of the literature is produced in the USA (187), followed by the UK (80), Austria (78), China (68), Germany (62), Italy (50), South Korea (32), and India (28). Fundamentally, we see that the origin of the research corresponds to the level of development of automotive related services, components and manufacturing of the automobile sector. This confirms Gawanmeh and Alomari [13] and Kennedy et al. [14] who highlight the connection between academic research and industries.

Figure 4. Scientific production by country

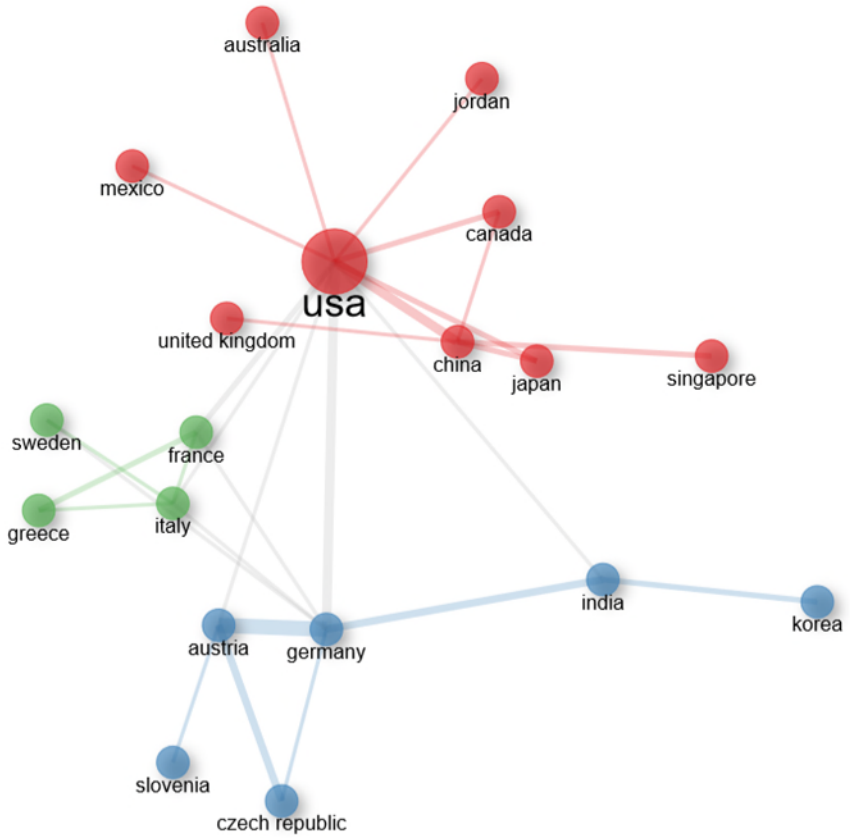


Figure 5. Country Collaboration Clusters

Figure 5, allows observing the main country collaboration clusters identified in the bibliometric analysis. [28] A cluster is a group of entities linked by article co-authorship relationships, that is, authors from different sites or institutions who contribute to the same publication. In Figure 5, each circle (node) represents a country, and the size of the node is determined by the number of publications contributed by the country. In addition, the groups of countries that usually publish jointly (cluster) are identified with colours. The countries located in the centre of the graph (e.g., USA or UK) are those with the largest number of nodes or interactions with other countries. The image shows the 30 countries with the largest number of publications, in which 3 large clusters of collaborations can be identified. These clusters do not imply that the countries that are in those clusters do not collaborate/interact with the others from other clusters, on the contrary. It is denoted by collaborations between the USA and Germany, or between Italy and Germany or France and Germany, which they are in different clusters. It can also be observed the collaboration on a global scale, where it is shown the importance of the USA, in terms of collaboration. It also can be observed the large nucleus of collaboration between Germany and Austria. These three countries mentioned are the ones that collaborate the most.

In terms of sources, there is a great variety of sources with the most common journals being *IEEE Access* (by IEEE) with 18 research pieces, followed by *Lecture Notes in Computer Science* (by Springer) with 12 and *ACM International Conference Proceeding Series* (by ACM) with 9 scientific materials.

In terms of citation, as shown in Figure 6, the top 3 sources that got more citations are *Lecture Notes in Computer Science (by Springer)* with 219 citations, followed by *IEEE Transactions on Intelligent Transportation Systems* (by IEEE) with 126 citations, and finally *IEEE Access* (by IEEE) with 119 citations.

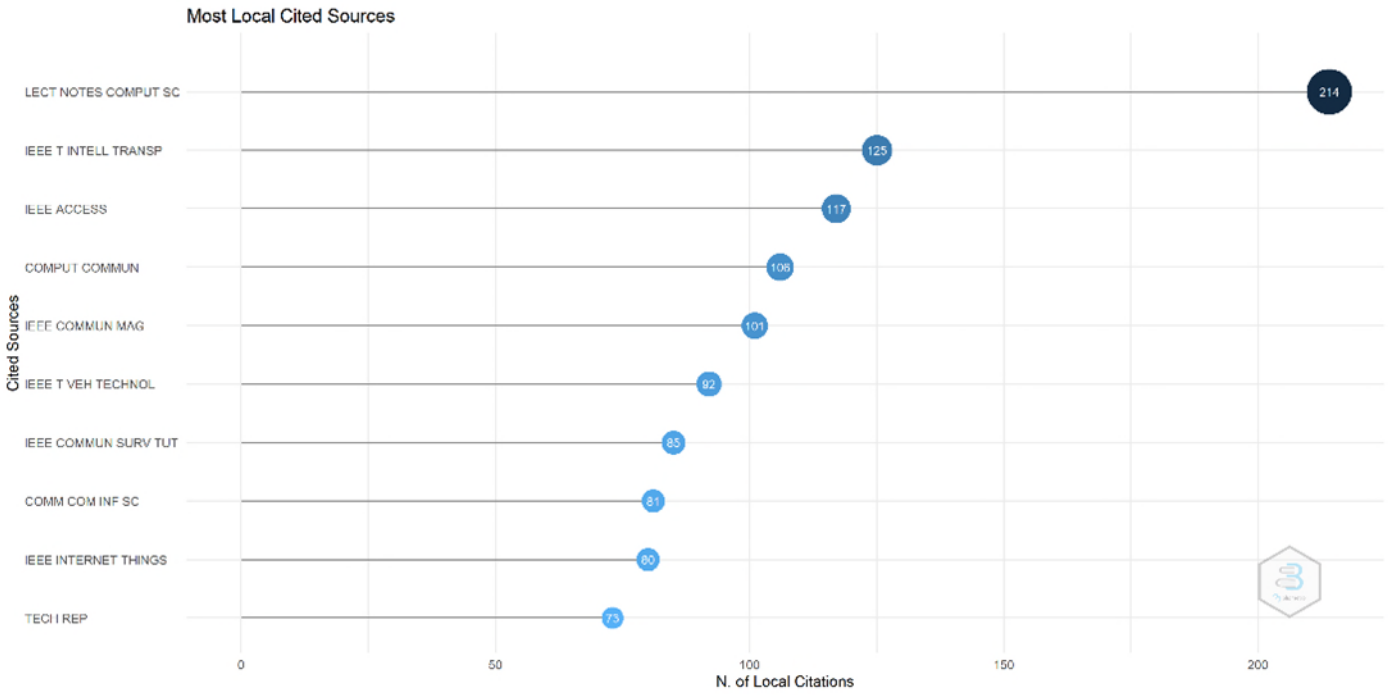


Figure 6. Analysis of Sources

The descriptive analyses also looks at the keywords. Figure 7 shows the word cloud that identifies the most used keywords, associated with the motor themes of the research materials. We identify the following:

- The most common or most used words are c*yber security* (including its variations, such as *security* or *cybersecurity*…) and *automotive* (or *automotive security/cyber security*). As previously mentioned, they were part of the main search criteria in both databases.
- As a second level in the importance of keywords, it is observed the keyword, *CPS* (cyber-physical systems) and its variations, and *embedded systems*.
- In that same second level, it can observe keywords related to connectivity: *Internet of Things* (IoT) and its variations; *connected vehicles*, *VANET* (vehicle ad-hoc network), *cloud computing*, *ITS* (intelligent transportation systems), etc.
- At a third level, we identified topics related to autonomous driving, such as *autonomous vehicles* and *machine learning*.
- In that same third level, there are words related to *functional safety* or *safety.*

- And finally, in a fourth level or keywords, we identify more niche concepts such as *privacy*, *intrusion detection* (with all the variations), *in-vehicle security* (*Controlled Area Network* and its variations…) and standards (such as *ISO 26262, ISO/ SAE 21434 or J3061*).

