American Journal of Computer Science and Technology
2024, Vol. 7, No. 4, pp. 122-138
https://doi.org/10.11648/j.ajcst.20240704.11

Research Article

Perception and Trust in Autonomous Vehicles Post Cyber Security Incidents

Adam Gorine* , **Sana Abid Khan**

School of Computing and Creative Technology, University of the West of England, Bristol, United Kingdom

Abstract

The integration of Autonomous Vehicles (AVs) into modern systems of transportation brings with it a new and transformative era. Central to the successful realisation of this transformation is the public's trust in these vehicles and their safety, particularly in the aftermath of cyber security breaches. The following research therefore explores the various factors underpinning this trust in the context of cyber security incidents. A dual-methodological approach was used in the study. Quantitative data was gathered from structured questionnaires distributed to and completed by a cohort of 151 participants and qualitative data, from comprehensive semi-structured interviews with AV technology and cyber security experts. Rigorous Structural Equation Modelling of the quantitative data then allowed for the identification of the key factors influencing public trust from the standpoint of the research participants including the perceived safety of AV technology, the severity of cyber security incidents, the historic cyber security track record of companies and the frequency of successful cyber security breaches. The role of government regulations, though also influential, emerged as less so. The qualitative data, processed via thematic analysis, resonated with the findings from the quantitative data. This highlighted the importance of perceived safety, incident severity, regulatory frameworks and corporate legacy in shaping public trust. Whilst cyber incidents no doubt erode trust in AVs, a combination of technological perception, regulatory scaffolding and corporate history critically impacts this. These insights are instrumental for stakeholders, from policymakers to AV manufacturers, in charting the course of AV assimilation successfully in future.

Keywords

Autonomous Vehicles, Cyber Attacks, Public Trust, Perceived Safety, Regulatory Frameworks

1. Introduction

Autonomous vehicles (AVs), once a concept confined to science fiction, is becoming a tangible reality, promising to redefine transportation by addressing challenges like reducing road accidents and optimising traffic flows. However, integrating AVs into our daily lives presents challenges beyond technological readiness. The increasing complexity of AV systems introduces potential vulnerabilities, especially in cybersecurity. Recent incidents have shown that cybersecurity breaches can have dire consequences, ranging from data theft to potential physical harm, profoundly eroding public Trust in this emerging technology.

It is imperative to understand the determinants of this Trust, especially in the post-cyber breach scenario. The increasing sophistication of cyber threats, coupled with the potentially catastrophic consequences of a successful attack on AV systems, underscores the urgency of this issue. Without a deep

*Corresponding author: adam.gorine@uwe.ac.uk (Adam Gorine)

Received: 9 August 2024; **Accepted:** 2 September 2024; **Published:** 18 October 2024

understanding of how cybersecurity incidents influence public Trust in AVs, stakeholders might face substantial barriers to accepting and adopting these technologies.

This research embarks on a journey to explore these determinants, aiming to offer insights that can guide policymakers, manufacturers, and other stakeholders in reinforcing the trustworthiness of AVs. By intertwining the potential of AVs with the challenges they face, especially concerning cybersecurity, this introduction sets the stage for a comprehensive exploration of public trust dynamics. The study utilises a mixed-methods approach, combining quantitative surveys with qualitative semi-structured interviews. However, it is worth noting that the rapidly evolving nature of AV and cybersecurity technology may render some findings less relevant over time.

2. Background on AV

2.1. AVs Technologies

The advent of autonomous vehicles (AVs) represents a substantial transformation in transportation technology, potentially reshaping the urban landscape and the very nature of personal mobility [2]. As these self-driving machines integrate advanced technologies like Artificial Intelligence (AI), machine learning, the Internet of Things (IoT), and big data analytics, they gain the capacity to understand and react to dynamic environments, navigate traffic, and make complex decisions autonomously [3].

The benefits of AVs are substantial. They promise increased efficiency in transportation, reduced traffic congestion, and minimised human-induced accidents, given that human error is a significant factor in many road accidents. Furthermore, AVs offer enhanced comfort and convenience, potentially providing mobility solutions for those unable to drive, such as the elderly or disabled.

Autonomous vehicles (AVs), often called self-driving or driverless cars, represent a significant advancement in transportation technology. These cars are capable of sensing their surroundings and operating without human intervention. Unlike traditional cars, autonomous vehicles do not require a human driver to take control or even be present. Studies show they can navigate any route and perform tasks an experienced human driver does [4].

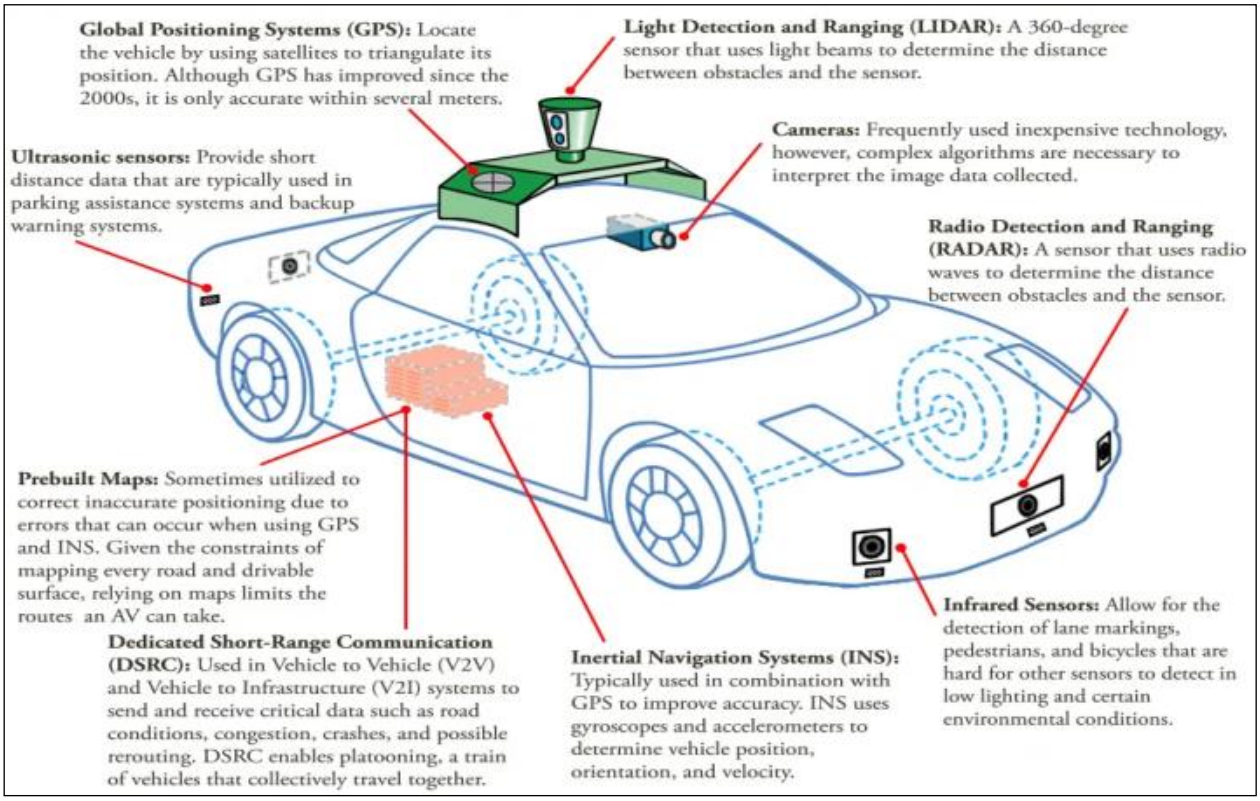

Figure 1. *The Technologies deployed in Autonomous Vehicles [5].*

AVs are designed to operate using an integrated system of sensors, cameras, radars, artificial intelligence (AI), and machine learning algorithms. These vehicles can perceive their environment, light detection and ranging (LIDAR), lane control, object or Collision Avoidance System (CAS), recognise objects, interpret sensory information, and execute navigational decisions, making them a pivotal element in the concept of smart cities [5] as shown in figure 1.

