IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 22 February 2024, accepted 1 March 2024, date of publication 4 March 2024, date of current version 8 March 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3373315

RESEARCH ARTICLE

Willingness to Pay for Smart Car Security

SOONBEOM KWON[1] AND HWANSOO LEE[2], (Member, IEEE)
[1]Department of Science and Technology Policy Convergence, Dankook University, Yongin 16890, South Korea
[2]Department of Industrial Security, Dankook University, Yongin 16890, South Korea

Corresponding author: Hwansoo Lee (hanslee992@gmail.com)

This work was supported by the Research Fund of Dankook University, in 2021.

ABSTRACT Smart cars have become more intelligent and technologically complex; however, consumers have raised concerns about their security because of hacking and technical safety. Although numerous studies have focused on the technological issues of smart cars, there is a need for new perspectives and discussions to examine drivers' perceptions of smart car security and safety. Understanding drivers' security perceptions and behaviors in a smart car environment is crucial for enhancing smart car security and driving industrial growth. Therefore, this study analyses the factors affecting drivers' willingness to pay (WTP) for smart car security based on protection motivation theory and explores the relationship between protective motivations and post-behavior. This study analyses how drivers' security vulnerabilities and severity perceptions in a smart car environment affect their WTP for security software. In addition, the comparative analysis discusses how security perceptions differ between traditional PC and smart car environments. The results of this study demonstrate that drivers are sensitive to smart car security and are willing to pay to strengthen security. Moreover, the results of this study suggest that the role of security solution companies is important for strengthening smart car security and expanding the market. This study has academic significance because it is an early study discussing driver behavior related to smart car security software on a theoretical basis. It is also significant because it provides practical implications for smart car security market growth and guides the formulation of effective security policies.

INDEX TERMS Perceived severity, perceived vulnerability, protection motivation theory, smart car security, willingness to pay (WTP).

I. INTRODUCTION

Information and communication technology in the era of the Fourth Industrial Revolution has led to the advancement of conventional industries, thereby creating new added value through convergence among industries [1]. The convergence of information and communication technology and the automobile industry has given rise to the concept of smart mobility by expanding the convenience and safety of movement [2]. Smart mobility is expected to revolutionize social infrastructures such as transportation networks and cities [3]. Among the various types of smart mobility, vehicles combined with information and communication technologies are defined as autonomous, connected, or smart cars. Smart cars refer to both connected and autonomous vehicles. This concept also refers to vehicles capable of two-way communication utilizing a computer with installed software (SW) [4]. According to the global research firm Statista, the globally connected car market was valued at 64.8 billion USD in 2021, is expected to grow by 18.1% annually and reach 191.8 billion USD by 2028 [5]. In other words, the smart car market is expected to grow rapidly in the future. Therefore, new marketing strategies are required to keep pace with the changing automobile industry.

Considering the large number of network devices and the growing number of electronic control devices in smart cars, these vehicles are becoming increasingly complex [6]. Smart cars use more computer systems and software than traditional cars do, making it easier for hackers to access and attack them and putting drivers at risk. Smart cars also collect and process a large amount of personal information about drivers and passengers, which increases the potential for privacy breaches. If the goal of a hacker's attack on a smart car is to hijack or take control of the vehicle, it can cause

The associate editor coordinating the review of this manuscript and approving it for publication was Tiago Cruz.

significant economic losses to the vehicle owner and social disruption [7]. Due to these features, it has been suggested that there remain numerous vulnerabilities in the security and privacy of smart cars [8].

For these reasons, consumers or drivers of smart cars have raised concerns regarding their security [9], [10]. Therefore, various studies have been conducted in social science fields, such as business administration and marketing, to address the negative perceptions of smart cars. For example, Xu et al. [10] and Talebian and Mishra [11] discussed factors that influence the acceptance of smart cars. Yu and Cai [12] analyzed how the perceived risks of smart cars affect trust and attitudes. Kim et al. [13] presented the factors that contribute to the reluctance of smart cars from the perspective of the theory of innovation resistance. However, most related studies have been conducted based on conventional technology acceptance theories, which limit the understanding of acceptance and spread in relation to the unique characteristics of smart cars. In particular, many studies have focused mainly on the acceptance of smart cars, although investigations should be conducted from new perspectives to examine the perception of smart car safety, the security issues that have been raised, and the impact of perceptions of security on acceptance.

Previous studies have emphasized safety as an important antecedent factor affecting the acceptance of smart cars [14], [15]. Hence, it is important to ensure the safety of smart cars in terms of both hardware and software, including electrical and infotainment systems. Software is a source of security vulnerabilities owing to the characteristics of smart cars, which involve the fusion of information and communication technology. Therefore, ensuring safety by strengthening the security of vehicle SW is critical [16]. In the future, when infotainment systems are updated in real time through networks such as over-the-air networks and in-vehicle apps using smartphones become more common, the importance of protection for in-vehicle software is expected to increase. However, vehicle SW is mostly provided by vehicle manufacturers, which limits user choices and investments in software security. Therefore, to strengthen vehicle SW security, vehicle owners must invest in this topic and increase their overall awareness of vehicle security.

In a conventional personal computer (PC) environment, investment in security software has been suggested as an effective way to strengthen security [17], [18]. In the smart car environment, investments in SW security can also be effective at strengthening the security of smart cars. Furthermore, existing research suggests that the security of smart cars cannot be enhanced using traditional information and communication technologies [19]. Therefore, new security technologies must be implemented to secure smart cars. As a result, evaluating willingness to pay (WTP) for security software, which can be considered a component of protection behavior, is crucial for understanding how smart car security can be enhanced.

