An Automotive Cybersecurity Trend Radar

Gabriel Simmann
Karlsruhe University of Applied Sciences
Institute of Energy Efficient Mobility
Karlsruhe, Germany
gabriel.simmann@h-ka.de

Reiner Kriesten
Karlsruhe University of Applied Sciences
Institute of Energy Efficient Mobility
Karlsruhe, Germany
reiner.kriesten@h-ka.de

Felix Sebastian Maag
Daimler Truck Holding AG
Stuttgart, Germany
felix_sebastian.maag@daimlertruck.com

Martin Mager
Daimler Truck Holding AG
Stuttgart, Germany
martin.mager@daimlertruck.com

Abstract

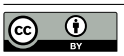
Driven by technological progress and, above all, software, our world is becoming ever faster, more flexible and more complex. Vehicles in particular are complex systems due to the number of components, communication, and millions of lines of code. Recent trends such as autonomous driving and artificial intelligence further accelerate these developments. As a result, the attack surface of vehicles is constantly increasing. To proactively address future security risks, we present the Automotive Cybersecurity Trend Radar (ACTR), an approach that applies the Innovation Radar methodology to identify and temporally classify emerging technologies relevant for the automotive cybersecurity sector. By systematically analyzing technology trends, academic research, and industry reports, this radar provides a structured view of upcoming challenges and opportunities. Our research highlights key topics for the future, including the impact of post-quantum cryptography, AI-driven security mechanisms, and confidential computing technologies. By incorporating these insights into early-stage strategic planning, manufacturers and suppliers can improve their preparedness for emerging cybersecurity-relevant technologies as well as benefit from technology developments, allowing strategic investments. The ACTR thus serves as a tool for industry stakeholders to anticipate, prioritize, and address automotive cybersecurity challenges before they become critical.

CCS Concepts

• **General and reference** → Surveys and overviews; • **Hardware** → Emerging technologies; • **Computer systems organization** → Embedded and cyber-physical systems; • **Security and privacy** → **Systems security**; *Software and application security*; *Cryptography*.

Keywords

Automotive, Security, Trend Radar, Foresight, Emerging technologies



CSCS '25, Taipei, Taiwan

ACM ISBN 979-8-4007-1928-8/2025/10
https://doi.org/10.1145/3736130.3762687

ACM Reference Format:
Gabriel Simmann, Reiner Kriesten, Felix Sebastian Maag, and Martin Mager. 2025. An Automotive Cybersecurity Trend Radar. In *Proceedings of the 2025 Cyber Security in CarS Workshop (CSCS '25), October 13–17, 2025, Taipei, Taiwan.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3736130.3762687

1 Introduction

The automotive industry is undergoing a rapid digital transformation, driven by the increasing integration of connected systems, autonomous functionalities [69], and software-defined architectures [48]. With this evolution, the technology landscape that vehicles require to satisfy customer needs is changing rapidly. However, new technologies introduce additional attack vectors for vehicles, which is why the number of cyber-attacks on vehicles is growing at an unprecedented rate [75, p.56]. At the same time, new security controls, such as intrusion detection systems [47] and cryptographic innovations [73], are continuously being developed to mitigate the resulting threats. This dynamic landscape of both, technologies for circumventing current security measures and new security controls, requires a forward-looking approach to cybersecurity. Future-critical technologies potentially affecting the security of automotive systems both in positive and negative ways such as quantum computers [1] and General Purpose Artificial Intelligence (GPAI) [77], are already foreseeable today and widely known. In addition to these well-known trends, however, there are numerous lesser-known trends with a potentially major impact. Examples include security measures such as honeypots [38] or cryptographic techniques for confidential computing [28]. This results in a wide range of relevant topics. Without a structured framework to identify and track the development of such technologies, adequately preparing for these innovations becomes a challenging task. Trend monitoring approaches are methods for identifying and analyzing technological trends to better plan for the future by providing early insights into technological shifts [71]. Applying such methodologies to the domain of automotive cybersecurity enhances strategic foresight and improves industry readiness for rapidly emerging challenges.

To address this need, we introduce the Automotive Cybersecurity Trend Radar (ACTR). This serves as a structured tool for identifying cybersecurity topics relevant to the automotive domain and monitoring their development trends [71, p.24-28]. By systematically assessing research trends and industry developments, the radar

provides an insight for the emergence and relevance of key automotive cybersecurity innovations. This recognition of emerging technologies in an early stage facilitates the investigation of their impact on cybersecurity. Possible attack vectors can be identified and their risk assessed. This approach enables the derivation of targeted security mechanisms. From the perspective of the original equipment manufacturer (OEM), design decisions addressing cybersecurity can be made at an early stage. From the perspective of a regulatory body, this enables the assessment of which security measures are suitable for which technologies, which is important for type approval and defining standards. Lastly, from the perspective of a customer, this results in a safer vehicle. Overall, the ACTR enables industry stakeholders to prioritize research and development efforts, align security strategies with future needs, and integrate emerging technologies into their long-term planning. Through this approach, the ACTR aims to prepare for evolving cyber threats.

To develop the ACTR, an overview of common foresight techniques and methodologies as well as existing technology trend radars is provided. Furthermore, a structured multi-step methodology for identifying, analyzing, filtering, and temporally classifying automotive cybersecurity trends is presented. The methodology focuses on various sources of information, mainly literature research and expert views. This approach ensures a systematic, repeatable, and objective identification of relevant topics. The methodology consists of the following key phases to extract important trends and information: *Data Collection and Source Identification*, *Trend Identification and Classification*, *Radar Visualization*, and *Iteration*.

This work is presented as follows: In Section 2, the background and related work is provided, focusing on existing technology trend radars, general foresight processes, and foresight work in automotive cybersecurity. Section 3 presents the methodology to derive and classify relevant topics. The results and identified topics are analyzed in Section 4 and the resulting trend radar is presented in Section 5. Finally, Section 6 concludes the work by summarizing key findings and providing an outlook on future work.

2 Background and Related Work

The subsequent section provides an overview of the extant literature and background information relevant to the present research. The related work splits into common methodologies for foresight processes, existing trend radars in related domains, as well as existing foresight works in cybersecurity and automotive.

2.1 Foresight Processes

Various foresight methods have been developed to manage uncertainties in foresight processes and enable informed decision making. This subsection gives an overview of foresight methods and their differences, providing a background for the method-decision process described subsequently. According to Popper [63], foresight methods can be classified in three types: qualitative, quantitative, and semi-quantitative. Furthermore, they can be categorized based on their primary sources of knowledge, which range from creativity, expertise, and interaction to evidence. Popular and widely used qualitative methods are literature reviews, scenario planning, brainstorming, and horizon scanning. Scenario planning involves the generation of multiple future scenarios, thereby illuminating the consequences of divergent technological developments and their attendant uncertainties. Horizon scanning facilitates the recognition of nascent domains and technologies that have yet to achieve full market establishment, yet hold the potential to become substantial in the imminent future. Literature reviews are mostly evidence-based, brainstorming on the other hand relies heavily on interaction and creativity [59]. Quantitative methods are, for example, bibliometrics and patent analysis [63], both relying on a quantitative analysis of either publications or patents making them mostly evidence-based. Within those methods a focus is set on investigating the evolution of numbers of articles over time and deriving statements from that information. Methods like delphi surveys and roadmapping are examples for semi-quantitative methods which rely mostly on expertise [63]. An example for a delphi survey in the cybersecurity domain is presented in [62]. In the delphi method, experts in various fields are regularly asked a series of questions about future technologies. Their answers are collected anonymously and discussed in several rounds to reach a consensus. This method is particularly useful for understanding how experts assess future developments in a particular area.

The selection of the appropriate foresight methods is mostly influenced by intuition and impulsiveness [59]. However, as shown by Popper [59, p.69], literature reviews, expert panels, and scenarios are the most widely used methods, which are of qualitative nature. The author showed that in most cases, several different foresight methods are applied instead of only one, which helps by combining different sources of knowledge.

2.2 Existing Technological Trend Radars

A relevant method to observe technological developments and help to appropriately prepare for future technical advances by visualizing and summarizing analysis results obtained by the mentioned foresight processes is the technology radar [71, p.24-26]. It can be applied to identify new technologies early on and assess their practical relevance for companies and the industry. The components and structure of such a trend radar are illustrated in Fig. 1. The radar is typically divided into various categories that cluster trends thematically. Additionally, the radar is segmented into distinct time clusters to visualize a temporal assessment of trends. The precise definition of this chronological classification is subject to variation and can range from the maturity of the respective technology, to the time until adoption, to specially defined categories.

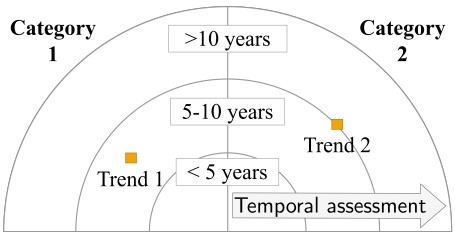


Figure 1: Structure of a trend radar.

Throughout recent years, several technology trend radars have been published, mainly from the industry. These radars differ in their scope, methods for assessment, used categories, as well as

Table 1: Existing technology trend radars according to their scope as well as the utilized temporal and impact assessment classes.