The level of autonomy in these vehicles can vary, as categorised by the Society of Automotive Engineers (SAE), into six levels, from Level 0 (no automation) to Level 5 (full automation), as depicted in Figure 2 as stated in the article [9]. As of this writing, most commercially available AVs are at Level 2 or 3, offering partial automation with some level of human intervention required. However, numerous companies are testing Level 4 and Level 5 vehicles, which can perform all driving tasks under certain (Level 4) or all (Level 5) conditions, with no human input [7].

The promise of Avs lies in their potential to revolutionise the transportation landscape. Reducing human error, which accounts for a significant percentage of road accidents, hopes to enhance road safety. They can also increase fuel efficiency, alleviate traffic congestion, and offer unprecedented mobility options for individuals unable to drive. However, AVs' widespread deployment and societal acceptance are contingent on various factors, including their performance, affordability, legal and regulatory issues, and public Trust [8]. This latter aspect, especially in the context of cyber security incidents, forms the focus of this research.

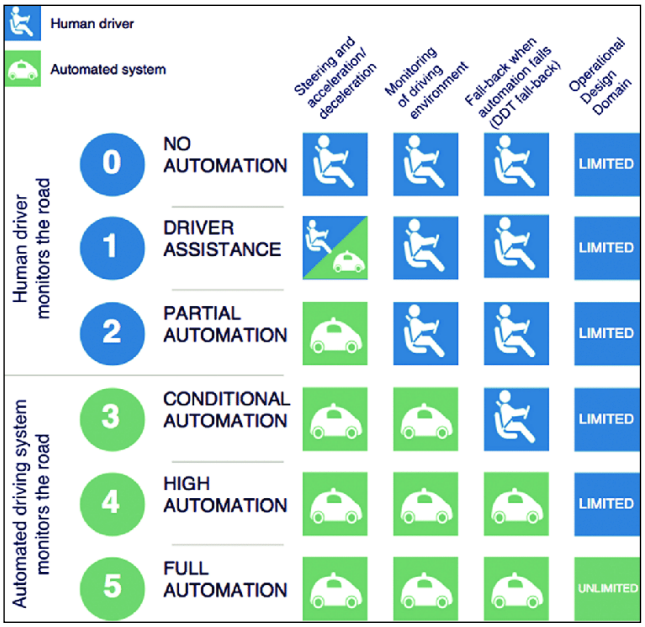

Figure 2. *SAE J3016 Levels of Driving Automation [9].*

2.2. AVs Cyber Security

However, as with any complex technology, deploying AVs introduces many challenges and concerns. Cyber security is a particularly crucial issue, given the heavy reliance of AVs on software, sensors, and connectivity for their operation, as explained in references [10]. The integration of connected technology implies a susceptibility to cyber threats, potentially resulting in severe consequences. These threats range from data breaches and privacy invasions to more severe implications like remote vehicle control or infrastructure manipulation, posing significant risks to personal Safety and broader public security.

Cybersecurity incidents involving autonomous vehicles (AVs) sometimes highlight these threats' seriousness and legitimacy. One notable incident occurred in 2015 when a vulnerability in the FCA Uconnect system exposed Fiat Chrysler vehicles to hackers, resulting in a recall of over 1 million cars, as mentioned in [10]. It is worth noting that this incident involved an internet-connected vehicle rather than an autonomous one.

In January 2022, David Colombo, a 19-year-old hacker who aims to educate the public about hacking possibilities instead of deceiving them, investigated third-party applications used by Tesla. He could access and control 25 Tesla's cars across 13 countries.

While Colombo could not physically drive or perform manoeuvres with them, he unlocked the cars and turned off their safety features. He even managed to play a Rick Astley song from YouTube through the car's audio systems. Additionally, he could start the engines, open windows, and adjust lighting settings – actions that could pose risks and distractions for drivers [11]. Colombo's ability to communicate instructions to the vehicles was rooted in a third-party application called Tesla Mate, which many Tesla owners use. This application controls vehicle operations through Tesla's API. After Colombo made this information public, Tesla Mate released an update to prevent access.

In 2019, the Tesla Model 3, the model at that time, experienced a security breach within minutes. Ethical hackers named Amat Cama and Richard Zhu exploited a vulnerability in the 'infotainment' system to access one of the vehicle's computing systems and execute their programming sequences [12].

In 2011, the Chevy Malibu was the first remote intrusion that attackers could gain control of. The hackers "manipulated the vehicle's radio using a Bluetooth stack weakness and inserted the malware codes by syncing their mobile phones with the radio". Once successfully inserted, the code sends messages to the car's ECU and locks the brakes [12].

These episodes bring the robustness of existing security measures under scrutiny, challenging their ability to protect AV systems against increasingly sophisticated and evolving cyber threats.

2.3. Trust and Public Perception of AVs

Public Trust is pivotal in accepting and adopting emerging technologies, such as AVs, that significantly influence personal Safety and lifestyle. Trust influences individual attitudes toward technology and can shape policy decisions and market dynamics [13].

For AVs, public Trust is influenced by various factors, including perceived Safety, reliability, the entity behind the technology (private company or government), Perceived usefulness, Perceived defects, perceived intelligence, perceived risk of privacy safety, negative emotions, the effec-

tiveness of regulatory oversight, and the frequency and severity of harmful incidents, such as accidents or cyber security breaches [14]. Cybersecurity incidents have been found to impact perception, which can potentially erode Trust in autonomous vehicles (AVs) and hinder their rate of adoption as stated in references [13].

3. Related Work

3.1. Trust in Autonomous Technology

The advent and expansion of autonomous technology, especially autonomous vehicles, has underscored the importance of Trust as a prerequisite for their broad acceptance and adoption. Trust in technology is a multifaceted concept influenced by several factors, and it represents a pivotal challenge for autonomous systems, particularly in situations where they substitute human decision-making [15].

Trust, as defined by the researchers [16] is "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party". In the realm of technology, one crucial aspect is the willingness of users to relinquish control and rely on the system to function correctly and safely.

The authors in the research paper [17] proposed a trust model for automation that heavily focuses on performance. According to this model, initial Trust is influenced by impressions, while the consistency of the system performance determines long-term Trust. As users witness system performance, their Trust tends to increase. It decreases in response to system failures.

Several factors can influence the level of Trust in technologies. The reliability and performance of the system are among the factors that shape userTrust [17]. This refers to how consistently technology can carry out its functions.

Perceived Safety and security also play a role in determining Trust. This encompasses Safety, privacy, and cyber security [18]. Any concerns regarding these areas can diminish Trust in autonomous technology.

The level of transparency and understandability of the system's functioning can also shape users' Trust. Users who understand how the technology works and make decisions are more likely to trust it [19].

Personal experience and familiarity with the technology is another influential factor. Users who have had positive experiences with autonomous technology are likely to trust it morethan those who have had negative experiences or no experience at all [20].

Social influence and societal acceptance can also impact individual trust levels in autonomous technology [21]. If technology is widely accepted and positively viewed by the public, individuals may be more inclined to trust it.

In the context of autonomous vehicles, authors in reference [24] found Trust to be the most dominant factor in adopting AVs—similarly, personalisation parameters. Perceived intelligence, Anthropomorphism, Likability perceived usefulness, perceived defects, perceived risks of traffic safety, perceived risk of privacy safety, negative emotions performance expectations, reliability, privacy and security (from hackers) are among the major factors that impact public Trust on Avs according to researchers [14].

However, recent research also shows that the level of Trust in AVs or AI-based cars increases and decreases with the nature and operations of the vehicle. Trust will be higher in partially automated technology, where human input and skills are also required to make a decision, than infully automated technology. It means that the level of trust changes with automation [22].

Reviewing these factors underlines Trust's complex and dynamic nature in autonomous technology. Trust is also worth noting that it is not always beneficial – excessive Trust can lead to over-reliance, while insufficient Trust can lead to under-utilisation of the technology. Therefore, achieving an appropriate level of Trust is key.

3.2. The Impact of Cyber Security Incidents on Public Trust

In recent years, the escalating cyber security threats have significantly influenced public Trust in many technologies, including autonomous vehicles. High-profile cyber security incidents, such as data breaches, cyberattacks, and the exposure of system vulnerabilities, not only affect the targeted organisations but can also erode the public Trust in the related technologies, according to the research paper [23].

