Article

The Intention of Passengers towards Repeat Use of Biometric Security for Sustainable Airport Management

Cheong Kim [1,2], Kun Chang Lee [1,3,*] and Francis Joseph Costello [1]

[1] SKK Business School, Sungkyunkwan University, Seoul 03063, Korea; saga@g.skku.edu (C.K.);
     f.costello@g.skku.edu (F.J.C.)
[2] Predictive Analytics and Data Science, Economics Department, Airports Council International (ACI) World,
     Montreal, QC H4Z 1G8, Canada
[3] Samsung Advanced Institute for Health Sciences & Technology (SAIHST), Sungkyunkwan University,
     Seoul 03063, Korea
*   Correspondence: kunchanglee@gmail.com

check for
updates

Abstract: More and more these days, airport security is having to adapt to a greater number of passengers while keeping within finer margins of precision when it comes to clearing passengers for security clearance. Therefore, analyzing potential upgrades in the security process and adopting them in a way that does not impact passenger experience has become a key activity for airport managers. One viable technological solution that is not only effective but also efficient is biometric security. This technology allows for passengers to safely clear security based on their unique biometric features. Despite its promise, airports and passengers alike are slow to adopt its use. Additionally, there were few studies that revealed insights into passengers' intentions toward repeat use of biometric security. Hence, in our novel attempts to uncover the underlying reasons, we implemented a study on passengers' initial and repeat usage intention based on perceived benefits and risks of biometric security technology. Based on 327 survey responses, we employed the use of SEM to extract first- and second-order constructs before evaluating our hypotheses on a finally accepted model. To be aligned with the novel attempt of this research, the results showed that both the perceived benefits and risks have a significant impact on passenger's initial and repeat use intention of biometric security. Therefore, for all practitioners engaged in sustainable airport management, strong consideration from this research should help in creating value for passengers while mitigating the risks of adopting biometric security within airport security settings.

Keywords: biometrics; perceived risk; perceived benefit; passenger intention; repeat use; sustainable airport management

1. Introduction

There has not been a dramatic change in aviation security since the late 1990s when walk-through metal detectors (WTMDs) and X-ray machines were introduced in the 1970s [1–3]. Nevertheless, 9/11 in 2001 brought the requirements for more robust and enhanced security procedures. From the perspective of sustainable airport management, this novel and severe security risk immediately became an evidently critical subject for airports. This was because even a single aviation security accident would have the effect of ceasing an entire terminals' operation and cause a potential safety threat to passengers. Therefore, this firm concept of rigorous aviation security is now an inexorable factor for airport authorities across the globe as they attempt to cope with risks from many perspectives, including terrorism [4,5]. An overarching philosophy of sustainable airport management with the

rigorous aviation security could provide not only the acquisition of adequate investment on the security infrastructure from the perspective of airport operators, but also convey the fundamental basis of competitiveness to airlines by establishing safety conditions for operating aircraft with confidence.

Meanwhile, the Airports Council International (ACI) forecasted global passenger traffic would increase more than double compared to 2018 (8.7 billion), reaching approximately 19.5 billion by 2040, including 8.9 billion and 10.6 billion for domestic and international passenger traffic, respectively [6]. However, such dramatic growth in passenger traffic has the potential negative influence in the context of aviation security that would also unenthusiastically affect sustainable airport management due to the higher possibility of loophole creation in aviation security. The security agents might need to deal with more inspections than they were supposed to do, and this overwhelming workload could be the cause of loopholes in aviation security due to the constrained attention of security agents to the inspections. However, there would be a limited resource of labor who would perform screening operations unless airports decided to increase the investment in human resources greatly. Additionally, maintaining a standard of excellence for all passenger facilitation can be dented by increased standby time, leading to the less sustainable management of airport operation [5].

Consequently, global airports have been pressing ahead with the adoption of cutting-edge applications like biometrics in order to bolster aviation security and bring upgraded passenger facilitation for sustainable terminal management [7,8]. In particular, biometric security has been found progressively more pertinent because it can guarantee accurate and convenient services at the same time, such as the identification stage [7,9].

In order to enhance both passenger facilitation and aviation security for sustainable airport management, to successfully implement provocative technologies such as biometrics, management depends on not only system operators, such as airport managers, but also on passengers' intention to use provocative technologies such as biometrics. For example, other information systems for acquiring sustainable management with operational efficiencies, such as enterprise resource planning (ERP), mostly depend on endogenous willingness to meet the goal. However, the success of biometric security adoption at airports depends on how likely passengers are willing to use. It cannot be assumed that passengers will frequently use the technology just because the technology shows cutting-edge features. A lack of intention by users could present a significant challenge to the successful implementation of a novel information system [10–12], and this unfortunate trial would bring failure in the successful establishment of sustainable operation management.

Then, what are the conceivable factors that induce passengers to possess or refuse the intention to use such innovative technologies at airports like biometric security gates? We have paid great attention to the perceived benefits [13] and risks [14–16] in this research as factors that might be related to the implementation of biometric security. Rogers [13] suggested that perceived benefits could be an important factor affecting the spread of innovation; on the other hand, Stone and Grønhaug [14], Featherman and Pavlou [15], and Garner [16] argued that the perceived risks might act as a role for consumers to become reluctant to accept the use of an innovation. Henceforth, if it is possible to maximize perceived benefits and minimize perceived risks at the time, it would be feasible for airport operators to elicit both enhanced aviation security as well as passenger facilitation for promising sustainable airport management. Besides, the impression from the initial trial of users might also strongly motivate the repeat use of the technology [17–19]. In this case, perceived benefits and perceived risks could act as a mediator between initial use and repeat use intention. In other words, if passengers perceive a satisfying experience, alongside perceived benefits, from using biometric security, they would more likely try the service again. However, if the first experience from biometric security is somewhat unsatisfactory, then there would be a higher possibility for passengers to not retry it.

Accordingly, this paper emphasized the probable cause of success and failure factors that might influence passengers' repeat use intentions of biometric security, such as the perceived benefits, perceived risks, and initial use intention. Most previous studies on users' use intention of biometrics dealt with ease of use and usefulness [20,21], and other prior research approached the issue from the

perspectives of innovation and security [22]. However, not many studies have attempted to analyze the problem from a diverse perspective, including the potential influence of perceived benefits, perceived risks, and initial use intention at the same time. Since biometric security procedures essentially require passenger's participation, discovering the role of such perception of passengers in these factors would be beneficial not only to the field of innovation research but also to practitioners in the field of airport management. Furthermore, it would also be fruitful to present implications in this paper for sustainable airport management by providing practical resolutions that could be applied to ensure rigorous aviation security as well as passenger facilitation by adequately implementing biometric security at airports.