Ref.	Scope	Temporal Assessment	Impact
[15]	Logistics	<5, 5-10 years	Low - High
[30]	Automotive	Watch, Prepare, Act	-
[21]	Cybersec.	<2, 2-5, >5 years	-
[55]	General	Hold, Assess, Trial, Adopt	-
[76]	General	Near, Mid & Long term	-

information they provide about the contained technologies. The radars summarized in Table 1 provide insights into relevant topics in each domain using different research methods and structures for the radar. One of the earliest published radars is the DHL Logistics Trend Radar [15], focusing on trends in logistics. The radar is split into the two categories *Social & Business* and *Technology* and uses an adoption timeline for temporal assessment, which states when a trend is expected to transition into the normal way of operating. An automotive trend radar is published by the BMW Group [30]. This radar covers cross-industry technology trends and provides insights into topics important for the BMW Group. The topics are structured by eight categories: *UI/UX*, *Data Era*, *Connectivity*, *Sustainability*, *AI and Robotics*, *Future Computing*, *Health and Wellbeing*, and *Energy*. For maturity assessment a classification into *Watch*, *Prepare* and *Act* is used. Another trend radar is published by Eviden with the Eviden Cyber Tech Radar [21]. This one concentrates on cybersecurity technologies, categorized into eight major cybersecurity domains of *Data Security*, *Advanced Detection & Response*, *Cyber Incident Response*, *Identity & Access Management*, *Endpoint & Mobile Security*, *Network Security*, *Application Security* and *Cloud Security*. Within those categories, the Eviden radar covers a wide range of cybersecurity technologies. Maturity assessment is presented through a classification into either *Emerging Technology*, *Proven Technology* or *Mainstream Technology*. Besides technically related radars, there is one from the insurance company MunichRE [55]. This radar gives insights into how technological advances will impact the insurance sector and covers various general technological developments. The radar is split into the categories *Human-centricity*, *Connected World*, *Artificial Intelligence* and *Enabling Technologies*. It covers a broad range of topics, including topics related to the automotive and cybersecurity sectors, especially within the categories *AI* and *Enabling Technologies*. For maturity assessment the four categories *Hold*, *Assess*, *Trial* and *Adopt* are used. A last trend radar is the trend radar about life, society and business trends by futurist Steve Well [76]. It covers a broad range of topics using six categories. The category *Technology & Scientific* is the most relevant for this work. It uses the categories *Near*, *Mid*, and *Long term* for maturity assessment.

2.3 Foresight and Reports in Automotive and Cybersecurity

In the following paragraphs, the background to foresight work and reports in various domains relevant to the work presented is given. Firstly, the general cybersecurity domain is covered, followed by the automotive domain, and finally the more specific automotive cybersecurity domain.

General Cybersecurity. Raban and Hauptman [62] provide a foresight on cyber security threats and corresponding technologies. For this purpose the authors employed horizon scanning and conducted a delphi survey. With those methods the potential positive and negative impact and maturity levels of identified technologies are assessed. For the assessment the authors use likert scale metrics [46], a method for measuring personal beliefs. According to this study the emerging technologies with the highest potential impacts on cyber defense capabilities are cyber resilience, Homomorphic Encryption (HE), and Artificial Intelligence (AI). For attack capabilities biohacking and Human-Machine-Interface (HMI), autonomous technologies and Internet of Things (IoT) are the technologies with the highest impact.

The European Union Agency for Cybersecurity (ENISA) published a report assessing emerging threats up to 2030 [20]. A delphi survey was utilized to develop a list of the top 10 threats, with consideration given to current developments. This list contains threats such as supply chain compromise of software dependencies, loss of privacy, and abuse of AI. The analysis demonstrates a dynamic threat landscape, with evolving attack vectors in various domains, including political, economic, and technological trends. The report underscores the imperative for proactive cybersecurity measures to counter future risks and ensure a resilient digital environment through 2030 and beyond. An annual Global Risks Report is published by the World Economic Forum [17], focusing on a broad range of global risks and assessing their probable impact over different time horizons. It covers technological risks like adverse outcomes of AI and quantum technologies and assesses their impacts and maturity levels based on experts knowledge from different areas. In [19] horizon scanning for cyber threats for the North Atlantic Treaty Organization (NATO) until 2030 is presented with the goal to help NATO to appropriately deal with upcoming cyber threats and new technologies. In addition to content pertinent to NATO, the publication addresses the ramifications and challenges posed by emerging technologies, including AI, autonomous devices, quantum computing and HMI. Furthermore, an overview of the most significant technologies is presented, with a focus on those that are projected to have the greatest impact over the ensuing decade. Additional work concerning global cybersecurity related challenges and developments in the future are given in [43, 80]. Technology-specific foresight is also existent, like for the rising quantum threat with the Quantum Threat Timeline Report 2024 [53].

Automotive. In the automotive domain reports and outlooks regarding important developments and changes are available. Mogge et al. [54] analyzed the domain and its most relevant developments to the year 2040. The authors identified four key trends: Polarization (from globalization to regionalization), Automation, Connectivity and Electrification. These megatrends are largely in line with the general picture in the literature and industry [9, 11, 34]. Especially the development towards software-defined vehicles (SDV) is omnipresent and is associated with great impact [48]. Also, electrification is presented as a megatrend, strongly influencing the cybersecurity of vehicles [64].

Automotive Cybersecurity. In automotive cybersecurity, a selected number of work offer insights and reports regarding future developments. Durlik et al. [16] provide a recent review of current cybersecurity challenges, threats and countermeasures for autonomous vehicles. Additionally, the authors present future challenges and expected relevant technologies with a focus on AI, blockchain, and legislative measures. Kim and Shrestha [42] provide a general overview of automotive cybersecurity. This overview encompasses a broad spectrum of vehicle-specific cybersecurity subjects such as security and privacy in intelligent autonomous vehicles, in-vehicle and inter-vehicle communication security, and embedded security. Additionally, they address the potential for future technologies. In addition to scientific research, there are studies and reports from companies. Upstream's annual Global Automotive Cybersecurity Report [79] and Automotive Cyber Trend Report [78] analyze the evolution of cyber attacks in automotive by investigating worldwide incidents. These reports give an insight on the current threat landscape and developments in this domain. For example, the 2024 report [79] points out that high-impact and large-scale attacks and the influence of emerging technologies, such as Generative AI (GenAI), are increasing.

The presented background and related work shows a variety of different foresight processes and works in the fields of automotive, cybersecurity, and the combination of both. Although there are many reports, surveys, and overviews on automotive security, these mainly focus on current topics and developments already having a notable impact on the industry. As a result, there is a lack of forward-looking work that deals with latest developments in this domain in both industry and academia. Therefore, this work aims to address this gap by providing the ACTR.

3 Methodology

Given the inherently imprecise nature of prognostications concerning technological developments, a methodology that is both consistent and capable of repetition is needed. Such a methodology will form the basis of the development of the ACTR, allowing for consistent and reliable identification of trends. This section presents the methodology applied and the steps carried out throughout this research, in order to identify the most relevant trends to include in the radar. The applied methodology is illustrated in Fig. 2. Within the figure, key phases are highlighted in orange, methods and work packages in white, and artifacts in blue. The applied methodology consists of four key-phases. First, relevant sources are identified and data is collected with the help of those. Second, represented on the left side, the identification of potential trends and the classification thereof is covered. Based on the collected data and an analysis of the identified trends, the radar visualization is defined within the third phase. The last phase is iteration, which minimizes any threats to validity by executing the methodology several times.

3.1 Data Collection and Source Identification

Collecting content for the radar requires appropriate sources of information. According to Popper [59], the selection of foresight methods is an important process which should be done based on various factors such as nature and capabilities of methods, domain, and

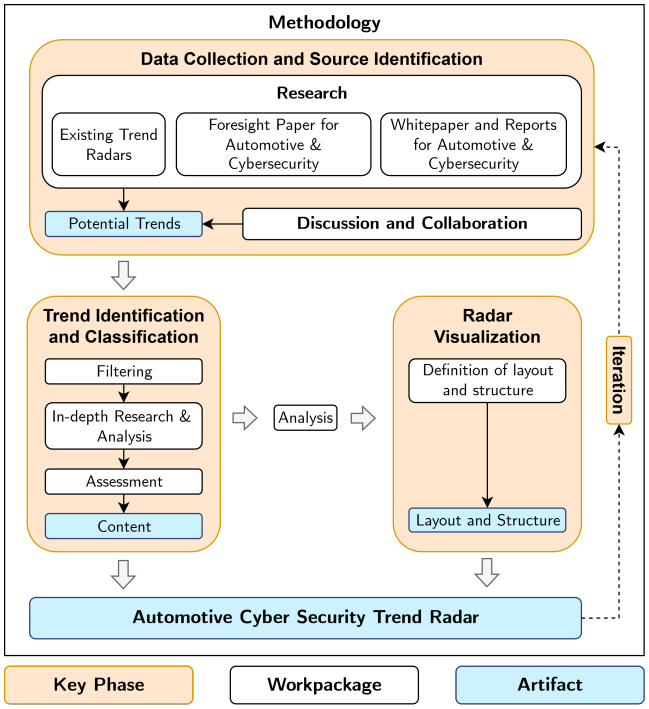


Figure 2: Methodology for the development of the Automotive Cybersecurity Trend Radar.