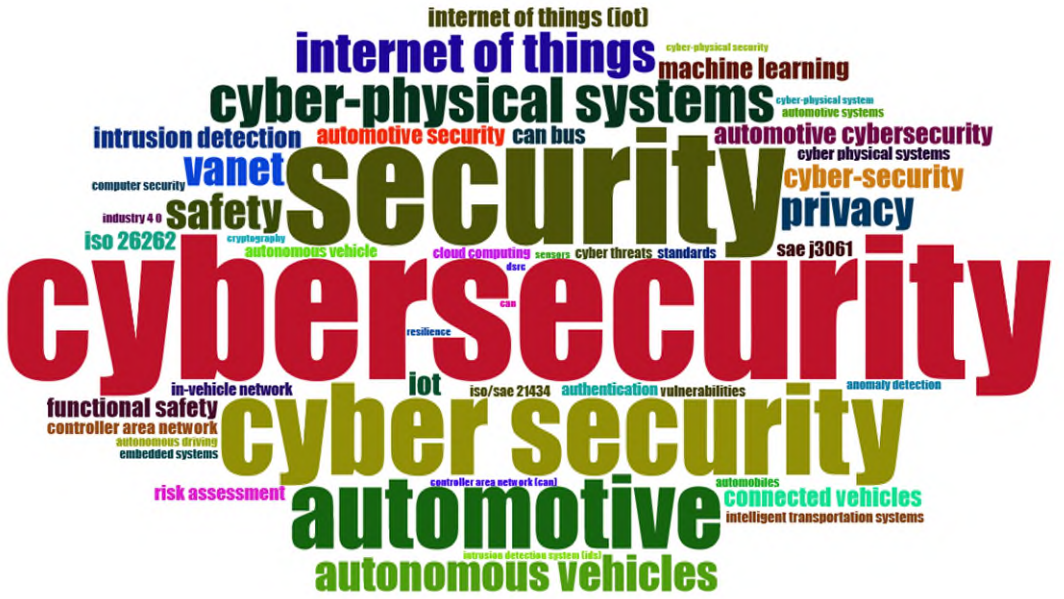


Figure 7. Word cloud of keywords

3.2. Relational Analysis: Research Scientific Fields

We employ the relational analysis to describe the cognitive structure of the research topics. To do this, we have performed an analysis of the keywords co-occurrence network, which explores the structure of a scientific field and attempts to find links between keywords. [28] Following Crocco and Chiaudano [34], the analysis was carried out using only Keyword Plus, given that being descriptors automatically generated by the Science Citation Index (SCI) through algorithms that extract keywords from all titles referenced in a text, that more clearly reflect the conceptual particularity of each publication. The parameters used for the development of the Co-occurrence network, was the Spinglass clustering algorithm, with normalization as the association type, with 50 nodes.

Figure 8 shows the result of this analysis in which four clusters that correspond to the main research scientific fields were obtained.

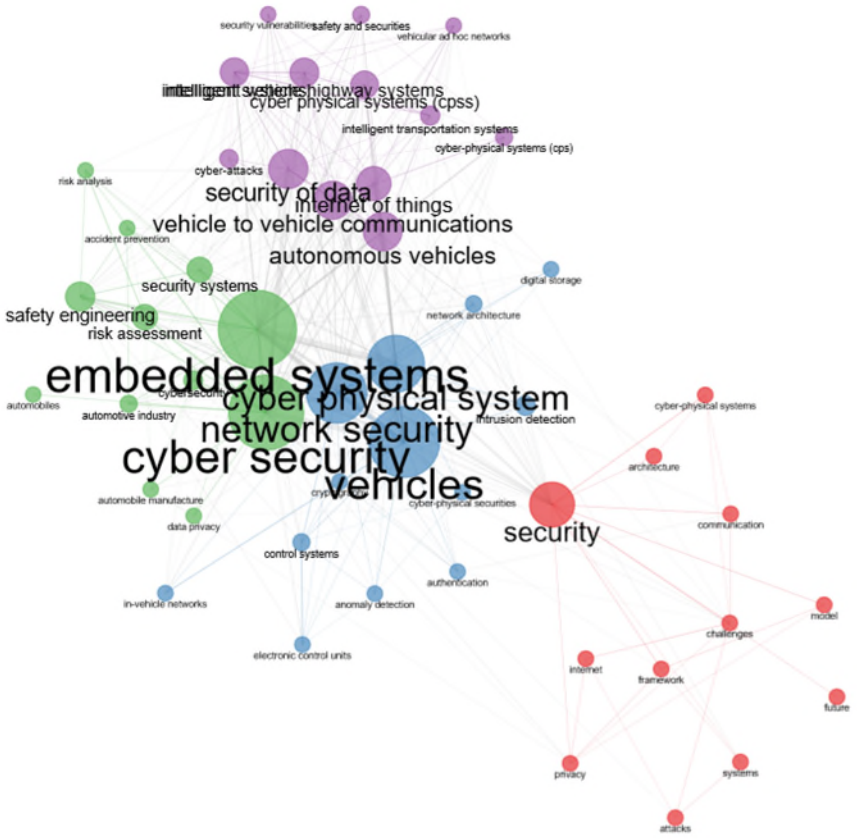


Figure 8. Co-occurrence Keyword Network

First, the keywords co-occurrence network shows a strong connection between the words "security", "cyber security", "embedded systems", "vehicles", "network security" and "cyber-physical systems"; Second, it also shows the existence of four main clusters that group the main research scientific field in the area of cybersecurity in the automotive industry (see Figure 8). In Table 1, we include a brief description of each cluster with the main keywords included, and the research field.

Table 1. Clusters of Research Scientific Fields

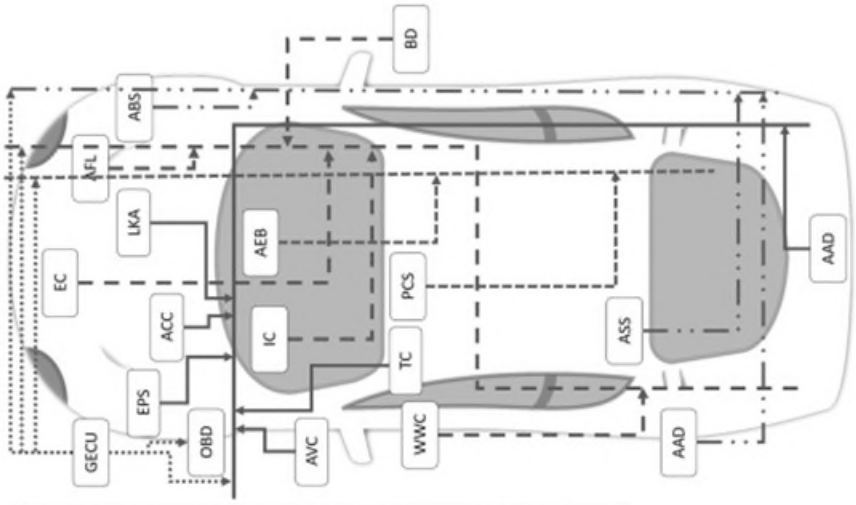
Cluster Colour	Main Fields	Keywords	Parent Field
BLUE	*Automotive Security*	*Automotive Security, Electronic Control Units (ECUs), Anomaly detection, authentication,* etc.	Automotive and IT security
GREEN	*Vehicle Engineering*	*Safety engineering, automobile manufacturing, risk assessments* and *analysis, accident prevention,* etc.	Supply Chain, Manufacturing
PURPLE	*Smart Vehicle*	*Security of data, vehicle-to-vehicle communications, intelligent transportation systems* (ITS), *internet of things* (IoT), *autonomous vehicles,* etc.	Connected Vehicles, Internet of Things
RED	*IT Security*	*Challenges, architecture, frameworks, attacks,* etc.	IT

Cluster 1: Automotive Security

The first cluster is the *Automotive Security* cluster (in blue in Figure 8). This cluster of research covers the security characteristics that make cars different from other technology devices. The *automotive security research* identified deals with the justification of the need for cybersecurity in the automotive industry. The association between cybersecurity and the automotive industry comes from different groups of papers.