The rest of the research is organized as follows. Chapter 2 of this paper describes the theoretical background, hypotheses, and research model. Next, chapter 3 presents the research methods used herein to gather and analyze the data, while Chapter 4 contains the analysis results of the dataset. Chapter 5 provides theoretical and practical implications derived from the results obtained and suggests limitations and future research to be performed subsequently.

2. Theoretical Background and Hypotheses

2.1. Aviation Security and Biometrics for Sustainable Airport Management

Aviation security was first developed at the initiative of the International Civil Aviation Organization (ICAO) and the International Air Transport Association (IATA) in the aftermath of a series of hijacking incidents in the late 1960s following the first ever hijacking incident in 1931 [23]. Security screening became a global standard for all passengers and carry-on baggage from the 1970s [24], and a security screening system consisting of door-shaped metal detector and X-ray machine became the norm in 1978 and persisted with little change till the 1990s [1,2]. Then, after the outbreaks of the Air India bombing attack in 1985 and the Pan Am bombing incident in 1988, a new step to match all boarding passengers, including transfer passengers to onboard baggage, was added to the aviation security regulations to prevent bombing attempts using baggage [25].

Next, aviation security regulations and regimes were increasingly strengthened around the world after the 9/11 attack in 2001 [8,26,27]. The ICAO amended Annex 17 to the Convention on International Civil Aviation to require domestic airports to comply with the same security standards as applicable to international airports as much as possible [24]. The United States founded the Transportation Security Administration (TSA) and transferred the aviation security screening authority from civilian airlines to the government in order to adopt a stricter security screening regime. The TSA required all airports in the world that operate US origin airlines to put in place a robust security screening regime, including the police involvement [28,29]. Additionally, security devices must execute performance upgrades every five years in a bid to keep the security equipment up to date. The United Kingdom also put in place tighter security measures and strengthened the security screening of passengers and baggage [30]. In addition to these activities, Switzerland, Sweden, and Denmark revamped the distribution of aviation security responsibilities; Japan required airlines to share security screening responsibilities, and the Chinese government increased onboard facility requirements and security personnel training programs [24].

Afterward, aviation security measures were improved with the extra strictness in response to new and emerging terror attack attempts [31], which further compounded airport operations in combination with the continued growth of the number of airline passengers. Complicated aviation security measures result in more significant inconvenience, privacy infringement, and standby time on the part of passengers [5]. With the greater tightening of aviation security, the aviation industry now faces increased challenges. Some include the reduction of security screening time and passenger waiting time, protection of passenger privacy during the security screening process, better work conditions for security agents, and enhanced security screening steps to eliminate human errors.

Security screening time and passenger waiting time must be reduced to help bolster passenger convenience and the operational efficiency of the aviation security process for sustainable airport management. Unlike buses or trains, whereby passengers can readily hop on as long as they present tickets, air flight requires a range of cumbersome steps before boarding. For example, international flight passengers are recommended to arrive at airports at least two hours in advance because they need to go through check-in, baggage drop, security screening with their documents all before boarding [27]. From the perspective of aviation security, identification documents review and security screening are the most stressful scene for passengers, and the highest portion of passengers show negative responses to such steps within the boarding process [32]. Potential solutions to address the continued growth of passenger volume to be accommodated by passenger terminals with limited space can include more advanced automated systems. Therefore, as a novel resolution of these requests from the aviation industry that requires the provision of both increased security level and passenger facilitation, biometric technologies have recently been in the limelight.

Biometrics refers to an "application that digitally processes an individual's unique biological features" [33]. Unique biological features, including physical characteristics such as fingerprint, iris, and facial image and behavioral traits such as voice, gait, and handwriting, can be used in identifying individuals. Biological features need to be universal, unique, permanent, and collectible if they are to be used for applications [34]. As biometrics analyzes biological data, it is easier to use than other authentication methods such as travel documents. This is because they do not need to always be carried by a passenger, are less likely to be lost, stolen, or reproduced. This unique advantage of biometrics ensures enhanced security requirements that the aviation industry has been needing for a while [34]. Likewise, if security procedures at airports could be replaced with biometric technologies that do not need human agents for passenger identification, then passenger queues can be shortened with dramatically enhanced operational efficiency. Therefore, biometric technologies are emerging as a solution that could improve both aviation security and passenger experience at the same time, with brilliant accuracy and convenience [35].

Passengers' perceived benefits attainable from biometrics applications used in the aviation security discipline are as follows. First, since automated gates are not operated by security personnel, several security lanes can be installed in parallel to reduce processing time, while improving the operational efficiency of airports. Additionally, as sophisticated systems perform authentication, the accuracy of the procedure can be enhanced with fewer human errors that are directly associated with the level of aviation security. These benefits of biometric security are quite distinct from the perspective of airport operators. Henceforth, several airports in the world are rushing to embed biometric technologies into their security systems to reserve sustainable airport management. Although biometrics as a concept is fairly old and early installations occurred some time ago, the majority of airports are still in the early stages of introduction, meaning more research is needed to understand how to induce passengers to use the biometric security. Therefore, studies that focus on the factors that might influence passengers' use intention of biometric security has valid grounds for research from the perspective of airport operators.

2.2. Perceived Risk and Passengers' Use Intention

The perceived risk could occur when users are uncertain about the outcome of their decision to purchase products or use services [36]. Bauer [36] distinguished perceived risks from objective risks and probabilistic risks and also claimed that although other risks exist in reality, consumers might respond only to subjectively perceived risks. In other words, perceived risks could be recognized by consumers when they decide to fulfill their goal of purchase. Besides, Garner [16] argued that perceived risk has six types—functional, temporal, financial, physical, social, and psychological risk—from the perspective of consumers' intention of using services.

First, the temporal risk is the concern about an unnecessary waste of time that might occur from adopting the innovation. Social risk refers to the adoption of innovative products or services that might give a negative impression to other members of society. Financial risk is the idea of causing

economic losses. Furthermore, physical risk reflects the use of an innovative product or a service that might harm their being, inflicting injuries. Lastly, Functional risk reflects concerns about whether the functions of the innovative product or service will work properly.