target groups. The trend radar requires a systematic identification of relevant technological developments, a process that should be based on both evidence and expertise. Therefore, a mix of methods capable of both is chosen. A literature review enables a structured analysis of existing research to capture already identified trends and relevant developments in science and industry. This allows recurring patterns, technological relevance and previous forecasts to be assessed. Discussion and collaboration with academia and industry complement this. While the literature review depicts known developments, expert discussions enable critical reflection, contextualization and the consideration of emerging trends that have not yet been comprehensively addressed in the literature. Together, these methods provide a scientifically sound yet practical basis for the ACTR by both systematically recording existing knowledge and adding new, future-relevant perspectives through expert assessments. Therefore, a combination of a literature review and discussions is chosen. In the first research phase, appropriate literature is identified. Existing trend and innovation radars from similar domains are an important resource, as many topics relevant for automotive security are already partially covered within other domains. The Eviden Cybersecurity Tech Radar [21] and the BMW Group Technologie Trend Radar [30] have been identified as the most relevant radars for this research. This is due to the similar domain of these radars in contrast to the other radars presented. Second, specific foresight work and paper for automotive and cybersecurity as well as the cross-domain of both are a resource (e.g., [62]), concentrating on foresight methods to possibly predict future developments based on experts knowledge. Furthermore,

whitepaper and industry reports provide valuable insights in current developments. This resource does not explicitly concentrate on trends far in the future, however, it provides information about trends which influence on the automotive cybersecurity is already relevant and notable. An example thereof is Upstream's analysis of current attack vectors in [79, pp.52-66], which shows for example the increasing relevance of API-based attacks and server-related incidents. Additionally, all resources giving insights into general automotive trends can provide valuable information for the radar, as new technological trends potentially open up new attack surfaces and require appropriate security controls. Lastly, discussion and collaboration with experts from academia and industry are a valuable source of information. Within the scope of this research, experts from academia and industry have been given their insight, knowledge, and comments. The participating experts work in various subfields of the automotive, security, and automotive security domains, thereby ensuring a broad range of expertise and diverse backgrounds.

3.2 Trend Identification and Classification

As a second key-phase, trend identification and classification is included. This phase starts with the outcome of the first key-phase, which are the potential trends. Subsequently, these trends are filtered using inclusion and exclusion criteria, and analyzed based on a more in-depth research afterwards. The outcome of this phase is the radar's actual content.

Filtering. The utilization of the aforementioned sources for collection and identification of potential trends results in a substantial number of technologies, methods, and techniques. The objective of this work is to provide meaningful insight into relevant technological trends. To that end, a filtering process is necessary to concentrate on the most significant trends. Consequently, a systematic filtering process was devised and implemented, employing a set of inclusion and exclusion criteria. The inclusion criteria are predicated on the observation that technologies deemed relevant to automotive cybersecurity can be classified into the following three categories:

- **TT:** Technological trends which potentially add to the attack surface in vehicles
- **TH:** Technological trends which potentially can be used to break security and therefore pose a threat
- **SC:** Security controls which potentially could be used in the automotive domain as well as technological trends which allow for new security mechanisms to be implemented

The first category encompasses technological trends (TT) within the automotive domain, which have the potential to introduce new vulnerabilities, thereby augmenting the attack surface of an automobile. An example for this category is the integration of 6G technology [32] for connectivity functionalities. The integration thereof poses several cybersecurity challenges and new attack vectors and security controls specifically for these technologies must be considered [70]. Another category encompasses technological trends that have potential to compromise security in some way and thus pose a threat (TH). Quantum computers are a popular example of this category, as they have the potential to break today's state-of-the-art encryption algorithms [53]. The third and final category comprises technologies that can either directly function as security controls (SC) to complicate cyberattacks on vehicles and assist in ensuring the fulfillment of security objectives or allow for new security mechanisms to be implemented. An example of this category is HE [28], a cryptographic technique that enables the processing of encrypted data without the need for prior decryption. An example for a technological trend that allows the implementation of new security mechanisms is Automotive Ethernet because of its higher bandwidth and different design compared to established communication protocols, such as Controller Area Network (CAN) [61]. It is possible to combine the categories identified. For instance, GenAI can be regarded as a security control [6], a technology capable of compromising security [91, p.3-4], and a technology that adds to attack surface [91, p.1-3]. Given the aim of the radar to identify both technologies that pose new threats and against which safeguards need to be put in place, and technologies that can be used for countermeasures, these definitions serve as criteria for inclusion.

In addition to these inclusion criteria, the establishment of the following exclusion criteria serves to refine the scope of the radar:

- Non-technical aspects
- Not vehicle related
- Widely adopted
- High-level concept
- Low granularity
- Redundancy
- Unclear automotive security relevance

The present work is focused on purely technical developments. Consequently, non-technical aspects, such as standardizations and regulatory requirements, are excluded from the scope. However, the technologies and security controls referenced in such documents are included. This criterion encompasses methods and systems, such as Cyber Security Management Systems. Finally, this criterion excludes process-related and supply-chain-related aspects. For this reason, it is summarized with the first exclusion criterion, *Non-technical aspects*. Furthermore, it should be noted that the scope of this radar is limited to topics directly related to the cybersecurity of a vehicle, which is implemented with the criterion *Not vehicle related*. This applies to subjects such as security protocols employed by companies for their network. As an additional criterion, the exclusion of technologies, concepts, and techniques that have already been widely adopted and are well-known, is implemented through the criterion *Widely adopted*. Given the dynamic nature of this field, elements that are not yet included in this category may be classified under this criterion in future iterations. These will be saved in subsequent iterations as archived trends, with the objective of maintaining traceability and archiving. In addition, abstract and high-level topics are excluded in order to ensure that the content of the radar remains concrete at a technical level. An example for that are the terms *Security for, with and against AI*. Instead, in that particular instance, the concrete technologies of Narrow AI and GenAI are integrated into the radar. Conversely, techniques, technologies, and trends that are overly detailed are excluded to maintain an overall perspective. That is addressed by the exclusion criterion of *Low Granularity*. Another criterion that functions to preserve a consistent level of abstraction across the radar is the *Redundancy* criterion. The process of exclusion of redundant topics

is implemented with the objective of avoiding duplication of trends. Furthermore, exclusion of trends that can be summarized with other trends is carried out for the purpose of maintaining a uniform level of abstraction. The primary objective of implementing this criterion is to maintain simplicity of the content and avoid excessive detail. An example is quantum key distribution in quantum cryptography. The final criterion, *Unclear Automotive Security Relevance*, pertains to the exclusion of trends for which the connection to cybersecurity in automotive is not yet clearly recognizable or researched. This assertion pertains to technologies that are nascent within the scientific community. Examples are DNA storage and neuromorphic computing, for which a paucity of academic research addressing their integration within automotive security was observed. Those trends can be re-examined in future iterations to re-evaluate their relevance. The defined inclusion and exclusion criteria are applied in the following manner:

To be included in the radar, an identified technology must fulfill at least one of the inclusion criteria and must not be subject to any exclusion criteria.

In-depth Research & Analysis. Following the filtering process, the remaining technologies undergo further investigation and analysis. Initially, a comprehensive collection of literature pertaining to each specific technology and its application in automotive is gathered. The search focuses on recent scientific surveys where available to provide a broad, scientific overview. In instances where no applicable recent surveys are extant, a search is conducted for recent primary studies.

Assessment. The gathered literature is analyzed to extract the information shown in Table 2 to assess technologies accordingly. Each identified technological trend gets described with the following properties. Initially, a temporal classification about when the respective technology becomes relevant is determined using the *Time Horizon* dimension. The three classes short, medium, and long are utilized in this context. Furthermore, a granular classification system is employed to differentiate within these broad classes, utilizing a numerical scale of 1-9, see Table 2. These numbered scales are exclusively employed for a relative ranking of trends and do not make reference to years or similar temporal units. The classification is determined by evaluating the statements within the pertinent literature and by conducting an assessment of the experts involved. Secondly, a technology's anticipated positive and negative impacts on automotive cybersecurity are evaluated using three levels: low, medium, and high. In addition, a more fine-grained numerical scale of 1-9 is employed. The assessment of this aspect is carried out on basis of the analysis of the gathered literature, extended by a discussion of the experts involved. The final three documented aspects pertain to the orientation, classification, categorization, and navigation between disparate trends. The *related to* property describes how trends relate to each other, thereby facilitating their categorization within the broader context. On the one hand, technologies and trends from the same domain are documented. In the example of HE, these are alternative technologies that can be employed for confidential calculations. Conversely, potential security measures are enumerated for trends that contribute to the attack surface, and vice versa. In case of the threat posed by quantum computers, for example, these are post-quantum secure cryptographic procedures. The *field* property categorizes the trends into higher-level categories. In this first version of the radar, the four categories Communication, Cryptography, Advanced Computing, System Design are used. These categories were defined after collecting and analyzing all relevant trends. They were chosen to ensure that each trend was allocated to a minimum of one category. This approach was undertaken to optimize the comprehensibility of the data while maintaining a sufficient level of granularity. The allocation of trends to specific categories facilitates swift orientation within the ACTR. Finally, the *category* property serves to document the assignment of trends to one or more of the categories defined.

Table 2: Information extracted in the analysis process. Numbered scales are purely numerical for relative classification of trends and do not refer to years or similar temporal units.

Name	Values
Time Horizon	Short (1-3), Medium (4-6), Long (6-9)
Positive Impact	Low (1-3), Medium (4-6), High (7-9)
Negative Impact	Low (1-3), Medium (4-6), High (7-9)
Related to	Related Trends
Field	Communication, Cryptography, Advanced Computing, System Design
Category	TT, TH, SC

3.3 Radar Visualization

For the definition of an appropriate layout and structure of the radar, existing trend and innovation radars are analyzed. From that, several options are extracted. In the next step, their applicability for the proposed ACTR is evaluated. This encompasses the evaluation of the possibilities for the presentation of various aspects delineated in Table 2. The visualization must provide the option to illustrate the *Category*, *Time Horizon* and *Impact Assessment* as well as the *Field* in a clear and concise manner. As only a single and clear presentation of the radar is to be provided within this paper, the focus here is on the presentation of the category and the time horizon. The category is visualized using color coding and the time horizon is visualized by the distance to the center of the radar. For a more detailed presentation and a customizable visualization, please refer to [25] (see Section 5.5).