In the context of AVs, cyber security incidents can have a particularly profound impact due to the tangible, immediate safety risks involved. A study conducted by researchers [24] revealed that cybersecurity incidents can lead to a significant decrease in public Trust in autonomous technology. Such incidents amplify public fears about the potential misuse of AVs or unauthorised access to theirdata, leading to a significant decline in their willingness to use such technology [25].

The role of regulations in preventing cyber security incidents is also a critical factor affecting public Trust. The amplification of these incidents through media outlets can contribute to lessening fear and increasingTrust, even if the actual probability of such incidents occurring is relatively high.

On the other hand, companies' responses to cybersecurity incidents significantly influence public trust recovery. Research by a reputable cyber security company, Varonis, found that transparent, prompt, and responsible handling of cyber security incidents can mitigate the loss of Trust to a certain extent [26]. This includes timely disclosure, taking responsibility, ensuring affected individuals are not unduly disadvantaged, and implementing measures to prevent similar incidents.

Furthermore, an individual's understanding of technology

can moderate the impact of cybersecurity incidents on Trust. For those with a low knowledge of technology, a single cybersecurity incident can significantly decrease Trust. In contrast, highly understanding individuals are likely to maintain their trust level unless they perceive a pattern of consistent security failures [27].

In the end, cyber security incidents can harm public Trust in autonomous technology, especially when the media amplifies these incidents or companies respond poorly. The extent to which these incidents are perceived as severe and frequent, how companies handle them, and individuals' comprehension of the technology all play a role in determining the impact on Trust. However, apart from these factors, some elements affect public Trust in autonomous vehicles (AVs) following cyber security incidents, which we will discuss in the next section.

3.3. Factors that Impact Public Trust on AVs Post Cyber Security Incident

Autonomous vehicles (AVs) are an emerging technology that has the potential to transform transportation completely. However, there are concerns regarding the cybersecurity risks associated with AVs. If an AV gets hacked, it could be exploited to cause harm to individuals or damage property. As a result, there is a growing worry about Trust in AVs [28].

Although literature discusses the factors influencing Trust in AVs after cybersecurity incidents, empirical studies on this domain are lacking [24]. Numerous studies, news articles, and reports have indicated that government regulations, the severity and frequency of cybersecurity incidents, the past track record of companies involved, and the perceived safety level of AV technology all contribute to shaping Trust in these vehicles.

For instance, according to research by the Pew Research Center, over 87% of Americans believe that government regulations should be implemented to ensure AV safety and that stringent testing adhering to standards should be conducted compared to vehicles [29]. Another study highlighted that many Americans expressed concerns about hacking risks associated with AVs [2].

Regulation and government supervision play a role in establishing confidence in autonomous vehicles (AVs). Research conducted by [28] highlights the significance of regulatory frameworks that govern safety standards, data protection measures and ethical considerations related to AVs. These studies demonstrate that defined policies can instilTrust in the public by showcasing governmental oversight, influencing their confidence level.

In another study [10] found that the severity of cybersecurity incidents can significantly impact public Trust in AVs. Reports also found that people were more likely to trust AVs if they believed the technology was secure.

The severity and the frequency of such incidents determine the impact of cyber security incidents on public Trust. Authors [24] highlight that more severe incidents leading to significant data breaches, substantial economic loss, or even loss of life tend to result in more profound reductions in public Trust. On the other hand, the researchers in [27] mentioned that frequent cyberattacks, regardless of their impact, could lead to a gradual erosion of Trust due to the perceived constant vulnerability of AVs.

For the severity and frequency of cyber incidents, it is common sense that the more severe and frequent they are, the less Trust there will be. People will be less likely to trust AVs if they believe that successful cyber security incidents involving AVs are frequent and severe.

The company's previous recordof manufacturing or operating an AV can also impact public Trust. Fromnewspapers and different internet sources [9], it can be deduced that if a company has a good history in tackling cyber security incidents and is reputable in securing user data and AVs, the public will have more Trust in them.

Finally, the perceived Safety of the technology can also impact public Trust in AVs. Several studies found that people were more likely to trust AVs if they believed the technology was safe [8]. The work of [3] underscores that if AVs are deemed safer than conventional vehicles, this perception can boost Trust. Conversely, concerns over system failures, the inability of AVs to handle unexpected situations, or fears about potential hacking could significantly diminish the perceived Safety of this technology, leading to lower levels of Trust.

This study maintains that public Trust in autonomous vehicles' cyber security is influenced by five key factors: government regulations, the severity and frequency of cyber security incidents, the company's past performance in addressing such incidents, and the perceived Safety of the technology. To explore this relationship, the study will undertake empirical analysis.

We set some hypotheses to assess the factors mentioned above:

1) H1: Government regulation for AVs significantly impacts public Trust in AVs after cyber security incidents.
2) H2: The severity of cyber security incidents related to AVs significantly impacts public Trust in AVs post-cyber security incidents.
3) H3: The frequency of (successful) cyber security incidents related to AVs significantly impacts public Trust in AVs after cyber security incidents.
4) H4: The Company's past track record in addressingcyber security incidents related to AVs has a notable impacton public Trust in AVs after cyber security incidents.
5) H5: Perceived Safety of AV technology significantly impacts public Trust in AVs after cyber security incidents.

3.4. Contribution

Although a significant amount of literature explores various aspects of public Trust in autonomous vehicles (AVs), there is a clear gap in understanding how cybersecurity incidents impact Trust. Most existing literature addresses public Trust in AVs independently of the cybersecurity dimension, treating

it more as literature reports than dedicated research.

The literature review reveals several crucial factors that shape public Trust: regulation and oversight, the severity and frequency of cyber security incidents, the company's track record, and perceived Safety. However, these factors have been typically discussed independently, with little consideration of their collective influence on public Trust in the context of AVs post-cyber security incidents. Also, there is no empirical evidence for these studies in the context of cyber security.

This research aims to fill this gap by comprehensively examining these factors in the context of cyber security incidents involving AVs. It seeks to contribute new empirical evidence on these critical determinants of public Trust, thus enriching academic and practical understanding of how Trust in AVs can be maintained and enhanced amidst growing cyber security threats. This research intends to bridge the existing divide, providing a unified perspective on the influence of cyber security incidents on public Trust in AVs.

4. Methodology

The research philosophy adopted for this study is positivism. Positivism operates under the belief that only observable and measurable phenomena can provide credible knowledge, prioritising objective analysis over subjective opinions [30]. Considering the study's empirical approach, which aims to acquire measurable data regarding public Trust in autonomous vehicles (AVs) following cybersecurity incidents, positivism emerges as a suitable and appropriate choice.

The research methodology progresses through the following stages:

4.1. Research Design

The research employs a mixed-methods design, integrating both quantitative and qualitative methodologies. This approach enables a comprehensive exploration of the research question, where quantitative methods provide statistical evidence, and qualitative methods delve into nuanced insights [31].

4.1.1. Population and Sampling Method

The target population for this research comprises adults familiar with AV technology, spanning both the UK and the US. A stratified random sampling approach is employed, ensuring representation across various demographics. The sample size for the quantitative study was 151 respondents, while the qualitative research was based on interviews with eight individuals. The demographics of the respondents and interviewees are given in Table 1.

4.1.2. Data Collection Methods

Quantitative Data: We administered an online survey of 151 respondents. The survey incorporates structured questions, utilisingLikert scale measurements to gauge perceptions about the factors impacting Trust in AVs post-security incidents.

Qualitative Data: We conducted Semi-structured interviews with eight knowledgeable individuals from the UK and US. These interviews delve deeper into the subject's nuances, capturing intricate details that quantitative data might miss [32].

4.2. Data Analysis

Quantitative Data Analysis:Initially, we subjected the collected data to screening for issues such as missing values, duplications, and outliers. Subsequently, it undergoes tests for normality, multicollinearity, scale validity, and reliability. Structural Equation Modelling (SEM) uses AMOS, while descriptive statistics and inferential analyses are executed using SPSS.

Qualitative Data Analysis: The qualitative data is subjected to thematic analysis, adhering to the authors' methodology in [1]. We perform initial coding on the interview transcripts and develop and interpret themes.

