vehicles

MDPI

Article

A fsQCA-Based Framework for Cybersecurity of Connected and Automated Vehicles: Implications for Sustainable Development Goals

Koppiahraj Karuppiah [1], Bathrinath Sankaranarayanan [2,*], Syed Mithun Ali [3] and Ramesh Priyanka [4]

[1] Department of Mechanical Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai 602104, India; koppiahraj1993@gmail.com
[2] Department of Mechanical Engineering, Kalasalingam Academy of Research and Education, Krishnankoil 626126, India
[3] Department of Industrial and Production Engineering, Bangladesh University of Engineering and Technology, Dhaka 1000, Bangladesh; mithun@ipe.buet.ac.bd
[4] Kalasalingam Business School, Kalasalingam Academy of Research and Education, Krishnankoil 626126, India; rpriyanka2597@gmail.com
* Correspondence: bathri@klu.ac.in

Abstract: Connected and automated vehicles (CAV) are increasingly recognized as a critical component of intelligent transportation systems (ITS), contributing to advances in transportation safety and mobility. However, the implementation of CAV in a real-world environment comes with various threats, and cybersecurity is among the most vulnerable. As the technology becomes more advanced and complex, it is essential to develop a comprehensive cybersecurity framework that can address these concerns. This research proposes a novel framework based on complexity theory and employs the fuzzy set qualitative comparative analysis (fsQCA) technique to identify combinations of security attacks that lead to achieving cybersecurity in CAV. Compared to structural equation modelling (SEM), the fsQCA method offers the advantage of demonstrating all possible ways to achieve the outcome. The study's findings suggest that in-vehicle networks and data storage security are the most crucial factors in ensuring the cybersecurity of CAV. The results can be useful for automotive designers in reducing the potential for attacks while developing secure networks.

Keywords: connected and automated vehicles; intelligent transportation system; fsQCA; cybersecurity; security attacks

check for updates

Citation: Karuppiah, K.; Sankaranarayanan, B.; Ali, S.M.; Priyanka, R. A fsQCA-Based Framework for Cybersecurity of Connected and Automated Vehicles: Implications for Sustainable Development Goals. *Vehicles* **2024**, *6*, 484–508. https://doi.org/10.3390/vehicles6010022

Academic Editor: Meng Li

Received: 20 December 2023
Revised: 26 February 2024
Accepted: 26 February 2024
Published: 28 February 2024

1. Introduction

The growing need for mobility in cities has led to increased vehicle ownership, resulting in traffic congestion and accidents. To address this issue, intelligent transportation systems (ITS) have emerged as a viable solution [1]. Among the advancements in ITS, connected and automated vehicles (CAVs) have become a focal point due to their potential to enhance quality of life, reduce accidents, and improve transportation efficiency [2]. Additionally, the increasing income levels of people have fueled their interest in quality-based lifestyles, making them more receptive to technological advancements, including CAVs, which offer attractive benefits compared to fuel-based transportation [3]. However, the use of CAVs also involves certain risks, particularly in terms of cybersecurity. Security risks pose a significant challenge to the implementation of CAVs in real-world environments [4]. While other risks associated with ITS depend on a country's environmental benefits, security risks are prevalent everywhere, particularly in advanced environments where they can have a greater impact. As CAVs handle more information and confidential data, sharing of information among vehicles increases the risk of security threats for users. These threats can manifest in various forms, including vehicle-to-everything networks, in-vehicle network attacks, data storage attacks, machine learning system attacks, slight attacks, and password and key attacks [5].

Addressing and solving all attacks can be challenging for automotive designers, leading to difficulties in the design process. Therefore, this paper aims to explore the cybersecurity issues related to CAVs and identify the most vulnerable security attacks that pose obstacles to ensure their cybersecurity. This study will focus on the following research questions:

- RQ1: What are the most vulnerable security attacks that threaten the cybersecurity of CAVs?
- RQ2: What countermeasures and strategies have been employed to mitigate these attacks?
- RQ3: Will removing these attacks ensure the cybersecurity of CAVs?

Answering these questions is crucial to reducing the design difficulties faced by automotive engineers. To identify the various security attacks and countermeasures, a literature review was conducted. The study employed these countermeasures to measure the removability of security attacks. The fuzzy set qualitative comparative analysis (fsQCA) method was used to analyze the security attacks. This method is capable of producing multiple paths to achieve an outcome, and through its application, the study produced results of various combinations of constructs (security attack checks) necessary to ensure the cybersecurity of CAVs.

Continuing this introduction section, the remainder of this paper is arranged as Section 2—Literature review, Section 3—Research Methodology, Section 4—Results, Section 5—Discussions, Section 6—Research implications, and Section 7—Conclusions.

2. Literature Review

The literature review is structured into two main sections, covering (i) connected and automated vehicles and (ii) security attacks that pose a threat to the cybersecurity of CAV.

2.1. Connected and Automated Vehicles (CAV)

The dynamic landscape of connected and automated vehicles (CAV) continues to captivate the realms of technology, transportation, and societal evolution. The symbiosis of autonomous vehicles (AV) and connected vehicles (CV) has catalyzed a paradigm shift, offering a spectrum of benefits that extends well beyond conventional modes of transport [6,7]. The taxonomy proposed by the Society of Automobile Engineers (SAE), classifying automation levels from 0 to 5, serves as a roadmap for understanding the trajectory of vehicle autonomy. Starting from Level 0 with no automation to the pinnacle of Level 5 characterized by full automation, this classification system illuminates the evolutionary journey of on-road motor vehicles [8]. This framework not only provides clarity in understanding the capabilities of CAVs but also sets the stage for a nuanced exploration of the associated benefits.

At the heart of the allure of CAVs lies their potential to enhance safety, reduce traffic congestion, and mitigate accidents. The promise of safe driving, facilitated by advanced automation features, has the potential to revolutionize the transportation landscape [9]. Real-time communication with road infrastructure and the internet forms the backbone of connected vehicles, ensuring an unprecedented flow of information that contributes to safer and more efficient journeys [10,11]. The societal implications of CAVs are profound. The prospect of reducing the number of cars per household, facilitated by the availability of driverless cars that can be shared among household members, hints at a transformative shift in how we perceive vehicle ownership [12,13]. This not only aligns with sustainability goals but also echoes the emerging trends of shared mobility, particularly relevant in densely populated urban areas.

In densely populated regions, the suitability of car-sharing models gains prominence. The ability of CAVs to adapt to shared usage patterns and cater to the transportation needs of diverse individuals underscores their versatility [14]. Beyond individual convenience, this shared mobility model contributes to the overarching goal of reducing the environmental footprint associated with traditional vehicular ownership [15]. As we delve into the multifaceted advantages of CAVs, it becomes apparent that the narrative extends beyond technological sophistication. The very fabric of urban living stands to be rewoven by the threads of reduced congestion, improved safety, and shared mobility. The potential of CAVs to accommodate non-licensed individuals in the realm of autonomous transportation adds a layer of inclusivity, transforming the vision of modern mobility into a reality accessible to a broader spectrum of the population [16].

2.2. Security Attacks That Pose a Threat to the Cybersecurity of CAV

The rise of connected and automated vehicles has brought forth a new set of cybersecurity concerns. As vehicles become more integrated with technology, they become more vulnerable to attacks that can compromise the safety and security of passengers, as well as the integrity of the vehicle itself [17]. In this section, we will discuss some of the major security attacks that pose a threat to the cybersecurity of connected and automated vehicles. One type of attack that has gained a lot of attention in recent years is the vehicle-to-everything (V2X) attack. V2X refers to the communication between a vehicle and its surrounding environment, including other vehicles, infrastructure, and pedestrians [18]. V2X technology enables vehicles to share data with each other and with the surrounding infrastructure, which can help to improve safety, efficiency, and mobility. However, this technology also introduces new security risks. Attackers can exploit vulnerabilities in the V2X network to gain access to sensitive data or to take control of the vehicle [19]. For example, an attacker could send false messages to a vehicle's onboard computer, causing it to make incorrect decisions or take unsafe actions [20]. Recent advancements in V2X security protocols have aimed to address vulnerabilities, introducing cryptographic measures and secure communication channels. The landscape of V2X attacks is dynamic, with attackers constantly adapting their strategies. As we explore the intricacies of V2X technology, it becomes apparent that ongoing research and proactive security measures are imperative to stay ahead of potential threats [21,22].

Another type of attack that poses a threat to the cybersecurity of connected and automated vehicles is the in-vehicle network attack [23]. In-vehicle networks are the communication systems that connect different electronic components within the vehicle, such as the engine control unit, the entertainment system, and the navigation system [24]. These networks are vulnerable to attacks that can compromise the functioning of the vehicle. An attacker who gains access to an in-vehicle network can potentially control the vehicle's systems, including the brakes, steering, and acceleration [25]. There is a need for advanced intrusion detection systems and secure network architectures to mitigate the risks associated with in-vehicle network attacks [26,27]. As vehicles evolve into sophisticated interconnected systems, the importance of robust cybersecurity measures at the network level becomes paramount. Machine learning system attacks are another type of cybersecurity threat to connected and automated vehicles [28]. Machine learning systems are increasingly being used in vehicles to enable autonomous driving and other advanced features. However, these systems are vulnerable to attacks that can manipulate the algorithms and compromise the integrity of the system [1]. The significance of adversarial machine learning techniques employed by attackers is the ability to manipulate the decision-making processes of these systems. The evolving nature of machine learning attacks necessitates ongoing research and the development of resilient algorithms to safeguard CAVs against potential intrusions [29]. Attackers can feed false data to the machine learning system, causing it to make incorrect decisions or take unsafe actions. Alternatively, an attacker could modify the software or hardware of the machine learning system, causing it to behave in unexpected ways.