Previous researchers cited perceived risk in the diverse field as a significant element that influences consumers' intention of purchasing products or using services, such as information technology [37–39], health [40,41], tourism [42–44], marketing [45,46], and policies [47,48]. Notably, Ariffin et al. [49] articulated that temporal risk (i.e., when the products do not meet the consumers' satisfaction, they need to spend time to return it) and social risk (i.e., loss on the social image over the online purchase) made consumers hesitate to use online purchasing. Lee [50] suggested that perceived risks, such as time risk (i.e., the delay caused by a slow website), social risk (i.e., disapproval of an individuals' relationship), and functional risk (i.e., malfunctions of online banking websites) significantly influence users' initial and repeat intention for internet banking use. Additionally, Copeland et al. [51] argued that physical risk, one of the components of perceived risk, of e-cigarettes (i.e., harm in the e-cigarette) that was compared to traditional cigarettes as a negative factor that influences college students' initial and repeatable use of e-cigarettes. Likewise, Cho et al. [52] suggested that functional risk and physical risk were significantly damaging to users that have the intention to initially and repeatedly use air for travel.

As these researchers suggested, we also presumed that perceived risks could be essential components to dissuade passengers from intending to use biometric security that would be directly connected to the unsuccessful implementation of the system. Therefore, in this research, we have adopted the temporal risk, social risk, physical risk, and functional risk as items for the perceived risk construct to discover the relationship with passengers' use/repeat use intention of biometric security at airports. First, the temporal risk was used, considering that it might take longer when passengers use biometric security than traditional procedures such as walk-through metal detectors (WTMDs) and X-ray machines. Second, the functional risk and physical risk were adopted because passengers might be worried that the biometric devices could be in malfunction and injure parts of their bodies. Furthermore, the social risk was also embraced as a factor that negatively influences passengers' first use and repeatable use intention of biometric security because biometric security services can produce users' misapprehensive images to other society members. The above four perceived risk variants were expected to have a negative influence on passengers' initial use intention and repeat use intention of biometric security that may arise during the implementation of the service. Additionally, being unable to mitigate perceived risk elements could lead to the demise of the biometric security system, thus posing a greater challenge on the long-term sustainability of airport management. Based on this discussion, we propose:

Hypothesis 1. *Perceived risk influences passengers' initial use intention of biometric security negatively.*

Hypothesis 2. *Perceived risk influences passengers' repeat use intention of biometric security negatively.*

2.3. Perceived Benefit and Passengers' Use Intention

The 'Diffusion of Innovation' theory from Rogers [13] has been cited in various fields that are related to innovation, such as information technology [53,54], education [55,56], media studies [57–59], organizational studies [60–62], marketing [63,64], policies [65–67]. 'Diffusion of Innovation' theory suggested that perceived benefits such as relative advantage, compatibility, trialability, complexity, and observability have an important influence on the adoption of innovation [13].

Relative advantage is about how much benefit an innovative product/service provides to the user compared to the existing products/services. Compatibility refers to whether the innovation fits the values of the consumers' society, or does it fit the personal experience of the consumer. Trialability is about getting more used to the innovation or easing anxiety through pilot use of the product or service. Complexity explains about the difficulty of using innovative products or services. Finally,

observability is considering the degree of visible effect that will appear from the consumers who use innovative technologies or services.

Prior studies in the field of innovation implementation pointed out that perceived benefit is a crucial component for users to attempt initial and repeat use of novel technologies. For example, Lee [50] suggested that perceived benefits, such as relative advantage (i.e., faster speed and increased transparency) and compatibility (i.e., internet banking provides most of the services that traditional banking methods provide), significantly influence consumers' initial intention of internet banking adoption. Additionally, Copeland, Peltier and Waldo [51] argued, the use of relative advantage -one of the components of perceived benefit- within e-cigarettes was used to compare them with traditional cigarettes to create a positive factor that influenced college students' initial and repeat use. Furthermore, Islam [68] indicated that perceived benefits (i.e., relative advantage and compatibility) from e-learning systems compared to the traditional educational approach were both contributing factors to inducing users to have initial and repeat use of e-learning systems. Likewise, Lee and Cho [69] suggested that trialability was significantly helpful for users to have the intention to initially and repeatedly use social media in a mobile broadband environment.

As this research argued, we also believe that perceived benefits could be a vital factor in inducing passengers to use biometric security that would be directly connected to the successful implementation of the system. Hence, in this study, we adopted the relative advantage, compatibility, and trialability as items for the passengers' perceived benefit construct to discover the relationship with passengers' use/repeat use intention of biometric security at airports. First, the relative advantage was used, considering that it is easy to compare the benefits of biometric security with the existing security method such as walk-through metal detectors (WTMDs) and X-ray machines. Second, compatibility was adopted because it was essential to decide if the usage of a new service (biometric security) fits passengers' needs with the existing values and experience formed by the current security procedure. Furthermore, trialability was also embraced as a factor that influences passengers' initial use and repeatable use intention of biometric security because biometric security services can be provided for a test-run before the airports decide to implement the system in earnest. The above three perceived benefit variants were expected to have a positive influence on passengers' initial use intention and repeat use intention of biometric security that may arise during the implementation of the service. Additionally, retaining these perceived benefit components would convey the successful application of biometric security for sustainable airport management. Henceforth, we propose the following hypotheses:

Hypothesis 3. *Perceived benefit influences passengers' initial use intention of biometric security positively.*

Hypothesis 4. *Perceived benefit influences passengers' repeat use intention of biometric security positively.*

2.4. Initial Use and Repeat Use

The importance of the initial impression cannot be overemphasized. In psychology, the initial impression is the event when an individual firstly confronts someone or something and shapes a perceptual persona of it [70]. In the context of service provider-user, the initial impression could be formed by several factors, such as passengers' perceived benefits and perceived risks [50]. Based on the case of biometric security at airports, passengers could either positively or negatively be impressed from initial use that could be formed from what they have recognized, such as perceived risks and perceived benefits, during the trial.

This initial experience of usage could also be influential in the next use. King et al. [71] articulated that the initial impressions (i.e., the design concept of websites) that users form have a strong influence on users' want to return and repeatably use the website. Additionally, King et al. [72] suggested that identification from the creation of a retailers' website (i.e., written, audio, and video content) during the first visit experience of users has a significant influence on the repeat visit and purchase intention.