The first group of the papers explains the association between cybersecurity and the automotive from a *technical perspective* (for example, [4,11,12,13,14,16,35,36]). This approach indicates that the increase in the technical complexity of vehicles makes it necessary to incorporate cybersecurity. For example, in Figure 9, we see the distribution of the principal Electronic Control Units (ECUs) that control a vehicle. [37] Khurram et al. [38], and Eiza and Ni [4] point out that the advance in vehicles is derived from the incorporation of IT systems into vehicles. These electronics and software additions have made significant contributions to vehicle safety, value, functionality, and connectivity. In fact, McAfee [36] points out that 90% of all innovations in automotive are based on electronics and software, with up to 80 processors being integrated into a high-end vehicle, which is also an important cost factor in automotive manufacturing. In this context, Rosenstatter and Olovsson [6] and Eiza and Ni [4] point out the need to protect the functionality of these electronics and software components. Rosenstatter and Olovsson [6], and Gawanmeh and Alomari [13] noted that while software security is a relatively well-established field, protecting automotive IT systems against tampering, is an emerging field of research. Moreover, Khurram et al. [38], Mejri et al. [39], and Raw et al. [40] emphasise the need for protection in an open-systems environment, where

vehicles have increased the number of external connections, increasing the use of shared information and communication in vehicles and thus the vulnerability to cyber-attacks.



EC	Engine control	ABS	Antilock braking system
GECU	Gateway ECU	AFL	Adaptive front lighting
LKA	Lane keep assist	BD	Blind-spot detection
AEB	Autonomous emergency braking	ASS	Active suspension control
ACC	Adaptive cruise control	AAD	Active aero-dynamics
EPS	Electronic power steering	OBD	On-board diagnostics
PCS	Precrash safety	AVC	Adaptive vibration control
WWC	Windshield wiper control	TC	Transmission control
IC	Instrument cluster	SS	Security system

Bus 1
Bus 2
Bus 3
Bus 4

Figure 9. Electronic Control Units (ECUs) in the automobile [37]

The second group of papers that justifies the need for cybersecurity in automotive comes from the *field of road safety*. [4,6,36,41] National Interministerial de la Sécurité Routière [42] argues that transportation is growing dramatically; roads are becoming more dangerous due to the effect of congestion and increased probability of collision [42], which requires that securing traffic becomes not only a necessity but also an obligation. Thus, assuming this premise, Mejri et al. [39] and Kennedy [33] point out that since new vehicles are smarter and more interconnected, it is essential to have security in the vehicle. For instance, the incorporation of new features, such as autonomous driving, remote diagnosis and software updates means the vehicle is exposed to more vulnerabilities. From the point of view of road safety, this implies that it must be protected since an incident could leave a whole fleet of vehicles out of service and cause innumerable accidents and hazards [40,43].

Finally, Kargl et al. [43], Eiza and Ni [4], Raw et al. [40], and Contreras-Castillo et al. [15] justify the need to incorporate cybersecurity into automotive by considering this as *a device from an*

interconnected world. Khurram et al. [38], Dattathreya et al. [44], and Han et al. [45] comment that cars become a new target for cyber-attacks as they become more and more connected. These authors point out, that while increasing autonomy and connectivity in vehicles brings many improvements in terms of functionality and convenience, it also brings new cyber threats present in an ecosystem that is part of a fully connected world. In fact, connected vehicles are an integral part of the smart city vision and a node in the Internet of Things (IoT) world [40,46,47,48,49,50].

Cluster 2: Vehicle Engineering

The second cluster is the *Vehicle Engineering* cluster (in green). In this cluster, the topics discussed are focused more on the classical vehicle engineering, manufacturing and supply chain perspective, looking at things like functional safety, embedded devices and standards and compliance, among others. Moreover, this line of research also deals with the relationship between cybersecurity and the automotive industry, highlighting the need to create and apply standards in this industry.

The first group of papers considers the research that covers supply chain security (see, for example,[1, 22, 35,51]). This stream investigates the security of the Trier 1/2 component supplier (security from devices that comes from outside the organisation), the security of the assembly line (software flashing, the hardware part number check, etc.), and security at trusted points for software updates and diagnosis services (either wired or wireless). In this line, Rosenstatter and Olovsson [6], and Schoitsch et al. [1] have related the cybersecurity concept with the supply chain, pointing out the peculiarities of the vehicle in terms of the supply chain. The cybersecurity must cover from the early stages of design to the final assembly and the end of life of the vehicle. This means that the implementation of cybersecurity in the automotive industry has its particularities with respect to other industries (see, for example, [35]). In this context, Eiza and Ni [4] analyse the weakest links where a car can be compromised in the supply chain. Moreover, Conway [22], and Mejri et al. [39] emphasise the new security threats that will arise from the implementation of smart manufacturing systems. These will make the car vulnerable during the assembly or configuration, which is when the "defences" are not yet active or put into place. Additionally, Rosenstatter and Olovsson [6], and Raw et al. [40] also point out the lack of security in the "trusted" centres where the vehicles are doing maintenance or being tested. These are also vulnerable points that can be exploited by attackers, possibly aiming to install malware into the vehicles.

A second group of the papers focuses on defining and conceptualising an *automotive security framework* [6,49, 50, 52,53,54,55,56,57]. Previous literature points out that in the automotive security framework there exists a complexity and diversity of criteria in the conceptualisation of, for example, the life cycle of a vehicle, its supply chain, the implementation of secure communication, or when considering the new requirements and technology for the vehicle. Moreover, the studies in this cluster mainly originate from two frameworks, from *IT* and industrial processes [5, 50, 53, 58, 59]. In general, this research points out the high complexity of determining an adequate security framework in the automotive industry. In this line, Papadimitratos et al. [60], Lu et al. [58], Pacheco et al. [53], Jeschke et al. [55], Razzaq et al. [49], and Maglaras et al. [56] note that there are several characteristics of frameworks that can be applied to build trustworthy services for smart cars. The vast majority divide the framework depending on the characteristics of the services they provide; in this way, the typology of threats is different and therefore the security measures will be more specific and effective. These authors show that the framework that is commonly used to develop secure smart vehicles is divided into four layers: *end devices, communications, services, and applications*. For example, cyber-attacks can be launched against each of these layers. Moreover, Leinmuller et al. [59] define threats in terms of the target, impact and mitigation methods for each layer of the framework.

The third group of the works has addressed *the challenges of developing a security framework for vehicles* [4,6, 35, 49, 53, 54,61,62,63,64,65]. Schoitsch et al. [1], and Pacheco et al. [53] note that one of the main characteristics that differentiate the automotive industry from other industries is its product life cycle. Vehicles are a package of components from numerous suppliers that are developed in isolation from the rest of the vehicle, making it more complicated to have effective security in place as compared to other industries. Papadimitratos et al. [60], SAE [35], and Bertino et al. [54] conclude that one of the biggest challenges when developing a security framework for the automotive industry is the suppliers and the supply chain since most of the components will have to come with built-in security and this will have to match with the rest of the vehicles' security.

Finally, a group of papers has investigated the standards for the automotive industry, the comparison of safety and protection standards with existing standards, and the process of creating a specific standard [1,5, 18, 35,36,66]. More in detail, Schoitsch et al. [1], Contreras-Castillo et al. [15] and Grubmüller et al. [66] highlight the content of the standards, which are derived from existing safety standards since the vehicle is in a safety-critical system so that if the vehicle is compromised by a

cybersecurity incident a safety hazard can occur. In this sense, they have inherited many common terms from the safety standards. Other authors point out that the content of the standards should derive from the classic IT cybersecurity since today's vehicles are highly interconnected and have many more IT components (see, for example, [1, 36]). For this reason, part of the research is related to automotive security standards coming from IT, although with obvious differences. Additionally, other studies note that another problem in this industry, in which the homologation of vehicles is critical, is the *choice of the supplier of the standard* since there are a large number of suppliers that operate at the national or international level (see, for example, [1,6]). Papadimitratos et al. [60], Dattathreya et al. [44], Haas and Möller [16], and Eiza and Ni [4] point out, that the development of security requirements based on the existing requirements in the automotive industry such as, safety requirements. Schoitsch et al. [1] point out that in many cases, as shown previously in the research line of the standards, current research tends to mimic or copy the safety requirements and adapt them to security. However, Gawanmeh and Alomari [13], Rosenstatter and Olovsson [6], Haas and Möller [16], Eiza and Ni [4], and Han et al. [45] position themselves against these methods since the design of safety requirements is focused on the physical security of the vehicle occupants and cybersecurity tries to cover not only the physical security of the vehicle occupants but also other things such as privacy and data integrity.

Cluster 3: Smart Vehicle

The third cluster refers to *Smart Vehicle* (in purple, see Figure 8). The research in this cluster focuses on the connected vehicle or the smart vehicle looking at how the vehicle is part of the smart city, connecting to other vehicles, infrastructure, and devices, and how it performs intelligence features like autonomous driving, data streaming, over-the-air diagnostics and software updates. This research approach considers the vehicle as an *interactive open system* as part of *IoT space* (see, for example,[17, 18,19, 20, 21, 38,40, 54,67,68,69,70) More in detail, the vehicle is integrated as an element of the IoT space/landscape, considering it as a node of the Smart City.