Data storage and analysis attacks are also a concern for the cybersecurity of connected and automated vehicles. As vehicles become more connected, they generate and store large amounts of data, including information about the vehicle's location, speed, and driving patterns [30]. These data are valuable to attackers, who can use it to gain insights into the behaviour and habits of the vehicle's owner. Additionally, attackers can exploit vulnerabilities in the data storage and analysis systems to gain access to sensitive data or to modify the data for malicious purposes. Recent advancements in secure data storage technologies and encryption methods have addressed some of these concerns, but continuous efforts are essential to stay abreast of emerging attack vectors [31]. Finally, infrastructure attacks are a concern for the cybersecurity of connected and automated vehicles. As vehicles become more connected, they rely more heavily on the surrounding infrastructure, such as traffic lights, road signs, and GPS systems. An attacker who gains access to the infrastructure can potentially disrupt the functioning of the vehicle or cause it to behave in unexpected ways [32]. For example, an attacker could modify the data being sent to the vehicle's navigation system, causing it to take a longer or more dangerous route. Recent incidents have highlighted the susceptibility of CAVs to disruptions caused by compromising infrastructure components [33]. As the integration between vehicles and infrastructure deepens, research focuses on developing resilient communication protocols and intrusion detection systems to fortify the cybersecurity posture of CAVs [34].

The six specific security attacks chosen for this study were selected based on their significance in recent research. Similarly, the countermeasures and strategies identified to address and mitigate security threats to ensure the cybersecurity of CAV were chosen based on the preference given in recent literature and by expert opinions. To collect the inputs and outputs of this study, various databases such as Google Scholar, Web of Science, SCOPUS, and IEEE Xplore were searched using keywords such as connected and automated vehicles, security of connected and automated vehicles, cybersecurity of CAV, ITS, countermeasures for cybersecurity threats of CAV, most vulnerable cybersecurity attacks of CAV, cyber risks of connected and automated vehicles, and strategies used to ensure the cybersecurity of CAV. A total of 26 items were collected, which were then categorized into seven major security attacks (constructs). Six of them were input variables, and one was an output variable that was tabulated in Table 1. These 26 variables were converted into a Likert scale questionnaire (Table A1 of Appendix A) to collect data from automobile engineers. The inclusion and exclusion criteria of the literature review are tabulated in Table 2. This literature review involved a comprehensive examination of the evolving landscape of connected and automated vehicles (CAVs) and the associated cybersecurity challenges. The exploration of CAVs spans from their foundational taxonomy, as proposed by the Society of Automobile Engineers (SAE), to the profound societal implications of enhanced safety, reduced traffic congestion, and transformed mobility patterns. On the cybersecurity front, the review delves into the multifaceted realm of security attacks targeting CAVs. From vehicle-to-everything (V2X) attacks leveraging communication vulnerabilities to in-vehicle network attacks compromising critical systems, each threat was dissected. Machine learning system attacks and Data storage and analysis threats underscore the evolving nature of cybersecurity challenges. The synthesis of countermeasures and strategies unveiled a mosaic of responses to the identified security threats. From advanced encryption and authentication protocols to the integration of machine learning for privacy assurance, the proactive measures are as dynamic as the challenges they aim to mitigate.

Table 1. Security attacks on connected and automated vehicles.

Area	Attack No.	Security Attacks	Reference(s)
CAV sensor	P1	Using multiple GPS receivers avoids blocking satellite signals from GPS.	[33]
	P2	Usage of redundant sensors on camera verification to avoid illusion and binding	[35]
	P3	Jamming avoidance by making protective glasses around a LiDAR which acts as light filters	[36]
Vehicle-to-everything network	P4	Usage of fog server with fog anonymizer to avoid eavesdropping in vehicular ad-hoc networks (VANETs)	[20]
	P5	Maintaining data integrity in dynamic route guidance by forged data filtering scheme	[25]
	P6	Using swarm algorithms for routing attacks	[37]
	P7	Detecting bandwidth and entropy to reduce denial of service attack	[38]
	P8	Implementing noisy control signals to avoid replay attacks	[39]
	P9	Registering vehicles with TFD to avoid communication of attackers who are under victim identity	[40]
In-vehicle network	P10	Encryption and cryptographic checksum to avoid proximity vulnerabilities	[41]
	P11	Doing network segmentation to avoid CAN and SAE vulnerabilities	[41]
	P12	Encryption and authentication to avoid flashing attacks	[42]
Infrastructure	P13	Content filtering for integrated business service attacks	[28]
	P14	Usage of certificateless aggregate signcryption (CL-A-SC) scheme to monitor road surface conditions	[43]
	P15	Incorporating software-defined networking (SDN) in an IoT environment	[44]
	P16	Using a cloud-based detection system for cloud infrastructure	[32]
Data storage and data analysis	P17	Conserving data mining to protect privacy leakage of user information	[45]
	P18	Using a telematics control unit (TCU) for remote control of vehicles	[46]
	P19	Adopting CVSS (common vulnerability scoring system) to measure the severity of software vulnerabilities	[47]
Machine learning system	P20	Performing data sanitization and robust learning to defend against misleading in the learning process	[48]
	P21	Ensuring the privacy of data by privacy homomorphism	[49]
	P22	Implementing neural networks for privacy assurance	[50]
	P23	Assessing risks earlier using dynamic risk assessment	[51]
Cybersecurity of CAV	P24	Providing better solutions for security issues in connected and automated vehicles (CAV)	Expert opinion
	P25	Strengthening the cybersecurity patterns	Expert opinion
	P26	Reduces attacker intentions in connected and automated vehicles	Expert opinion

Table 2. Inclusion and exclusion criteria of the literature review.

Inclusion Criteria	Exclusion Criteria
Studies focusing on cybersecurity of connected and automated vehicles	Research article not in English
Studies analyzing the countermeasures for avoiding various security attacks	Proxy and repetitive work
Security attacks of CAV	Incomplete data
Studies published between 2015 to 2022	Proceeding papers, editorial materials, thesis

2.3. Research Gap and Contributions

The research paper addresses the critical gap in the field of cybersecurity of connected and automated vehicles (CAVs). Several studies have been conducted on the security issues of CAVs; however, they lack a comprehensive framework to address the cybersecurity challenges effectively. This study proposes a novel framework based on complexity theory and employs the fuzzy set qualitative comparative analysis (fsQCA) technique to identify combinations of security attacks that lead to achieving cybersecurity in CAV. This approach is unique compared to existing research that relies on structural equation modelling (SEM), which does not show all possible combinations of factors leading to an outcome. In contrast, fsQCA provides a comprehensive analysis of all possible combinations, making it a suitable method to address complex issues such as CAV cybersecurity. Moreover, our study's contribution lies in identifying in-vehicle networks and data storage security as the most crucial factors in ensuring the cybersecurity of CAVs, which is different from the factors identified in previous studies. This insight can guide automotive designers in developing secure networks that reduce the potential for attacks, which is critical to ensure the safety and reliability of CAVs.

3. Research Methodology

3.1. Data Collection, Sampling, and Survey Instrument

This empirical study involved the collection of data from automotive experts in 12 selected industries. The 48 respondents who participated in the study held various positions, including chief technical officer, automobile designer, production engineer, automotive developer, and instrumentation engineer. The respondents were selected using simple random sampling, and their demographic profiles are presented in Table 3 and illustrated in Figures 1 and 2. The study found that automotive developers and automobile designers were the most common participants, with many respondents having over 10 years of experience. The study used a 5-point Likert scale questionnaire consisting of 26 items across seven constructs to collect primary data from the respondents. The Likert scale was deemed appropriate for measuring the latent constructs and was consistent with the nature of the questionnaire statements. The reliability of the scale was evaluated using the Cronbach alpha test, with constructs having a Cronbach alpha of greater than 0.7 being considered reliable for the study. Table A1 in the Appendix A presents the seven constructs and 26 items, with the scale ranging from strongly agree to strongly disagree. Table A2 in the Appendix A presents the Demographic information of experts The data were collected using Google Forms, with demographic information also included in the questionnaire. The internal consistency of each construct was evaluated, and all constructs were found to have good internal consistency, with reliability scores above the predetermined threshold. No rewards were provided to the respondents for their participation.

Table 3. Demographic profile of the respondents.

Features			Number of Articles	Percentage (%)
Respondents (n = 48)	Experience	<3 years	1	3
		3–5 years	1	3
		5–10 years	4	10
		>10 years	3	7
	Designation	Chief technical officer	1	3
		Automobile engineer	3	7
		Production engineer	3	7
		Automotive developer	5	13
		Instrumentation engineer	2	5

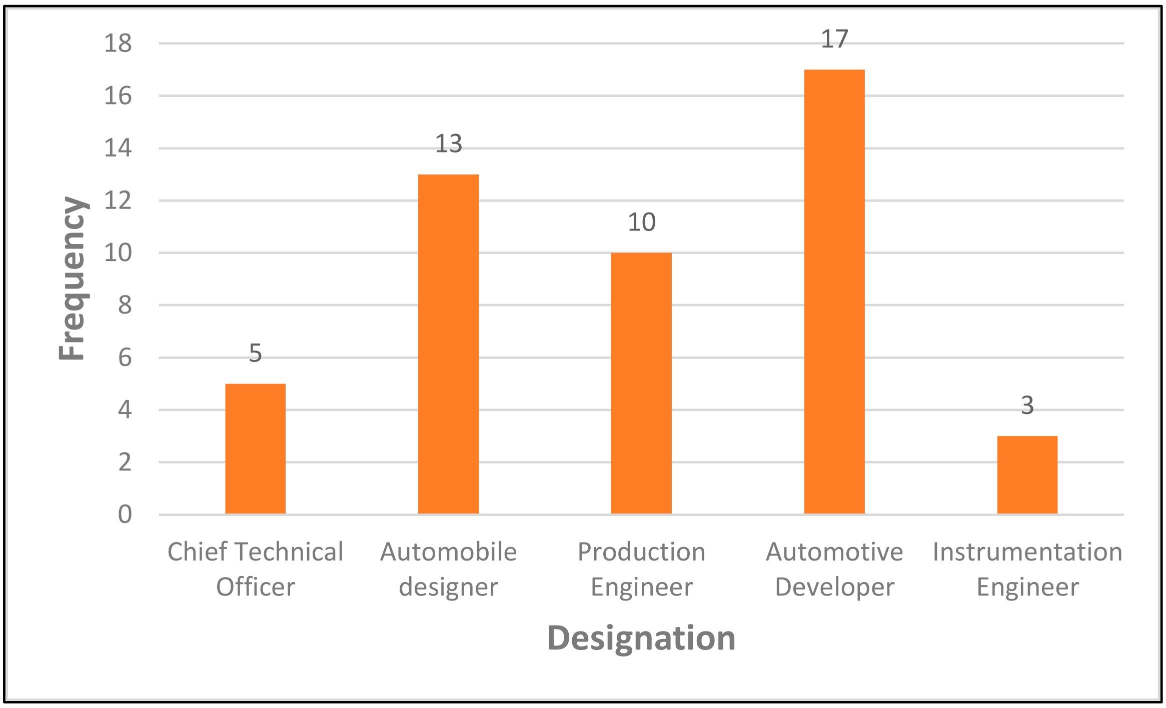


Figure 1. Designation of Respondents.