In this study, we analyzed the factors that can affect WTP for the SW security of smart cars using protection motivation theory (PMT), which highlights the relationship between protection motivation and behavior. Given that PMT is a theory with strong explanatory power that can be used to predict the protective behavior-related willingness of individuals, it can be used as an appropriate theory for measuring vehicle owner perceptions of vehicle security. Therefore, we utilized PMT to analyze the effect of trust in software providers (TPs) on the relationship between protection motivation and behavior. Our goal was to identify the importance of SW security in a smart car environment by comparing SW security awareness between smart cars and common PC environments.

II. RELATED LITERATURES

A. SMART CARS

Smart cars are expected to become increasingly automated and digitized [20]. Numerous electronic control devices are installed inside smart cars, and many of these devices are targets for various types of hacking [21], [22]. Consequently, the security of smart cars is becoming increasingly important, and academia is continuously conducting research to address these problems. At the 2010 IEEE Symposium on Security and Privacy, Koscher et al. [23] presented the first study on vehicle cybersecurity threats. In 2011, Checkoway et al. [24] conducted a study on attack surfaces that could access the internal network of a vehicle. Additional studies on vehicle security have been conducted since then. However, along with growing interest in vehicle cybersecurity, concerns regarding general vehicle security have also been growing.

In light of these concerns, research on the willingness to accept smart cars has been actively conducted based on business management and marketing approaches [11], [25]. Additionally, research has been conducted based on various theoretical approaches using the technology acceptance model [10], diffusion of innovation [11], unified theory of acceptance and use of technology (UTAUT) [26], and UTAUT version 2 [27]. The perceived safety of smart cars has been found to affect user willingness to accept them [10]. Additionally, the perceived safety risks of smart cars indirectly impact consumer willingness to accept them [27]. These findings indicate that safety has an important influence on the willingness to accept smart cars, and safety concerns should be resolved to increase the willingness to accept smart cars. As described earlier, previous studies have focused mainly on the user perspective to increase the intention to accept smart cars and have analyzed this willingness using various theoretical approaches [12], [13].

According to the results of studies analyzing the willingness to accept the functions of smart cars from the user perspective, perceived security risks affect the willingness to accept in-vehicle infotainment (IVI) data services [12]. In other words, users consider safety to be important for smart cars, and safety concerns must be resolved to increase user willingness to accept smart car functions. However, the aforementioned studies largely ignored user perspectives regarding SW security, which is crucial for the safety of smart cars.

B. BEHAVIORAL WTP IN A SECURITY CONTEXT

Behavioral willingness concepts from various perspectives have been used to discuss consumer willingness to accept new technologies. In the marketing field, terms such as WTP [28], [29], willingness to purchase [30], and willingness to buy [31] are used, whereas willingness to provide [32] and willingness to disclose [33] are used in the information system field. Although research suggesting that willingness does not lead to behavior may render the measurement of behavioral willingness meaningless [34], [35], understanding consumer behavioral willingness can play a key role in establishing marketing strategies because it helps identify consumer needs. Therefore, it is necessary to analyze consumer behavioral willingness toward product acceptance strategies that meet their needs. Furthermore, it is important to use an appropriate behavioral willingness measurement tool according to the research purpose to analyze behavioral willingness accurately.

The WTP is a behavioral willingness concept that is suitable for explaining smart car users' willingness to use SW security. It refers to the amount of money a consumer is willing to pay for a certain good or service [36]. Consumers pay a high price if they believe that the quality of a good or service is high [37]. The WTP helps to analyze the quality of goods and services that consumers desire; hence, it can be used to identify consumer needs in the marketing field. The two methods used to calculate WTP are price- and value-based determination [38]. The price-based determination method estimates the price that can produce a target profit after covering all costs involved in the production and sales of a product. Conversely, the value-based determination method estimates prices based on consumer perceptions and demand for a product's value [39]. This approach can be used as an appropriate method for explaining smart car users' willingness to use security SW. Furthermore, the WTP for SW security can be used as a key variable to explain consumer WTP.

C. PMT

PMT is a theory with strong explanatory power that can be used to predict individuals' willingness to engage in protective behaviors [40]. As a theory used in health science, the PMT was originally developed by [41] to analyze the factors that influence an individual's behavior during threatening situations [41]. However, it is currently used in various fields, including technological research, to predict the behavioral willingness of individuals in the information security domain [42], [43]. For example, Crossler et al. [44] used PMT to analyze the factors that determine compliance with "bring your own device" policies. Bélanger et al. [45] used PMT to analyze the determinants of early conformance with information security policies. Furthermore, research using PMT has been conducted in recent years in the field of information security to predict the protection-behavior-related willingness of individuals [46], [47].

The PMT was considered suitable for this study, where we analyzed the factors affecting the willingness to use smart car security SW. We considered the two main variables of PMT to analyze the factors affecting the willingness to use smart car security SW: perceived severity (PS) and perceived vulnerability (PV) [41]. According to PMT, PS refers to the magnitude of a threat, and PV refers to the degree to which one believes that a threatening event will occur [41], [48]. In this study, PS was defined as the degree of damage caused by a security incident that may occur when using a smart car. PV was defined as the probability of a security incident occurring when using a smart car.

D. TRUST IN PROVIDER

Trust has been studied in various fields, including business administration, psychology, and economics [49]. It plays an important role in the relationships between individuals and between individuals and organizations [50]. However, this concept is characterized by its abstract and complex nature, which makes it difficult to define and measure [51], [52]. Consequently, trust has been defined differently depending on researchers' perspectives. Rousseau et al. [53] defined trust as "a psychological state comprising the intention to accept vulnerability based on positive expectations of the intentions or behavior of another." Morgan and Hunt [54] defined trust as a belief in a group with confidence. According to Wang et al. [55], trust is "the degree of consumer perceptions regarding whether the products they buy are reliable and safe." From these perspectives, trust in smart car SW security can be defined as an attitude of accepting vulnerabilities based on positive expectations of SW security. In other words, consumer trust in a provider is the belief in that provider's ability to provide the desired product to the consumer. Trust in providers can play a key role in increasing the WTP for smart car SW security because it can help achieve strong marketing performance based on consumer trust.