Table 1. *Demographic Summary of the Respondents/Sample.*

Variable		Participants	
		Number	Percentage
Gender	Male	105	69.54%
	Female	46	30.46%
Age (years)	18-30	36	23.84%
	31-40	73	48.34%
	41-50	28	18.54%
	50 and above	14	9.27%
Education	IT/Computing	39	25.83%
	Management	24	15.89%
	Business/Finance	31	20.53%
	Engineering	41	27.15%
	Others	16	10.60%
Country	UK	86	56.95%
	US	65	43.05%
Understand Cybersecurity in AV	Yes	97	64.24%
	No	54	35.76%

5. Quantitative Data Analysis

Exploring public Trust in autonomous vehicles, particularly post-cybersecurity incidents, is primarily exploratory due to

limited empirical research at the intersection of technology and human psychology. This forms the essence of our study, merging quantitative data with qualitative insights to thoroughly understand the research area. Before analysing data, we verify its accuracy, handle missing values, and check for normality.

5.1. Data Accuracy, Missing Data, and Normality

Skewness and kurtosis provide quantitative measures to describe the deviation of a dataset from a normal distribution. We checked the univariate normality through skewness and kurtosis. The acceptable limits of skewness and kurtosis are between -2.58 and +2.58, as stated in the paper [33]. Table 2 shows that the skewness and kurtosis are within the limit; hence, the normality is correct.

Table 2. *Skewness and Kurtosis Summary.*

Variable	Skewness	Kurtosis
Government Regulations (GR)	-0.523	0.437
Severity of Cyber Security Incidents (SCI)	-0.308	0.948
Frequency of (Successful) Cyber security Incidents (FCI)	-0.103	1.368
History of the Company (HC.)	-0.281	0.401
Perceived Safety of Technology (PST)	0.144	0.891
Trust (TR.)	-0.039	1.126

5.2. Multicollinearity

The highly correlated variables create a multicollinearity issue, leading to a high regression coefficient standard error. Multicollinearity can also lead to model instability [33]. We assess multicollinearity through tolerance and Variable Inflation Factor (VIF). The acceptable tolerance value is more than 0.1, and the VIF value is less than tenas stated in the article [33]. Tolerance and VIF values were calculated for this study in SPSS and depicted in Table 3, which shows that all the tolerance values are more than 0.1 and VIF values are below 10; hence, we conclude that there is no issue of multicollinearity in research data.

Table 3. *Tolerance and VIF Summary.*

Variable	Tolerance	VIF
Government Regulations (GR)	0.668	1.498
Severity of Cyber Security Incidents (SCI)	0.737	1.356
Frequency of (Successful) Cyber security Incidents (FCI)	0.744	1.344
History of the Company (HC.)	0.797	1.254
Perceived Safety of Technology (PST)	0.713	1.403

5.3. Demographic Analysis

The valid data includes responses from 151 respondents. Table 4 below summarises the respondents' demographic profiles. It shows that 69.54% of males and 30.46% of Females participated in the survey. 48.34% of the respondents were between 31 and 40 years old. Respondents had different educational backgrounds, of which 27.15% had engineering backgrounds, whereas 25.83 had IT/Computer or information security-related education. 56.24% of the people living in the UK and 43.05% were in the US; similarly, 64.24% of the respondents had knowledge of cyber security in autonomous cars, whereas 35.76% had no knowledge of cyber security in AV.

Table 4. *Demographic Summary of the Respondents/Sample.*

Variable	Participants	
Gender	**Number**	**Percentage**
Male	105	69.54%
Female	46	30.46%
Age (years)		
18-30	36	23.84%
31-40	73	48.34%
41-50	28	18.54%
50+	14	9.27%
Education		
ICT/Computing	39	25.83%
Management	24	15.89%
Finance/Business	31	20.53%
Engineering	41	27.15%
Others	16	10.60%
Country		
UK	86	56.95%
US	65	43.05%
Understand Cybersecurity in AV		
YES	97	64.24%
NO	54	35.76%

5.4. Measurement Scales Analysis

To ensure the quality of research findings and assess the impact of constructs on the research, the assessment of measurement scale is critical. Scale reliability and validityare crucial in confirming the research's quality, consistency, and accuracy.

5.4.1. Scale Reliability

Scale reliability is checked through internal consistency and inter-item correlations. The internal consistency is measured through Cronbach's alpha, which assesses the homogeneity and quality of items. According to the author [33], Cronbach's alpha greater than 0.70 indicates good internal consistency, whereas Cronbach's alpha below 0.70 indicates inconsistent items and needs improvement. Table 5 shows that Cronbach's values for all constructs are above 0.70 between 0.833 and 0.894, confirming high-scale reliability in the data.

The inter-item correlation shows the reliability among items. According to [20], a high positive correlation indicates high reliability, whereas a low correlation between items depicts poor reliability. According to the author, the minimum acceptable correlation is 0.30 [33]. The inter-item correlation was calculated in SPSS and found between 0.52 and 0.70 for all items. Consequently, we confirm a high level of reliability among the items in this study.

Table 5. *Cronbach's Alpha (Reliability) of constructs.*

Variable	Item	Cronbach's Alpha	Comment
Government Regulations (GR)	4.00	0.849	High Reliability
Severity of Cyber Security Incidents (SCI)	3.00	0.833	High Reliability
Frequency of (Successful) Cyber security Incidents (FCI)	3.00	0.867	High Reliability
History of the Company (HC.)	3.00	0.840	High Reliability
Perceived Safety of Technology (PST)	4.00	0.849	High Reliability
Trust (TR)	3.00	0.874	High Reliability

5.4.2. Scale Validity

Scale validity ensures that the scale accurately measures the intended constructs or assesses how effectively it does so.

The researchers in the article [28] have proposed to apply confirmatory factor analysis (CFA) for discriminant and convergent validity to measure the validity of latent constructs. Confirmatory factor analysis (CFA) tests the constructs' measurement and their consistency with latent in the theoretical model [33]. CFA measures the correlation between variables or factors and constructs; thus, CFA assesses the goodness of fit of the hypothesised model and model constructed based on data collected during the research [34]. The CFA assessment is conducted through convergent and discernment validity.

5.4.3. Convergent Validity

Convergent validity is verified by factor loading, average variance extracted (AVE), and composite reliability (CR). The acceptable value of factor loading is 0.30, but 0.70 or more is considered high. Poor factor loading adversely affects the goodness of model fit. Constructs in this study had a high factor loading, having more than 0.70 on their associated theoretical constructs. According to the research paper [34], the acceptable limit of AVE value is greater than or equal to 0.50, whereas the acceptable value for CR is 0.70 or above.

Table 6 shows the convergent validity illustrating all AVE values exceeding 0.50 acceptable range and the composite eligibility values are more than 0.70. Thus, factor loading, AVE, and CR support the convergent validity of the proposed research model.

Table 6. *Average Variance Extracted and Composite Reliability.*

Construct	Average Variance Extracted	Composite Reliability
Government Regulations (GR)	0.682	0.896
Severity of Cyber Security Incidents (SCI)	0.632	0.837
Frequency of (Successful) Cyber security Incidents (FCI)	0.684	0.866
History of the Company (HC.)	0.641	0.843
Perceived Safety of Technology (PST)	0.586	0.850
Trust (TR)	0.695	0.872

5.4.4. Discriminant Validity

The discriminant validity assessment is crucial in Confirmatory Factor Analysis (CFA). It evaluates the internal correlations among items within a latent construct and their correlations with other measures in the model, as outlined in reference [20]. Discriminant validity is determined by comparing inter-item correlations with the square root of AVE. Specifically, the square root of the AVE for eachconstruct should exceed its correlations with otherconstructs. Table 7 confirms that AVE values surpass correlation values. The diagonal values, representing square roots, further validate that these values exceed correlation values and AVE for each construct. Another indication of discriminant validity is comparing the maximum shared square variance (MSV) with the AVE. MSV assesses the extent to which factors share common variance, and a high MSV indicates a heightened level of multicollinearity. Table 7 shows AVE and MSV results, illustrating that square roots are more than AVE and MSV; hence, discriminant validity is ensured.

Table 7. Discriminant Validity - Comparison of AVE and MSV.