First, Radanliev et al. [18], Bertino et al. [54], and Eiza and Ni [4] emphasise the *relationship between vehicles and smart cities*. These authors comment on the importance of cybersecurity in vehicles that are connected to a Smart City. Moreover, Kargl et al. [43], and Khurram et al. [38] mention the position of the Smart vehicle not only as a consumer but also as an information provider, which makes cybersecurity for vehicles critical in the environment of Smart Cities.

Second, the literature has focused on the vehicle as the main actor and has dealt with *the security issues of Vehicle-ad-hoc Networks (VANETs)* [38, 40, 63, 71, 72, 73, 74, 75]. Raw et al. [40], and Khurram et al. [38] find that one of the biggest issues with VANETs is the technical limitations associated with them, such as limited computing power, and sudden loss of signals in the vehicles or problems with real-time communication exchange. VANETs are also full of challenges since the existing security systems and measures are limited on this platform. These authors identify that the impediments or common challenges that exist to implementing security in Smart vehicles are real-time constraints, data consistency liability, low tolerance for error, cryptographic key distribution and high mobility, among others.

A third group of works deals with security trends or *models for external vehicle networks* [4, 18, 46, 52, 63, 73, 76, 77, 78]. Mejri et al. [39], Mccluskey [75], and Malhi et al. [79] comments on different ways to secure the vehicle and ad-hoc-networks. In general, most of the research that deals with this topic focus solely on cryptography, with most of the research aiming to find an algorithm that interacts well with IoT devices and vehicles. There are also a limited number of authors (for example, [40]) who discuss implementing security measures in the vehicles, such as IDS (Intrusion Detection Systems) and other similar systems, all of them from classic *IT network security*. Rosenstatter and Olovsson [6], and Khurram et al. [38] cover interactions with the manufacturer (e.g. assembly line, dealership, garage, etc.) for processes such as software updates or diagnostic services.

A final group of researchers have emphasised the *standards for smart vehicles* [1, 6, 33, 36]. The smart vehicle requires standards to be used in the development of a vehicle. If a vehicle wants to communicate with other systems or devices, they must be compatible[38, 60]. Moreover, this requires the security standards to be developed so that they can securely enable communication/interaction of the systems without compromising the vehicle or third parties (see, for example, [1, 68]).

Cluster 4: IT Security

The fourth cluster is on *IT Security (*in red, in Figure 8). This cluster includes research focused on IT security-related issues, such as protection from external cyber-attacks, internet connectivity and vulnerabilities.

The first line of research in this cluster identifies the security requirements that a vehicle will need [5, 12, 15, 16, 35, 38, 40, 44, 45, 59, 60]. Papadimitratos et al. [60], Mejri et al. [39], and Dattathreya et al. [44] find that the requirements are inherited from IT, such as secure communication and authentication (through communication encryption) both in the vehicle's internal network and in the

communication of the vehicle with other systems. Other researchers such as Eiza and Ni [4], and Hasrouny et al. [80] indicate that intelligent vehicles or ITS (intelligent transportation systems) are an important source of new security requirements. Moreover, other requirements are not directly extrapolated from IT security and are exclusive to vehicles; these tend to be generally less technical than those mentioned above [5, 35, 36, 40, 45, 74, 81, 82, 83].

The second group of works in the automotive cybersecurity landscape deals with *attacks on vehicles* [1, 33, 36, 39, 40, 53, 81, 84, 85, 86, 87, 88, 89]. In this topic, Rawat et al. [85], McAfee [36], Yaqoob et al. [87], La Hoa and Cavalli [81], and Shams et al. [88] looks at all the possible attacks that can be performed to vehicles or that could affect vehicles (as part of an IoT network). Most of the attacks on vehicles are unique to the automotive sector and affect specialised hardware and software that is used by the vehicles. The main areas and components that are subject to attack are listed in Table 2.

Table 2. Typology of attack/vulnerability and vehicle components.

Vehicles Components	Description	Type of Attack/Vulnerability
Hardware Components	All hardware components that a vehicle is made-of, this includes all the structure components (doors, roof, chassis, seats, steering wheel…), and all internal components (ECUs, Cables. Sensors, Actuators, and other parts…).	Hardware is safety-critical to the vehicles, thus any vulnerability or attack that will compromise the physical hardware of the vehicle will make any security control invalid (for example compromising the OBDII port of the vehicle). Therefore, the physical security of the vehicle is key to ensuring the integrity and availability of the hardware.
Software Components	The vehicle is loaded with all types of software, that needs to work in other to be able to operate the vehicle safely, some of the software is just to check that hardware parts are correct (or doing what they are supposed to do), such as door lock (make sure the doors of the vehicle are close, if not an alarm and a warning light will appear) or seat belt warning, engine check (checking all the parts and fluids are correct), etc. Other Software is more complex and it performs a set of complex actions and decisions, such as Automatic Parking Assistance (taking into consideration numerous variables and sensors inputs to park safely the car), Automatic Emergency Assistance (if the vehicle crashes an emergency assistance call will be made on behalf of the driver, sending data such as vehicle details and location…), Hill Descends Control (which allows 4x4 vehicles to descend safely through rough terrain), Adaptive Cruise Control, etc.	Compromised software can cause confidentiality, integrity, and availability to the vehicle and its components, and could cause a hazardous situation to the vehicle, its occupants, and other road users. As previously mentioned, the software is everywhere on vehicles and performing different tasks, thus, having a very wide software threat landscape that could be exploited by an attacker. Most of the software is connected to other components and other software (as the vehicle needs to work as one), making it easier for an attacker to compromise the rest of the vehicle once an initial software has been compromised.
Attacks by Components and Control Module		
Engine Control Module (ECM),	Controls and monitors a series of actuators and sensors associated with the	If an attacker can alter or manipulate the Engine Control Module, this could lead to engine failure,

	ICE (Internal Combustion Engine) to ensure optimal engine performance.	which could cause a crash or potential safety hazard.
Telematics Control Unit (TCU),	The TCU collects telemetry data from the vehicle (location, speed, engine data, battery data. diagnostics, etc), and wirelessly reports the data.	A buffer overflow could compromise the TCU and allow and attacker to execute arbitrary code, which could disable the infotainment system of the vehicle.
Electronic Brake Control Module (EBCM)	Monitors the sensors and actuators of the braking systems and can activate the ABS (Anti-lock Braking System) or traction control system when necessary.	A spoofing attack may result in the ABS controller receiving incorrect data and not being able to do its function causing a possible car crash.
Battery Control Module (BCM)	Monitors the state of the battery and measured current, voltage and temperature values to evaluate the state of the battery and to determine actions on the on-board electrical system.	If the Battery Control Module is compromised, it could lead to the potential explosion of the battery and the whole electric vehicle could catch fire.
CAN/FlexRay/LIN/Ethernet Network	The vehicle has an internal communications network that interconnects components inside the vehicle. There are currently 4 types of networks used on vehicles: CAN (Controlled Area Network), FlexRay, LIN (Local Interconnect Network), and Ethernet.	If the network is compromised, this could cause disruption on messages being transmitted, and some of them will affect safety-critical functions. For example, if the vehicle uses a by-wire system (for instance brake-by-wire) or any other autonomous driving feature, this will make disruptions network communication critical both the authenticity of the messages, together with the speed of the transmission.
Infotainment Systems	In-vehicle Infotainment is a set of hardware and software components that are aimed to make the vehicle journey more comfortable, this could be by providing entertainment options (such as Radio, Music, Phone Connectivity, TV for passengers…), and/or driver assistance options (Global Satellite Navigation…).	Infotainment is essential for the comfort and assistance of the driver and its passengers. Infotainment is the most vulnerable part of the vehicle, as it is very complex software-wise, reliant on many third-party providers, and can also connect to the internet. Compromising the infotainment can make the car 'unusable' in some cases (such as Tesla vehicles, where most of the vehicle functions are activated through the infotainment).
Tyre Pressure Monitoring System (*TPMS)*	The Tyre Pressure Monitoring System monitors the pressure inside the vehicle tyres. The pressure information is sent wirelessly to the other components of the vehicle.	It is a popular 'entry point' for attackers to access the vehicle. Moreover, most of the current TPMSs do not support cryptographic modules for the security of the transmitted data, due to limitation of resources or cost. If the tyre pressure warning message is tampered with or denied, this may result in the driver missing the opportunity to stop the vehicle safely.
Remote Keyless System	A remote keyless system is a feature that allows unlocking and opening the vehicle from a distance by using a unit that sends signals to the car from a wireless transmitter (or Key fob). There is also Passive keyless entry (PKE) where the driver will not have to engage with the vehicle other than getting close to it with the wireless transmitter (or Key fob).	An attack on this module could lead to the theft of the vehicle. Furthermore, most of the cyber defences of the vehicle are designed to rely on the integrity of the vehicle components and assume that an attacker does not have access to the physical components of the vehicle. Therefore, if the Keyless entry system is compromised, this could cause that many of the security controls become ineffective.
Advanced Driver-Assistance System (*ADAS)*	An Advanced Driver-Assistance System (ADAS) consists of a group of electronic technologies and ECUs that assist drivers in driving and parking functions. ADAS uses sensors in the vehicle such as radar and cameras (or LIDAR) to perceive the outside to decide the next safe action of the vehicle. ADAS can enable different levels of autonomous driving depending on the features,	Denial/Alteration/Malicious use could lead to injury of vehicle occupants and other road users (hazardous events, crash vehicle, and weaponised vehicle)