3.4 Iteration

The trend radar herein is not necessarily exhaustive. Errors can occur in all phases and pose threats to validity of the study's findings. Moreover, the trend radar encompasses a wide array of subjects, making it impractical to exhaust all intricate elements thoroughly and comprehensively. An iterative process is proposed to minimize these inaccuracies over time and subsequent revisions of the radar. This will be achieved in the following ways: Firstly, the website (see Section 5.5) will provide an opportunity to submit suggestions for topics and improvements, as well as constructive criticism. Secondly, the methodology presented here will be repeated at appropriate intervals, allowing developments in the literature to be taken into account.

4 Analysis

This section presents an analysis of the applied methodology described in Section 3. Implementing the first phase and the filtering process of the second phase of the methodology yields the result illustrated in Fig. 3.

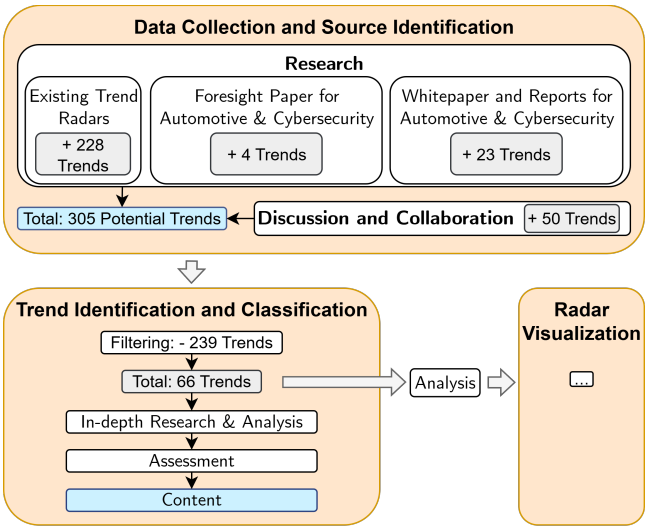


Figure 3: Amount of trends in different steps of the filtering process.

In the initial phase of the study, the utilization of all identified resources resulted in 305 distinct potential trends within the data collection stage. The majority of these initially originate from existing trend radars, followed by 50 Trends from discussion, 23 from white papers and industry reports, and 4 from foresight papers. It is important to acknowledge, that an endeavor was made to identify an original and verifiable source for each trend to ensure documentation and traceability of the results. Topics that were originally identified through discussions and expert knowledge were thus often subsequently validated by sources such as the existing trend radars. It is noteworthy that a significant number of the technologies and trends identified are documented in multiple sources. Consequently, the statistics in Fig. 3 illustrate one possible source of information for each trend. This explains the high number of trends that can be ascribed to the existing trend radars, as these were the first resources to be examined. Moreover, the Eviden Cyber Trend Radar [21] in particular contains a substantial number of technologies, trends, methods, and techniques at a detailed technical level, which also contributes to the high initial number. The filtering process reduced the number of trends to 66, with the exclusion reasons distributed as illustrated in Fig. 4.

The non-vehicle-relevant criterion accounts for the largest share, which is due to the fact that the Eviden Radar [21] contains a high number of non-vehicle-specific, more general cybersecurity trends, technologies, and methods. These primarily relate to the IT security of company infrastructures or networks. The second most common exclusion criterion is redundancy, which demonstrates that numerous trends are replicated across various information sources, occasionally under different names or at different levels

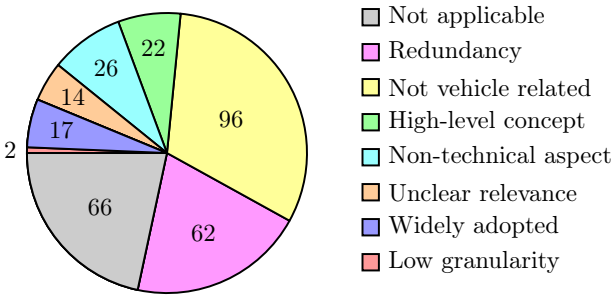


Figure 4: Distribution of the applied exclusion criteria.

of abstraction. These trends are subsequently summarized under a single aspect. The remaining four exclusion criteria are distributed over approximately the same percentage. In this evaluation, it is pertinent to consider, that in certain instances, multiple exclusion criteria are applicable. For the sake of clarity, however, only one criterion is given in these statistics.

The remaining 66 trends subsequently proceed to the last steps of the *Trend Identification and Classification* phase. This encompasses the in-depth research, analysis, and assessment thereof, which results in the actual content of the ACTR presented in Section 5. The trends are also analyzed to delineate the suitable visualization and structure of the radar in the third phase *Radar Visualization*.

5 The Automotive Cybersecurity Trend Radar

The extracted and remaining trends are collected and assessed as described in Section 3. Given the extensive nature of the list, only a selection of the most relevant points is collected in Table 3 and presented in the ACTR shown in Fig. 5. As explained in the *Trend Identification and Classification* step of the methodology (see Section 3), the trends resulting from the filtering step can be categorized into the following four fields: *Communication*, *Cryptography*, *Advanced Computing*, and *System Design*. It should be noted that certain trends may be applicable to multiple fields. However, for the sake of clarity, each trend is assigned to the best fitting category. In this paper, the focus is on presenting a concise overview of two trends per field, emphasizing depth over breadth. The selection of trends across the four categories was deliberately chosen based on their technological novelty and under-representation in mainstream discourse. While numerous trends, concepts, and technologies, including Quantum Computing and Vehicle-to-Everything (V2X), and their impact on automotive cybersecurity are already well-acknowledged, this selection underscores emerging or less conspicuous subjects. For more detailed information, the entire trend radar with all identified trends and further background information, please refer to [25], which is further explained in section 5.5.

5.1 Communication

The first category pertains to technologies and concepts associated with the domain of *Communication*. These include technologies for wireless communication such as 6G [89] and Non-Terrestrial Networks [83], in-vehicle communication, as well as connectivity

Table 3: Selected content of the Automotive Cyber Security Trend Radar. Impact is denoted as +, ++, +++ for low, medium, and high positive impact respectively; and -, - -, - - - for low, medium, and high negative impact.

Topic	Time Horizon	Impact	Field	Category	References
Automotive Ethernet	Short	++/- -	Communication	TT/SC	[14, 61]
Vehicle Ad-hoc Network (VANET)	Medium	- - -	Communication	TT	[22]
Trust Management	Medium	+++	Communication	SC	[23, 27, 39]
Zero Knowledge Proofs (ZKP)	Medium	++	Communication	SC	[29, 36, 45, 88]
6G	Long	++/- -	Communication	TT/SC	[32, 70, 89]
Crypto Agility	Medium	+++	Cryptography	SC	[5, 49]
Functional Encryption (FE)	Medium	++	Cryptography	SC	[10, 44, 81]
Post-Quantum Cryptography	Medium	+++	Cryptography	SC	[3, 37, 49, 73]
Secure Multi-Party Computation (SMPC)	Long	+++	Cryptography	SC	[40, 85, 90]
Quantum Cryptography	Long	++	Cryptography	SC	[60]
Homomorphic Encryption (HE)	Long	+++	Cryptography	SC	[28]
Honeypots	Short	+++	System Design	SC	[18, 24, 33, 38]
Digital Identities	Medium	+++	System Design	SC	[4, 26, 35, 41]
Zero Trust	Medium	+++	System Design	SC	[7, 31, 66]
Wireless Power Transfer	Medium	- -	System Design	TT	[8, 82, 86]
Synthetic Data	Short	++/- -	Advanced Computing	TT/SC	[13, 50, 56, 58, 68]
Generative Artificial Intelligence (GenAI)	Short	+++/-	Advanced Computing	TT/TH/SC	[6, 91]
Federated Learning (FL)	Medium	+++/- -	Advanced Computing	TT/SC	[52, 72, 84, 87]
General Purpose Artificial Intelligence (GPAI)	Medium	+++/-	Advanced Computing	TT/TH/SC	[77]
Quantum Computing	Medium	+/- - -	Advanced Computing	TH/SC	[1, 53]
Vetaverse	Long	- -	Advanced Computing	TT	[74]
Vehicle Computing	Long	-	Advanced Computing	TT	[51]

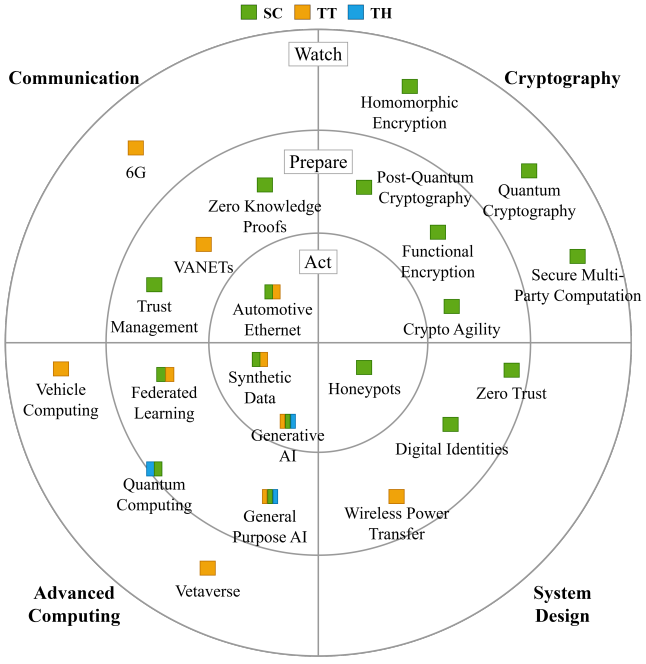


Figure 5: The Automotive Cybersecurity Trend Radar.

to other devices, infrastructure, and vehicles such as V2X or Vehicle Ad-hoc Networks (VANET) [12] (see Table 3). However, it also includes concepts and techniques to secure such communication paradigms, like Zero Knowledge Proofs (ZKP) [29] and Trust Assessment, which are the two selected aspects that are described in more detail.