Trust plays a key role in reducing perceived risk and increasing WTP. Previous studies have shown that trust, as well as the PV of technology, reduces the perception of risk and uncertainty [56], [57]. Netemeyer et al. [58] found that customers have a high WTP for brands that provide trust, whereas Roosen et al. [59] indicated that trust in a product increases WTP. This finding implies that trust can be a key variable for reducing the perceived risk of a product and increasing WTP.

III. RESEARCH MODEL AND HYPOTHESES

In this study, we analyzed whether PS and PV protection motivations affect the WTP for security SW, which is a protection behavior, based on PMT. In particular, we examined how TP affects the relationship between protection motivation and behavior and analyzed the importance of SW security in smart car environments by comparing the perceptions of SW security between smart car environments and typical PC environments. Fig. 1 presents a schematic of our research model.

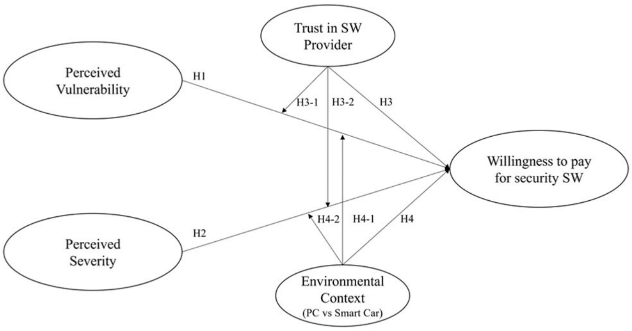

FIGURE 1. Research model.

When an individual is exposed to a risk, they identify appropriate protective behaviors by assessing the risk of an incident and the cost and benefit of the risk. This risk assessment is conducted by evaluating PVs and PSs. As PV and PS increase, protection motivation also increases [41]. Some studies have shown that an increase in PV and PS leads to an increase in the WTP for safe products. This finding implies that the WTP for safe products increases as the assessed risk increases [60], [61]. According to studies conducted in this context, an increase in PS and PV during the COVID-19 period led to an increase in the WTP for face masks [61]. Furthermore, the greater the PS and PV are for the disease, the greater the WTP for vaccines outside of the pocket [60]. This indicates that as the PV and PS of a risky situation increase, the WTP for safe products is also expected to increase. Similarly, as the PV and PS of smart car security risks increase, the WTP for smart car SW security is also expected to increase. Therefore, we propose the following hypotheses.

Hypothesis 1. PV has a positive impact on WTP.

Hypothesis 2. PS has a positive impact on WTP.

In general, consumers do not have a high WTP for SW security. Considering the unique nature of the SW security market, which is different from that of the general SW market, it is expected that factors other than functionality and quality will have significant impacts on WTP. In fact, a recent study indicated that SW users were less willing to pay for security features. However, the WTP increases when SW security is accompanied by third-party certification [62]. An increase in WTP based on third-party certification can be interpreted as a result of low user trust in providers. Therefore, trust in providers is expected to be an important factor in increasing the WTP for SW security. Accordingly, we propose the following hypotheses.

Hypothesis 3. TP has a positive impact on WTP.

Hypothesis 3-1. TP moderates the relationship between PV and WTP.

Hypothesis 3-2. TP moderates the relationship between PS and WTP.

Hacking in common PC environments causes personal information leakage or computer damage only, whereas hacking in smart car environments can directly harm drivers physically and even lead to loss of life [7]. Therefore, awareness of the security risks of smart cars is expected to be greater than that of security risks in common PC environments. Accordingly, the WTP for SW security in smart car environments is expected to be greater than that in common PC environments. Consequently, we propose the following hypotheses.

Hypothesis 4. The environmental context of providers can have a positive impact on WTP.

Hypothesis 4-1. The environmental context moderates the relationship between PV and WTP.

Hypothesis 4-2. The environmental context moderates the relationship between PS and WTP.

IV. MATERIALS AND METHODS

A. ANALYTICAL PROCEDURE

To validate our research model and hypotheses, survey data were collected from 300 drivers through an online survey platform (https://www.opensurvey.co.kr/). A total of 293 data points were used for analysis after excluding insincere respondents who answered with only one or more data points. Responses were collected on a seven-point Likert scale, and Jamovi and SmartPLS 4 were used to analyze the collected data. Descriptive statistics, paired-sample t tests, and partial least squares (PLS) structural equation modeling were used to test the hypotheses.

B. MEASUREMENT ITEMS

Table 1 presents the variables and measurement items considered in this study. The items related to security vulnerability and severity in PC and smart car environments were developed based on the procedure presented by [63]. The WTP items were modified based on the study by [62]. Additionally, we incorporated a single question on the TP based on the findings presented by [64].

C. RESEARCH DATA

The demographic characteristics of the participants are presented in Table 2. The sex split was 49.7% male and 50.5% female. The age split was also relatively even, with 25.3% in their 20s, 25.9% in their 30s, 24.6% in their 40s, and 24.2% in their 50s. Regarding education, 13.7% had a high school diploma, 76.1% had a college degree, and 10.2% had a graduate degree. Regarding experience with using security SW, such as antivirus SW, 7.5% of the respondents had no experience, and 86.7% had used only free security SW. Additionally, 47.4% of respondents had more than eight years of driving experience.

TABLE 1. Measurement items.