		sensors, and actuators that are in the vehicle.	
Mobile Control	*(Smartphone)*	Nowadays, most car manufacturers offer a smartphone app that lets you control vehicle functions without being inside the car. Whether it's using your phone as a key or using the HVAC (heating, ventilation, and air conditioning), status on vehicle charging, metrics, diagnostics data, etc.	Vehicles connected to the app are vulnerable to the functions that the app can control (this could include, lock of the vehicle, air-conditioning…), as these are managed in an uncontrolled environment, compared with the rest of the vehicle. Thus, having a different security tolerance compared with other features of the vehicle. These types of applications provide a perfect entry point for attackers.

Attacks may vary from in-vehicle attacks (when the attacker compromises a component inside the vehicle, or in the vehicle parts), network type attacks (such as DoS, Bluetooth attacks, etc), IoT attacks that may affect the availability of vehicles to perform in a normal behaviour, malware attacks on the vehicle, to hardware-oriented attacks (induces malfunction of hardware within the vehicle). The literature notes that attacks can be generally classified depending on their objective; for example, attack on integrity or trust, attack on authenticity or identification, attack on availability, and attack on confidentiality [1,13,33, 39, 40, 53, 85, 86]. Malla and Sahu [86] conclude that the first action to developing effective security measures for the vehicle is to understand what can be compromised by the attacker.

3.3. Prospective Analysis: Future Research.

For the prospective future research on cybersecurity in the automotive industry, we have used a strategic map (Figure 10). A strategic map is a two-dimensional graph, which uses the rank values of centrality and density, which produces a 2X2 quadrant on basis of high and low-rank values of centrality and density. These four quadrants are classified as *motor* quadrant (upper right), transversal or *basic* quadrant (lower right), *peripheral* quadrant (upper left) and *emerging* or disappearing quadrant (lower left). [26, 28] It is evident from the strategic map that the entire research base is structured into 8 themes: five motor themes/right upper quadrant (privacy, systems and impact, trust, IoT management, wireless sensor networks cybersecurity; cyber-physical and cloud); three basic themes/right lower quadrant (Internet things and information; security systems models; challenges attacks communication); one niche themes/ left upper quadrant (anomaly detection).

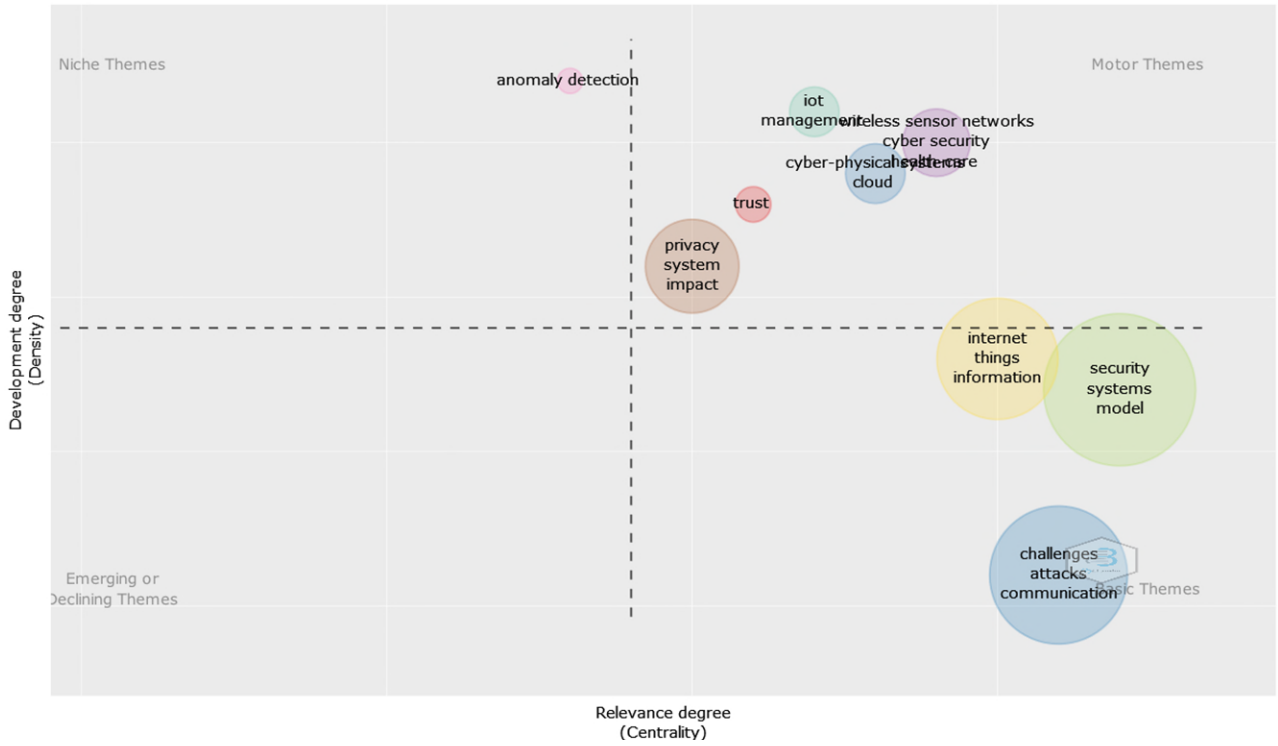


Figure 10. Strategic Map

First, *base themes* in the right lower quadrant or base theme quadrant include three themes: security models, IoT and attacks. The themes in the base quadrant have low density (weak internal tie strength) and high centrality (strong external tie strength). Analysing this thematic structure, we can observe that these three themes are the largest in terms of size of research, but with a low density of connection between topics. The later can be attributed to the diverse origin of the literature, which makes cybersecurity research in this area diverse and unconnected. Figure 8 shows that the first research approach comes from the *IT area*, which emphasises the use of IT frameworks and requirements, focusing on attacks and their possible solutions from cryptography. This line of research displays a limited scope derived from the heterogeneity of components that include the automotive industry, the extent of cybersecurity both in the life of the product and throughout the supply chain, and the problem that cybersecurity ranges in this industry that cannot be covered by IT. The second line comes from *IoT*, which considers the vehicle an open system in interaction with the Smart City. Although this research emphasises the protection of communications with the car, its contribution, for now, is very limited. The third line originates

from the research on *industrial sectors*. In this line, a vehicle is a production unit, in which security is an extrapolation of security in the industrial sectors, dealing with issues such as the life cycle and supply chain. Thus, the search for standards or cybersecurity models is the main work developed in this line.

In the upper right quadrant there are five themes, which are represented by five spheres of different sizes, denoting the volume of research within a theme (Figure 10). Themes within the motor quadrant have a high-rank value of density (degree of tie strength within the theme) and centrality (degree of tie strength with other themes) and are hence considered as a developed theme. A first analysis shows an interesting diversity of topics, including privacy issues, IoT, networks, and cyber-physical care, with an extensive interconnection between them. However, we see two important shortcomings. First, the size of the circles represents the number of works in each area, resulting in a low volume of work in general. Second, if we compare Figures 8 and 10, they show that some topics do not appear in Figure 10 as driving topics in the development of research in automotive cybersecurity. More in detail, an important gap is on the subject of *standards*, despite the joint development of the OEMs for the *ISO/SAE 21434 Road vehicles – Cybersecurity engineering* standard, there are still gaps in terms of what the security requirements must be for the vehicle. Thus, given the *heterogeneity of technology* that vehicles from different manufacturers have (and even within the same automaker), the cybersecurity requirements are different. Moreover, we also note another important gap in the research on the engineering *framework* point of view. Vehicles have a mixture of inherited technologies and legacy components from previous vehicles and newer technology to satisfy the new customer demands. Finally, a gap can also be observed in Figure 10 on the *supply chain* topic. In general, the works in this topic do not cover or elaborate on the supply chain security, when from a manufacturing point of view, it is the most important to manage an effective cybersecurity strategy for the vehicles.