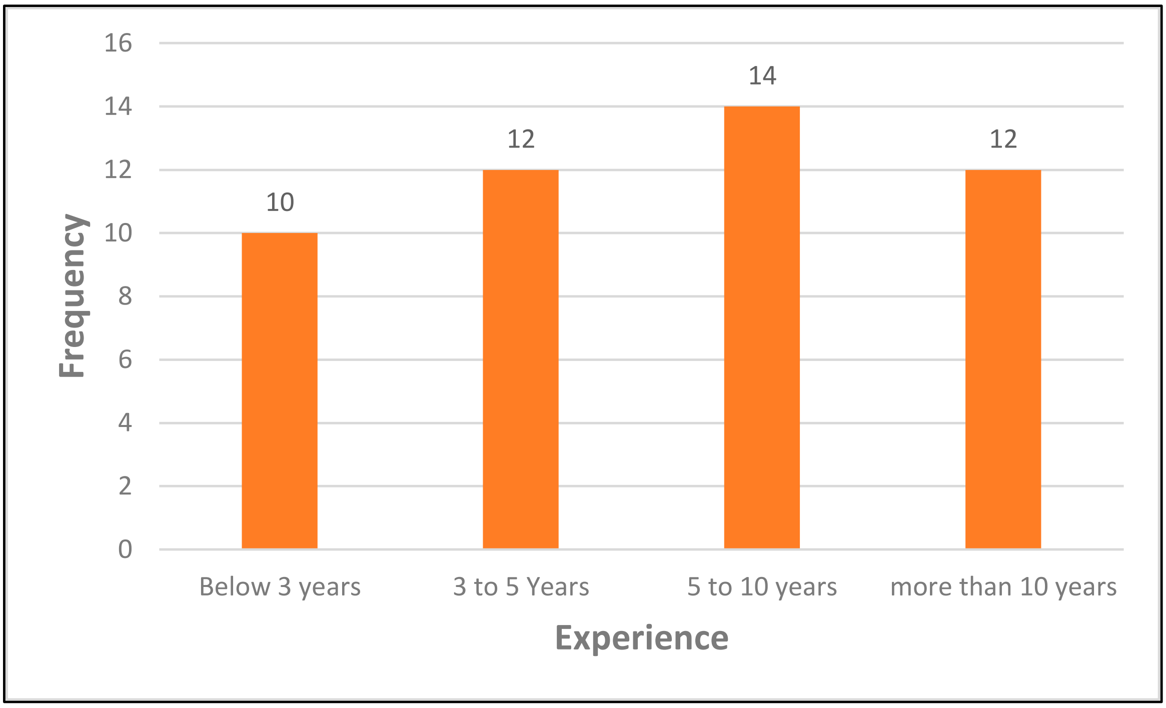


Figure 2. Work experience of the respondents.

3.2. *Reliability and Validity Analysis*

To ensure the reliability and validity of each construct, factor analysis was performed. This involved assessing the Cronbach alpha, average variance extracted, and composite reliability of each construct to identify the most influential combination of inputs and reduce measurement variables. The 26 measurements in the questionnaire were consolidated into 7 measurements, with 6 as the input and 1 as the output. Factor analysis was only conducted for the 7 major constructs. The Cronbach alpha was used to evaluate the internal consistency reliability, with a threshold value of 0.7. Constructs with a Cronbach alpha value greater than 0.7 were deemed suitable for further study, while those with a lower value required the removal of the problematic measurement or item. The SPSS V26 total statistics measurement was used to identify the problematic item. The average variance extracted was then tested to establish the convergent validity of the constructs, with a threshold value of 0.5. Composite reliability, which also had a threshold value of 0.7, was assessed to determine the reliability of the constructs. This factor analysis method helped to identify which measurement or item should be removed and which was unsuitable for the study. The factor analysis results and calculations for the 3 construct tests are presented as SPSS software results below and the summary given in Table 4.

Calculations for CR, ICR, and AVE using SPSS.

Condition 1

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0.847	0.853	3

Item Statistics

	Mean	Std. Deviation	N
Multiple GPS sensor	3.8958	0.95069	48
Redundant sensor	3.6667	0.75324	48
LiDAR	3.3958	0.76463	48

Item-Total Statistics

	Scale Mean If Item Deleted	Scale Variance If Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha If Item Deleted
Multiple GPS sensor	7.0625	1.890	0.738	0.566	0.781
Redundant sensor	7.2917	2.551	0.666	0.450	0.833
LiDAR	7.5625	2.336	0.770	0.597	0.741

Scale Statistics

Mean	Variance	Std. Deviation	N of Items
10.9583	4.722	2.17293	3

Condition 2

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0.909	0.911	6

Item Statistics			
	Mean	**Std. Deviation**	**N**
Fog server	2.7292	0.86884	48
Data filtering	2.7708	0.75059	48
Swarm algorithm	2.7292	0.73628	48
Bandwidth detection	2.5417	0.77070	48
Noisy control signals	2.4375	0.98729	48
TFD	2.3958	0.89299	48

Item-Total Statistics					
	Scale Mean If Item Deleted	**Scale Variance If Item Deleted**	**Corrected Item-Total Correlation**	**Squared Multiple Correlation**	**Cronbach's Alpha If Item Deleted**
Fog server	12.8750	12.197	0.739	0.562	0.894
Data filtering	12.8333	12.780	0.763	0.607	0.892
Swarm algorithm	12.8750	13.346	0.660	0.492	0.905
Bandwidth detection	13.0625	12.570	0.782	0.652	0.889
Noisy control signals	13.1667	10.993	0.835	0.718	0.880
TFD	13.2083	12.083	0.734	0.617	0.895

Scale Statistics			
Mean	**Variance**	**Std. Deviation**	**N of Items**
15.6042	17.436	4.17561	6

Condition 3

Reliability Statistics		
Cronbach's Alpha	**Cronbach's Alpha Based on Standardized Items**	**N of Items**
0.893	0.893	4

Item Statistics			
	Mean	**Std. Deviation**	**N**
Encryption	2.5625	0.89695	48
Network segmentation	2.5833	0.91868	48
Aurhentication	2.5000	0.92253	48
Content filtering	2.5208	0.89893	48

Item-Total Statistics					
	Scale Mean If Item Deleted	Scale Variance If Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha If Item Deleted
Encryption	7.6042	5.861	0.771	0.599	0.859
Network segmentation	7.5833	5.610	0.818	0.680	0.841
Aurhentication	7.6667	6.014	0.696	0.487	0.887
Content filtering	7.6458	5.851	0.772	0.619	0.859

Scale Statistics			
Mean	Variance	Std. Deviation	N of Items
10.1667	10.014	3.16452	4

Condition 4

Reliability Statistics		
Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0.870	0.870	3

Item Statistics			
	Mean	Std. Deviation	N
CL-A-SC	2.9167	0.87113	48
SDN	2.6458	0.86269	48
Cloud-based detection	2.4792	0.87494	48

Item-Total Statistics					
	Scale Mean If Item Deleted	Scale Variance If Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha If Item Deleted
CL-A-SC	5.1250	2.495	0.781	0.611	0.790
SDN	5.3958	2.627	0.726	0.531	0.840
Cloud-based detection	5.5625	2.549	0.747	0.566	0.821

Scale Statistics			
Mean	Variance	Std. Deviation	N of Items
8.0417	5.402	2.32432	3

Condition 5

Reliability Statistics		
Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0.872	0.873	3

Item Statistics			
	Mean	**Std. Deviation**	**N**
Data mining	3.2292	0.97281	48
TCU	3.3333	0.99645	48
CVSS	2.7292	1.02604	48

Item-Total Statistics					
	Scale Mean If Item Deleted	**Scale Variance If Item Deleted**	**Corrected Item-Total Correlation**	**Squared Multiple Correlation**	**Cronbach's Alpha If Item Deleted**
Data mining	6.0625	3.422	0.772	0.611	0.804
TCU	5.9583	3.317	0.782	0.622	0.795
CVSS	6.5625	3.400	0.712	0.507	0.859

Scale Statistics			
Mean	**Variance**	**Std. Deviation**	**N of Items**
9.2917	7.147	2.67342	3

Condition 6

Reliability Statistics		
Cronbach's Alpha	**Cronbach's Alpha Based on Standardized Items**	**N of Items**
0.852	0.852	4

Item Statistics			
	Mean	**Std. Deviation**	**N**
Data sanitization	3.0417	0.87418	48
Privacy homomorphism	3.3125	0.80309	48
Neural networks	3.2708	0.73628	48
Dynamic risk assessment	3.4167	0.79448	48

Item-Total Statistics					
	Scale Mean If Item Deleted	**Scale Variance If Item Deleted**	**Corrected Item-Total Correlation**	**Squared Multiple Correlation**	**Cronbach's Alpha If Item Deleted**
Data sanitization	10.0000	3.872	0.730	0.559	0.796
Privacy homomorphism	9.7292	4.202	0.699	0.512	0.808
Neural networks	9.7708	4.521	0.666	0.489	0.823
Dynamic risk assessment	9.6250	4.282	0.679	0.497	0.816

Scale Statistics			
Mean	**Variance**	**Std. Deviation**	**N of Items**
13.0417	7.147	2.67342	4

Condition 7

Reliability Statistics		
Cronbach's Alpha	**Cronbach's Alpha Based on Standardized Items**	**N of Items**
0.854	0.862	3