Variable	Measurement Category		Researcher
Perceived Vulnerability	PV1	It is likely that I will have viruses or malware installed on my smart car (computer).	[63]
	PV2	It is possible that I will have a hacking attack on my smart car (computer).	
	PV3	It is possible that the information about my smart car (computer) will be leaked.	
Perceived Severity	PS1	I believe that having a smart car (computer) infected by malware is a serious problem.	[63]
	PS2	I believe that having a smart car (computer) attacked by a hacker is a serious problem.	
	PS3	If the information on my smart car (computer) is leaked or my smart car (computer) is controlled by a hacker, it can cause serious problems.	
WTP	WTP1	I am willing to pay to install security SW for my smart car (computer).	[62]
	WTP2	I prefer to pay for smart car (computer) security over using freeware.	
	WTP3	I am willing to pay something for smart car (computer) security.	
Trust in SW Providers	TP	Security SW developed by a security SW company is trustworthy for my smart car (computer).	[64]

V. RESULTS

A. MEASUREMENT MODEL VERIFICATION

To verify our measurement model, we checked the average variance extracted (AVE), composite reliability (CR), and outer loading of the measurement items for convergent validity. Additionally, Cronbach's α and rho_a were used as values representing internal consistency [65]. In general, an outer loading value of at least 0.7 indicates that the item is not problematic, and an AVE value of a minimum of 0.5 indicates that convergent validity is secured. Cronbach's alpha, rho_a, and CR were considered to represent internal consistency and convergent validity if they were a minimum of 0.7. As listed in Table 3, all the items exceeded the corresponding thresholds, confirming that there were no problems associated with focus, validity, or internal consistency.

TABLE 2. Research data.

Category		N (%)
GSex	Male	145 (49.5%)
	Female	148 (50.5%)
Age (Years)	20-	74 (25.3%)
	30-	76 (25.9%)
	40-	72 (24.6%)
	50-	71 (24.2%)
Educational Background	High School	40 (13.7%)
	Undergraduate Degree	223 (76.1%)
	Graduate Degree	30 (10.2%)
Security SW Use	No Use	22 (7.5%)
	Use (Free)	254 (86.7%)
	Use (Paid)	17 (5.8%)
Driving Experience (Years)	<2	97 (33.1%)
	2-4	28 (9.6%)
	4-6	16 (5.5%)
	6-8	13 (4.4%)
	>8	139 (47.4%)

To verify the discriminant validity of the measurement model, we calculated the Fornell–Larcker criterion and heterotrait–monotrait ratio of correlations (HTMT) [65]. According to the Fornell–Larcker criterion, discriminant validity is achieved when the square root of the AVE of each latent variable is greater than the correlation between the latent variables. Discriminant validity is considered secure if the HTMT value is less than 0.85. As shown in Table 4, all the thresholds were satisfied, verifying the discriminant validity between the constructs.

B. HYPOTHESIS TESTING RESULTS

To evaluate the explanatory power of our research model, we checked the R2 value, and to verify our hypotheses, we checked the significance of the hypotheses. The R2 value was 0.549, indicating strong explanatory power for the research model. A PLS analysis of the total sample was conducted and the results are presented in Table 5. Based on the bootstrapping results, H1 (path coefficient = 0.226, t = 3.184, $p < 0.001$), H2 (path coefficient = 0.350, t = 4.887, $p < 0.001$), and H3 (path coefficient = 0.346, t = 6.016, $p < 0.001$) were supported. TP was found to be a significant

TABLE 3. Measurement model evaluation.

Constructs	Item	Mean	Loading	α	rho_a	CR	AVE
Perceived Vulnerability	PV1	4.799	0.925	0.929	0.933	0.955	0.876
	PV2	4.922	0.954				
	PV3	4.853	0.927				
Perceived Severity	PS1	5.174	0.948	0.948	0.948	0.966	0.906
	PS2	5.341	0.968				
	PS3	5.352	0.939				
WWTP	WTP1	5.017	0.911	0.908	0.918	0.942	0.844
	WTP2	4.853	0.924				
	WTP3	4.983	0.921				

TABLE 4. Discriminant validity (HTMT).

Constructs	PV	PS	WTP
PV	0.952		
PS	0.767 (0.815)	0.936	
WTP	0.651 (0.694)	0.595 (0.641)	0.919

moderator of the relationship between PS and WTP (H3-1: path coefficient $= 0.350$, $t = 1.992$, $p < 0.05$). was

TABLE 5. PLS analysis results.

Hypotheses	Path Coefficient	t value	p value	Results
H1 (PV→WTP)	0.226	3.184	0.001	Sig.
H2 (PS→WTP)	0.350	4.887	0.000	Sig.
H3 (TP→WTP)	0.346	6.016	0.000	Sig.
H3-1 (TP*PV → WTP)	-0.056	0.727	0.467	N.S.
H3-2 (TP*PS->WTP)	0.350	1.992	0.046	Sig.

C. COMPARATIVE ANALYSIS

A paired-sample t test was conducted to compare PS, PV, and WTP between PC and smart car environments, and PLS multigroup analysis was conducted to verify the moderating effect of environmental context. The results are presented in Table 6. First, the results of the paired-sample t test indicated that PS, PV, and WTP were significantly greater in the smart car environment than in the PC environment, confirming the influence of the environmental context. The results of the analysis of differences in path coefficients according to the environmental context indicated that the relationship between PS and WTP was significantly stronger in the smart car environment. Although the difference in path coefficients between PVs and WTPs was not statistically significant, the relationship that was not significant in the PC environment was significant in the smart car environment, suggesting the strong influence of the environmental context. In other words, the security risk perception was greater in the smart car environment than in the PC environment, and t. Additionally, the influence of PV and PS on WTP was greater in the smart car environment.

TABLE 6. Environmental contextual differences.