With respect to prior research, we posit that passengers' initial use of biometrics might affect their repeat use intention. For example, if passengers' experience of initial biometric security procedures were not satisfying, then they would be reluctant to use it again. On the other hand, if passengers agreed that the initial use of biometric security was beneficial to them, there would be a higher possibility for them to reuse it. Meanwhile, the repeat use intention of biometric security could be considered as a lifeline for the successful implementation of the service because there would be a critical waste of time and budget if passengers did not repeatedly use it. Of course, this failure in biometric security implementation caused by underutilization would also damage sustainable airport management as a new solution would need to be found potentially hindering a good service as passenger numbers increase. Therefore, it is articulated that the repeat use intention of passengers must be secured when airports consider implementing biometric security procedures at terminals. Hence, we propose the following hypothesis:

Hypothesis 5. *Initial use intention influences passengers' repeat use intention of biometric security positively.*

In this study, we formulated the model to consider a mediation effect from perceived risk and perceived benefit on passengers' repeat use intention of biometric security. This was viewed through passengers' initial use intention of biometric security to reveal the indirect impact of the research model. In addition to the mediating effect, the research model also adopted four control variables: age, gender, education, and monthly income, to avoid plausible illegitimate effects.

2.5. Research Model

The following constructs were formulated based on the hypotheses that we derived from the theoretical background. In the context of biometric security implementation for sustainable airport management, we suggest that perceived risk (PR) and perceived benefit (PB) act as antecedents of initial use intention (IUI) and repeat use intention (RUI). Note that two formative endogenous second-order constructs were used: PR was formed with temporal risk (TI), social risk (SO), physical risk (PH), and functional risk (FU); PB was formed with relative advantage (RA), compatibility (CO), and trialability (TR). Figure 1 depicts the proposed research model of this study.
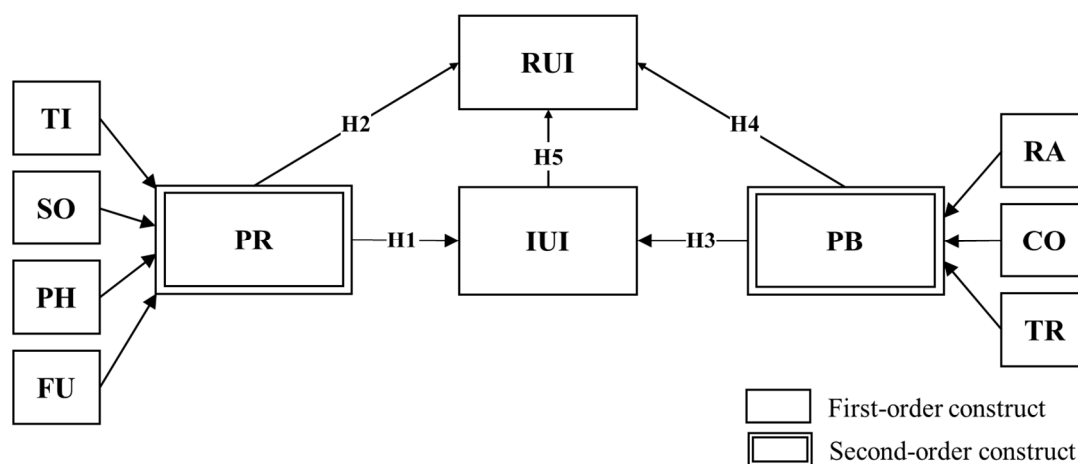

Figure 1. Research Model.

3. Research Method

3.1. Sampling & Surveying

A survey was conducted on 362 panelists from an online research agency in the Republic of Korea from September 7 to 15, 2019. The survey respondents were limited to adults aged 20 years or older who had air flight experience. With insincere responses and missing values excluded, a statistical

analysis was performed on 327 responses in total as valid samples. The demographic properties of the participants are shown in Table 1.

Table 1. Demographic properties.

Variables		Frequency	%
Gender	Female	163	49.8%
	Male	164	50.2%
Age	20s	78	23.8%
	30s	84	25.7%
	40s	80	24.5%
	50s~	85	26.0%
Education	~High School	84	25.7%
	Undergraduate	225	68.8%
	Postgraduate	18	5.5%
Monthly Income (KRW)	~2M	48	14.7%
	2M~5M	157	48.0%
	5M~8M	98	30.0%
	8M~	24	7.3%

3.2. Survey Questions

This study measures variables, using measurement tools proven to be reliable and valid in prior studies. All the survey questions were adapted from previous research and modified to be consistent with the context of biometric security. Additionally, the survey participants were provided with information on biometric security in advance and requested to answer the questions based on their direct and indirect experience of the service. Except for demographic survey questions, the construct items were measured with a seven-point Likert scale that ranged from "strongly disagree (1)" to "strongly agree (7)." The mean and standard deviation values of the constructs, as well as the literature where the scales were adopted from, are shown in Table 2.

Table 2. Survey Questions.

Type (the Number of Questions)		Avg. (SD)	Question	Source
Perceived Risk	Temporal Risk (3)	3.27 (0.876)	It will take too much time to learn how to use biometric security.	Stone and Grønhaug [14]
		3.40 (0.897)	If I use biometric security, I think it will require more unnecessary procedures. It will take more time.	
		3.33 (0.883)	I think I will waste even more time since I have to learn how to use biometric security.	
	Social Risk (3)	3.44 (0.866)	Using biometric security will have a negative impact on my perception/reputation.	Featherman and Pavlou [15]
		3.80 (0.891)	If I use biometric security, I'm sure that other people will find me strange.	
		3.12 (0.956)	I'll use biometric security after seeing other people using it without going through any trouble.	

Table 2. *Cont.*

Type (the Number of Questions)		Avg. (SD)	Question	Source
Physical Risk (3)		3.41 (0.932)	I am concerned about the physical fatigue caused by the use of biometric security.	Stone and Grønhaug [14]
		3.25 (0.970)	I'm worried that biometric security might cause physical discomfort or other physical side effects.	
		2.94 (0.962)	Since biometric security has yet to be verified as safe, I am concerned about the physical risks using the system.	
Functional Risk (3)		2.52 (0.909)	I'm not sure whether the biometric security system will work as well as it is said.	
		2.86 (0.868)	I'm not sure if biometric security will provide me with as much convenience and benefits as I'd expect.	
		2.86 (0.877)	I'm not sure if the speed and convenience offered by biometric security will be practical enough.	
Perceived Benefits	Relative Advantage (3)	2.45 (0.845)	Biometric security will be more interesting compared to the conventional boarding system.	Rogers [13]
		2.59 (1.014)	If I use biometric security, other people will think of me as being smart.	
		2.68 (0.971)	The use of biometric security will require less work from my side compared to the conventional boarding procedure.	
	Compatibility (3)	3.03 (0.748)	Using biometric security is in line with my values.	
		3.17 (0.864)	Biometric security is not much different from the conventional boarding system.	
		2.69 (0.770)	Introducing the biometric security procedure to the current boarding system is not a big problem.	
	Trialability (3)	2.41 (0.781)	If I could try biometric security right now, I think it would make me more open to the idea of using it in the future.	
		2.42 (0.847)	If airlines or airports hold events about using biometric security, it would definitely motivate me to use the system in the future.	
		2.28 (0.796)	If there are more types of biometric security in the future, it would be helpful for us to use the system with ease.	
Initial Use Intention (3)		2.60 (0.869)	I would use biometric security for my airport security procedure.	Lee [50]
		2.77 (0.807)	Using biometric security for dealing with my airport security procedures is something I would do.	
		2.65 (0.808)	I would see myself using biometric security for dealing with my airport security procedure.	
Repeat Use Intention (3)		2.35 (0.893)	I plan to continue using biometric security for airport security procedures.	Chiu, Wang, Fang and Huang [18]
		2.39 (0.865)	I consider biometric security to be my first choice for airport security procedures in the future.	
		2.26 (0.830)	It is likely that I will continue using biometric security in the future.	