Item Statistics			
	Mean	**Std. Deviation**	**N**
ITS	3.3750	1.02366	48
Cybersecurity	3.1458	0.79866	48
Reduced attacker intention	3.1250	0.91384	48

Item-Total Statistics					
	Scale Mean If Item Deleted	**Scale Variance If Item Deleted**	**Corrected Item-Total Correlation**	**Squared Multiple Correlation**	**Cronbach's Alpha If Item Deleted**
ITS	6.2708	2.500	0.712	0.530	0.821
Cybersecurity	6.5000	3.021	0.789	0.623	0.754
Reduced attacker intention	6.5208	2.851	0.702	0.518	0.817

Scale Statistics			
Mean	**Variance**	**Std. Deviation**	**N of Items**
9.6458	5.851	2.41881	3

AVE and CR

Condition 1

Λ	λ^2	$1 - \lambda^2$	**CR**	**AVE**
0.878	0.770884	0.229116	0.966424	0.734851
0.792	0.627264	0.372736		
0.898	0.806404	0.193596		

Condition 2

Λ	λ^2	$1 - \lambda^2$	**CR**	**AVE**
0.848	0.719104	0.280896	0.98801	0.645291
0.801	0.641601	0.358399		
0.764	0.583696	0.416304		
0.833	0.693889	0.306111		
0.849	0.720801	0.279199		
0.716	0.512656	0.487344		

Condition 3

Λ	λ^2	$1 - \lambda^2$	CR	AVE
0.781	0.609961	0.390039	0.964828	0.670849
0.897	0.804609	0.195391		
0.796	0.633616	0.366384		
0.797	0.635209	0.364791		

Condition 4

Λ	λ^2	$1 - \lambda^2$	CR	AVE
0.877	0.769129	0.230871	0.965346	0.715194
0.817	0.667489	0.332511		
0.842	0.708964	0.291036		

Condition 5

Λ	λ^2	$1 - \lambda^2$		
0.887	0.786769	0.213231	0.969806	0.761937
0.901	0.811801	0.188199		
0.829	0.687241	0.312759		

Condition 6

Λ	λ^2	$1 - \lambda^2$	CR	AVE
0.808	0.652864	0.347136	0.968294	0.663694
0.854	0.729316	0.270684		
0.764	0.583696	0.416304		
0.83	0.6889	0.3111		

Condition 7

Λ	λ^2	$1 - \lambda^2$	CR	AVE
0.845	0.714025	0.285975	0.958219	0.728897
0.871	0.758641	0.241359		
0.845	0.714025	0.285975		

The reliability and validity analysis, conducted through factor analysis, aimed to ensure the robustness of the measurement instruments used in the study across seven major constructs. Each construct was assessed based on Cronbach's alpha, average variance extracted (AVE), and composite reliability (CR). In Condition 1, the sensor assessment (SEA) construct exhibited high internal consistency reliability, as reflected by a Cronbach's alpha of 0.847, a CR of 0.966424, and an AVE of 0.734851. Similar results were observed in Condition 2 for the vehicle-to-everything network assessment (V2X) construct, with a Cronbach's alpha of 0.909, CR of 0.98801, and AVE of 0.645291. Conditions 3 through 7, representing in-vehicle network assessment (VNA), infrastructure assessment (ISA), data storage assessment (DSA), machine learning assessment (MLA), and cybersecurity (CSO), respectively, all demonstrated strong internal consistency reliability and reliability of measurement, with Cronbach's alpha values ranging from 0.852 to 0.909, CR values ranging from 0.958219 to 0.98801, and AVE values ranging from 0.645291 to 0.761937. These findings collectively affirm the reliability and validity of the measurement instruments, providing a solid foundation for the subsequent analysis and interpretation of the study results.

Table 4. Factor analysis for reliability and validity tests.

Condition and Outcome	Abbreviation	Item Combinations	Description	Factor Analysis

Sensor assessment	SEA	P1 to P3	Sensor security was assured by SE1 to SE3 statements	ICR = 0.847
				CR = 0.966424
				AVE = 0.734851

Vehicle-to-everything network assessment	V2X	P4 to P8	V2X security was assured by VE1 to VE6 statements	ICR = 0.909
				CR = 0.98801
				AVE = 0.645291

In-vehicle network assessment	VNA	P9 to P12	In-vehicle network security was assured by IV1 to IV4 statements	ICR = 0.893
				CR = 0.964828
				AVE = 0.670849

Infrastructure assessment	ISA	P13 to P15	Infrastructure security was assured by IS1 to IS3 statements	ICR = 0.870
				CR = 0.965346
				AVE = 0.715194

Data Storage assessment	DSA	P16 to P18	Data storage and analysis security was assured by DS1 to DS3 statements	ICR = 0.872
				CR = 0.969806
				AVE = 0.761937

Machine learning Assessment	MLA	P19 to P22	Machine learning system security was assured by ML1 to ML4 statements	ICR = 0.852
				CR = 0.968294
				AVE = 0.663694

Cybersecurity	CSO	P23 to P25	Defining better assurance for cybersecurity of CAV	ICR = 0.854
				CR = 0.958219
				AVE = 0.728897

3.3. *fsQCA—Fuzzy Set Qualitative Comparative Analysis*

In the intricate field of CAV cybersecurity, where causality is often intertwined and data exhibit inherent uncertainties, fsQCA emerges as a methodological cornerstone. This approach, grounded in fuzzy logic, proves particularly beneficial in navigating the complex causal relationships among myriad variables influencing the security landscape of connected and automated vehicles [52]. Traditional statistical methods often falter in handling the inherent ambiguity and imprecision present in real-world data, a challenge vividly apparent in the realm of CAV cybersecurity. The utilization of fuzzy logic within the fsQCA methodology serves as a robust solution to this problem. Through a set of membership functions, fsQCA assigns degrees of membership to different categories or values, thereby providing a nuanced and context-aware interpretation of the data. fsQCA's unique strength lies in its ability to unravel complex combinations of factors associated with a specific outcome or phenomenon. This is particularly pertinent in the domain of CAVs, where a multitude of interconnected elements contribute to the overall cybersecurity posture. Even in scenarios characterized by limited or uncertain data, fsQCA stands out by identifying multiple causal pathways or configurations leading to the same outcome. Figure 3 [53] delineates the systematic steps involved in the fsQCA method, offering a visual guide to its application in the context of CAV cybersecurity. The process encompasses defining the scope and parameters of the study, identifying relevant variables, specifying membership functions to handle imprecise data, and systematically analyzing various causal configurations. This methodological transparency ensures the reproducibility of results and enables researchers to delve into the intricacies of CAV cybersecurity with confidence.

In comparing the fsQCA approach with traditional methods like structural equation Modeling (SEM), several advantages emerge. While SEM is widely used for assessing linear relationships among variables, fsQCA excels in analyzing complex, non-linear causal configurations within a limited sample size. SEM relies on assumptions of normality and linearity, which might not fully capture the intricate dynamics of cybersecurity factors in the context of CAVs. The fsQCA methodology, on the other hand, embraces fuzzy logic, accommodating imprecise and ambiguous data. This flexibility is particularly advantageous when dealing with multifaceted phenomena, allowing for a more nuanced exploration of causal pathways. Moreover, fsQCA is adept at identifying equifinality, acknowledging that diverse combinations of factors can lead to the same outcome—a feature crucial in understanding the multifaceted nature of cybersecurity challenges in CAVs. Overall, the application of fsQCA offers a more holistic and context-sensitive perspective, uncovering intricate causal relationships that might be overlooked by more traditional linear methods like SEM.

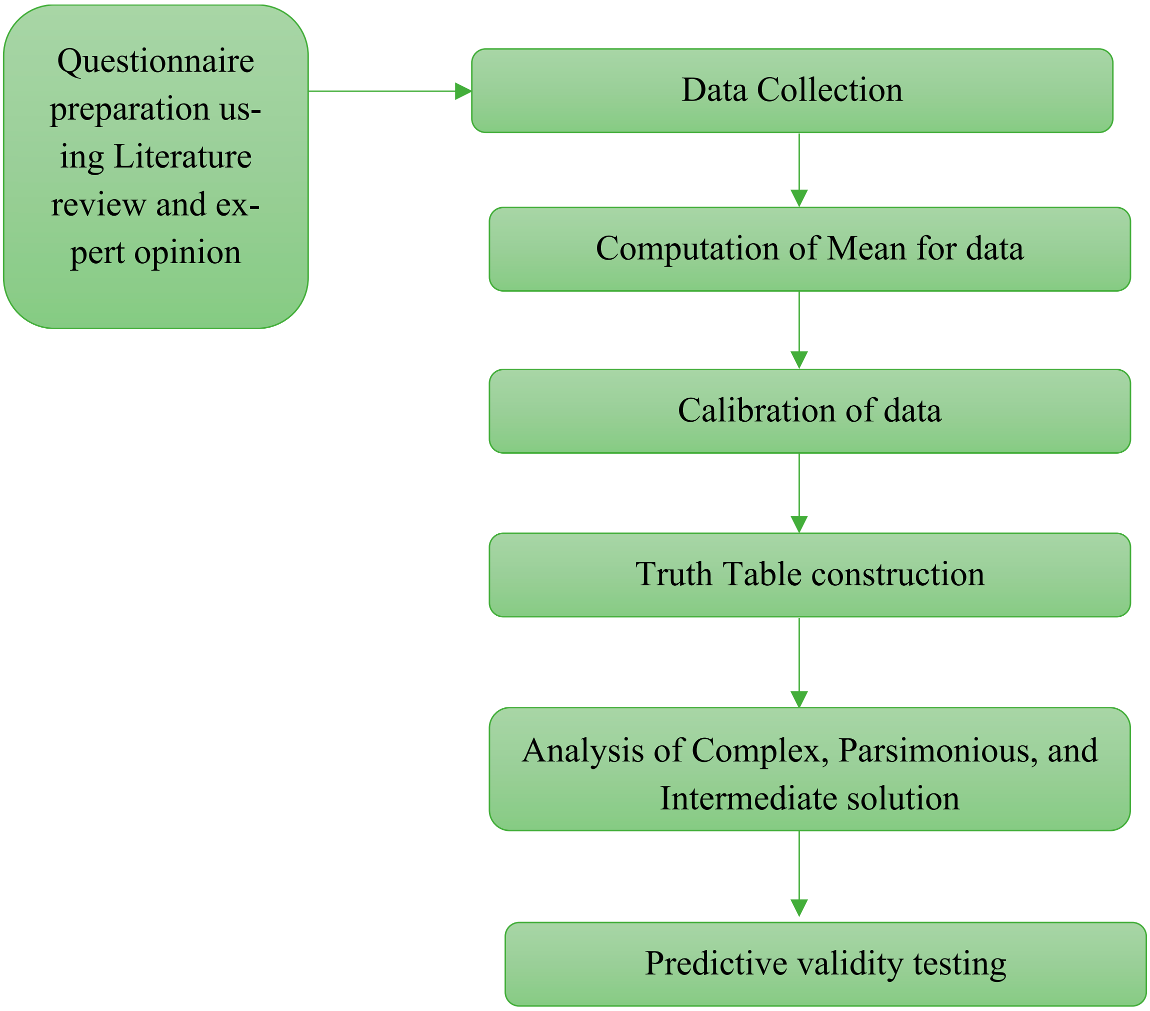

Questionnaire preparation using Literature review and expert opinion
Data Collection
Computation of Mean for data
Calibration of data
Truth Table construction
Analysis of Complex, Parsimonious, and Intermediate solution
Predictive validity testing