	PC Context	Smart Car Context	Difference	t value	p value	Results
PV (Mean)	4.278	4.858	-0.580	-6.850	0.000	Sig.
PS (Mean)	4.420	5.289	-0.869	-9.350	0.000	Sig.
WTP (Mean)	3.950	4.951	-1.001	-12.300	0.000	Sig.
PV->WTP (Path Coefficient)	0.162	0.234**	-0.071	0.608	0.272	N.S.
PS->WTP (Path Coefficient)	0.272**	0.472***	-0.200	1.718	0.043	Sig.

VI. DISCUSSION AND CONCLUSION

A. DISCUSSION

The first major finding of this study is that PVs and PSs have significant effects on WTP in smart car environments. In particular, PS was found to have a relatively high impact on smart car security investment. This is because drivers are more sensitive to the consequences of vulnerabilities in the security of smart cars than in traditional PC environments. This indicates that PS is more important than PV when translating security threats into actions. Previous research has also confirmed that PS has the strongest influence on information security behavior [66].

Second, this study revealed that trust in security SW companies not only has a direct effect on WTP but also has an interactive effect with PS. Various marketing studies have shown that trust in a brand or company is a key component of customer purchase intentions regarding a given product [67], [68]. The results of this study also indicate that trust in a provider is important for smart car security SW. Another interesting finding is the moderating effect of TP on PS and WTP. Chang et al. [69] argued that the security awareness of a provider or product itself influences purchase decisions. This is because security threats can affect consumer experiences with products. When consumers perceive security threats, their trust in a product or provider reduces their PS [68]. Therefore, the results of this study indicate that in a smart car environment, as drivers become aware of the severity of security threats and their TP increases, their intention to pay for security SW may also increase. This implies that if a security company offers reliable and paid SW specialized for smart cars, many users will be willing to pay for it.

Third, a comparative analysis of the PC and smart car environments revealed that PV, PS, and WTP were significantly greater in the smart car environment than in the PC environment. The results indicated that drivers perceive security threats to be more serious in smart car environments than in PC environments. They are also more likely to pay for secure SW for smart cars. Security risks are more critical in an Internet of Things (IoT) environment in which physical objects are connected than in a traditional PC environment [70]. In the case of smart cars, which are representative devices in IoT environments, the security risk is closely tied to the physical safety of drivers [7]. This finding agrees with those of previous studies indicating that perceived risk affects consumer product choice and behavioral intentions [71], [72]; this finding explains why security risk in the smart car environment also affects product purchase intentions for smart car security SW.

Finally, the impacts of PVs and PSs on WTP were found to be significantly different. According to the results of our analysis, in the traditional PC environment, perceived security vulnerabilities do not lead to increased WTP for security SW, whereas in a smart car environment, both PV and PS significantly affect purchase intentions. One reason for this may be that many security SW packages are available for free in PC environments. Additionally, it can be understood that users are aware of a certain level of security vulnerability in PCs and are willing to accept it. This also means that it is difficult to spread paid security SW. However, in the case of smart cars, there is significant potential for inducing drivers to invest in security.

The main academic contribution of our study is that it elucidates WTP behaviors in the context of security SW in smart cars, which represent a new technological environment, in the absence of theoretical discussions on behaviors related to security SW. This study also revealed that the perceptions and payment behaviors related to security SW may differ depending on the environment. In terms of practical contributions, given that people are highly aware of the security concerns and risks of smart cars, the results of this study indicate that the security of smart cars must be strengthened to increase their usage. This study demonstrated the need for development through trusted and specialized security companies. Furthermore, drivers are more sensitive to security threats related to smart cars and are more likely to pay for secure SW in the context of smart cars. This implies that security concerns are expected to motivate purchase intentions for paid security SW in the smart car environment, in contrast to the traditional PC environment, and that if trust in security SW companies is a prerequisite, then security concerns are expected to lead to the activation of the smart car security SW market.

B. CONCLUSION

In this study, we examined the security perceptions and behaviors of individuals in a smart car environment. Based on the PMT, this paper proposed a research model, and we analyzed the empirical impact of security vulnerability and severity in the smart car environment on the WTP for security SW. The results confirm that the sensitivity to security and privacy risks is greater in smart car environments than in traditional PC environments and that the attitude of consumers toward investing in security SW is stronger. This shows that smart car manufacturers, security companies, and even governments need to take different approaches to strengthening smart car security ecosystems, and further research is needed in this area.

Given that this study focused on discussing core factors based on the PMT theory, there might be limitations in terms of elucidating the various factors affecting the WTP for smart car security SW. Thus, future studies should further explore specific factors, such as user attitudes, preferences, and experiences related to smart car security, that influence user perceptions and behaviors in the smart car security domain. Furthermore, this study analyzed self-reported data with a relatively small sample size; therefore, an expanded study is needed to provide a more in-depth discussion through an experimental study. Although this study has limitations in terms of smart car security behavior, it provides a basis for expanding the theory because smart car security behavior is different from that in traditional environments.

REFERENCES

[1] F. F. Adedoyin, F. V. Bekun, O. M. Driha, and D. Balsalobre-Lorente, "The effects of air transportation, energy, ICT and FDI on economic growth in the industry 4.0 era: Evidence from the United States," *Technological Forecasting Social Change*, vol. 160, Nov. 2020, Art. no. 120297.

[2] D. Attias, "The autonomous car, a disruptive business model?" in *The Automobile Revolution: Towards a New Electro-Mobility Paradigm*. Cham, Switzerland: Springer, 2017, pp. 99–113.

[3] J. Park, C. Nam, and H.-J. Kim, "Exploring the key services and players in the smart car market," *Telecommun. Policy*, vol. 43, no. 10, Nov. 2019, Art. no. 101819.

[4] H. Manivasakan, R. Kalra, S. O'Hern, Y. Fang, Y. Xi, and N. Zheng, "Infrastructure requirement for autonomous vehicle integration for future urban and suburban roads–current practice and a case study of Melbourne, Australia," *Transp. Res. A, Policy Pract.*, vol. 152, pp. 36–53, Oct. 2021.