Construct	CR	AVE	MSV	GR	HC	PST	FCI	SCI	TR
GR	0.900	0.680	0.449	0.826					
HC	0.840	0.640	0.358	0.328	0.801				
PST	0.850	0.590	0.439	0.422	0.449	0.766			
FCI	0.870	0.680	0.369	0.527	0.334	0.372	0.827		
SCI	0.840	0.630	0.444	0.498	0.347	0.483	0.337	0.795	
TR	0.870	0.700	0.449	0.670	0.599	0.663	0.607	0.666	0.830

Note: GR = Government Regulations, SCI = Severity of Cyber Security Incidents, FCI = Frequency of (Successful) Cyber security Incidents (FCI), HC = History of the Company, PST = Perceived Safety of Technology, TR = Trust

5.5. Research Model Assessment

The structure equation modelling (SEM) was conducted using Analysis of Moment Structures (AMOS) based on research data after satisfactory scale validity and reliability tests. SEM analyses the research model, direct paths, and hypotheses on constructs in the research model. According to the paper [33], SEM is a two-step approach; one is CFA (consists of measurement model), and the other is structural model (path analysis) analysis. The second step is defining the relationship between endogenous and exogenous constructs through structural modelling.

5.5.1. Measurement Model

In the measurement model, the relationship of the factors is assessed with related constructs. For instance, the relationship between GR1, GR2, GR3, and GR4 is assessed with G.R. The measurement model is verified based onscale validity, internalconsistency, and model fit. There are several indices of goodness of fit in AMOS. There are three broad categories of model fit in literature: incremental fit, absolute fit, and parsimonious fit [6]. The following criteria in Table 8 have been defined for model acceptance on the suggested literature [35].

Table 8. Criteria for model goodness of fit.

Category Name	Index	Full Name	Acceptable Level	Acceptable Range of Good Fit
Absolute Fit	RMSEA	Root Mean Square of Error Approximation	< 0.08	< 0.05
	GFI	Goodness of Fit Index	>0.90	>0.94
Incremental Fit	CFI	Comparative Fit Index	>0.90	>0.94
	TLI	Tucker-Lewis Index	>0.90	>0.94
	IFI	Incremental-Fit Index	>0.90	>0.94
Parsimonious Fit	ChiSa/DF	Chi-Square/Degree of Freedom	< 5.0	< 5.0

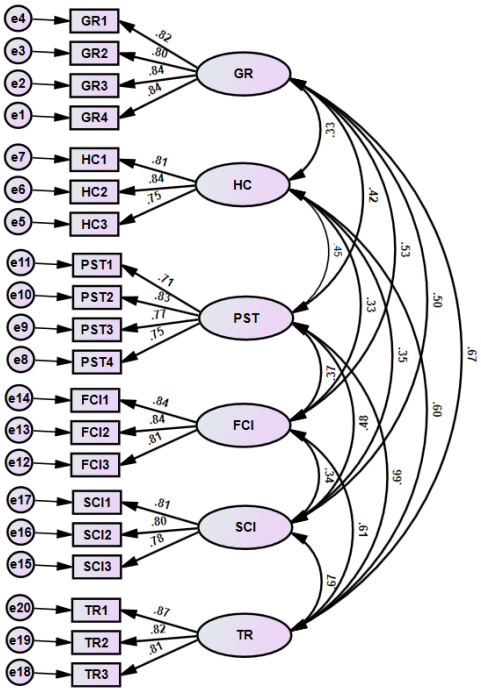

Figure 3. *Measurement Model with path coefficients.*

The model fit result of the measurement model isChiSq=209.434, D =155.0, ChiSq /DF=1.35, CFI=0.968, SRMR=0.050, RMSEA=0.048, PClose=0.550.

The following measurement model in Figure 3 depicts the results of each latent variable (constructs) shown in oval shapes. The two-headed arrows between the constructs specify the covariances of the two constructs linked with them. The paths with single-headed arrows connect factors with constructs depicting hypothesised measures.

This result meets the suggested criteria of model goodness of fit. Moreover, all the factors have successfully loaded with sufficient estimates from 0.75 to 0.87. The correlation coefficients between the constructs are below 0.85, i.e., between 0.33 and 0.67, which satisfy the criteria recommended by [9].

5.5.2. Structural Model Assessment

The structure model was developed to examine the hypotheses of this research. In this stage, correlations between constructs are assessed. The structural model in Figure 4 was drawn in AMOS by creating a relationship through a single arrow line showing direct paths from exogenous variables such as Government Regulations (GR), Severity of Cyber Security Incidents (SCI), Frequency of (Successful) Cyber security Incidents (FCI), History of the Company (HC), Perceived Safety of Technology (PST) and to endogenous variable Trust (TR). These paths show the hypotheses. The hypothesis is deemed acceptable when its coefficient is significant when p<0.05, according to the authors in the research paper [33]. The p-values of standardised path coefficients (beta) for the exogenous construct and endogenous constructs of the research model were examined to assess the correlation strength.

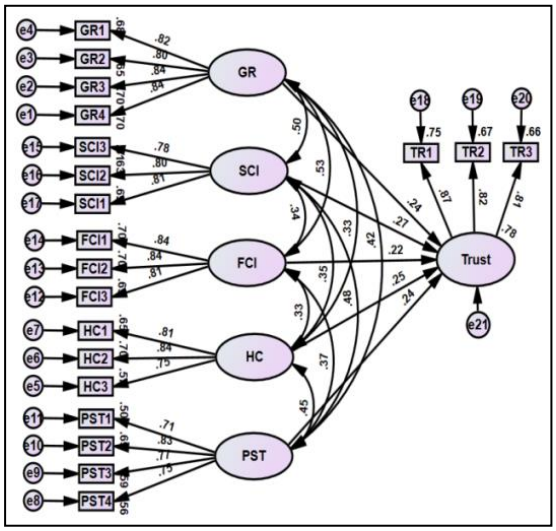

Figure4. *Structural model.*

The structure model was assessed for the goodness of fit based on criteria defined for model fit as follows:The model fit result was found as Chi-Square (X2) = 209.434, df = 155.0, Chi-Square (X2)/df = 1.351, CFI = 0.968, SRMR = 0.050, RMSEA = 0.048, pClose=0.550 show that the model is fit and meets all the cut-off criteria of model fit.

Furthermore, the standardised path coefficients of the construct were analysed, and the result indicates that the coefficients of all the hypotheses are significant, having p-value<0.05; thus, all the hypotheses are supported, as shown in Table 9. The perceived Safety of technology (PST) has the highest positive impact on the Trust (TR), having a coefficient value β = 0.296 and a p-value of 0.002. Thus, it supports the hypothesis H5. The Severity of Cyber Security Incidents (SCI) (β = 0.273, p=0.001) and the previous history of the company (HC) (β = 0.273, p<0.001) have the same impact on the Trust (TR), thus supporting hypotheses H2 and H4. The Frequency of (Successful) Cyber security Incidents (FCI) (β = 0.244, p=0.003) also hada significant impact on the public Trust. If fewer incidents are treated well, it increases Trust; hence, hypothesis H3 is supported based on a significant coefficient and p-value <0.005. Government regulation (GR) (β = 0.191, p=0.002) has the lowest impact on the Trust of autonomous vehicles with a coefficient. Thus, H1 is supported. The overall result supports the research model, and all constructs explain a 78% variance of Trust in the research model with R^2=0.78.

Table 9. Summary of Result of Structure Model.

Hypotheses	Strcuture Path			Estimate			Results
				SRW	CR (t-value)	P-value	
H1	TR	←	GR	0.191	3.025	0.002	Hypothesis
H2	TR	←	SCI	0.273	3.236	0.001	Hypothesis
H3	TR	←	FCI	0.244	2.93	0.003	Hypothesis
H4	TR	←	HC	0.273	3.47	< 0.001	Hypothesis
H5	TR	←	PST	0.296	3.07	0.002	Hypothesis

Figure 4 illustrates the structural model of research with standardised path coefficients from endogenous constructs to exogenous constructs (i.e. Trust).

5.6. Summary

The above chapter presents a quantitative analysis of the research data. The raw data was collected through questionnaires from respondents. The data underwent a screening process, which was checked for missing values, outliers, normality, and scale validity, and finally, 151 recordswere selected for analysis of the model. All the factors achieved the scale reliability and validity tests. Thus, data was found reliable and satisfactory for the model analysis and further research assessment.