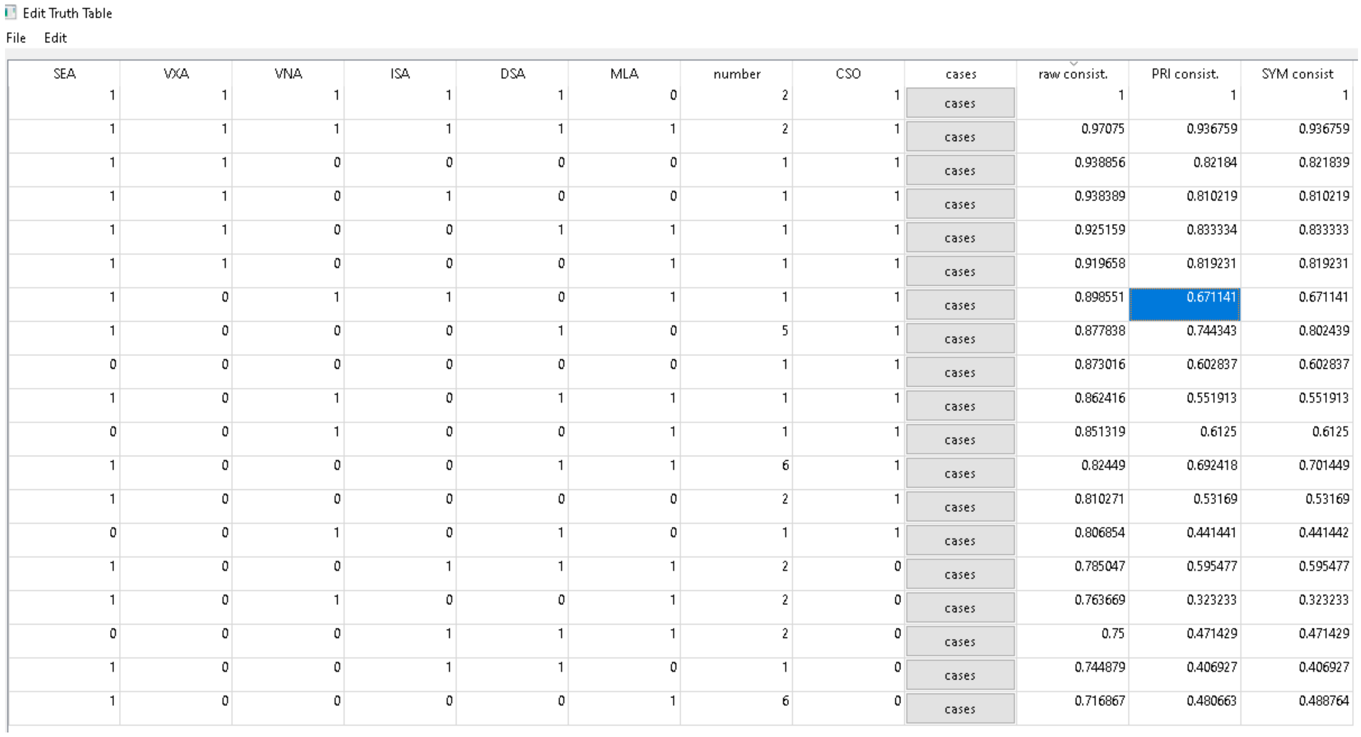
Figure 3. Flowchart of the fsQCA technique.

3.3.1. Calibration of Data

To implement the fsQCA method, the first step is to calibrate the values of the raw data into fuzzy sets, which are then represented in binary values of 0s and 1s. This process involves setting threshold values that indicate full membership, cross-over membership, and non-full membership, which are determined based on the data being analyzed and are typically fixed using percentiles. In this study, we used threshold values of 4 for full membership, 3 for cross-over membership, and 2 for non-full membership. The calibration process can be performed in fsQCA by navigating to the "Analyze" menu, selecting "Compute the variable", giving a name to the target variable, and then calibrating the variable using the command "calibrate (x, n1, n2, n3)", where n1, n2, and n3 represent the threshold values. This step is crucial in ensuring that the data are transformed into a suitable format for analysis, allowing for accurate identification of causal pathways and relationships between variables.

3.3.2. Truth Table Construction

To obtain fuzzy set values, a truth table was constructed shown in Figure 4 with binary values of 0 and 1, using the calibrated data. This step can be performed using the "Truth table algorithm" option under "Analyze". The resulting truth table is represented in binary values of 0 s and 1 s. Once the truth table is obtained, the next step is to derive three types of solutions—complex, parsimonious, and intermediate. This is achieved through the "Analyze" option, followed by editing the code, and setting the code as 1 and 0.8, which eliminates unneeded cases in the truth table. The specific standard analysis is then applied to obtain the three types of solutions. These steps are crucial in the fsQCA method as they help to identify the most influential combinations of inputs that lead to achieving the desired output. The gray cells in the figure signify instances where the specified conditions are replicated, indicating the presence of these conditions across multiple cases.



SEA	VXA	VNA	ISA	DSA	MLA	number	CSO	cases	raw consist.	PRI consist.	SYM consist
1	1	1	1	1	0	2	1	cases	1	1	1
1	1	1	1	1	1	2	1	cases	0.97075	0.936759	0.936759
1	1	0	0	0	0	1	1	cases	0.938856	0.82184	0.821839
1	1	0	1	0	0	1	1	cases	0.938389	0.810219	0.810219
1	1	0	0	1	1	1	1	cases	0.925159	0.833334	0.833333
1	1	0	0	0	1	1	1	cases	0.919658	0.819231	0.819231
1	0	1	1	0	1	1	1	cases	0.898551	0.671141	0.671141
1	0	0	0	1	0	5	1	cases	0.877838	0.744343	0.802439
0	0	0	0	0	0	1	1	cases	0.873016	0.602837	0.602837
1	0	1	0	1	1	1	1	cases	0.862416	0.551913	0.551913
0	0	1	0	0	1	1	1	cases	0.851319	0.6125	0.6125
1	0	0	0	1	1	6	1	cases	0.82449	0.692418	0.701449
1	0	0	0	0	0	2	1	cases	0.810271	0.53169	0.53169
0	0	1	0	1	0	1	1	cases	0.806854	0.441441	0.441442
1	0	0	1	1	1	2	0	cases	0.785047	0.595477	0.595477
1	0	1	0	0	1	2	0	cases	0.763669	0.323233	0.323233
0	0	0	1	1	1	2	0	cases	0.75	0.471429	0.471429
1	0	0	1	1	0	1	0	cases	0.744879	0.406927	0.406927
1	0	0	0	0	1	6	0	cases	0.716867	0.480663	0.488764

Figure 4. Truth table.

3.3.3. Analysis of Solutions

Three solutions (complex, parsimonious, and intermediate) were obtained through specific standard analysis. These solutions were analyzed to identify different combinations of conditions that lead to achieving an outcome. The intermediate and parsimonious solutions were used to derive different conditions. The constructs present in both parsimonious and intermediate solutions were considered core constructs and represented by large circles. The constructs present only in the intermediate solution were considered peripheral constructs and represented by small circles. The findings were classified into necessary and sufficient conditions. The results of the three solutions were tabulated in Table 5, providing different combinations with the presence and absence of constructs to achieve the outcome. This process helps in identifying the most influential factors that lead to the desired outcome.

Table 5. Analysis of necessary conditions.

	Cybersecurity (CSO)		~Cybersecurity (~CSO)	
Conditions Tested	**Consistency**	**Coverage**	**Consistency**	**Coverage**
SEA	0.858655	0.675531	0.853020	0.428687
~SEA	0.273814	0.744661	0.354356	0.615599
VXA	0.461250	0.805496	0.316943	0.397453
~VXA	0.693069	0.613664	0.824639	0.522975
VNA	0.376238	0.757388	0.429717	0.552577
~VNA	0.777740	0.681017	0.811331	0.453812
ISA	0.445886	0.759302	0.470337	0.511628
~ISA	0.713213	0.678247	0.778728	0.473652
DSA	0.669512	0.721487	0.665954	0.458425
~DSA	0.497440	0.699808	0.595404	0.535063
MLA	0.701263	0.678112	0.789418	0.487620
~MLA	0.470127	0.777527	0.478888	0.505959

4. Results from fsQCA

Both the necessary and sufficient conditions were examined to ensure the cybersecurity of CAV. The necessary conditions were analyzed and their results are presented in Table 5. None of the conditions were found to be sufficient to assure cybersecurity of CAV, as all of them had a consistency value lower than 0.9. Therefore, the sufficiency conditions were analyzed. The fuzzy set outcomes are presented in Table 6, which shows two signs. The black circle represents the presence of a condition, while the empty white circle represents the absence of a condition. Additionally, the black and white circles are divided into larger and smaller ones to indicate core and peripheral conditions, respectively. The core conditions are represented by large black and white circles, while the conditions present in the intermediate solution but not in the parsimonious solution are represented by small black and white circles. Table 6 also includes the consistency and coverage values for each solution, the overall consistency, and the coverage extracted from the intermediate solution. Consistency was measured to understand the subset relations, while coverage was used to understand empirical relevance. The overall consistency of our solution was 0.810098, which was greater than the zero-threshold value of 0.75, and the overall coverage value of 0.734039 indicated that the outcome was covered by all ten identified solutions.