[5] Statista. (2021). *Size of the Global Connected Car Market Between 2019 and 2020, With a Forecast Through 2028.* [Online]. Available: https://www.statista.com/statistics/725025/connected-cars-global-market-size-projection/

[6] Q. Xu, B. Wang, F. Zhang, D. S. Regani, F. Wang, and K. J. R. Liu, "Wireless AI in smart car: How smart a car can be?" *IEEE Access*, vol. 8, pp. 55091–55112, 2020.

[7] R. L. Trope and T. J. Smedinghoff, "Why smart car safety depends on cybersecurity," *Scitech Lawyer*, vol. 14, no. 4, pp. 8–13, 2018.

[8] V. Singh, V. Singh, and S. Vaibhav, "A review and simple meta-analysis of factors influencing adoption of electric vehicles," *Transp. Res. D, Transp. Environ.*, vol. 86, Sep. 2020, Art. no. 102436.

[9] J. H. Kim, G. Lee, J. Lee, K. F. Yuen, and J. Kim, "Determinants of personal concern about autonomous vehicles," *Cities*, vol. 120, Jan. 2022, Art. no. 103462.

[10] Z. Xu, K. Zhang, H. Min, Z. Wang, X. Zhao, and P. Liu, "What drives people to accept automated vehicles? Findings from a field experiment," *Transp. Res. C, Emerg. Technol.*, vol. 95, pp. 320–334, Oct. 2018.

[11] A. Talebian and S. Mishra, "Predicting the adoption of connected autonomous vehicles: A new approach based on the theory of diffusion of innovations," *Transp. Res. C, Emerg. Technol.*, vol. 95, pp. 363–380, Oct. 2018.

[12] Z. Yu and K. Cai, "Perceived risks toward in-vehicle infotainment data services on intelligent connected vehicles," *Systems*, vol. 10, no. 5, p. 162, Sep. 2022.

[13] J. Kim, S. Kim, and C. Nam, "User resistance to acceptance of in-vehicle infotainment (IVI) systems," *Telecommun. Policy*, vol. 40, no. 9, pp. 919–930, Sep. 2016.

[14] J. C. Zoellick, A. Kuhlmey, L. Schenk, D. Schindel, and S. Blüher, "Amused, accepted, and used? Attitudes and emotions towards automated vehicles, their relationships, and predictive value for usage intention," *Transp. Res. F, Traffic Psychol. Behaviour*, vol. 65, pp. 68–78, Aug. 2019.

[15] L. Montoro, S. A. Useche, F. Alonso, I. Lijarcio, P. Bosó-Seguí, and A. Martí-Belda, "Perceived safety and attributed value as predictors of the intention to use autonomous vehicles: A national study with Spanish drivers," *Saf. Sci.*, vol. 120, pp. 865–876, Dec. 2019.

[16] H.-K. Kong, T.-S. Kim, and M.-K. Hong, "A security risk assessment framework for smart car," in *Proc. 10th Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput. (IMIS)*, Jul. 2016, pp. 102–108.

[17] M. Çakanyıldırım, W. T. Yue, and Y. U. Ryu, "The management of intrusion detection: Configuration, inspection, and investment," *Eur. J. Oper. Res.*, vol. 195, no. 1, pp. 186–204, May 2009.

[18] W. Liu, H. Tanaka, and K. Matsuura, "An empirical analysis of security investment in countermeasures based on an enterprise survey in Japan," in *Proc. WEIS*, 2006, pp. 1–15.

[19] J. Yoo and J. H. Yi, "Code-based authentication scheme for lightweight integrity checking of smart vehicles," *IEEE Access*, vol. 6, pp. 46731–46741, 2018.

[20] J. Meyer, H. Becker, P. M. Bösch, and K. W. Axhausen, "Autonomous vehicles: The next jump in accessibilities?" *Res. Transp. Econ.*, vol. 62, pp. 80–91, Jun. 2017.

[21] K. Kim, J. S. Kim, S. Jeong, J.-H. Park, and H. K. Kim, "Cybersecurity for autonomous vehicles: Review of attacks and defense," *Comput. Secur.*, vol. 103, Apr. 2021, Art. no. 102150.

[22] G. De La Torre, P. Rad, and K.-K.-R. Choo, "Driverless vehicle security: Challenges and future research opportunities," *Future Gener. Comput. Syst.*, vol. 108, pp. 1092–1111, Jul. 2020.

[23] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental security analysis of a modern automobile," in *Proc. IEEE Symp. Secur. Privacy*, May 2010, pp. 447–462.

[24] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Comprehensive experimental analyses of automotive attack surfaces," in *Proc. USENIX Secur. Symp.*, San Francisco, CA, USA, vol. 4, 2021, pp. 447–462.

[25] L. Buckley, S.-A. Kaye, and A. K. Pradhan, "Psychosocial factors associated with intended use of automated vehicles: A simulated driving study," *Accident Anal. Prevention*, vol. 115, pp. 202–208, Jun. 2018.

[26] R. Madigan, T. Louw, M. Wilbrink, A. Schieben, and N. Merat, "What influences the decision to use automated public transport? Using UTAUT to understand public acceptance of automated road transport systems," *Transp. Res. F, Traffic Psychol. Behaviour*, vol. 50, pp. 55–64, Oct. 2017.

[27] A. Z. Benleulmi and T. Blecker, "Investigating the factors influencing the acceptance of fully autonomous cars," in *Digitalization in Supply Chain Management and Logistics: Smart and Digital Solutions for an Industry 4.0 Environment*, vol. 23. Berlin, Germany: epubli GmbH, 2017, pp. 99–115.

[28] M. K. Hidrue, G. R. Parsons, W. Kempton, and M. P. Gardner, "Willingness to pay for electric vehicles and their attributes," *Resource Energy Econ.*, vol. 33, no. 3, pp. 686–705, Sep. 2011.