3.3. Measures

The research model of this study was analyzed using SmartPLS 3.0, which has been widely used to verify the results of structural equation models [73–79]. Partial least square (PLS) is an adequate

methodological approach to discover relationships between constructs based on the analysis results [80]. The general mathematical equation to explain PLS is:

$$X = TP^T + E \tag{1}$$

$$Y = UQ^T + F \tag{2}$$

where *X* is predictors and *Y* is responses; *T* is projections of *X* and *Y*; *U* is projections of *P* and *Q*, *E* and *F* are errors, presumed to be impartial and indistinguishably dispersed random normal variables [81]. *X* and *Y* would be decomposed to acquire the greatest covariance between *T* and *U* [81].

We implemented two formative second-order constructs: perceived risk, with four dimensions (temporal risk, social risk, physical risk, and functional risk), and perceived benefit, with three dimensions (relative advantage, compatibility, and trialability). The repeated indicator approach was applied to these formative second-order constructs [82]. Furthermore, the analysis used latent variable scores (LVS) in order to experiment with the final research model [83–85]. The flooding-out effect could appear when second-order formative constructs are adopted because of repeated indicators. However, the research model in this paper could appropriately predict second-order formative constructs without any flooding-out influence by implementing this two-stage approach [85].

4. Results

Before the primary analysis, the one-factor analysis was applied to tackle common method bias [86] because all the data samples were self-reported. The test result discovered that the most significant percentage that the factor explained was 29.8% of the variance that is smaller than 50%. Henceforth, the substantial impact in common method bias did not occur in the sample [86–88].

4.1. Assessing the First-Order Constructs

First of all, the validity and reliability of the first-order constructs were evaluated. The Cronbach's Alpha index is widely used to measure the reliability of constructs, and if the index was over 0.600, the construct could be determined as acceptable; otherwise, the constructs should be reformulated, for example, excluding one or more items in the construct [89]. As presented in Table 3, Cronbach's *α* showed the inner consistency of the research model, ranged from 0.726 to 0.885 [89]. In addition to Cronbach's *α* validation, composite reliability scores ranged from 0.811 to 0.962, and the average variance extracted (AVE) [80], ranged from 0.644 to 0.813 were also evaluated in order to establish the convergent validity of the construct level. The results in Table 3 show that the variance obtained are all greater than 0.5 [90].

Table 3. Reliability and Validity of the First-order Constructs.

Construct		Cronbach's *α*	Composite Reliability	AVE
PR	TI	0.800	0.882	0.714
	SO	0.762	0.863	0.679
	PH	0.828	0.897	0.745
	FU	0.781	0.873	0.697
PB	RA	0.763	0.863	0.68
	CO	0.726	0.844	0.644
	TR	0.810	0.887	0.724
IUI		0.775	0.868	0.689
RUI		0.885	0.929	0.813

Then, the Fornell-Larcker criterion was used to evaluate discriminant validity for the first-order constructs. The Fornell-Larcker criterion using average variance extracted (AVE) is a widely used statistical standard, and AVE could be derived by using the amount of variance captured among

constructs with measurement errors [80]. Hence, the AVE square root of each construct should be more significant than the correlations between constructs under the diagonal line [80]. The analysis results showed, as indicated in Table 4, confirming discriminant validity between the constructs [80].

Table 4. Discriminant Validity.

Construct		TI	SO	PH	FU	RA	CO	TR	IUI	RUI
	TI	0.845								
PR	SO	0.600	0.824							
	PH	0.453	0.541	0.863						
	FU	0.346	0.331	0.430	0.835					
	RA	−0.119	−0.262	−0.151	−0.089	0.825				
PB	CO	−0.111	−0.275	−0.198	−0.243	0.290	0.803			
	TR	−0.253	−0.447	−0.301	0.346	0.475	0.450	0.851		
IUI		−0.351	−0.543	−0.485	−0.332	0.397	0.392	0.463	0.830	
RUI		−0.486	−0.611	−0.532	−0.277	0.352	0.289	0.672	0.672	0.902

4.2. Assessing the Second-Order Constructs

Next, we verified the significance of the second-order formative constructs (PR and PB) using a bootstrap analysis with 1000 samples to evaluate the upward dimensional effects, as Marakas, Johnson and Clay [83] suggested. The results indicated that every first-order construct (TI, SO, PH, FU, RA, CO, and TR) that was included in the second-order formative constructs (PR and PB) are substantial with significant *t*-values, as presented in Table 5.

Table 5. Dimension Effect for the Second-order Formative Constructs.

Construct		Original β	Mean β	STDEV	*t*-Value	*p*-Value
	TI → PR	0.335	0.332	0.022	15.490	0.000
PR	SO → PR	0.390	0.395	0.027	14.684	0.000
	PH → PR	0.355	0.353	0.020	18.098	0.000
	FU → PR	0.265	0.264	0.018	14.640	0.000
	RA → PB	0.422	0.421	0.031	13.715	0.000
PB	CO → PB	0.423	0.421	0.031	13.829	0.000
	TR → PB	0.559	0.560	0.041	13.590	0.000