Furthermore, structure equation modelling (SEM) was applied to the data in AMOS to assess the model's goodness of fit. The result revealed that the model satisfactorily achieved the level of good fit. All the hypotheses have significant coefficient values with p-values<0.05; thus, all hypotheses were supported. The model satisfies all the criteria of model goodness fit.

6. Qualitative Analyais

We examined the gathered data in the preceding section (V) and derived comprehensive quantitative results. This section aims to corroborate and enhance the validity of these findings through the implementation of semi-structured interviews, followed by qualitative analysis.

6.1. Data and Content Analysis

Thematic analysis allowed a deep exploration into the perception of public Trust in AVs post cyber security incidents. By rigorously following the authors' steps [1], as shown in Figure 5, this study ensures the validity and reliability of the TA process and its findings.

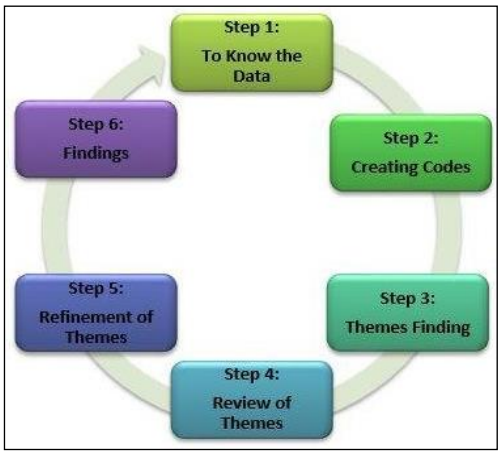

Figure 5. Six-Step Thematic Analysis Approach [1].

6.2. Analysis of the Interview Content

The analysis of the interviews begins by examining the demographics of eight interviewees. This demographic overview provides an essential context for understanding their experiences and perceptions, such as their relationship to autonomous technology and cyber security, age, and education level. The interviewees were from the UK and US and possessed cybersecurity and autonomous technology knowledge.

We asked the interviewees the following open-ended questions:

Q1: What do you believe influences people's Trust in the reliability and security of autonomous vehicles?

Q2: How do you think the actions or track record of the companies producing autonomous vehicles play into public perception and Trust?

Q3: Regarding AVs, how do you perceive the role of regulations or governmental oversight in shaping public confidence?

Q4: How does the frequency and handling of security breaches or incidents related to AVs shape your opinion or trust in them?

Q5: What are your views on the safety measures embedded within autonomous technology?

6.3. Findings

The analysis process involved systematically organising the initial codes presented in Table 10 into broader categories, eventually leading to the emergence of key themes. The process followed the authors' methodology [1], allowing for a layered and in-depth data exploration. The following themes emerged:

Table 10. *Identifying the initial codes.*

Interview Line/Except	Initial Code
A regulatory framework sanctioned by the government acts as a backbone for public Trust.	RegulatoryFramework Importance
History matters a lot. Think of it as a reference check.	Company History Significance
Major breaches, even if rare, stick in public memory and erode Trust	Impact of Major Breaches
If incidents are few and far between and are promptly addressed, it bodes well for Trust.	Incident Frequency & Response Time
A well-defined, stringent, yet fair regulatory environment is an assurance for many.	Assurance from Regulation
Not all cybersecurity issues are the same. A minor glitch is one thing; a car getting hijacked is another.	Varying Severities and Impact on Trust
Major incidents can be game-changers in terms of public perception	High Impact of Severe Incidents
A company's past becomes its testament.	Historical Testament
Repeated breaches can erode Trust, but a company's response can moderate the rate of erosion.	Impact & Response to Repeated Breaches
The foundational tech safety reassures people that, at its core, the system is designed to be safe and secure.	Foundational Tech Safety Importance

6.3.1. Major Themes

Extracting major themes involved the amalgamation of theinitial codes (Table 10) into overarching themes, as shownin Table 11.

1) Severity and Its Implications:

This theme incorporated codes associated with the interviewees' adverse perceptions due to cyber security incidents and AV context. The codes such as 'impact of major breaches', 'varying severities and impact on trust', and 'high impact of severe incidents' were particularly prominent, revealing the harsh reality of the relationship betweenthe severity of cyber breaches and its impact on public Trust.

2) Regulatory Backbone and Assurance:

Codes revolving around regulatory backbone and assurance, including *'regulatory framework importance' and 'assurance from regulation*', were grouped under this theme. These codes brought forward the interviewees' perceptions of how government oversight on the Safety and security of AVs transformed public Trust in AVs, leading to a greater awareness of and acceptance of AVs.

3) Company's Historical Impact:

Codes related to the company's historical impact was gathered into this theme. The inclusion of *'company history significance' and 'historical testament' indicated a high relationship between public trust perception and the company's history of tackling cyber incidents and incorporating* security features.

4) Incident Management & Trust:

This theme incorporated codes highlighting issues about managing security incidents. The *'incident frequency & response time' and 'impact & response to repeated breaches' codes* shed light on the public's perception and the companies' response to cyber incidents on their respective vehicles.

5) Safety Imperative:

The last theme revolved around the safety features and the overall safety perception of AV technology that impacts public Trust. Codes such as *'safety feature emphasis' and 'foundational tech safety importance'*were integral to this theme.

Table 11. Generated Themes from the Interviews.

Codes	Themes
Impact of major breaches, varying severities and impact on Trust, high impact of severe incidents	Severity and Its Implications
Regulatory framework importance, assurance from regulation	Regulatory Backbone and Assurance
Company history significance, historical testament	Company's Historical Impact
Incident frequency & response time, impact & response to repeated breaches	Incident Management & Trust
Safety feature emphasis, foundational tech safety importance	Safety Imperative

6.3.2. Defining and Naming the Extracted Themes

To ensure clarity, each theme was defined and named to represent its essence accurately:

1) Severity and Its Implications:

Emphasises how the gravity of a cyber security incident in AVs shapes public Trust, indicating that the public does not view all breaches equally. Severe incidents can notably alter public perception and are long-remembered.

2) Regulatory Backbone and Assurance:

Reflects the significance and comfort the public derives from structured regulations and governmental oversight.

3) Company's Historical Impact:

Emphasises the weight of acompany's history and its direct influence on public Trust.

4) Incident Management & Trust:

Highlights the Correlationbetween the frequency of incidents, their management, and the subsequent Trust or mistrust from the public.

5) Safety Imperative:

It stresses the foundational and emphasisesthe importance of Safety in AV tech in garnering Trust.

By identifying these themes, the study provides a nuanced understanding of the perceptions of public Trust on AVs and autonomous technology post cyber security incidents, offering valuable insights that can inform future research, interventions, and policies.

A detailed discussion of the qualitative and quantitative findings has been presented in the following sections.

7. Synthesis of Quantitative and Qualitative Findings

7.1. Key Findings

In this meticulous journey to comprehend the landscape of public Trust concerning autonomous vehicles (AVs) after cyber security incidents, we reached several profound conclusions.

1) Government Regulation and Oversight:

The weight of governmental regulations in shaping public Trust cannot be overstated. Both quantitative and qualitative datasets highlight the paramount importance of regulations in the realm of Avs.

2) Severity of Cyber Security Incidents:

Interestingly, the depth and implications of a cyber breach hold more significant sway in determining public Trust than mere superficial analyses would suggest. Major breaches resonated for extended periods, reflecting public wariness and diminished Trust.

3) Frequency of (Successful) Cyber security Incidents:

Beyond severity, the recurring narrative of breaches erodes confidence and Trust. Consistency in safety records seems to be a linchpin for fostering Trust in AVs.

4) Company's Historical Performance:

A Company's legacy, encapsulating its past decisions, actions, and responsiveness to cyber threats, emerged as a pillar of public Trust. Past mistakes or triumphs shape current perceptions significantly.

5) Perceived Safety of AV Technology:

The bedrock of Public Trust is seemingly AV technology's perceived operational and cyber security safety.

7.2. Discussion of Findings

Following the thorough quantitative and qualitative analysis, this section delves into a deep discussion of the findings, juxtaposing the outcomes of both methodologies to underline the results' cohesiveness and integrity.