[29] P. Liu, Q. Guo, F. Ren, L. Wang, and Z. Xu, "Willingness to pay for self-driving vehicles: Influences of demographic and psychological factors," *Transp. Res. C, Emerg. Technol.*, vol. 100, pp. 306–317, Mar. 2019.

[30] V. Benson, J.-N. Ezingeard, and C. Hand, "An empirical study of purchase behavior on social platforms: The role of risk, beliefs and characteristics," *Inf. Technol. People*, vol. 32, no. 4, pp. 876–896, 2019.

[31] X. Tian, Q. Zhang, Y. Chi, and Y. Cheng, "Purchase willingness of new energy vehicles: A case study in Jinan city of China," *Regional Sustainability*, vol. 2, no. 1, pp. 12–22, Jan. 2021.

[32] D. Kim, K. Park, Y. Park, and J.-H. Ahn, "Willingness to provide personal information: Perspective of privacy calculus in IoT services," *Comput. Hum. Behav.*, vol. 92, pp. 273–281, Mar. 2019.

[33] S. Sun, J. Zhang, Y. Zhu, M. Jiang, and S. Chen, "Exploring users' willingness to disclose personal information in online healthcare communities: The role of satisfaction," *Technological Forecasting Social Change*, vol. 178, May 2022, Art. no. 121596.

[34] P. Sheeran and T. L. Webb, "The intention-behavior gap," *Social Pers. Psychol. Compass*, vol. 10, no. 9, pp. 503–518, Sep. 2016.

[35] P. Sheeran, G. Godin, M. Conner, and M. Germain, "Paradoxical effects of experience: Past behavior both strengthens and weakens the intention-behavior relationship," *J. Assoc. Consum. Res.*, vol. 2, no. 3, pp. 309–318, Jul. 2017.

[36] S. Kalish and P. Nelson, "A comparison of ranking, rating and reservation price measurement in conjoint analysis," *Marketing Lett.*, vol. 2, no. 4, pp. 327–335, Nov. 1991.

[37] V. A. Zeithaml, "Consumer perceptions of price, quality, and value: A means-end model and synthesis of evidence," *J. Marketing*, vol. 52, no. 3, pp. 2–22, Jul. 1988.

[38] A. Chaudhuri and M. B. Holbrook, "The chain of effects from brand trust and brand affect to brand performance: The role of brand loyalty," *J. Marketing*, vol. 65, no. 2, pp. 81–93, Apr. 2001.

[39] G. Armstrong, S. Adam, S. Denize, and P. Kotler, *Principles of Marketing*. Richmond VIC, Australia: Pearson, 2014.

[40] P. Ifinedo, "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," *Comput. Secur.*, vol. 31, no. 1, pp. 83–95, Feb. 2012.

[41] R. W. Rogers, "A protection motivation theory of fear appeals and attitude Change1," *J. Psychol.*, vol. 91, no. 1, pp. 93–114, Sep. 1975.

[42] A. C. Johnston and M. Warkentin, "Fear appeals and information security behaviors: An empirical study," *MIS Quart.*, vol. 34, no. 3, pp. 549–566, 2010.

[43] N. Thompson, T. J. McGill, and X. Wang, "Security begins at home': Determinants of home computer and mobile device security behavior," *Comput. Security*, vol. 70, pp. 376–391, Sep. 2017.

[44] R. E. Crossler, J. H. Long, T. M. Loraas, and B. S. Trinkle, "Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap," *J. Inf. Syst.*, vol. 28, no. 1, pp. 209–226, Jun. 2014.

[45] F. Bélanger, S. Collignon, K. Enget, and E. Negangard, "Determinants of early conformance with information security policies," *Inf. Manage.*, vol. 54, no. 7, pp. 887–901, Nov. 2017.

[46] S. Abraham and I. Chengalur-Smith, "Evaluating the effectiveness of learner controlled information security training," *Comput. Secur.*, vol. 87, Nov. 2019, Art. no. 101586.

[47] K. A. Saban, S. Rau, and C. A. Wood, "'SME executives' perceptions and the information security preparedness model," *Inf. Comput. Secur.*, vol. 29, no. 2, pp. 263–282, Aug. 2021.

[48] R. W. Rogers, "Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation," in *Social Psychophysiology: A Sourcebook*. New York, NY, USA: Guilford Press, 1983, pp. 153–176.

[49] X. Li, T. J. Hess, and J. S. Valacich, "Why do we trust new technology? A study of initial trust formation with organizational information systems," *J. Strategic Inf. Syst.*, vol. 17, no. 1, pp. 39–71, Mar. 2008.

[50] R. C. Nyhan, "Changing the paradigm: Trust and its role in public sector organizations," *Amer. Rev. Public Admin.*, vol. 30, no. 1, pp. 87–109, Mar. 2000.

[51] C. L. Corritore, B. Kracher, and S. Wiedenbeck, "On-line trust: Concepts, evolving themes, a model," *Int. J. Hum.-Comput. Stud.*, vol. 58, no. 6, pp. 737–758, Jun. 2003.

[52] E. Bonsón Ponte, E. Carvajal-Trujillo, and T. Escobar-Rodríguez, "Influence of trust and perceived value on the intention to purchase travel online: Integrating the effects of assurance on trust antecedents," *Tourism Manage.*, vol. 47, pp. 286–302, Apr. 2015.

[53] D. M. Rousseau, S. B. Sitkin, R. S. Burt, and C. Camerer, "Not so different after all: A cross-discipline view of trust," *Acad. Manage. Rev.*, vol. 23, no. 3, pp. 393–404, Jul. 1998.

[54] R. M. Morgan and S. D. Hunt, "The commitment-trust theory of relationship marketing," *J. Marketing*, vol. 58, no. 3, p. 20, Jul. 1994.