Zero Knowledge Proofs. ZKPs [29] are cryptographic techniques and protocols. They can be used to allow parties to prove to each other that they know a secret or have done something without revealing the underlying secret and details about it. This feature enables the extensive utilization of ZKPs, particularly in contexts involving the processing of sensitive data, where strict protection measures are paramount. Lavin et al. [45] provide a comprehensive review of applications for ZKPs, ranging from various application in blockchain, to identity-proofing, to machine learning. For automotive security the potential of ZKPs lies in applications that are in need of two parties, respectively vehicles trusting each other, authenticate themselves and still provide privacy protection. Examples are anonymous authentication and information sharing for VANETs and the IoV [36, 88], which are subject to recent investigations. Because of the potential of ZKP and the recent scientific efforts, ZKPs are included into the radar with a time horizon in the medium term and a medium positive impact as a security control.

Trust Management. A prominent trend is increasing connectivity and communication within and between vehicles, as well as with other road users and infrastructure. This necessitates to determine whether and to what extend the communication partner can be trusted or not. Trust Management and Trust Assessment are playing an increasingly important role in this regard. Various concepts for

trust management have already been developed and presented in other domains, such as IoT, yet numerous challenges persist [23]. In the literature, approaches for trust assessment in the automotive context are already available, for example, in vehicle platooning systems [27] or cooperative intersection management [39]. Due to these current efforts and existing approaches of the application in the automotive domain and its promising capabilities, it has been included in the radar with a medium-term time horizon and high positive impact.

5.2 Cryptography

Technologies and concepts mainly related to *Cryptography* include topics such as quantum-safe cryptography [49], techniques for processing encrypted data like HE [28], and Secure Multi-Party Computation (SMPC) [85]. The two topics to be emphasized in this category are crypto agility [5] and Functional Encryption (FE) [10].

Crypto Agility. Recent developments and breakthroughs in the field of Quantum Computing [1, 53] suggest that functional quantum computers will become readily accessible in the foreseeable future. While this represents a positive technological advance for many applications, it also poses the risk that current cryptographic methods can be broken. While, according to current knowledge, it is possible to secure symmetric algorithms (e.g. Advanced Encryption Standard (AES) [57]) against quantum attacks using longer keys, public-key algorithms like Rivest-Shamir-Adleman (RSA) [65] are particularly affected to be broken [53]. As public-key algorithms are widely used in the automotive domain [49], attacks by quantum computers pose a significant potential threat. Due to such developments, the rapid migration of new cryptographic methods, as well as the ability to switch to a longer key length or even securely renew a key, is becoming increasingly relevant. The ability to integrate new cryptographic primitives, algorithms, and different key lengths into a system quickly and without in-depth intervention or interruption of the system is defined as crypto agility [5]. This becomes even more relevant because of the long development time and service lifetimes of vehicles [49]. For these reasons, crypto agility is currently considered highly relevant in the medium term.

Functional and Attribute-based Encryption. FE [10] is a generalization of specialized encryption systems for applications such as searching on encrypted data and expressive access control. A FE scheme is a public-key encryption scheme that allows the generation of specialized decryption keys, which allow the party holding this key to only learn the output of a function performed on what the ciphertext is encrypting, but not the plaintext itself. This approach contrasts with the conventional public-key cryptography, which allows that either the complete data is decrypted or it remains inaccessible. In the context of automotive security research, the potential application of FE schemes, particularly attribute-based encryption, is being examined [44, 81]. Examples include secure Over-the-Air (OTA) updates of vehicle software [44] and integration into VANETs [81]. As the amount of research available to date on the application of those techniques in automotive security is limited, it is not yet clear how and when they can be expected to be widely adopted. Therefore, they are considered relevant in the medium to long term, with the potential for a moderately positive impact.

5.3 Advanced Computing

Advanced Computing includes topics relating to various forms and evolutionary stages of AI, to related technologies, such as Federated Learning (FL) [84], hardware-related topics, such as chiplets, and possible future concepts, such as vehicle computing [51]. This paper focuses synthetic data and FL.

Synthetic Data. A topic that can have both a positive and negative impact on automotive security is synthetic data. Synthetic data is artificially generated data that simulates real data and is used for training machine learning models, testing, and data analyses. This can eliminate the need for real, sensitive and personal data and the pseudonymization thereof to develop security mechanisms which rely on training machine learning models [50]. This prevents privacy breaches and the disclosure of sensitive data. In addition, synthetic attack data can be used to test security mechanisms as for example proposed by Rosenstatter and Melnyk [67] for testing VANETs. However, the use of synthetic data also poses a risk. Firstly, its integrity must be ensured, and secondly its use can result in new vulnerabilities and threats. The authors of [56] emphasize the risks of unintended disclosure of sensitive information about a vehicle's system and the risk that attackers use reverse engineering to find system vulnerabilities by analyzing the synthetic data. Recently, various research is ongoing that investigates opportunities and challenges of using synthetic data in automotive security [13, 58]. For these reasons, synthetic data is categorized as relevant in the short term, which can have both a medium positive and negative impact.

Federated Learning. FL is a method of distributed learning in which models are trained locally on devices and only model updates are sent to a central server to update the global model [84]. Various recent surveys explore the use of FL in automotive security [52, 72, 87][2, p.22-23]. On the one hand, it holds potential for mitigating privacy concerns regarding training data, as local training data must not be transmitted to a server anymore. On the other hand, it opens up new attack surfaces. Indirect privacy leakage and malicious edge devices tampering with the global model by including poisoned training data are examples thereof [87]. Therefore, FL techniques can be used as a future security control but its integration also opens up new attack surfaces which must be considered. Consequently, it is considered relevant in the medium term, with potential for a high positive and a moderately negative impact.

5.4 System Design

System Design covers a wide range of topics from the area of functionalities like X-by-wire, to shifts in the E/E architectures, and security mechanisms which can be integrated into the system. Two such concepts that have been identified are honeypots and digital identities.

Honeypots. The concept of honeypots [24, 38], which comes from the areas of threat intelligence and intrusion detection in classic IT systems and IoT, represents a relevant development in the automotive security sector. Honeypots are parts of a system that

simulate relevant and interesting content for attackers in order to lure them in and specifically record their activity. Security measures can be derived on basis of these recordings and integrated into real relevant parts of the system. Furthermore, an alarm can be triggered as soon as an intrusion into the honeypot is detected. According to recent work by Ilg et al. [33], this concept is already widespread in traditional IT systems, but has yet to become established in the automotive sector. The authors argue that the evolution of vehicle architectures towards more centralized architectures facilitates the introduction of honeypots due to the SDV, high-performance units, and OTA capabilities. This is why honeypots are rated as a relevant technology in the short term, with the potential for a high positive impact on automotive security.

Digital Identities. With the rapid development towards SDV and increasing possibilities for communication with third-party devices, such as charging stations or external apps, digital identities for Electronic Control Units (ECU), software, and workloads are becoming increasingly relevant. Within the ACTR, digital identities is a general category for concepts and techniques for identifying and authorizing devices and software. Approaches can be hardware-based, such as physical unclonable functions [26], or software-based such as pre-shared keys [41]. Examples for the application of these approaches in the automotive domain are authentication in IoV [4] and In-Vehicle Networks [35]. Another concept closely associated with digital identities is the Zero Trust security model [31, 66], which operates on the assumption that no individual is inherently trustworthy. This principle applies universally to all individuals both within and outside a network. Consequently, it necessitates continuous verification of users for each access request. In the automotive industry, the adoption of Zero Trust has the potential to enhance the security of connected vehicle systems by ensuring that only authenticated and authorized entities can access critical functions [7]. Zero Trust already has a wide range of applications from cloud computing to IoT. The application in connected vehicles comes with a variety of challenges ranging from general problems, such as vendor lock-in, to device- and protocol-specific challenges, such as the broadcast nature of the CAN bus and the delays in V2V authentication [7, p.14-19]. However, it is an active area of research with a wide range of solutions provided in the literature, making it a promising security control with the potential for a high positive impact in the medium term.

5.5 Dissemination and Continuous Improvements: The ACTR Website

The entire ACTR, with all identified trends, their interrelationships, and background information, is available at [25]. This website can be used to navigate within the radar, filter for specific trends, and find more detailed information. In addition, the website serves as a tool for the continuous maintenance and updating of the ACTR. To this end, options for suggesting new trends and constructive criticism, and participation in the further development have been implemented. This allows scientists and industry experts from various professional backgrounds to contribute their expertise and thus contribute to the further improvement of the ACTR.

5.6 Discussion

In its current form, the ACTR contains 66 trends divided into four categories: Communication, Cryptography, System Design, and Advanced Computing. Trends were selected based on literature research and the expertise of the involved authors and further members of the participating institutions with various backgrounds in automotive security. The methodology ensures the initial status of the radar, its structure, and its content are valid and substantial. However, it is unfeasible to fully cover all relevant topics, so the radar must be improved and adapted through further iterations (see Section 3). This applies to the selection and assessment of topics as well as the structure of the radar.