7.2.1. Government Regulation and Oversight on AVs

The quantitative results indicated a significant influence of government regulation on public Trust with a coefficient value of $\beta = 0.191$, supporting hypothesis 1. This insight was further substantiated in the qualitative thematic analysis, which underscored the "regulatory assurance" theme. Interviewees frequently referenced the comforting role of government oversight, emphasising how effective and transparent regulatory frameworks can bolster public Trust in AVs, especially following cyber security incidents. The mutual validation of quantitative and qualitative findings accentuates the criticality of robust government policies and their role in

fostering Trust. These results are in line with the arguments stated by the authors in [24] and Wang et al. (2023), who state that role of regulations in preventing cybersecurity incidents is critical in affecting public Trust.

7.2.2. Severity of Cyber Security Incidents

Hypothesis 2, suggesting a significant influence of the severity of cyber security incidents on Trust, was endorsed by a coefficient value of $\beta = 0.273$ in the quantitative data. This was mirrored in the "severity and its implications" theme from the qualitative interviews. Respondents were particularly vocal about how the gravity of a cyber security incident in AVs shaped public Trust. Minor glitches were distinguished from significant breaches, with the latter having lasting impacts on public perception. The congruence of both findings implies the indelible mark severe cyber security breaches leave on public Trust, which was also augmented by He, Meng, and Qu (2020) and [2], who found that the severity of cybersecurity incidents can have a significant impact on public Trust in AVs.

7.2.3. Frequency of (Successful) Cyber Security Incidents

Quantitatively, the frequency of successful cyber security incidents substantially impacted public Trust, confirmed by $\beta = 0.244$, validating Hypothesis 3. This aligns harmoniously with the qualitative theme "consistency in cyber security", where interviewees implied that fewer incidents, when managed efficiently, can bolster public Trust. Consistency and predictability in ensuring AV cyber security are thus pivotal in fostering and maintaining public Trust. The results are similar to the arguments of researchers [24], who highlighted that the more frequent and severe the incidents are – those leading to significant data breaches, substantial economic loss, or even loss of life – the more they tend to result in more profound reductions in public Trust. The high frequency of security incidents leads to a gradual erosion of Trust due to the perceived constant vulnerability of Avs.

7.2.4. Previous Record/ History of the Company Producing the AV

A company's track record in managing cyber security incidents emerged as a significant factor in the quantitative analysis, presenting a coefficient value of $\beta = 0.273$, thereby supporting Hypothesis 4. Qualitatively, the theme "legacy of trustworthiness" resonated with this result. Respondents recurrently referred to the reliability of a company based on past performance, accentuating that a history devoid of significant breaches or, conversely, a history showcasing proficient management of breaches was instrumental in gaining their Trust. This cross-validation establishes the quintessential role of corporate history in shaping public Trust, and the outcomes are aligned with the reports of [9, 36], which deduced that if a company has a good history in tackling cyber security incidents and is reputable in securing the user data and the AVs, the public will have more Trust on them.

7.2.5. Perceived Safety of the AV Technology

Hypothesis 5, proposing the significant impact of the perceived Safety of AV technology on Trust, was strongly supported by the quantitative data, reflecting a coefficient value of $\beta = 0.296$. This was intricately aligned with the qualitative theme of "safety first". Interviewees often conveyed their Trust as contingent on their perception of the technology's Safety. Safety, both in terms of physical operation and cyber security, emerged as a non-negotiable cornerstone for Trust in AVs. The findings also align with the literature, such as [8] and Ma et al. (2020), who believed that public Trust enhances the public belief that technology is safe and secure. The authors in reference [1] also underscore that if AVs are deemed safer than conventional vehicles, this perception can boost Trust. The author in reference [10] reports that people are more likely to trust AVs if they believe the technology is secure.

In synthesising both quantitative and qualitative findings, it is apparent that Trust in AVs post cyber security incidents is multifaceted. The mutual validation of results across both quantitative and qualitative methodologies offers compelling evidence supporting the identified factors influencing public Trust in AVs, especially in the aftermath of cyber security incidents. As underscored by the analyses, the interplay of these factors provides invaluable insights into the intricate fabric of public Trust in the rapidly evolving realm of autonomous vehicles.

8. Conclusion

With its myriad promises and challenges, the dawn of the autonomous vehicle (AV) era has been a compelling backdrop against which this research journey unfolded. This paper sheds light on the intricate web of factors determining public Trust in AVs, especially in the aftermath of cybersecurity incidents. Our exploration underscored the importance of AV technology's perceived Safety in influencing Trust. The public highly values the technological reliability and resilience of these vehicles. Concurrently, the severity of cybersecurity incidents and the historical record of the company manufacturing the AV were found to be vital components shaping Trust. These two facets underline the dual significance of the magnitude of cybersecurity breaches and the manufacturers' proactive and retrospective responses to them.

Furthermore, the frequency of successful cybersecurity breaches emerged as another influential dimension. The research found that reduced incidents, when paired with adept management and containment, could amplify the public Trust in the technology. Finally, the role of government regulations, though comparatively subtle, cannot be sidestepped. While its influence might not be as profound as the abovementioned factors, government regulation provides a foundational AV operations and security framework, acting as a silent sentinel overseeing the AV landscape. A

mosaic of technological safety perceptions, the gravity and regularity of cybersecurity mishaps, corporate historical performance, and the overarching arm of regulations amalgamate to shape public Trust in AVs, particularly following cybersecurity disturbances.

The findings from this study lay down a foundational understanding of public Trust in AVs. Yet, continual exploration becomes imperative with the evolving technological landscape and shifting societal perceptions. Potential avenues for future research might encompass studying perceptions from diverse global regions, especially emerging economies. Assessing Trust in tandem with these evolutions will prove insightful as AV technology progresses. A detailed exploration into how different regulatory paradigms across nations impact trust could guide policy framings.

Abbreviations

AI	Artificial Intelligence
AMOS	Analysis of Moment Structures
AV	Autonomous Vehicles
AVE	Average Variance Extracted
CAS	Collision Avoidance System
CFA	Confirmatory Factor Analysis
CR	Composite Reliability
FCI	Frequency of (Successful) Cyber Security Incidents
GR	Government Regulations
HC	History of the Company
IoT	Internet of Things
LIDAR	Light Detection and Ranging
MSV	Maximum Shared Square Variance
PST	Perceived Safety of Technology
SAE	Society of Automotive Engineers
SCI	Severity of Cyber Security Incidents
SEM	Structure Equation Modelling
TR	Trust
VIF	Variable Inflation Factor

Author's Statement

Research Involving Humans and /or Animals

We engage individuals to participate in questionnaires exploring Perception and Trust in Autonomous Vehicles following Cyber Security Incidents. There are no ethical concerns, as the survey adheres strictly to GDPR on data privacy. All surveys are conducted using Qualtrics, ensuring robust privacy safeguards.

Informed Consent

We confirm that all participants in this study provided informed consent before participating. They were fully informed about the purpose of the study, the procedures involved, any potential risks or benefits, and their rights as participants. Additionally, they were assured of confidentiality and their right to withdraw from the study at any time without penalty.

Author Contributions

Adam Gorine: Conceptualization, Resources, Supervision, Writing review and editing, Project Administration, Validation

Sana Abid Khan: Data Curation, Methodology, Formal analysis, Visualization, Software, Investigation, Writing original draft

Data Availability Statement

The online survey is done using Qualtrics:https://www.qualtrics.com/academic-solutions/uwe-bristol/

The data is held on UWE OneDrive Server: https://uweacuk-my.sharepoint.com/:f:/r/personal/adam_gorine_uwe_ac_uk/Documents/SNComputerScience?csf=1&web=1&e=kondCb.

Conflicts of Interest

The authors declare no conflicts of nterest.