[55] Y. Wang, J. R. Huscroft, B. T. Hazen, and M. Zhang, "Green information, green certification and consumer perceptions of remanufctured automobile parts," *Resour., Conservation Recycling*, vol. 128, pp. 187–196, Jan. 2018.

[56] R. C. Mayer, J. H. Davis, and F. D. Schoorman, "An integrative model of organizational trust," *Acad. Manage. Rev.*, vol. 20, no. 3, pp. 709–734, Jul. 1995.

[57] M. Hengstler, E. Enkel, and S. Duelli, "Applied artificial intelligence and trust—The case of autonomous vehicles and medical assistance devices," *Technological Forecasting Social Change*, vol. 105, pp. 105–120, Apr. 2016.

[58] R. G. Netemeyer, B. Krishnan, C. Pullig, G. Wang, M. Yagci, D. Dean, J. Ricks, and F. Wirth, "Developing and validating measures of facets of customer-based brand equity," *J. Bus. Res.*, vol. 57, no. 2, pp. 209–224, Feb. 2004.

[59] J. Roosen, A. Bieberstein, S. Blanchemanche, E. Goddard, S. Marette, and F. Vandermoere, "Trust and willingness to pay for nanotechnology food," *Food Policy*, vol. 52, pp. 75–83, Apr. 2015.

[60] Z. Hou, J. Chang, D. Yue, H. Fang, Q. Meng, and Y. Zhang, "Determinants of willingness to pay for self-paid vaccines in China," *Vaccine*, vol. 32, no. 35, pp. 4471–4477, Jul. 2014.

[61] Q. Ding, S. Lin, and S. Wang, "Determinants and willingness to pay for purchasing mask against COVID-19: A protection motivation theory perspective," *Int. J. Environ. Res. Public Health*, vol. 19, no. 7, p. 4268, Apr. 2022.

[62] P. Sanyal, N. Menon, and M. Siponen, "An empirical examination of the economics of mobile application security," *MIS Quart.*, vol. 45, no. 4, pp. 2235–2260, Dec. 2021.

[63] B. Hanus and Y. A. Wu, "Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective," *Inf. Syst. Manage.*, vol. 33, no. 1, pp. 2–16, Jan. 2016.

[64] B. Suh and I. Han, "The impact of customer trust and perception of security control on the acceptance of electronic commerce," *Int. J. Electron. commerce*, vol. 7, no. 3, pp. 135–161, 2003.

[65] C. Fornell and D. F. Larcker, "Evaluating structural equation models with unobservable variables and measurement error," *J. Marketing Res.*, vol. 18, no. 1, p. 39, Feb. 1981.

[66] Z. Tang, A. S. Miller, Z. Zhou, and M. Warkentin, "Does government social media promote users' information security behavior towards COVID-19 scams? Cultivation effects and protective motivations," *Government Inf. Quart.*, vol. 38, no. 2, Apr. 2021, Art. no. 101572.

[67] H. L. Neumann, L. M. Martinez, and L. F. Martinez, "Sustainability efforts in the fast fashion industry: Consumer perception, trust and purchase intention," *Sustainability Accounting, Manage. Policy J.*, vol. 12, no. 3, pp. 571–590, May 2021.

[68] M. Harrigan, K. Feddema, S. Wang, P. Harrigan, and E. Diot, "How trust leads to online purchase intention founded in perceived usefulness and peer communication," *J. Consum. Behaviour*, vol. 20, no. 5, pp. 1297–1312, Sep. 2021.

[69] Y. Chang, X. Dong, and W. Sun, "Influence of characteristics of the Internet of Things on consumer purchase intention," *Social Behav. Personality, Int. J.*, vol. 42, no. 2, pp. 321–330, Mar. 2014.

[70] A. D. Jurcut, P. Ranaweera, and L. Xu, "Introduction to IoT security," in *IoT Security: Advances in Authentication*, 2020, pp. 27–64.

[71] N. Koester, P. Cichy, D. Antons, and T. O. Salge, "Perceived privacy risk in the Internet of Things: Determinants, consequences, and contingencies in the case of connected cars," *Electron. Markets*, vol. 32, no. 4, pp. 2333–2355, Dec. 2022.

[72] G. Mortimer, S. M. Fazal-e-Hasan, M. Grimmer, and L. Grimmer, "Explaining the impact of consumer religiosity, perceived risk and moral potency on purchase intentions," *J. Retailing Consum. Services*, vol. 55, Jul. 2020, Art. no. 102115.

SOONBEOM KWON received the M.S. degree from the Interdisciplinary Graduate Program, IT Law, Dankook University, South Korea. He is currently pursuing the Ph.D. degree with the Department of Science and Technology Policy Convergence, Dankook University. He has been involved in various research projects and published article related to industrial security topics, such as smart car security certification systems and information privacy. His research interests include industrial security, smart car security, and digital forensic. He also won a number of awards at academic conferences and research paper contests.

HWANSOO LEE (Member, IEEE) received the Ph.D. degree in business and technology management from Korea Advanced Institute of Science and Technology (KAIST), South Korea. He is currently an Associate Professor with the Department of Industrial Security, Dankook University, South Korea. He has experience with information systems as a Developer and a System Analyst. His research interests include industrial security and information privacy, electronic commerce, and enterprise information systems. His research has appeared in journals, such as *Government Information Quarterly*, *Information & Management*, *Computers in Human Behavior*, *Behavior & Information Technology*, *Industrial Management and Data Systems*, *Information Systems and e-Business Management*, *Journal of Global Information Management*, and *Telematics and Informatics*. He has received best paper awards at various international and domestic conferences. He is also serving as an Editorial Review Board Member for *Industrial Management and Data Systems* and *Journal of Computer Information Systems*.