6 Conclusion

In this work, we presented an Automotive Cybersecurity Trend Radar. The applied methodology provides a systematic and repeatable approach to gather and analyze literature relevant for the future in automotive security. It includes various sources of information, such as recent academic surveys and foresight works, industry reports, whitepaper, and existing trend radars from similar domains. Through the application of clearly defined exclusion and inclusion criteria, a structured narrowing down and selection of topics was achieved, resulting in a comprehensive collection of trends which were categorized according to their degree of maturity and impact. The trend radar in its version presented in this work is based on extensive literature research and the expertise of a number of experts from industry and science in this field. However, given the extensive nature of the subject matter, it is advantageous for a diverse array of experts to contribute their knowledge. Therefore, we welcome any feedback and constructive criticism from the automotive security community.

7 Outlook

The ACTR can be utilized by OEMs and suppliers to monitor relevant emerging technologies and, based on the research carried out, determine when to take a closer look at which technology. Consequently, novel attack vectors can be deduced and assessed, thereby facilitating the design of adequate security mechanisms early on. In future, the ACTR can be expanded with various extensions. A key aspect is continuous review and renewal of selected trends. On the one hand, this can be done by re-executing the methodology presented, whereby the literature-based approach is pursued further and adaptation to current developments is made possible. On the other hand, in addition to the feedback mechanisms provided with the website (see 5.5), it is proposed to introduce a committee for continuous maintenance of the radar, whereby knowledge from industry and academia can be directly incorporated. The proposed future developments will be available online at [25].

Acknowledgments

The presented work has been funded by the Daimler Truck Holding AG in Stuttgart, Germany.
Special thanks to all our colleagues for their expertise, valuable input, and constructive discussions.

References

[1] Muhammad AbuGhanem. 2025. IBM Quantum Computers: Evolution, Performance, and Future Directions. *The Journal of Supercomputing* 81, 5 (April 2025), 687. doi:10.1007/s11227-025-07047-7

[2] Jameel Ahmad, Muhammad Umer Zia, Ijaz Haider Naqvi, Jawwad Nasar Chattha, Faran Awais Butt, Tao Huang, and Wei Xiang. 2024. Machine Learning and Blockchain Technologies for Cybersecurity in Connected Vehicles. *WIREs Data Mining and Knowledge Discovery* 14, 1 (2024), e1515. doi:10.1002/widm.1515

[3] Gorjan Alagic, Daniel Apon, David Cooper, Quynh Dang, Thinh Dang, John Kelsey, Jacob Lichtinger, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Daniel Smith-Tone, and Yi-Kai Liu. 2022. *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process.* Technical Report NIST Internal or Interagency Report (NISTIR) 8413. National Institute of Standards and Technology. doi:10.6028/NIST.IR.8413-upd1

[4] Mona Alkanhal, Abdulaziz Alali, and Mohamed Younis. 2024. A Distributed Lightweight PUF-Based Mutual Authentication Protocol for IoV. *IoT* 5, 1 (March 2024), 1–19. doi:10.3390/iot5010001

[5] Nouri Alnahawi, Nicolai Schmitt, Alexander Wiesmaier, Andreas Heinemann, and Tobias Graßmeyer. 2022. On the State of Crypto Agility. In *18. Deutscher IT-sicherheitskongress.* SecuMedia Verlags-GmbH, Germany, 103–126.

[6] Martin Andreoni, Willian Tessaro Lunardi, George Lawton, and Shreekant Thakkar. 2024. Enhancing Autonomous System Security and Resilience With Generative AI: A Comprehensive Survey. *IEEE Access* 12 (2024), 109470–109493. doi:10.1109/ACCESS.2024.3439363

[7] Malak Annabi, Abdelhafid Zeroual, and Nadhir Messai. 2024. Towards Zero Trust Security in Connected Vehicles: A Comprehensive Survey. *Computers & Security* 145 (Oct. 2024), 104018. doi:10.1016/j.cose.2024.104018

[8] Tommaso Bianchi, Alessandro Brighente, and Mauro Conti. 2024. DynamiQS: Quantum Secure Authentication for Dynamic Charging of Electric Vehicles. In *Proceedings of the 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '24).* Association for Computing Machinery, New York, NY, USA, 174–184. doi:10.1145/3643833.3656115

[9] Vik Bogdanov. 2024. Top 10 Automotive Cybersecurity Trends 2024. https://www.rinf.tech/top-10-automotive-cybersecurity-trends-2024/

[10] Dan Boneh, Amit Sahai, and Brent Waters. 2011. Functional Encryption: Definitions and Challenges. In *Theory of Cryptography*, Yuval Ishai (Ed.). Springer, Berlin, Heidelberg, 253–273. doi:10.1007/978-3-642-19571-6_16

[11] Capgemini and Dr. Bratzel Center of Automotive Management GmbH & Co. KG. 2024. *Studie-Software-Revolution-Autos-neu-denken - Digital Automotive Innovation Radar.* Technical Report. Dr. Bratzel Center of Automotive Management GmbH & Co. KG, Germany. 48 pages. https://www.capgemini.com/de-de/wp-content/uploads/sites/8/2024/09/Studie-Software-Revolution-Autos-neu-denken.pdf

[12] Shanzhi Chen, Jinling Hu, Li Zhao, Rui Zhao, Jiayi Fang, Yan Shi, and Hui Xu. 2023. *Cellular Vehicle-to-Everything (C-V2X).* Springer Nature, Singapore. doi:10.1007/978-981-19-5130-5

[13] Amit Chougule, Kartik Agrawal, and Vinay Chamola. 2023. SCAN-GAN: Generative Adversarial Network Based Synthetic Data Generation Technique for Controller Area Network. *IEEE Internet of Things Magazine* 6, 3 (Sept. 2023), 126–130. doi:10.1109/IOTM.001.2300013

[14] Marco De Vincenzi, Gianpiero Costantino, Ilaria Matteucci, Florian Fenzl, Christian Plappert, Roland Rieke, and Daniel Zelle. 2024. A Systematic Review on Security Attacks and Countermeasures in Automotive Ethernet. *ACM Comput. Surv.* 56, 6 (Jan. 2024), 1–38. doi:10.1145/3637059

[15] DHL Group. 2024. Logistics Trend Radar. Insights. Shaping Tomorrow. https://www.dhl.com/de-en/home/innovation-in-logistics/logistics-trend-radar.html?locale=true

[16] Irmina Durlik, Tymoteusz Miller, Ewelina Kostecka, Zenon Zwierzewicz, and Adrianna Łobodzińska. 2024. Cybersecurity in Autonomous Vehicles—Are We Ready for the Challenge? *Electronics* 13, 13 (Jan. 2024), 2654. doi:10.3390/electronics13132654

[17] Ellissa Cavaciuti-Wishart, Sophie Heading, Kevin Kohler, and Saadia Zahidi. 2024. *The Global Risks Report 2024: 19th Edition* (19th ed.). World Economic Forum, Cologny/Geneva, Switzerland. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf

[18] Elin Eriksson and Lisa Fahlbeck. 2022. *Investigating the Use of Honeypots in Vehicles.* Master's Thesis. Chalmers University of Technology, Gothenburg, Sweden. 44 pages. https://odr.chalmers.se/server/api/core/bitstreams/3df6ac22-2f05-479b-a7ec-da34e871487b/content

[19] Amy Ertan, Kathryn Floyd, Piret Pernik, and Tim Stevens (Eds.). 2021. *Cyber Threats and NATO 2030: Horizon Scanning and Analysis.* NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia. https://kclpure.kcl.ac.uk/portal/en/publications/cyber-threats-and-nato-2030-horizon-scanning-and-analysis

[20] European Union Agency for Cybersecurity, Rossella Mattioli, and Apostolos Malatras. 2024. *Foresight Cybersecurity Threats for 2030 - Update - Extended Report.* European Union Agency for Cybersecurity. https://data.europa.eu/doi/10.2824/349493

[21] EVIDEN. 2023. Eviden Cybersecurity Tech Radar. https://eviden.com/publications/tech-radar/cybersecurity/

[22] Eslam Farsimadan, Leila Moradi, and Francesco Palmieri. 2025. A Review on Security Challenges in V2X Communications Technology for VANETs. *IEEE Access* 13 (2025), 31069–31094. doi:10.1109/ACCESS.2025.3541035

[23] Davide Ferraris, Carmen Fernandez-Gago, Rodrigo Roman, and Javier Lopez. 2024. A Survey on IoT Trust Model Frameworks. *The Journal of Supercomputing* 80, 6 (April 2024), 8259–8296. doi:10.1007/s11227-023-05765-4

[24] Javier Franco, Ahmet Aris, Berk Canberk, and A. Selcuk Uluagac. 2021. A Survey of Honeypots and Honeynets for Internet of Things, Industrial Internet of Things, and Cyber-Physical Systems. *IEEE Communications Surveys & Tutorials* 23, 4 (2021), 2351–2383. doi:10.1109/COMST.2021.3106669

[25] Gabriel Simmann, Reiner Kriesten, Felix Maag, and Martin Mager. 2025. Automotive Cybersecurity Trend Radar. https://automotivesecuritytrends.com/

[26] Yansong Gao, Said F. Al-Sarawi, and Derek Abbott. 2020. Physical Unclonable Functions. *Nature Electronics* 3, 2 (Feb. 2020), 81–91. doi:10.1038/s41928-020-0372-5