Finally, we observe the scant relevance of quadrant three, niche themes, and the fourth quadrant, which corresponds to emerging themes. In general, if we compare Figures 8 and 10, with the exception of anomalous detection as a niche topic, we observe a low or null representation of topics, showing that there are important gaps for the future of research in automotive cybersecurity. First, there is a clear gap when vehicle security is developed, which causes the vehicle to have numerous vulnerabilities, this problem can be traced back to *vehicle design,* existing research do

not look at the part of the vehicle's lifecycle when it is in the hands of a customer and the vehicle is "complete" (from a manufacturing perspective). Another gap is that the researchers do not address *zero-day exploits* and *design flaws*, causing vehicle vulnerabilities to be patched, but not resolved, in many cases causing the patch to produce another vulnerability. Moreover, Figure 8 has not included the updates in the vehicles and the software guarantee (for the maintenance of this, including security patches). Finally, we also note that topics from new developments in the automotive industry, such as autonomous vehicles, do not appear as niches or emerging topics.

4. Conclusion

This study reports the scientific research related to automotive cybersecurity from 2006 to 2022. A total of 517 research publications, including empirical research papers, theoretical and conceptual articles, systematic literature reviews, and conference papers have been analysed. By understanding, analyzing, and reporting scientific research related to cybersecurity in the automotive industry, we have been able to appreciate the extent of the domain knowledge accumulated over the years. The publication trends, as per institutions, and countries, are explored and reported. Further, this study has assessed the keywords patterns, strategic map, and co-occurrence keywords network, showing the cognitive map of the research, and the future thematic research.

Our bibliometric review of automotive cybersecurity allows us to derive important conclusions for research and implications for policy-makers. From the point of view of research, we can conclude that there are four lines of research that, with different approaches and origins, address cybersecurity in the car. The first line focuses in cybersecurity for the vehicle (Automotive Security), where the technical aspects of the automobile and transport prevail in the investigation; the second line (Vehicle Engineering) from the perspective of supply chain and manufacturing addresses cybersecurity in the car as a process to be developed in car manufacturing; the third (Smart Vehicle) considers the car as a device in the environment of smart cities; and the last line comes from IT security, which from a general cybersecurity perspective addresses cybersecurity problems in the car.

A second conclusion from the point of view of research arises from our bibliometric analysis, where we find important future challenges for the research on cybersecurity in automotive. A first challenge, in line with McAfee [36], is that the future of vehicles is something that is *not completely*

clear today. Onishi [90] comments that the future of vehicle ownership will disappear to make way for a new model of share-ownership. Zhang et al. [91] point out that this will depend on how IoT devices and the concept of a Smart City are developed in the future since share-ownership models require a functioning Smart City. Another point to consider in the future challenges of the research on automotive is the *assembly process*. As with the supply chain and Smart Manufacturing, this entails new security measures, especially around the authenticity and identification of devices [5, 35, 90,92]. The next challenge relates to the importance that *autonomous driving* will obtain in the near future. Fully-autonomous vehicles cannot be conceived on the road with other vehicles that are not as technologically advanced since these vehicles would be unpredictable for the autonomous driving systems [15,33, 36, 75]. The last challenge is how *cybersecurity standards* are dictated. As previously explained, the OEMs (Original Equipment Manufacturer) offer different combinations of features to customers, which provides varying levels of complexity to vehicles, and not all vehicles offer the same type of features, making it difficult for strict standards to apply to low-cost vehicles or vehicles with fewer features.

As implications for managers and policy-makers, we must consider that the implementation of cybersecurity in the car must be integrated into a model that contains both the life stages of the vehicle and the connectivity of the vehicle in the context of IoT. First, given the vehicle development life-cycle, it should be a *multistage model*. Cybersecurity will need to be embedded in all the stages from the concept design, the implementation, to the final stages of the verification and validation process (including penetration testing). To be an effective multistage security model it will also need to cover security on components or software provided by suppliers. Second, it should be a *multi-level model*, as a consequence of the interconnection of the vehicle and the emerging threats from those connections (Vehicle2Vehicle communication, software over the air updates, smartphone control applications, etc.). As we have seen in previous points, security design such as defence-in-depth and multi-layer security will need to be considered, to protect the vehicles critical systems (such as autonomous driver systems, software updates, physical security mechanisms) and sub-systems (such as autonomous parking, autonomous emergency braking, key fob/RFID (Radio-frequency identification) security, control by smartphone, etc.). Third, the model must include the *time dimension*, considering that the cybersecurity process must understand the whole life of the vehicle, from the moment the software is flashed into the vehicle in the production line to the moment the vehicle is recycled. Finally, the model should be *multi-feedback*, structuring

the process design as a feedback system, and including incident response, diagnosis services and vehicle updates; the multi-feedback model is essential to keep the security level and maintain the controls of the vehicle.

Table 3. Vehicle Cyber Security Model

Characteristics of the model	**Topics**
Multistage Model	Security is embedded in all stages of the development life-cycle of the vehicle: Design, Implementation, and Testing & Validation.
Multi-Level Model	Defence-in-depth and Multi-Layer security
Time Variable	All life of the vehicle: from the assembly the, to use by the customer until recycling of the vehicle
Multi-Feedback	Feedback system throughout the life of the vehicle

Like all research, this study contains some limitations. A first limitation arises from the dispersion of works in the area of cybersecurity, which can mean that some works have been left out from this SLR. A second limitation stems from the incipient nature of cybersecurity studies (as evidence by the number of works since 2016), which may mean that predicting future lines of research may contain a certain bias, as the research is not yet very consolidated.

References

[1] Schoitsch, E., Schmittner, C., Ma, Z., Gruber, T. The need for safety and cyber-security co-engineering and standardization for highly automated automotive vehicles. *Advanced Microsystems for Automotive Applications*, Springer Cham. 2016; 251-261.

[2] GRVA. *Draft Recommendation on Cyber Security of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 GRVA*. Secretary of the UN Task Force on Cyber Security; 2018. https://www.unece.org/fileadmin/DAM/trans/doc/2018/wp29grva/GRVA-01-17.pdf

[3] Amin, M., Tariq, Z. Securing the Car: How Intrusive Manufacturer-Supplier Approaches Can Reduce Cybersecurity Vulnerabilities. *Technology Innovation Management Review*, 2015; *5*(1):1-25.

[4] Eiza, M. H., Ni, Q. Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity. *IEEE Vehicular Technology Magazine*, 2017; 12(2): 45-51.

[5] Macher, G., Armengaud, E., Kreiner, C., Brenner, E., Schmittner, C., Ma, Z. Krammer, M. Integration of security in the development lifecycle of dependable automotive CPS. *Solutions for Cyber-Physical Systems Ubiquity*, IGI Global, 2018; 383-423.

[6] Rosenstatter, T., Olovsson, T. Open Problems when Mapping Automotive Security Levels to System Requirements. *Proceedings of the 4th International Conference on Vehicle Technology and Intelligent Transport Systems*, VEHITS, 2018; 251-260.

[7] Von Solms, R., Van Niekerk, J. From information security to cyber security. *Computers & Security*, 2013; 38: 97-102.

[8] Boyes, H. Security, privacy, and the built environment. *IT Professional*, 2015; 17(3): 25-31.

[9] Mohamed, M. Challenges and benefits of Industry 4.0: an overview. *International Journal of Supply and Operations Management*, 2018; 5(3): 256-265.

[10] Rojko, A. Industry 4.0 concept: background and overview. *International Journal of Interactive Mobile Technologies*, 2017; 11(5): 77-90.

[11] Axelrod, C. W. Cybersecurity in the age of autonomous vehicles, intelligent traffic controls and pervasive transportation networks. *IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, IEEE Xplore, 2017; 1-6. https://ieeexplore.ieee.org/abstract/document/8001966.

[12] Cheah, M., Shaikh, S. A., Bryans, J., Wooderson, P. Building an automotive security assurance case using systematic security evaluations. *Computers & Security*, 2018; 77: 360-379.

[13] Gawanmeh, A., Alomari, A. Taxonomy analysis of security aspects in cyber physical systems applications. *IEEE International Conference on Communications Workshops (ICC Workshops,* IEEE Xplore, 2018; 1-6. https://ieeexplore.ieee.org/abstract/document/8403559

[14] Kennedy, J., Holt, T., Cheng, B. Automotive cybersecurity: assessing a new platform for cybercrime and malicious hacking. *Journal of Crime and Justice*, 2019; 42(5): 632-645.

[15] Contreras-Castillo, J., Zeadally, S., Guerrero-Ibañez, J. A. Internet of vehicles: architecture, protocols, and security. *IEEE Internet of Things Journal*, 2017; 5(5): 3701-3709.