To ensure higher cybersecurity of CAV, solutions 2, 3, and 5 were found to be the most effective. Solution 2 combined sensor assessment (SEA) and vehicle-to-everything network assessment (VXA) to achieve higher cybersecurity, while also excluding in-vehicle network assessment (VNA), data storage assessment (DSA), and machine learning system assessment (MLA). Solution 3 combined SEA, VXA, and MLA while excluding VNA and infrastructure assessment (ISA). A combination of all five constructs, SEA, VXA, VNA, ISA, and DSA, was found to provide the greatest security assurance for CAV vehicles. The other solutions represented varying combinations of these constructs, with solution 1 representing the absence of all constructs except for VXA; solution 4 including SEA, DSA, and MLA; solution 6 including VNA and DSA; solution 7 including VNA and MLA, solution 8 including SEA, VNA, and MLA; solution 9 including only SEA; and solution 10 including both SEA and DSA. These findings suggest that more than one configuration is necessary to achieve the desired outcome of higher cybersecurity for CAV vehicles.

Table 6. fsQCA findings.

Combination of Constructs	SEA	VXA	VNA	ISA	DSA	MLS	Raw Coverage	Unique Coverage	Consistency
VXA*~VNA*~ISA*~DSA*~MLA		●	◦	○	○	○	0.224309	0.017412	0.816149
SEA*VXA*~VNA*~DSA*~MLA	•		◦		○	○	0.180608	0.033117	0.904274
SEA*VXA*~VNA*~ISA*MLA	•	●	◦	○		•	0.237282	0.035165	0.929145
SEA*~VXA*~ISA*DSA*MLA	•	◦		○	●	•	0.361215	0.001707	0.796687
SEA*VXA*VNA*ISA*DSA	•	●	●	●	●		0.21987	0.097302	0.975758
~SEA*~VXA*VNA*~ISA*DSA*~MLA	○	◦	●	◦	●	○	0.088426	0	0.806854
~SEA*~VXA*VNA*~ISA*~DSA*MLA	○	◦	●	○	○	•	0.121202	0.015705	0.851319
SEA*~VXA*VNA*ISA*~DSA*MLA	•	◦	●	●	○	•	0.148173	0.0191191	0.898551
SEA*~VXA*~VNA*~ISA*~MLA	•	◦	◦	○		○	0.315466	0	0.829443
SEA*~VXA*~VNA*~ISA*DSA	○	◦	◦	○	●		0.430864	0.00341403	0.833003
Solution coverage: 0.734039							Solution consistency: 0.810098		

Note: The black circle represents the presence of a condition, while the empty white circle represents the absence of a condition. Additionally, the black and white circles are divided into larger and smaller ones to indicate core and peripheral conditions, respectively. The core conditions are represented by large black and white circles, while the conditions present in the intermediate solution but not in the parsimonious solution are represented by small black and white circles.

Practical Case Studies

Practical case studies are included to illustrate its real-world application. These case studies provide tangible examples of how the proposed method can be implemented in diverse scenarios within the automotive industry.

Case Study 1: Implementation in Automotive Manufacturing

In this case study, we applied the methodology to a real-world scenario in an automotive manufacturing setting. By involving key stakeholders such as production engineers, automotive developers, and instrumentation engineers, we were able to assess the cybersecurity of connected and automated vehicles (CAVs) within the manufacturing process. The results demonstrate the method's practical utility in identifying and mitigating potential cybersecurity risks in an industry-specific context.

Case Study 2: Cybersecurity Assessment in Vehicle-to-Everything (V2X) Communication

The second case study focuses on the practical application of the methodology in assessing the cybersecurity of V2X communication in connected vehicles. By collaborating with experts in the field and utilizing the proposed method, we were able to identify the specific security measures needed to ensure the integrity and reliability of V2X communication, thereby enhancing the overall cybersecurity of CAVs.

Case Study 3: Integrating Cybersecurity Measures in Automotive Design

This case study delves into the incorporation of cybersecurity measures during the design phase of connected and automated vehicles. Through collaboration with automobile designers and chief technical officers, we explored the implementation of the proposed method to enhance the cybersecurity features embedded in the vehicle design process. The results highlight the practical implications of our methodology in influencing the overall security posture of CAVs.

5. Discussions

One of the main conclusions drawn from the study is the importance of addressing data storage and in-vehicle network attacks. These two constructs were present as core countermeasures in the majority of the solutions identified, indicating their crucial role in ensuring the cybersecurity of CAVs. In particular, the study highlights the need for secure data storage practices and secure communication protocols within the vehicle's network to prevent attacks that may compromise the confidentiality and integrity of data. These findings are consistent with previous research on CAV cybersecurity, which has emphasized the importance of securing in-vehicle networks and preventing unauthorized access to vehicle data. Another interesting finding of this study is the importance of data storage assessment in ensuring the cybersecurity of CAVs. Solution 10 identifies the presence of data storage assessment alone as sufficient to provide adequate security, without the need for other constructs. This highlights the importance of regular security assessments and testing to identify and mitigate potential vulnerabilities in CAV systems.

Additionally, the study identifies the vehicle-to-everything network (V2X) as another important construct in ensuring CAV cybersecurity. V2X enables vehicles to communicate with other vehicles and the surrounding infrastructure, which has the potential to improve safety and efficiency on the road. However, it also introduces new security risks, which must be addressed through secure communication protocols and authentication mechanisms. The study's findings highlight the need for continued research and development of secure V2X communication technologies to support the widespread adoption of CAVs. Overall, the findings of this study provide a valuable framework for stakeholders in the automotive industry to evaluate and implement effective cybersecurity countermeasures for CAVs. By addressing the most critical constructs identified in the study, including data storage and in-vehicle network security, stakeholders can improve the overall security and safety of CAVs, ensuring their widespread adoption in the future.

6. Research Implications

6.1. Theoretical Implications

This study makes a significant contribution to the literature on connected and automated vehicles (CAV) by presenting conditions and configurations that can achieve the desired outcome of cybersecurity. Previous studies on CAV security were mostly based on previous literature, with only a few empirical studies that collected real data from respondents. The importance of V2X (vehicle-to-everything) network security for CAV cybersecurity was identified in previous collective reviews of cybersecurity attacks [32]. Longitudinal safety of CAV was identified using the Rear End Collision Risk Index (RCRI) method, which resulted in several focal points [54]. Other studies focused on specific cyber-attacks, which had a limitation in analyzing their importance in relation to other attacks [55].

Most previous studies used structural equation modelling (SEM) to identify multiple paths to achieve the outcome, but this approach only focuses on the main effects of variables that lead to the outcome. To address this limitation, we used fuzzy set qualitative comparative analysis (fsQCA), which identifies multiple possible paths to achieve the dependent outcome variable. This research focused on analyzing the countermeasures used to avoid cyber-attacks that could compromise the cybersecurity of CAVs. By leveraging the knowledge of automobile engineers involved in CAV-related activities, we identified the paths to achieve higher cybersecurity by answering the question of which attacks should be removed along with their countermeasures to ensure cybersecurity. The countermeasures included under attack were highly preferred measures identified through reviews and expert opinions. Adopting specific strategies to prevent cyber-attacks will enhance the importance of those attacks in achieving the cybersecurity of CAVs. This paper is one of the first to investigate security attacks by their countermeasures, and it provides a better understanding of the conditions that must be followed to ensure CAV cybersecurity. The results of this study provide a comprehensive framework that can be used to achieve the desired outcome of CAV cybersecurity. By identifying the most critical constructs that must be considered, such as the in-vehicle network and data storage, we provide practical guidance to stakeholders involved in ensuring CAV cybersecurity. We also identified constructs that are not necessary to consider, such as the infrastructure network. Overall, this study makes a significant contribution to the literature on CAV cybersecurity by presenting a comprehensive framework that can be used to achieve the desired outcome of CAV cybersecurity.

6.2. Managerial Implications

The findings of this study can be utilized by CAV designers as well as researchers who seek to reduce cybersecurity attacks. The increased adoption of CAVs can contribute to achieving SDG 9 and 11. The responsibility of establishing the necessary infrastructure for secure and seamless movement of CAVs lies with the government in order to meet SDG 9. Boosting infrastructure can also increase the rate of industrialization. Cybersecurity attacks are a major security threat for designers involved in intelligent transportation systems (ITS) that make CAVs. This study identifies possible conditions to avoid security threats and presents countermeasures to mitigate them. The importance of employing particular strategies to avoid security attacks and ensuring the cybersecurity of CAVs is highlighted. The results revealed that the security checks on in-vehicle networks and data storage are crucial to achieving cybersecurity. CAV designers can focus on these two attacks to resolve security issues. Additionally, the study offers several combinations of the presence and absence of attacks that lead to achieving the desired outcome, providing multiple paths for security checks. Furthermore, the increased adoption of connected and autonomous vehicles (CAVs) can contribute to achieving SDG 9 (Industry, Innovation, and Infrastructure) and SDG 11 (Sustainable Cities and Communities). By identifying the necessary infrastructure for secure and seamless movement of CAVs, this study highlights the responsibility of governments in meeting SDG 9. Governments play a vital role in establishing the infrastructure needed for CAVs, which can enhance transportation efficiency, reduce congestion, and promote sustainable urbanization. In addition to the benefits related to SDG 9, the transition towards CAVs can have a positive impact on SDG 11. CAVs can help countries reduce transportation pollution, lower greenhouse gas emissions, and promote sustainable mobility solutions. By integrating CAVs into urban transportation systems, cities can improve air quality, enhance accessibility, and create more livable and sustainable communities. The adoption of CAVs aligns with the broader agenda of sustainable living practices and offers numerous benefits for individuals and countries globally. Moreover, CAVs can facilitate equitable access to transportation, enhance road safety, and improve the overall quality of life for people in both urban and rural areas.