[27] Keno Garlichs, Alexander Willecke, Martin Wegner, and Lars C. Wolf. 2019. TriP: Misbehavior Detection for Dynamic Platoons Using Trust. In *2019 IEEE Intelligent Transportation Systems Conference (ITSC).* IEEE, Auckland, New Zealand, 455–460. doi:10.1109/ITSC.2019.8917188

[28] Craig Gentry. 2009. *A Fully Homomorphic Encryption Scheme.* Ph. D. Dissertation. Stanford University, Stanford, CA, USA. https://crypto.stanford.edu/craig/craig-thesis.pdf

[29] Oded Goldreich, Silvio Micali, and Avi Wigderson. 1986. Proofs That Yield Nothing but Their Validity and a Methodology of Cryptographic Protocol Design. In *27th Annual Symposium on Foundations of Computer Science (Sfcs 1986).* IEEE, Toronto, ON, Canada, 174–187. doi:10.1109/SFCS.1986.47

[30] BMW Group. 2025. BMW Group Technologie Trend Radar 2025. https://www.bmwgroup.com/de/innovation/technologie-trend-radar.html

[31] Yuanhang He, Daochao Huang, Lei Chen, Yi Ni, and Xiangjie Ma. 2022. A Survey on Zero Trust Architecture: Challenges and Future Trends. *Wireless Communications and Mobile Computing* 2022, 1 (2022), 13. doi:10.1155/2022/6476274

[32] Hatem Ibn-Khedher, Mohammed Laroui, Mohammed Alfaqawi, Ahlam Magnouche, Hassine Moungla, and Hossam Afifi. 2024. 6G-edge Support of Internet of Autonomous Vehicles: A Survey. *Transactions on Emerging Telecommunications Technologies* 35, 1 (2024), e4918. doi:10.1002/ett.4918

[33] Niclas Ilg, Dominik Germek, Paul Duplys, and Michael Menth. 2024. Work-in-Progress: Emerging E/E-Architectures as Enabler for Automotive Honeypots. In *2024 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW).* IEEE, Vienna, Austria, 361–366. doi:10.1109/EuroSPW61312.2024.00046

[34] Chris Jacobs. 2023. Drei Megatrends treiben Speicherbedarf moderner Autos in die Höhe. https://www.elektronikpraxis.de/drei-megatrends-treiben-speicherbedarf-moderner-autos-in-die-hoehe-a-f0ecdba0f1b1d03db5f7702ba361e011/

[35] Haoran Jiang, Guo Wan, Yehua Wei, and Jiangwei Li. 2024. ECU Authentication Method Based on PUF for In-Vehicle Networks. In *2024 IEEE 14th International Symposium on Industrial Embedded Systems (SIES).* IEEE, Chengdu, China, 99–103. doi:10.1109/SIES62473.2024.10767929

[36] Wenxian Jiang and Zhenping Guo. 2025. An Anonymous Authentication Scheme for Internet of Vehicles Based on TRUG-PBFT Main–Secondary Chains and Zero-Knowledge Proof. *IEEE Internet of Things Journal* 12, 7 (April 2025), 7763–7777. doi:10.1109/JIOT.2024.3429342

[37] David Joseph, Rafael Misoczki, Marc Manzano, Joe Tricot, Fernando Dominguez Pinuaga, Olivier Lacombe, Stefan Leichenauer, Jack Hidary, Phil Venables, and Royal Hansen. 2022. Transitioning Organizations to Post-Quantum Cryptography. *Nature* 605, 7909 (May 2022), 237–243. doi:10.1038/s41586-022-04623-2

[38] Ramesh Chandra Joshi and Anjali Sardana. 2011. *Honeypots: A New Paradigm to Information Security* (1st ed.). Science Publishers, P.O. Box 699, Enfield, New Hampshire, USA.

[39] Frank Kargl, Nataša Trkulja, Artur Hermann, Florian Sommer, Anderson Ramon Ferraz De Lucena, Alexander Kiening, and Sergej Japs. 2023. Securing Cooperative Intersection Management through Subjective Trust Networks. In *2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring).* IEEE, Florence, Italy, 1–7. doi:10.1109/VTC2023-Spring57618.2023.10200789

[40] Junaid Ahmed Khan, Weiyi Wang, and Kaan Ozbay. 2024. BELIEVE: Privacy-Aware Secure Multi-Party Computation for Real-Time Connected and Autonomous Vehicles and Micro-Mobility Data Validation Using Blockchain—A Study on New York City Data. *Transportation Research Record* 2678, 3 (March 2024), 410–421. doi:10.1177/03611981231180200

[41] Hamza Khemissa and Pascal Urien. 2023. Towards a Centralized Security Architecture for SOME/IP Automotive Services. In *2023 IEEE 20th Consumer Communications & Networking Conference (CCNC).* IEEE, Las Vegas, NV, USA, 977–978. doi:10.1109/CCNC51644.2023.10059950

[42] Shiho Kim and Rakesh Shrestha. 2020. *Automotive Cyber Security: Introduction, Challenges, and Standardization* (1 ed.). Springer Singapore, Singapore. doi:10.

1007/978-981-15-8053-6

[43] Bert-Jaap Koops. 2016. Megatrends and Grand Challenges of Cybercrime and Cyberterrorism Policy and Research. In *Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities*, Babak Akhgar and Ben Brewster (Eds.). Springer, Cham, 3–15. doi:10.1007/978-3-319-38930-1_1

[44] Michele La Manna. 2022. *Applying Attribute Based Encryption in IoT and Automotive Scenario.* Ph. D. Dissertation. Università degli Studi di Firenze, Florence, Italy. https://flore.unifi.it/handle/2158/1264303#

[45] Ryan Lavin, Xuekai Liu, Hardhik Mohanty, Logan Norman, Giovanni Zaarour, and Bhaskar Krishnamachari. 2024. A Survey on the Applications of Zero-Knowledge Proofs. doi:10.48550/arXiv.2408.00243 arXiv:2408.00243 [cs]

[46] Rensis Likert. 1932. A Technique for the Measurement of Attitudes. *Archives of Psychology* 22 140 (1932), 1–55.

[47] Trupil Limbasiya, Ko Zheng Teng, Sudipta Chattopadhyay, and Jianying Zhou. 2022. A Systematic Survey of Attack Detection and Prevention in Connected and Autonomous Vehicles. *Vehicular Communications* 37 (Oct. 2022), 100515. doi:10.1016/j.vehcom.2022.100515

[48] Zongwei Liu, Wang Zhang, and Fuquan Zhao. 2022. Impact, Challenges and Prospect of Software-Defined Vehicles. *Automotive Innovation* 5, 2 (April 2022), 180–194. doi:10.1007/s42154-022-00179-z

[49] Nils Lohmiller, Sabrina Kaniewski, Michael Menth, and Tobias Heer. 2025. A Survey of Post-Quantum Cryptography Migration in Vehicles. *IEEE Access* 13 (2025), 10160–10176. doi:10.1109/ACCESS.2025.3528562

[50] Siti-Farhana Lokman, Abu Talib Othman, and Muhammad-Husaini Abu-Bakar. 2019. Intrusion Detection System for Automotive Controller Area Network (CAN) Bus System: A Review. *EURASIP Journal on Wireless Communications and Networking* 2019, 1 (July 2019), 184. doi:10.1186/s13638-019-1484-3

[51] Sidi Lu and Weisong Shi. 2023. Vehicle Computing: Vision and Challenges. *Journal of Information and Intelligence* 1, 1 (May 2023), 23–35. doi:10.1016/j.jiixd.2022.10.001

[52] Javaid Ahmad Malik, Sagheer Abbas, Altaf Hussain, Muhammad Saleem, and Rahat Qudsi. 2024. Next-Generation Protection: Leveraging Federated Learning and Blockchain for Intrusion Detection in Smart Vehicle Network. *Power System Technology* 48, 1 (May 2024), 931–952. doi:10.52783/pst.353

[53] Michele Mosca and Marco Piani. 2024. *Quantum Threat Timeline Report 2024.* Technical Report. Global Risk Institute. https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/

[54] Felix Mogge, Brandon Boyle, Jan-Philipp Hasenberg, Ron Zhen, Isaac Chan, Shual Shl, and Lukas Saller. 2024. *Automotive Outlook 2040.* Technical Report. Roland Berger GmbH, Munich, Germany. 46 pages. https://www.rolandberger.com/de/Insights/Global-Topics/Automotive-2040/

[55] Munich Re. 2021. Tech Trend Radar 2021 – Manage Uncertainty with Confidence | Munich Re. https://www.munichre.com/en/company/innovation/tech-trend-radar-2021.html

[56] Swapnil Nandanwar, Sumitra Biswal, and Vishal Gupta. 2024. Investigating Vulnerabilities and Potential Security Threats in Current Synthetic Data Generation and Usage in the Automotive Domain. In *2024 IEEE International Conference on Omni-layer Intelligent Systems (COINS).* IEEE, London, United Kingdom, 1–6. doi:10.1109/COINS61597.2024.10622294

[57] National Institute of Standards and Technology (NIST). 2023. Advanced Encryption Standard (AES). FIPS 197. doi:10.6028/NIST.FIPS.197-upd1

[58] Krish Parikh. 2024. Driving Privacy Forward: Mitigating Information Leakage within Smart Vehicles through Synthetic Data Generation. doi:10.48550/arXiv.2410.08462 arXiv:2410.08462 [cs]

[59] Rafael Popper. 2008. How Are Foresight Methods Selected? *Foresight* 10, 6 (Jan. 2008), 62–89. doi:10.1108/14636680810918586

[60] Tejasweeni Pradhan and Pramod Patil. 2024. Quantum Cryptography for Secure Autonomous Vehicle Networks: A Review. In *2024 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS).* IEEE, Bhopal, India, 1–10. doi:10.1109/SCEECS61402.2024.10482142

[61] Nordine Quadar, Abdellah Chehri, Benoit Debaque, Imran Ahmed, and Gwangil Jeon. 2024. Intrusion Detection Systems in Automotive Ethernet Networks: Challenges, Opportunities and Future Research Trends. *IEEE Internet of Things Magazine* 7, 2 (March 2024), 62–68. doi:10.1109/IOTM.001.2300109

[62] Yoel Raban and Aharon Hauptman. 2018. Foresight of Cyber Security Threat Drivers and Affecting Technologies. *Foresight* 20, 4 (Aug. 2018), 353–363. doi:10.1108/FS-02-2018-0020

[63] Rafael Popper. 2008. Foresight Methodology. In *The Handbook of Technology Foresight*, Luke Georghiou, Jennifer Cassingena Harper, Michael Keenan, Ian Miles, and Rafael Popper (Eds.). Edward Elgar Publishing, Cheltenham, 44–88.