[16] Haas, R. E., Möller, D. P. Automotive connectivity, cyber attack scenarios and automotive cyber security. *IEEE International Conference on Electro Information Technology (EIT)*, IEEE Xplore, 2017; 635-639. https://ieeexplore.ieee.org/abstract/document/8053441

[17] Olufowobi, H., Bloom, G. Connected cars: Automotive cybersecurity and privacy for smart cities. In *Smart Cities Cybersecurity and Privacy*, Elsevier: NJ 2019; 227-240

[18] Radanliev, P., Montalvo, R. M., Cannady, S., Nicolescu, R., De Roure, D., Nurse, J. R., Huth, M. Cyber Security Framework for the Internet-of-Things in Industry 4.0. *IET Full* paper, 2019; 1-7.

[19] Möller, D. P., Haas, R. E. Automotive Cybersecurity. In *Guide to Automotive Connectivity and Cybersecurity*, Springer, Cham, 2019; 265-377.

[20] Scalas, M., Giacinto, G. Automotive cybersecurity: Foundations for next-generation vehicles. *2nd International Conference on new Trends in Computing Sciences* (ICTCS), IEEE Xplore, 2019; 1-6. https://ieeexplore.ieee.org/abstract/document/8923077

[21] El-Rewini, Z., Sadatsharan, K., Selvaraj, D. F., Plathottam, S. J., Ranganathan, P. Cybersecurity challenges in vehicular communications. *Vehicular Communications*, 2020; *23*: 100214.

[22] Conway, J. The Industrial Internet of Things: an evolution to a smart manufacturing enterprise. *Schneider Electric White Paper*, 2016. https://dev.ee.co.za/wp-content/uploads/2016/02/An-Evolution-to-a-smart-manufacturing-enterprise-IoT1.pdf

[23] Sharma, A., Koohang, A., Rana, N. P., Abed, S. S., Dwivedi, Y. K. Journal of Computer Information Systems: Intellectual and Conceptual Structure. *Journal of Computer Information Systems,* 2022; 1-31. http://doi.org/10.1080/08874417.2021.2021114

[24] Baker, H. K., Kumar, S., Goyal, K., Sharma, A. International review of financial analysis: A retrospective evaluation between 1992 and 2020. *International Review of Financial Analysis*, 2021, 78: 101946. https://doi.org/10.1016/j.irfa.2021.101946

[25] Sharma, A., Rana, N. P., Nunkoo, R. Fifty years of information management research: A conceptual structure analysis using structural topic modeling. *International Journal of Information Management*, 2021; 58: 102316.

[26] Pereira, V., Bamel, U. Extending the resource and knowledge based view: A critical analysis into its theoretical evolution and future research directions. *Journal of Business Research*, 2021; 132: 557-570.

[27] Singh, S., Dhir, S., Das, V. M., Sharma, A. Bibliometric overview of the Technological Forecasting and Social Change journal: Analysis from 1970 to 2018. *Technological Forecasting and Social Change*, 2020; 154: 119963.

[28] Aria, M., Cuccurullo, C. Bibliometrix: An R-tool for comprehensive science mapping analysis. *Journal of Informetrics*, 2017; 11(4): 959-975.

[29] Kitchenham, B. *Procedures for Performing Systematic Reviews. NICTA Technical Report 0400011T.1* Keele University and National ICT Australia Ltd, 2004; 1–28. http://www.it.hiof.no/~haraldh/misc/2016-08-22-smat/Kitchenham-Systematic-Review-2004.pdf

[30] Brereton, P., Kitchenham, B. A., Budgen, D., Turner, M., Khalil, M. Lessons from applying the systematic literature review process within the software engineering domain. *Journal of Systems and Software*, 2007; 80(4): 571-583.

[31] Denyer, D., Tranfield, D. Producing a systematic review. In D. A. Buchanan & A. Bryman (Eds.), *The Sage handbook of organizational research methods*. Sage Publications Ltd, 2009.

[32] Hou, T., Wang, V. Industrial espionage–A systematic literature review (SLR). *Computers & Security*, 2020; 98: 102019.

[33] Kennedy, C. New threats to vehicle safety: how cybersecurity policy will shape the future of autonomous vehicles. *Michigan Telecommunication & Technology Law Review*, 2016; 23: 343-356.

[34] Crocco, E., Chiaudano, V. Systematic Literature Review on the development of Digital Skills in Business Organisations. In ITAIS2020: *XVII Conference of the Italian chapter of ais-organizing in a digitized world: diversity, equality and inclusion,* 2020; 1-11. https://iris.unito.it/retrieve/handle/2318/1768585/698230/56.pdf.

[35] SAE. SAE J3061 Vehicle Cybersecurity Systems Engineering Committee. *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems. SAE International*, 2016.

[36] McAfee. *Automotive Security Best Practices 1 Automotive Security Best Practices. Recommendations for security and privacy in the era of the next-generation car*. White Paper, McAfee, 2017. https://www.mcafee.com/enterprise/en-us/assets/white-papers/wp-automotive-security.pdf

[37] Narayanan, S. N., Khanna, K., Panigrahi, B. K., Joshi, A. Security in smart cyber-physical systems: a case study on smart grids and smart cars. *Smart cities cybersecurity and privacy*, 2019; 147-163. https://doi.org/10.1016/B978-0-12-815032-0.00011-1

[38] Khurram, M., Kumar, H., Chandak, A., Sarwade, V., Arora, N., Quach, T. Enhancing connected car adoption: Security and over the air update framework. *IEEE 3rd World Forum on Internet of Things (WF-IoT),* IEEE Xplore, 2016; 194-198. https://ieeexplore.ieee.org/abstract/document/7845430

[39] Mejri, M. N., Ben-Othman, J., Hamdi, M. Survey on VANET security challenges and possible cryptographic solutions. *Vehicular Communications*, 2014; 1(2): 53-66.

[40] Raw, R. S., Kumar, M., Singh, N. Security challenges, issues and their solutions for VANET. *International Journal of Network Security & its Applications*, 203; 5(5): 95-105

[41] Kang, M. J., Kang, J. W. Intrusion detection system using deep neural network for in-vehicle network security. *PloS one*, 2016; 11(6): e0155781.

[42] NISR. Bilan 2013 de la sécurité routière. Observatoire français interministériel de la sécurité routière. France, 2013. https://www.onisr.securite-routiere.gouv.fr/etat-de-l-insecurite-routiere/bilans-annuels-de-la-securite-routiere/bilan-2013-de-la-securite-routiere

[43] Kargl, F., Ma, Z., Schoch, E. Security engineering for VANETs. In K. Lemke, Ch. Paar, M. Wolf (eds.). *Embedded Security in Cars*. Springer, 2016.

[44] Dattathreya, M. S., Bechtel, J. E., Mikulski, D. On Synthesising Technical Cybersecurity Requirements for Automotive Embedded Systems. *International Conference on Computational*

Science and Computational Intelligence (CSCI), IEEE Xplore, 2016; 1074-1076. https://ieeexplore.ieee.org/abstract/document/7881498

[45] Han, K., Weimerskirch, A., Shin, K. G. Automotive cybersecurity for in-vehicle communication. *IQT Quarterly,* 2014; 6(1): 22-25.

[46] Al-Qutayri, M., Yeun, C., Al-Hawi, F. Security and privacy of intelligent VANETs. *Computational Intelligence and Modern Heuristics*. IntechOpen, 2010. https://www.intechopen.com/books/computational-intelligence-and-modern-heuristics/security-and-privacy-of-intelligent-vanets

[47] Kleberger, P., Olovsson, T., Jonsson, E. Security aspects of the in-vehicle network in the connected car. *IEEE Intelligent Vehicles Symposium (IV)*, IEEE Xplore, 2011; 528-533. https://ieeexplore.ieee.org/abstract/document/5940525

[48] Wang, P., Valerdi, R., Zhou, S., Li, L. Introduction: Advances in IoT research and applications. *Information Systems Frontiers*, 2015; 17(2): 239-241.

[49] Razzaq, M. A., Gill, S. H., Qureshi, M. A., Ullah, S. Security issues in the Internet of Things (IoT): a comprehensive study. *International Journal of Advanced Computer Science and Applications,* 2017; 8(6): 383-388.

[50] Boyes, H., Hallaq, B., Cunningham, J., Watson, T. The industrial internet of things (IIoT): An analysis framework. *Computers in Industry*, 2018; 101: 1-12.

[51] Thun, J. H., Hoenig, D. An empirical analysis of supply chain risk management in the German automotive industry. *International Journal of Production Economics*, 2011; 131(1): 242-249.

[52] Ning, H., Liu, H., Yang, L. T. Cyber entity security in the internet of things. *Computer*, 2013; 46(4): 46-53.