6.3. Long-Term Impacts and Future Research Directions

Due to the necessity to examine the long-term impacts of implementing the proposed framework on CAV cybersecurity and sustainability goals, future research should focus on this direction. Recognizing the dynamic nature of both technological advancements and emerging cybersecurity threats, future research endeavors will include the sustained effects and implications of the proposed framework over an extended timeframe. This extended analysis will involve continuous monitoring and evaluation of the cybersecurity measures implemented in CAVs, considering evolving threats and technological advancements. We aim to explore the enduring effectiveness of the proposed countermeasures and their contribution to the long-term resilience of CAVs against emerging cybersecurity threats. Additionally, we will assess the framework's impact on broader sustainability goals, particularly its influence on reducing transportation-related pollution, lowering greenhouse gas emissions, and promoting sustainable mobility solutions.

7. Conclusions

The development of connected and automated vehicles (CAV) has opened up a new era in transportation. However, with this technological advancement comes the risk of cyber-attacks, which can pose a threat to the safety and security of passengers and vehicles alike. This study aimed to identify the possible paths for achieving cybersecurity in CAV by analyzing six major security constructs and their countermeasures using the fuzzy set qualitative comparative analysis (fsQCA) technique. The results of this study showed that in-vehicle network security and data storage security checks are the most important measures to consider in ensuring the cybersecurity of CAV. The findings of this study are significant for automobile engineers, policymakers, and researchers who are involved in the development of CAV. By identifying the conditions and configurations required for achieving cybersecurity in CAV, designers can implement measures to prevent potential security threats. Policymakers can also take steps to establish the necessary infrastructure and regulations to ensure the smooth and secure movement of CAV, thus meeting sustainable development goals (SDGs) 9 and 11. However, the study does have some limitations, such as the exclusion of certain countermeasures for eliminating security attacks. Future research can focus on collecting and analyzing additional countermeasures and strategies to address these limitations. While findings may not be broadly generalizable across all industries, they provide valuable insights within the specific context of connected and automated vehicles. Future research with larger sample sizes could further validate and extend our findings to a broader audience.

Author Contributions: Conceptualization, K.K. and B.S.; methodology, K.K.; software, R.P.; validation, K.K., B.S. and S.M.A.; formal analysis, B.S.; investigation, S.M.A.; resources, R.P.; data curation, K.K.; writing—original draft preparation, R.P. and K.K; writing—review and editing, B.S. and S.M.A.; visualization, R.P.; supervision, S.M.A. and B.S.; project administration, B.S. and S.M.A.; funding acquisition, K.K. and B.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data are contained within the article.

Acknowledgments: We would like to thank the anonymous reviewers for their comments that allowed to further enhance the outcome of this research.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A

Table A1. 5-Point Likert scale questionnaire of construct measurements.

Construct	Attack No.	Statements	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
		Input					
Sensor attack assessment (SEA)	P1	Using multiple GPS receivers avoids blocking of satellite signals from GPS.					
	P2	Usage of redundant sensors on camera verification to avoid illusion and binding					
	P3	Jamming avoidance by making protective glasses around a LiDAR which acts as light filters					
Vehicle-to-everything network assessment (VXA)	P4	Usage of fog server with fog anonymizer to avoid eavesdropping in vehicular ad-hoc networks (VANETs)					
	P5	Maintaining data integrity in dynamic route guidance by forged data filtering scheme					
	P6	Using swarm algorithms for routing attacks					
	P7	Detecting bandwidth and entropy to reduce denial of service attack					
	P8	Implementing noisy control signals to avoid replay attacks					
	P9	Registering vehicles with TFD to avoid communication of attackers who are under victim identity					

Table A1. *Cont.*

Construct	Attack No.	Statements	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
		Input					
In-Vehicle network assessment (VNA)	P10	Encryption and cryptographic checksum to avoid close proximity vulnerabilities					
	P11	Doing network segmentation to avoid CAN and SAE vulnerabilities					
	P12	Encryption and authentication to avoid flashing attacks					
	P13	Content filtering for integrated business service attacks					
Infrastructure network assessment (ISA)	P14	Usage of certificateless aggregate signcryption (CL-A-SC) scheme to monitor road surface conditions					
	P15	Incorporating software defined networking (SDN) in IoT environment					
	P16	Using cloud-based detection system for cloud infrastructure					
Data storage assessment (DSA)	P17	Conserving data mining to protect privacy leakage of user information					
	P18	Using telematics control unit (TCU) for remote control of vehicles					
	P19	Adopting CVSS (common vulnerability scoring system) to measure severity of software vulnerabilities					
Machine learning system assessment (MLA)	P20	Performing data sanitization and robust learning to defend against misleading in learning process					
	P21	Ensuring privacy of data by privacy homomorphism					
	P22	Implementing neural networks for privacy assurance					
	P23	Assessing risks earlier using dynamic risk assessment					
		Output					
Cybersecurity of CAV (CSO)	P24	Providing better solutions for security issues in connected and automated vehicles (CAV)					
	P25	Strengthening the cybersecurity patterns					
	P26	Reduces attacker intentions in connected and automated vehicles					

Table A2. Demographic Information of experts.

Demographic Information					
Company Name					
Designation of Respondent in The Company	Chief Technical Officer	Automobile Designer	Production Engineer	Automotive Developer	Instrumentation Engineer
E-mail of the respondent					
Work experience of respondent	Below 3 years	3 to 5 years	5 to 10 years	More than 10 years	

References

1. Guanetti, J.; Kim, Y.; Borrelli, F. Control of Connected and Automated Vehicles: State of the Art and Future Challenges. *Annu. Rev. Control* **2018**, *45*, 18–40. [CrossRef]
2. Elliott, D.; Keen, W.; Miao, L. Recent Advances in Connected and Automated Vehicles. *J. Traffic Transp. Eng. (Engl. Ed.)* **2019**, *6*, 109–131. [CrossRef]
3. Alnasser, A.; Sun, H.; Jiang, J. Cyber Security Challenges and Solutions for V2X Communications: A Survey. *Comput. Netw.* **2019**, *151*, 52–67. [CrossRef]
4. Alwakeel, A.M.; Alnaim, A.K.; Fernandez, E.B. A Survey of Network Function Virtualization Security. In Proceedings of the SoutheastCon 2018, St. Petersburg, FL, USA, 19–22 April 2018; pp. 1–8.
5. Chattopadhyay, A.; Lam, K.-Y.; Tavva, Y. Autonomous Vehicle: Security by Design. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 7015–7029. [CrossRef]
6. Becker, J.C.; Simon, A. Sensor and Navigation Data Fusion for an Autonomous Vehicle. In Proceedings of the IEEE Intelligent Vehicles Symposium 2000 (Cat. No.00TH8511), Dearborn, MI, USA, 5 October 2000; pp. 156–161.
7. Figueiredo, L.; Jesus, I.; Machado, J.A.T.; Ferreira, J.R.; Martins de Carvalho, J.L. Towards the Development of Intelligent Transportation Systems. In Proceedings of the ITSC 2001, 2001 IEEE Intelligent Transportation Systems, Proceedings (Cat. No.01TH8585), Oakland, CA, USA, 25–29 August 2001; pp. 1206–1211.
8. Lee, D.; Hess, D.J. Regulations for On-Road Testing of Connected and Automated Vehicles: Assessing the Potential for Global Safety Harmonization. *Transp. Res. Part A Policy Pract.* **2020**, *136*, 85–98. [CrossRef]
9. Vahidi, A.; Sciarretta, A. Energy Saving Potentials of Connected and Automated Vehicles. *Transp. Res. Part C Emerg. Technol.* **2018**, *95*, 822–843. [CrossRef]
10. Bansal, P.; Kockelman, K.M. Forecasting Americans' Long-Term Adoption of Connected and Autonomous Vehicle Technologies. *Transp. Res. Part A Policy Pract.* **2017**, *95*, 49–63. [CrossRef]
11. Uhlemann, E. Introducing Connected Vehicles [Connected Vehicles]. *IEEE Veh. Technol. Mag.* **2015**, *10*, 23–31. [CrossRef]
12. Bajpai, J.N. Emerging Vehicle Technologies & the Search for Urban Mobility Solutions. *Urban Plan. Transp. Res.* **2016**, *4*, 83–100. [CrossRef]
13. Yang, C.Y.D.; Fisher, D.L. Safety Impacts and Benefits of Connected and Automated Vehicles: How Real Are They? *J. Intell. Transp. Syst.* **2021**, *25*, 135–138. [CrossRef]
14. Khan, S.K.; Shiwakoti, N.; Stasinopoulos, P.; Warren, M. Modelling cybersecurity regulations for automated vehicles. *Accid. Anal. Prev.* **2023**, *186*, 107054. [CrossRef] [PubMed]
15. Rana, M.M.; Hossain, K. Connected and autonomous vehicles and infrastructures: A literature review. *Int. J. Pavement Res. Technol.* **2023**, *16*, 264–284. [CrossRef]
16. Feng, Y.; Chen, Y.; Zhang, J.; Tian, C.; Ren, R.; Han, T.; Proctor, R.W. Human-centred design of next generation transportation infrastructure with connected and automated vehicles: A system-of-systems perspective. *Theor. Issues Ergon. Sci.* **2023**, 1–29. [CrossRef]
17. Vdovic, H.; Babic, J.; Podobnik, V. Automotive Software in Connected and Autonomous Electric Vehicles: A Review. *IEEE Access* **2019**, *7*, 166365–166379. [CrossRef]
18. Basu, R.; Araldo, A.; Akkinepally, A.P.; Nahmias Biran, B.H.; Basak, K.; Seshadri, R.; Deshmukh, N.; Kumar, N.; Azevedo, C.L.; Ben-Akiva, M. Automated Mobility-on-Demand vs. Mass Transit: A Multi-Modal Activity-Driven Agent-Based Simulation Approach. *Transp. Res. Rec. J. Transp. Res. Board* **2018**, *2672*, 608–618. [CrossRef]
19. Deka, D.; Blickstein, S.G.; Brown, C.T.; Rosenthal, S.; Yang, S. The Perception of Autonomous Vehicles' Traffic Safety Impact on People with Disability, Pedestrians, and Bicyclists Report Authors: Acknowledgments. New Jersey Bicycle and Pedestrian Resource Center. 2021. Available online: https://njbikeped.org/wp-content/uploads/2022/09/AV-Safety-Perception-Report.pdf (accessed on 20 December 2023).
20. Arif, M.; Wang, G.; Zakirul Alam Bhuiyan, M.; Wang, T.; Chen, J. A Survey on Security Attacks in VANETs: Communication, Applications and Challenges. *Veh. Commun.* **2019**, *19*, 100179. [CrossRef]
21. Chen, H.; Liu, J.; Wang, J.; Xun, Y. Towards secure intra-vehicle communications in 5G advanced and beyond: Vulnerabilities, attacks and countermeasures. *Veh. Commun.* **2023**, *39*, 100548. [CrossRef]
22. Thantharate, P.; Thantharate, A.; Kulkarni, A. GREENSKY: A Fair Energy-Aware Optimization Model for UAVs in Next-Generation Wireless Networks. *Green Energy Intell. Transp.* **2023**, *3*, 100130. [CrossRef]
23. Khan, J.A.; Wang, L.; Jacobs, E.; Talebian, A.; Mishra, S.; Santo, C.A.; Golias, M.; Astorne-Figari, C. Smart Cities Connected and Autonomous Vehicles Readiness Index. In Proceedings of the 2nd ACM/EIGSCC Symposium on Smart Cities and Communities, Portland, OR, USA, 10–12 September 2019; ACM: New York, NY, USA, 2019; pp. 1–8.
24. Huo, Y.; Tu, W.; Sheng, Z.; Leung, V.C.M. A Survey of In-Vehicle Communications: Requirements, Solutions and Opportunities in IoT. In Proceedings of the 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, Italy, 14–16 December 2015; pp. 132–137.
25. Lin, L. Deep Learning-Based Human-Driven Vehicle Trajectory Prediction and Its Application for Platoon Control of Connected and Autonomous Vehicles. In Proceedings of the Automated Vehicles Symposium 2018, San Francisco, CA, USA, 9–12 July 2018; pp. 1–30.