[64] Hassan Rehan. 2024. The Future of Electric Vehicles: Navigating the Intersection of AI, Cloud Technology, and Cybersecurity. *Valley International Journal Digital Library* 12, 04 (April 2024), 1127–1143. doi:10.18535/ijsrm/v12i04.ec04

[65] Ronald Linn Rivest, Adi Shamir, and Leonard Max Adleman. 1978. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Commun. ACM* 21, 2 (Feb. 1978), 120–126. doi:10.1145/359340.359342

[66] Scott Rose, Oliver Borchert, Stu Mitchell, and Sean Connelly. 2020. *Zero Trust Architecture.* NIST Special Publication 800-207. National Institute of Standards and Technology (NIST). 59 pages. doi:10.6028/NIST.SP.800-207

[67] Thomas Rosenstatter and Kateryna Melnyk. 2023. Towards Synthetic Data Generation of VANET Attacks for Efficient Testing. In *2023 IEEE Intelligent Vehicles Symposium (IV).* IEEE, Anchorage, AK, USA, 1–7. doi:10.1109/IV55152.2023.10186685

[68] Thomas Rosenstatter, Kim Strandberg, Rodi Jolak, Riccardo Scandariato, and Tomas Olovsson. 2020. REMIND: A Framework for the Resilient Design of Automotive Systems. In *2020 IEEE Secure Development (SecDev).* IEEE, Atlanta, GA, USA, 81–95. doi:10.1109/SecDev45635.2020.00028

[69] SAE International. 2021. Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles. J3016_202104. 2021. https://www.sae.org/standards/content/j3016_202104/

[70] Paul Scalise, Matthew Boeding, Michael Hempel, Hamid Sharif, Joseph Delloiacovo, and John Reed. 2024. A Systematic Survey on 5G and 6G Security Considerations, Challenges, Trends, and Research Areas. *Future Internet* 16, 3 (March 2024), 67. doi:10.3390/fi16030067

[71] Sven Schimpf, Claus Lang-Koetz, Dieter Spath, and Fraunhofer-Institut für Arbeitswirtschaft und Organisation (Eds.). 2010. *Technologiemonitoring: Technologien identifizieren, beobachten und bewerten.* Fraunhofer-Verl, Stuttgart.

[72] Sonal Shamkuwar, Arijit Mondal, Rohan More, Smita Bodare, and Aditya Pendalwar. 2024. Federated Learning in Automated Vehicles. In *Proceedings of 4th International Conference on Artificial Intelligence and Smart Energy*, S. Manoharan, Alexandru Tugui, and Zubair Baig (Eds.). Springer Nature Switzerland, Cham, 301–314. doi:10.1007/978-3-031-61475-0_24

[73] Kyung-Ah Shim. 2022. A Survey on Post-Quantum Public-Key Signature Schemes for Secure Vehicular Communications. *IEEE Transactions on Intelligent Transportation Systems* 23, 9 (Sept. 2022), 14025–14042. doi:10.1109/TITS.2021.3131668

[74] Sadia Jabeen Siddiqi, Sana Saleh, Mian Ahmad Jan, and Muhammad Tariq. 2025. Securing the Vetaverse: Web 3.0 for Decentralized Digital Twin-enhanced Vehicle–Road Safety. *Future Generation Computer Systems* 164 (March 2025), 107555. doi:10.1016/j.future.2024.107555

[75] Florian Sommer. 2024. *Automatic Attack Path Generation in Automotive Model-Based Security Testing.* Ph. D. Dissertation. Universität Ulm. doi:10.18725/OPARU-53899

[76] Steve Wells. 2025. Reinventing the Future - Trend Radar by Steve Wells. https://www.fibresonline.com/data-sources/informing-choices

[77] Isaac Triguero, Daniel Molina, Javier Poyatos, Javier Del Ser, and Francisco Herrera. 2024. General Purpose Artificial Intelligence Systems (GPAIS): Properties, Definition, Taxonomy, Societal Implications and Responsible Governance. *Information Fusion* 103 (March 2024), 102135. doi:10.1016/j.inffus.2023.102135

[78] Upstream Security Ltd. 2023. *H1'2023 Automotive Cyber Trend Report.* Trend Report. Upstream Security Ltd. https://upstream.auto/reports/h1-2023-automotive-cyber-trend-report/

[79] Upstream Security Ltd. 2024. *2024 Global Automotive Cybersecurity Report.* Technical Report. Upstream Security Ltd. 138 pages. https://upstream.auto/resources/

[80] Tasha Van Dasselaar, Jason Giddings, and Sydney Stewart. 2023. Applications of Foresight for Defence and Security: The Future of Crime. In *Safety and Security Science and Technology: Perspectives from Practice*, Anthony J. Masys (Ed.). Springer International Publishing, Cham, 75–101. doi:10.1007/978-3-031-21530-8_5

[81] Vandani Verma and Chinmay. 2024. Enhancing Privacy in VANET Through Attribute-Based Encryption and Blockchain Integration: Uncovering the Benefits and Challenges. In *Cryptology and Network Security with Machine Learning*, Atul Chaturvedi, Sartaj Ul Hasan, Bimal Kumar Roy, and Boaz Tsaban (Eds.). Springer Nature, Singapore, 277–293. doi:10.1007/978-981-97-0641-9_19

[82] Hui Wang, Nima Tashakor, Wei Jiang, Wei Liu, C. Q. Jiang, and Stefan M. Goetz. 2024. Hacking Encrypted Frequency-Varying Wireless Power: Cyber-Security of Dynamic Charging. *IEEE Transactions on Energy Conversion* 39, 3 (Sept. 2024), 1947–1957. doi:10.1109/TEC.2024.3355743

[83] Xiaonan Wang, Yang Guo, and Yuan Gao. 2024. Unmanned Autonomous Intelligent System in 6G Non-Terrestrial Network. *Information* 15, 1 (Jan. 2024), 38. doi:10.3390/info15010038

[84] Qiang Yang, Yang Liu, Tianjian Chen, and Yongxin Tong. 2019. Federated Machine Learning: Concept and Applications. *ACM Trans. Intell. Syst. Technol.* 10, 2 (Jan. 2019), 19. doi:10.1145/3298981

[85] Andrew C. Yao. 1982. Protocols for Secure Computations. In *23rd Annual Symposium on Foundations of Computer Science (Sfcs 1982).* IEEE, Chicago, IL, USA, 160–164. doi:10.1109/SFCS.1982.38

[86] Jiacheng Zhang. 2024. A Review of Wireless Charging Technology for Electric Vehicles. In *Ninth International Conference on Electromechanical Control Technology and Transportation (ICECTT 2024)*, Vol. 13251. SPIE, Guilin, China, 1383–1390. doi:10.1117/12.3039589

[87] Rongqing Zhang, Jingxin Mao, Hanqiu Wang, Bing Li, Xiang Cheng, and Liuqing Yang. 2024. A Survey on Federated Learning in Intelligent Transportation Systems. *IEEE Transactions on Intelligent Vehicles* (2024), 1–17. doi:10.1109/TIV.2024.3446319

[88] Xiaohong Zhang, Xingxing Chen, Shuling Liu, and Shaojiang Zhong. 2024. Anonymous Authentication and Information Sharing Scheme Based on

Blockchain and Zero Knowledge Proof for VANETs. *IEEE Transactions on Vehicular Technology* 73, 12 (Dec. 2024), 18043–18058. doi:10.1109/TVT.2024.3432553

[89] Zhengquan Zhang, Yue Xiao, Zheng Ma, Ming Xiao, Zhiguo Ding, Xianfu Lei, George K. Karagiannidis, and Pingzhi Fan. 2019. 6G Wireless Networks: Vision, Requirements, Architecture, and Key Technologies. *IEEE Vehicular Technology Magazine* 14, 3 (Sept. 2019), 28–41. doi:10.1109/MVT.2019.2921208

[90] Chuan Zhao, Shengnan Zhao, Minghao Zhao, Zhenxiang Chen, Chong-Zhi Gao, Hongwei Li, and Yu-an Tan. 2019. Secure Multi-Party Computation: Theory, Practice and Applications. *Information Sciences* 476 (Feb. 2019), 357–372. doi:10.1016/j.ins.2018.10.024

[91] Banghua Zhu, Norman Mu, Jiantao Jiao, and David Wagner. 2024. Generative AI Security: Challenges and Countermeasures. doi:10.48550/arXiv.2402.12617 arXiv:2402.12617 [cs]