Next, as Marakas, Johnson and Clay [83], and Loch, Straub and Kamel [84] recommend, latent variable scores for the highest-level constructs were formulated to form the final structural equation model after we had validated the second-order constructs' dimension effect. After the formation of the final model, as presented in Figure 2, we evaluated discriminant validity using the heterotrait–monotrait (HTMT) ratio. Table 6 proved that the results of the HTMT ratio evaluation were smaller than 1.00 for discriminant validity as a recommended criteria [91].
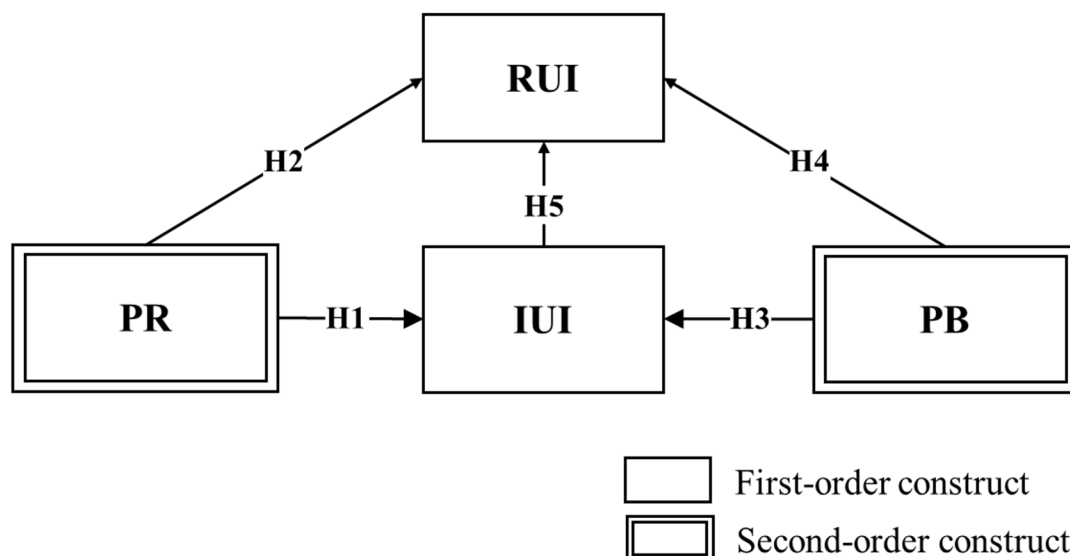
Figure 2. The Final Research Model.

Table 6. Heterotrait-Monotrait (HTMT) Ratio for Discriminant Validity.

Construct	PR	PB	IUI	RUI
PR				
PB	0.377			
IUI	0.570	0.539		
RUI	0.642	0.529	0.672	

4.3. Assessing the Final Research Model

In connection with biometric security in the departure hall, hypothesis 1 found that perceived risks significantly negatively influence the passengers' initial use intention of biometric security ($\beta = -0.428$, $p < 0.000$). In addition to the test result of hypothesis 1, the test result of hypothesis 2 also indicated that perceived risks significantly negatively impact on the passengers' repeat use intention of biometric security ($\beta = -0.363$, $p < 0.000$). These two results imply that perceived risks such as temporal, social, physical, and functional risk behave as psychological barriers that prevent passengers from using biometric security procedures.

On the other hand, the perceived benefits indicted the complete opposite result than that of the perceived risks. In the context of biometric security use by passengers, hypothesis 3 found that perceived benefit influences the initial use intention of passengers positively ($\beta = 0.377$, $p < 0.000$). Likewise, the test result of hypothesis 4 presented that perceived benefits also have a significant positive effect on passengers' repeat use intention of biometric security ($\beta = 0.200$, $p < 0.001$). These results suggest that perceived benefits have a somewhat strong influence on inducing passengers to use biometric security in the context of airport security procedures.

Meanwhile, passengers' initial use intention of biometric security has a significantly positive influence on the repeat use intention, according to the test result of hypothesis 5 ($\beta = 0.357$, $p < 0.000$). This result implies that how passengers embrace the initial use of biometric security affects the next usage intention. In other words, if passengers thought that the biometric identification stage in the airport was beneficial and relevant to them from the first use, there would be a higher possibility for them to use it repeatedly. Figure 3 and Table 7 below summarize the results of the structural equation model analysis and hypotheses tests.
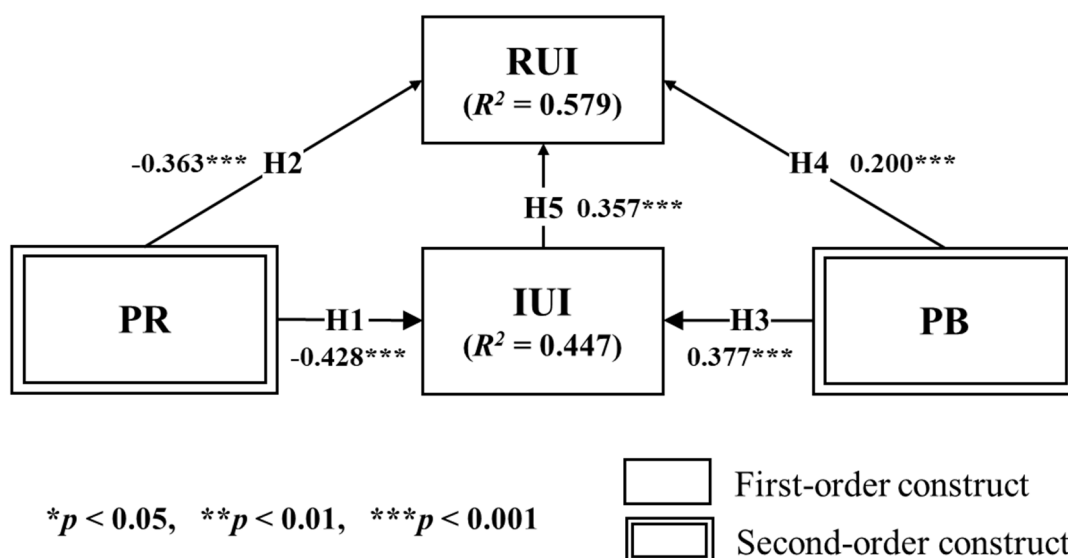
Figure 3. Results of PLS-SEM Hypothesis Testing on the Final Research Model.

Table 7. Overall Results of Hypotheses Tests.

	Hypothesis	Results
H1	Perceived risk influences passengers' initial use intention of biometric security negatively.	Accepted
H2	Perceived risk influences passengers' repeat use intention of biometric security negatively.	Accepted
H3	Perceived benefit influences passengers' initial use intention of biometric security positively.	Accepted
H4	Perceived benefit influences passengers' repeat use intention of biometric security positively.	Accepted
H5	Initial use intention influences passengers' repeat use intention of biometric security positively	Accepted

Furthermore, according to the results of the mediation effect analysis, there were significant mediation effects for both PR → IUI → RUI ($\beta = -0.154$, $p < 0.000$) and PB → IUI → RUI ($\beta = 0.136$, $p < 0.000$), respectively. On the other hand, there was no significant effect of the four control variables, such as age, gender, education, and monthly income at $p < 0.05$.