References

[1] Braun, V. and Clarke, V. (2006). Using Thematic Analysis in Psychology. *Qualitative Research in Psychology*, 3(2), pp.77–101. https://doi.org/10.1191/1478088706qp063oa

[2] Nastjuk, I., Herrenkind, B., Marrone, M., Brendel, A. B. and Kolbe, L. M. (2020). What drives the acceptance of autonomous Driving? An investigation of acceptance factors from an end-user's perspective. *Technological Forecasting and Social Change*, 161, p. 120319. https://doi.org/10.1016/j.techfore.2020.120319

[3] Biswas, A. and Wang, H. C (2023). Autonomous Vehicles Enabled by the Integration of IoT, Edge Intelligence, 5G, and Blockchain, Sensor, 23(4), p. 1963. https://doi.org/10.3390/s23041963

[4] Synopsys (2019). *What is an autonomous car? How are self-driving cars?* Available at: https://www.synopsys.com/automotive/what-is-autonomous-car.html

[5] Tempo Automation (2019). *Features of Today's BestAutonomous Cars*. Tempo. Available at: https://www.tempoautomation.com/blog/features-of-todays-best-autonomous-cars/

[6] Broeck, J. V. den, Cunningham, S. A., Eeckels, R. and Herbst, K. (2005). Data Cleaning: Detecting, Diagnosing, and Editing Data Abnormalities. *PLoS Medicine*, [online] 2(10), p. e267. https://doi.org/10.1371/journal.pmed.0020267

[7] Serban, A. et al. (2020). A Standard Driven SoftwareArchitecture for Fully Autonomous Vehicles. Journal ofAutomotive Software Engineering Vol. 00(0), Feb 2020, pp. 1-14. Available at: https://doi.org/10.2991/jase.d.200212.001

[8] Taeihagh, A. and Lim, H. S. M. (2018). Governing Autonomous vehicles: Emerging Responses for Safety, liability, privacy, cybersecurity, and Industry Risks. *Transport Reviews*, 39(1), pp. 103–128.

[9] SAE International (2021). *SAE Levels of DrivingAutomation™ Refined for Clarity and International Audience*. Available at: https://www.sae.org/blog/sae-j3016-update

[10] Giordani, J. (2021). Cyberattacks On Vehicles Pose A Threat To Drivers And Manufacturers. Available at: https://www.forbes.com/sites/forbestechcouncil/2021/12/10/cyberattacks-on-vehicles-pose-a-threat-to-drivers-and-manufacturers/

[11] Colombo, D. (2022). *How I got access to 25+ Tesla's around the world. By accident. And curiosity.* [online] Medium. Available at: https://medium.com/@david_colombo/how-i-got-access-to-25-teslas-around-the-world-by-accident-and-curiosity-8b9ef040a028

[12] Truong, J. (2021). *How to Hack Self-Driving Cars: Vulnerabilities in Autonomous Vehicles | HackerNoon*. Available at: https://hackernoon.com/how-to-hack-self-driving-cars-vulnerabilities-in-autonomous-vehicles-jh3r37cz

[13] Seetharaman, A., Patwa, N., Jadhav, V., Saravanan, AS andSangeeth, D. (2020). Impact of Factors Influencing Cyber Threatson Autonomous Vehicles. *Applied Artificial Intelligence*, pp. 1–28. https://doi.org/10.1080/08839514.2020.1799149

[14] Kaur, K. and Rampersad, G. (2018). Trust in driverless cars: Investigating key factors influencing the adoption of driverless cars. *Journal of Engineering and Technology Management*, 48, pp. 87–96. https://doi.org/10.1016/j.jengtecman.2018.04.006

[15] Luo, X., Li, H., Zhang, J. and Shim, J. P. (2010). Examining multi-dimensional Trust and multi-faceted risk in initial acceptance of emerging technologies: An empirical study of mobile banking services. *Decision Support Systems*, 49(2), pp. 222–234. https://doi.org/10.1016/j.dss.2010.02.008

[16] Mayer, R. C., Davis, J. H. and Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. *The Academy of Management Review*, 20(3), pp. 709–734. https://doi.org/10.2307/258792

[17] Lee, J. D. and See, K. A. (2004). Trust in Automation: Designing for Appropriate Reliance. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 46(1), pp. 50–80. https://doi.org/10.1518/hfes.46.1.50_30392

[18] Kaplan, A. D., Kessler, T. T., Brill, J. C. and Hancock, P. A., 2023. Trust in artificial intelligence: Meta-analytic findings. *Human factors*, *65*(2), pp. 337-359.

[19] Tenhundfeld, N., Demir, M. and de Visser, E. (2022). Assessment of Trust in Automation in the 'Real World': Requirements for New Trust in Automation Measurement Techniques for Use by Practitioners. https://doi.org/10.1177/15553434221096261

[20] Hoff, K. A. and Bashir, M. (2014). Trust in Automation: Integrating Empirical Evidence on Factors That Influence Trust. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 57(3), pp. 407–434. https://doi.org/10.1177/0018720814547570

[21] Zmud, J. P. and Sener, I. N. (2017). Towards an Understandingof the Travel Behavior Impact of Autonomous Vehicles. *Transportation Research Procedia*, 25, pp. 2500–2519. https://doi.org/10.1016/j.trpro.2017.05.281

[22] Klein, U., Depping, J., Wohlfahrt, L. and Fassbender, P.(2023). Application of artificial intelligence: risk perception andTrust in the work context with different impact levels andtask types.

[23] Mármol, F. G., Pérez, M. G. and Pérez, G. M. (2016). I Don't Trust ICT: Research Challenges in Cyber Security. *Trust Management X*, pp. 129–136. https://doi.org/10.1007/978-3-319-41354-9_9

[24] Choi, J. K. and Ji, Y. G. (2015). Investigating the Importance of Trust on Adopting an Autonomous Vehicle. *International Journal of Human-Computer Interaction*, 31(10), pp. 692–702. https://doi.org/10.1080/10447318.2015.1070549

[25] Byrne, B. M. (2016). Structural Equation Modeling with AMOS: Basic Concepts, Applications, and Programming. 3rd Edition New York: Routledge. https://doi.org/10.4324/9781315757421

[26] Buckbee, M. (2020). *Analysing Company Reputation After a Data Breach*. [online] Available at: https://www.varonis.com/blog/company-reputation-after-a-data-breach

[27] Lazányi, K. (2023). Perceived Risks of Autonomous Vehicles. *Risks*, 11(2), p. 26. https://doi.org/10.3390/risks11020026

[28] Winkelman, Z., Buenaventura, M., Anderson, J. M., Beyene, N. M., Katkar, P. and Baumann, G. C. (2019). When AutonomousVehicles Are Hacked, Who Is Liable? Available at: https://www.rand.org/pubs/research_reports/RR2654.html

[29] Rainie, L., Funk, C., Anderson, M. and Tyson, A. (2022). *Americans cautious about the deployment ofdriverless cars*. Pew Research Center: Internet, Science &Tech. Available at: https://www.pewresearch.org/internet/2022/03/17/Americans-cautious-about-the-deployment-of-driverless-cars/

[30] Saunders, M., Lewis, P. and Thornhill, A. (2019). *Research Methods for Business Students*. 8th ed. United Kingdom: Pearson.

[31] Creswell, J. W. and Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches*. Thousand Oaks, California: Sage Publications, Inc.

[32] Turner, D. (2010). Qualitative Interview Design: a Practical-Guide for Novice Investigators. *The Qualitative Report*, 15(3), pp. 754–760. https://doi.org/10.46743/2160-3715/2010.1178

[33] Hair, J., Black, W. C., Babin, B. J., and Anderson, R. E. (2010). Multivariate data analysis: A Global Perspective. 7th ed. Upper Saddle River: Pearson Education, Cop.

[34] Marsh, H. W., & Yeung, A. S. (1998). Longitudinal Structural Equation Models of Academic Self-Concept and Achievement: Gender Differences in the Development of Math and English Constructs. American Educational Research Journal, 35, 705-738. https://doi.org/10.3102/00028312035004705

[35] Khan, S. K, Shiwakoti, N., Stasinopoulos, P. and M. Warren, M. "Cybersecurity Readiness for Automated Vehicles," 2022 International Conference on Frontiers of Artificial Intelligence and Machine Learning (FAIML), Hangzhou, China, 2022, pp. 7-12. https://doi.org/10.1016/j.aap.2020.105837

[36] Dutton, W. H., & Shepherd, A. (2006). Trust in the Internet as an experience technology: Challenges for governance and policy**.** *Journal of Information Technology*, 21(3), 195–207. https://doi.org/10.1080/13691180600858606