[53] Pacheco, J., Satam, S., Hariri, S., Grijalva, C., Berkenbrock, H. IoT Security Development Framework for building trustworthy Smart car services. *IEEE Conference on Intelligence and Security Informatics (ISI)*, IEEE Xplore, 2016; 237-242. https://ieeexplore.ieee.org/abstract/document/7745481

[54] Bertino, E., Choo, K. K. R., Georgakopolous, D., Nepal, S. Internet of Things (IoT) Smart and Secure Service Delivery. *ACM Transaction on Internet Technology*, 2016; 16(4): 22-29.

[55] Jeschke, S., Brecher, C., Meisen, T., Özdemir, D., Eschert, T. (2017). Industrial internet of things and cyber manufacturing systems. *Industrial internet of things*, Springer: Cham, 2017; 3-19.

[56] Maglaras, L. A., Kim, K. H., Janicke, H., Ferrag, M. A., Rallis, S., Fragkou, P., Cruz, T. J. Cyber security of critical infrastructures. *ICT Express*, 2018; 4(1): 42-45.

[57] Fu, K., Kohno, T., Lopresti, D., Mynatt, E., Nahrstedt, K., Patel, S., Zorn, B. Safety, security, and privacy threats posed by accelerating trends in the internet of things. *arXiv preprint arXiv:2008.00017*, 2020. https://arxiv.org/abs/2008.00017

[58] Lu, Y., Morris, K. C., Frechette, S. Current standards landscape for smart manufacturing systems. *National Institute of Standards and Technology, NISTIR*, *8107*, 2016; 1-35.

[59] Leinmuller, T., Schoch, E., Maihofer, C. Security requirements and solution concepts in vehicular ad hoc networks. Fourth Annual Conference on Wireless on Demand Network Systems and Services, IEEE Xplore, 2007; 84-91. https://ieeexplore.ieee.org/abstract/document/4142712

[60] Papadimitratos, P., Gligor, V., Hubaux, J. P. *Securing vehicular communications-assumptions, requirements, and principles.* Diva-portal.org, 2006. https://www.diva-portal.org/smash/get/diva2:429038/FULLTEXT01.pdf

[61] Bloss, R. Unmanned vehicles while becoming smaller and smarter are addressing new applications in medical, agriculture, in addition to military and security. *Industrial Robot: An International Journal*, 2014; 1(1):82-86.

[62] Da Xu, L., He, W., Li, S. Internet of things in industries: A survey. *IEEE Transactions on Industrial Informatics*, 2014; 10(4): 2233-2243.

[63] Abomhara, M., Køien, G. M. Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, 2015; 4(1): 65-88.

[64] Kumar, S. A., Vealey, T., Srivastava, H. Security in internet of things: Challenges, solutions and future directions. In *2016 49th Hawaii International Conference on System Sciences (HICSS)*, IEEE Xplore, 2016; 5772-5781. https://ieeexplore.ieee.org/abstract/document/7427903

[65] Amoozadeh, M., Raghuramu, A., Chuah, C. N., Ghosal, D., Zhang, H. M., Rowe, J., Levitt, K. Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. *IEEE Communications Magazine*, 2015; 53(6): 126-132.

[66] Grubmüller S., Plihal J., Nedoma P. Automated Driving from the View of Technical Standards. In: Watzenig D., Horn M. (eds) *Automated Driving*. Springer, Cham, 2017.

[67] Yan, G., Olariu, S., Weigle, M. C. Providing VANET security through active position detection. *Computer Communications*, 2008; 31(12): 2883-2897.

[68] Engoulou, R. G., Bellaïche, M., Pierre, S., Quintero, A. VANET security surveys. *Computer Communications*, 204; 44: 1-13.

[69] Patsakis, C., Dellios, K., Bouroche, M. Towards a distributed secure in-vehicle communication architecture for modern vehicles. *Computers & Security*, 2014; 40, 60-74.

[70] Mishra, R., Singh, A., & Kumar, R. VANET security: Issues, challenges and solutions. *International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, IEEE Xplore, 2016; 1050-1055. https://ieeexplore.ieee.org/abstract/document/7754846

[71] Dak, A. Y., Yahya, S., Kassim, M. A literature survey on security challenges in VANETs. *International Journal of Computer Theory and Engineering*, 2012; 4(6): 1007-1010.

[72] Tangade, S. S., Manvi, S. S. A survey on attacks, security and trust management solutions in VANETs. In *2013 Fourth international conference on computing, communications and networking technologies (ICCCNT)*, IEEE Xplore, 2013; 1-6. https://ieeexplore.ieee.org/abstract/document/6726668

[73] Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., Qiu, D. Security of the Internet of Things: perspectives and challenges. *Wireless Networks*, 2014; 20(8): 2481-2501.

[74] Qu, F., Wu, Z., Wang, F. Y., Cho, W. A security and privacy review of VANETs. *IEEE Transactions on Intelligent Transportation Systems*, 2015; 16(6): 2985-2996.

[75] Mccluskey, B. Connected cars–the security challenge. Connected Cars Cyber Security. *Engineering & Technology*, 2017; 12(2): 54-57.

[76] Sadeghi, A. R., Wachsmann, C., Waidner, M. Security and privacy challenges in industrial internet of things. *52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, IEEE Xplore, 2015; 1-6. https://ieeexplore.ieee.org/abstract/document/7167238

[77] Chaubey, N. K. Security analysis of vehicular ad hoc networks (VANETs): a comprehensive study. *International Journal of Security and Its Applications*, 2016; 10(5): 261-274.

[78] Wollschlaeger, M., Sauter, T., Jasperneite, J. The future of industrial communication: Automation networks in the era of the internet of things and industry 4.0. *IEEE Industrial Electronics Magazine*, 2017; 11(1): 17-27.

[79] Malhi, A. K., Batra, S., Pannu, H. S. Security of vehicular ad-hoc networks: A comprehensive survey. *Computers & Security*, 2020; 89: 101664.

[80] Hasrouny, H., Samhat, A. E., Bassil, C., Laouiti, A. VANet security challenges and solutions: A survey. *Vehicular Communications*, 2017; 7: 7-20.

[81] La, V. H., Cavalli, A. R. Security attacks and solutions in vehicular ad hoc networks: a survey. *International Journal on AdHoc Networking Systems (IJANS)*, 2014; 4(2): 1-20.

[82] Gillani, S., Shahzad, F., Qayyum, A., Mehmood, R. A survey on security in vehicular ad hoc networks. *International Workshop on Communication Technologies for Vehicles,* Springer: Berlin, Heidelberg, 2013; 59-74.

[83] Parkinson, S., Ward, P., Wilson, K., Miller, J. Cyber threats facing autonomous and connected vehicles: Future challenges. *IEEE Transactions on Intelligent Transportation Systems*, 2017; 18(11): 2898-2915.

[84] Al-Kahtani, M. S. Survey on security attacks in vehicular ad hoc networks (VANETs). 6th *International Conference on Signal Processing and Communication Systems,* IEEE Xplore, 2012; 1-9. https://ieeexplore.ieee.org/abstract/document/6507953

[85] Rawat, A., Sharma, S., Sushil, R. VANET: Security attacks and its possible solutions. *Journal of Information and Operations Management*, 2012; 3(1): 301-304.

[86] Malla, A. M., Sahu, R. K. Security attacks with an effective solution for dos attacks in VANET. *International Journal of Computer Applications*, 2013; 66(22): 45-49.

[87] Yaqoob, I., Ahmed, E., ur Rehman, M. H., Ahmed, A. I. A., Al-garadi, M. A., Imran, M., Guizani, M. The rise of ransomware and emerging security challenges in the Internet of Things. *Computer Networks*, 2017; 129: 444-458.

[88] Shams, E. A., Rizaner, A., Ulusoy, A. H. Trust aware support vector machine intrusion detection and prevention system in vehicular ad hoc networks. *Computers & Security*, 2018; 78, 245-254.

[89] Khan, S. K., Shiwakoti, N., Stasinopoulos, P., Chen, Y. Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions. *Accident Analysis & Prevention*, 2020; 148: 105837.

[90] Onishi, H. Paradigm change of vehicle cyber security. *4th International Conference on Cyber Conflict (CYCON 2012),* IEEE Xplore, 2012; 1-11. https://ieeexplore.ieee.org/abstract/document/6243987

[91] Zhang, Z. K., Cho, M. C. Y., Wang, C. W., Hsu, C. W., Chen, C. K., Shieh, S. IoT security: ongoing challenges and research opportunities. *IEEE 7th international conference on service-*

oriented computing and applications, IEEE Xplore, 2014; 230-234. https://ieeexplore.ieee.org/abstract/document/6978614

[92] Dhamgaye, A., Chavhan, N. Survey on security challenges in VANET 1. *International Journal of Computer Science and Network*, 2013; 2(1): 88-96.