5. Conclusions

5.1. Discussion and Implications

In this study, we discovered about the relationship between perceived risk, perceived benefit, initial use intention, and repeat use intention of biometric security procedures at airports. The fundamental overarching philosophy of implementing biometric security technology is to acquire both enhanced aviation security and passenger facilitation for sustainable airport management. However, there still exist some field practitioners at airports who just would like to adopt the innovative technology to follow the trend or to keep up with the competition with market-leading airports without a profound understanding of passengers' insight. This unconcerned attitude of airport operators could harm not only the successful adoption of the service but also sustainable airport management. Therefore, this research raised the alarm over such unconcerned attitudes by providing fruitful discussion for airport operators by building an appropriate implementation strategy of biometric security procedures.

The following practical implications were derived to facilitate the deployment of biometric technologies by airport operators. As both passengers' perceived benefits and perceived risks are found to have significant impacts on passenger's initial and repeat use intention of biometrics security,

practitioners at airports should consider this fact for creating value and mitigating the risk of using the service. The perceived benefit was revealed as a component that impacts on both passengers' use intentions of biometric security services. Providing the value of products and services to users is one of the essential activities for firms, and this research also discovered a similar finding. For instance, airports could advertise the beneficial points of biometric security processes to passengers, such as not needing to face security agents that would significantly decrease the possibility of disease infection (i.e., COVID-19)

The most important implication of this study was that perceived risk had a relatively more substantial influence on both initial and repeat use intention than perceived benefit. This result emphasized that the field practitioners at airports should make considerable efforts to eliminate risk factors for guiding passengers to use the service without hesitation. For example, as an opposite approach to the perceived benefit, airport operators should relieve passengers' anxiety of disease infection (i.e., COVID-19) by frequently sterilizing biometric security devices, to mitigate passengers' perception of risk factors. Of course, it is crucial to let passengers know that those devices are regularly cleaned using promotional materials. Additionally, providing information about less contact with the security agents as well as probable additional installation of thermal skin temperature for fever detection on the biometric security devices could be articulated to turn passengers' perceived risks into perceived benefits of using biometric security, especially in this COVID-19 pandemic situation.

Furthermore, this study articulated that the first usage experience was also an imperative element for passengers to use biometric security procedures repeatedly. Since passengers do not choose whether to use biometric security before visiting the airport, offering them an enjoyable experience of using biometric security would have advantages in that passengers would not think adversely of the initial trial. Additionally, as the mediation test results showed, this engaging experience would be aligned with passengers' perceptions toward benefits and risks. In other words, if passengers perceived more beneficial aspects than non-beneficial aspects during their initial trial, there would be a positive likelihood for a more lucrative result from the implementation of biometric security technology.

5.2. Limitations & Suggestions for Future Studies

Despite the implications as mentioned above, there still are limitations in this study. Firstly, this research only employed self-reported cross-sectional data samples. The self-reported cross-sectional survey could be hypothetically vulnerable to standard method variance [88]. In order to mitigate the bias, obtaining a longitudinal dataset from the third-party measures might need to be implemented. Likewise, the implication of this research would have potentially more profound generalizability with longitudinal datasets that could be applied to not only airports in Korea but also several airports in the world.

Furthermore, even though biometrics could be applied across the whole spectrum of the boarding process performed at airports from the perspective of enhancing operational efficiency for sustainable airport management [7,92], this study just focused on the security procedure. Biometric technologies could mitigate laborious tasks of presenting identification documents and flight tickets at each of the airport scenes in the same manner as at the security checkpoint. However, as there are other environmental factors presented by operational circumstances in other various areas of the airport, critiques from passengers may be varied and reflected in their intention to use biometric services based on other operational areas of the airport. In other words, there needs to be more research on the implementation of biometric technologies within the entire airport to contribute to acquiring a more sustainable airport management flow through maximizing aviation security and operational efficiency together. Therefore, future studies need to obtain non-cross-sectional data samples and expand the scope of domains compatible with biometric applications in airports. The implementation of biometrics could be broadened from the pre-boarding process to other serviceable areas of the airport, such as check-in, bag-drop, boarding gate operations, departure and arrival identification procedures, and even duty-free shops as a single token service. Henceforth, if future studies consider longitudinal data

samples and a range of compatible applications, more meaningful contributions will be developed that were not derived from this study for more sustainable airport management.

References

1. Lee, J.H. Study on future airport security screening. *Korea Civ. Aviat. Dev. Assoc.* **2012**, *1*, 115–134.
2. Price, J.; Forrest, J. *Practical Aviation Security: Predicting and Preventing Future Threats*; Butterworth-Heinemann: Oxford, UK, 2016.
3. Goo, S. Fliers to be rated for risk level: New system will scrutinize each passenger, assign color code. *The Washington Post*, 9 September 2003; A01.
4. Schwaninger, A. Increasing efficiency in airport security screening. *WIT Trans. Built Environ.* **2005**, *82*, 405–416.
5. Hong, J.; Oh, J.; Lee, H. Smart Airport and Next Generation Security Screening Technology. *Electron. Telecommun. Trends* **2019**, *34*, 73–82.
6. ACI. Annual World Airport Traffic Forecast 2019–2040. Available online: https://aci.aero/wp-content/uploads/2019/10/WATF_2019-2040.pdf (accessed on 3 May 2020).
7. Negri, N.A.R.; Borille, G.M.R.; Falcão, V.A. Acceptance of biometric technology in airport check-in. *J. Air Transp. Manag.* **2019**, *81*, 101720. [CrossRef]
8. Kalakou, S.; Psaraki-Kalouptsidi, V.; Moura, F. Future airport terminals: New technologies promise capacity gains. *J. Air Transp. Manag.* **2015**, *42*, 203–212. [CrossRef]
9. Jain, A.K.; Kumar, A. Biometric recognition: An overview. In *Second Generation Biometrics: The Ethical, Legal and Social Context*; Springer: Berlin, Germany, 2012; pp. 49–79.
10. John, G.D.; Stephen, B.J.; Clayton, L. Making usable, useful, productivity-enhancing computer applications. *Commun. ACM* **1991**, *34*, 74–85.
11. McCarroll, T. What new age. *Time* **1991**, *138*, 44–46.
12. Nickerson, R.S. Why interactive computer systems are sometimes not used by people who might benefit from them. *Int. J. Man-Mach. Stud.* **1981**, *15*, 469–483. [CrossRef]
13. Rogers, E.M. *Diffusion of Innovations*, 5th ed.; Free Press: New York, NY, USA, 2003; p. xxi. 551p.
14. Stone, R.N.; Grønhaug, K. Perceived risk: Further considerations for the marketing discipline. *Eur. J. Mark.* **1993**, *27*, 39–50. [CrossRef]
15. Featherman, M.S.; Pavlou, P.A. Predicting e-services adoption: A perceived risk facets perspective. *Int. J. Hum. -Comput. Stud.* **2003**, *59*, 451–474. [CrossRef]
16. Garner, S.J. Perceived risk and information sources in services purchasing. *Mid-Atl. J. Bus.* **1986**, *24*, 49–58.
17. Raymond, M.A.; Tanner, J.F., Jr. Selling and sales management in action: Maintaining customer relationships in direct sales: Stimulating repeat purchase behavior. *J. Pers. Sell. Sales Manag.* **1994**, *14*, 67–76.
18. Chiu, C.M.; Wang, E.T.; Fang, Y.H.; Huang, H.Y. Understanding customers' repeat purchase intentions in B2C e-commerce: The roles of utilitarian value, hedonic value and perceived risk. *Inf. Syst. J.* **2014**, *24*, 85–114. [CrossRef]
19. Fang, Y.-H.; Chiu, C.-M.; Wang, E.T. Understanding customers' satisfaction and repurchase intentions: An integration of IS success model, trust, and justice. *Internet Res.* **2011**, *21*, 479–503. [CrossRef]
20. James, T.; Pirim, T.; Boswell, K.; Reithel, B.; Barkhi, R. Determining the intention to use biometric devices: An application and extension of the technology acceptance model. *J. Organ. End User Comput. (JOEUC)* **2006**, *18*, 1–24. [CrossRef]
21. Morosan, C. Theoretical and empirical considerations of guests' perceptions of biometric systems in hotels: Extending the technology acceptance model. *J. Hosp. Tour. Res.* **2012**, *36*, 52–84. [CrossRef]