26. Anwar, A.; Anwar, A.; Moukahal, L.; Zulkernine, M. Security assessment of in-vehicle communication protocols. *Veh. Commun.* **2023**, *44*, 100639. [CrossRef]
27. Muhammad, Z.; Anwar, Z.; Saleem, B.; Shahid, J. Emerging Cybersecurity and Privacy Threats to Electric Vehicles and Their Impact on Human and Environmental Sustainability. *Energies* **2023**, *16*, 1113. [CrossRef]
28. Chen, X.; Xu, B.; Qin, X.; Bian, Y.; Hu, M.; Sun, N. Non-Signalized Intersection Network Management With Connected and Automated Vehicles. *IEEE Access* **2020**, *8*, 122065–122077. [CrossRef]
29. Nagarajan, J.; Mansourian, P.; Shahid, M.A.; Jaekel, A.; Saini, I.; Zhang, N.; Kneppers, M. Machine Learning based intrusion detection systems for connected autonomous vehicles: A survey. *Peer-to-Peer Netw. Appl.* **2023**, *16*, 2153–2185. [CrossRef]
30. Bertino, E.; Ferrari, E. Big data security and privacy. In *A Comprehensive Guide through the Italian Database Research over the Last 25 Years*; Springer International Publishing: Cham, Switzerland, 2017; pp. 425–439.
31. Han, J.; Ju, Z.; Chen, X.; Yang, M.; Zhang, H.; Huai, R. Secure Operations of Connected and Autonomous Vehicles. *IEEE Trans. Intell. Veh.* **2023**, *8*, 4484–4497. [CrossRef]
32. Chowdhury, M.; Islam, M.; Khan, Z. Security of Connected and Automated Vehicles. *Bridge* **2019**, *49*, 46–56.
33. Parkinson, S.; Ward, P.; Wilson, K.; Miller, J. Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 2898–2915. [CrossRef]
34. Alsobeh, A.; Shatnawi, A. Integrating Data-Driven Security, Model Checking, and Self-adaptation for IoT Systems Using BIP Components: A Conceptual Proposal Model. In Proceedings of the 2023 International Conference on Advances in Computing Research, Orlando, FL, USA, 8–10 May 2023; Springer Nature Switzerland: Cham, Switzerland, 2023; pp. 533–549.
35. Takefuji, Y. Connected Vehicle Security Vulnerabilities [Commentary]. *IEEE Technol. Soc. Mag.* **2018**, *37*, 15–18. [CrossRef]
36. Monteuuis, J.-P.; Petit, J.; Zhang, J.; Labiod, H.; Mafrica, S.; Servel, A. Attacker Model for Connected and Automated Vehicles. In Proceedings of the ACM Computer Science in Car Symposium, Munich, Germany, 13–14 September 2018.
37. Sun, X.; Yu, F.R.; Zhang, P. A Survey on Cyber-Security of Connected and Autonomous Vehicles (CAVs). *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 6240–6259. [CrossRef]
38. Kumar, S.; Mann, K.S. Detection of Multiple Malicious Nodes Using Entropy for Mitigating the Effect of Denial of Service Attack in VANETs. In Proceedings of the 2018 4th International Conference on Computing Sciences (ICCS), Jalandhar, India, 30–31 August 2018; pp. 72–79.
39. Merco, R.; Biron, Z.A.; Pisu, P. Replay Attack Detection in a Platoon of Connected Vehicles with Cooperative Adaptive Cruise Control. In Proceedings of the 2018 Annual American Control Conference (ACC), Milwaukee, WI, USA, 27–29 June 2018; pp. 5582–5587.
40. Appathurai, A.; Manogaran, G.; Chilamkurti, N. Trusted FPGA-based Transport Traffic Inject, Impersonate (I2) Attacks Beaconing in the Internet of Vehicles. *IET Netw.* **2019**, *8*, 169–178. [CrossRef]
41. Kang, T.U.; Song, H.M.; Jeong, S.; Kim, H.K. Automated Reverse Engineering and Attack for CAN Using OBD-II. In Proceedings of the 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall), Chicago, IL, USA, 27–30 August 2018; pp. 1–7.
42. Alam, F.; Mehmood, R.; Katib, I.; Altowaijri, S.M.; Albeshri, A. TAAWUN: A Decision Fusion and Feature Specific Road Detection Approach for Connected Autonomous Vehicles. *Mob. Netw. Appl.* **2023**, *28*, 636–652. [CrossRef]
43. Chen, Y.; Lu, Z.; Xiong, H.; Xu, W. Privacy-Preserving Data Aggregation Protocol for Fog Computing-Assisted Vehicle-to-Infrastructure Scenario. *Secur. Commun. Netw.* **2018**, *2018*, 1378583. [CrossRef]
44. Kim, Y.; Nam, J.; Park, T.; Scott-Hayward, S.; Shin, S. SODA: A Software-Defined Security Framework for IoT Environments. *Comput. Netw.* **2019**, *163*, 106889. [CrossRef]
45. Turesson, H.K.; Kim, H.; Laskowski, M.; Roatis, A. Privacy Preserving Data Mining as Proof of Useful Work. In *Research Anthology on Convergence of Blockchain, Internet of Things, and Security*; IGI Global: Hershey, PA, USA, 2022; pp. 402–420.
46. Foster, I.; Prudhomme, A.; Koscher, K.; Savage, S. Fast and Vulnerable: A Story of Telematic Failures. In Proceedings of the 9th USENIX Workshop Offensive Technologies, WOOT 2015, Washington, DC, USA, 10–11 August 2015.
47. Sheehan, B.; Murphy, F.; Mullins, M.; Ryan, C. Connected and Autonomous Vehicles: A Cyber-Risk Classification Framework. *Transp. Res. Part A Policy Pract.* **2019**, *124*, 523–536. [CrossRef]
48. Chan, P.P.K.; He, Z.-M.; Li, H.; Hsu, C.-C. Data Sanitization against Adversarial Label Contamination Based on Data Complexity. *Int. J. Mach. Learn. Cybern.* **2018**, *9*, 1039–1052. [CrossRef]
49. Liu, X.; Zhang, X.; Yu, J.; Fu, C. Query Privacy Preserving for Data Aggregation in Wireless Sensor Networks. *Wirel. Commun. Mob. Comput.* **2020**, *2020*, 9754973. [CrossRef]
50. Dong, C.; Wang, H.; Ni, D.; Liu, Y.; Chen, Q. Impact Evaluation of Cyber-Attacks on Traffic Flow of Connected and Automated Vehicles. *IEEE Access* **2020**, *8*, 86824–86835. [CrossRef]
51. Le, A.; Maple, C.; Watson, T. A Profile-Driven Dynamic Risk Assessment Framework for Connected and Autonomous Vehicles. In Proceedings of the Living in the Internet of Things: Cybersecurity of the IoT—2018, London, UK, 28–29 March 2018.
52. Gligor, D.; Bozkurt, S. FsQCA versus Regression: The Context of Customer Engagement. *J. Retail. Consum. Serv.* **2020**, *52*, 101929. [CrossRef]
53. Kraus, S.; Ribeiro-Soriano, D.; Schüssler, M. Fuzzy-Set Qualitative Comparative Analysis (FsQCA) in Entrepreneurship and Innovation Research—The Rise of a Method. *Int. Entrep. Manag. J.* **2018**, *14*, 15–33. [CrossRef]

54. Li, Y.; Tu, Y.; Fan, Q.; Dong, C.; Wang, W. Influence of Cyber-Attacks on Longitudinal Safety of Connected and Automated Vehicles. *Accid. Anal. Prev.* **2018**, *121*, 148–156. [CrossRef]
55. Zhao, C.; Gill, J.S.; Pisu, P.; Comert, G. Detection of False Data Injection Attack in Connected and Automated Vehicles via Cloud-Based Sandboxing. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 9078–9088. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.