22. Morosan, C. Voluntary Steps toward Air Travel Security: An Examination of Travelers' Attitudes and Intentions to Use Biometric Systems. *J. Travel Res.* **2012**, *51*, 436–450. [CrossRef]

23. Choi, J.T. *Terror, Terrorists & Terrorism*; Dae Young Co.: Seoul, Korea, 1997.

24. Lee, K.S. Review of legal and institutional changes in the global aviation security environment. *J. Aerosp. Ind.* **2010**, *72*, 22–41.

25. Hoffman, B. Aviation Security and Terrorism: An analysis of the potential threat to air cargo integrators. *Terror. Political Violence* **1998**, *10*, 54–69. [CrossRef]

26. Lyon, D. Surveillance, security and social sorting: Emerging research priorities. *Int. Crim. Justice Rev.* **2007**, *17*, 161–170. [CrossRef]

27. Blalock, G.; Kadiyali, V.; Simon, D.H. The impact of post-9/11 airport security measures on the demand for air travel. *J. Law Econ.* **2007**, *50*, 731–755. [CrossRef]

28. Kim, J.W. Risk Management and Strategies in Airport Security Check. *Korea Secur. Sci. Assoc.* **2013**, *34*, 89–113.

29. Kim, J.H. *Improving Aviation Security Equipment Performance Standards and Activating Domestic Development*; The Korea Transport Institute: Sejong City, Korea, 2013.

30. Butcher, L. *Aviation: Security*; House of Commons Library: London, UK, 2011.

31. Wong, S.; Brooks, N. Evolving risk-based security: A review of current issues and emerging trends impacting security screening in the aviation industry. *J. Air Transp. Manag.* **2015**, *48*, 60–64. [CrossRef]

32. SITA. *Passenger IT Trends Survey 2015*; SITA: Brussels, Belgium, 2015.

33. Hopkins, R. An introduction to biometrics and large scale civilian identification. *Int. Rev. Law Comput. Technol.* **1999**, *13*, 337–363. [CrossRef]

34. Prabhakar, S.; Pankanti, S.; Jain, A.K. Biometric recognition: Security and privacy concerns. *IEEE Secur. Priv.* **2003**, *1*, 33–42. [CrossRef]

35. Kim, C.; Costello, F.J.; Lee, K.C. Integrating Qualitative Comparative Analysis and Support Vector Machine Methods to Reduce Passengers' Resistance to Biometric E-Gates for Sustainable Airport Operations. *Sustainability* **2019**, *11*, 5349. [CrossRef]

36. Bauer, R.A. *Consumer Behavior as Risk Taking*; Taylor & Francis: Chicago, IL, USA, 1960; pp. 384–398.

37. Hussain, S.; Ahmed, W.; Jafar, R.M.S.; Rabnawaz, A.; Jianzhou, Y. eWOM source credibility, perceived risk and food product customer's information adoption. *Comput. Hum. Behav.* **2017**, *66*, 96–102. [CrossRef]

38. De Kerviler, G.; Demoulin, N.T.; Zidda, P. Adoption of in-store mobile payment: Are perceived risk and convenience the only drivers? *J. Retail. Consum. Serv.* **2016**, *31*, 334–344. [CrossRef]

39. Roy, S.K.; Balaji, M.; Kesharwani, A.; Sekhon, H. Predicting Internet banking adoption in India: A perceived risk perspective. *J. Strateg. Mark.* **2017**, *25*, 418–438. [CrossRef]

40. Dong, P.; Zhong, C.-B. RETRACTED: Visual Darkness Reduces Perceived Risk of Contagious-Disease Transmission From Interpersonal Interaction. *Psychol. Sci.* **2018**, *29*, 1049–1061. [CrossRef]

41. Butler, K.M.; Rayens, M.K.; Wiggins, A.T.; Rademacher, K.B.; Hahn, E.J. Association of Smoking in the Home with Lung Cancer Worry, Perceived Risk, and Synergistic Risk. *Oncol. Nurs. Forum* **2017**, *44*, E55.

42. Park, S.; Tussyadiah, I.P. Multidimensional facets of perceived risk in mobile travel booking. *J. Travel Res.* **2017**, *56*, 854–867. [CrossRef]

43. Holm, M.R.; Lugosi, P.; Croes, R.R.; Torres, E.N. Risk-tourism, risk-taking and subjective well-being: A review and synthesis. *Tour. Manag.* **2017**, *63*, 115–122. [CrossRef]

44. Curras-Perez, R.; Ruiz, C.; Sanchez-Garcia, I.; Sanz, S. Determinants of customer retention in virtual environments. The role of perceived risk in a tourism services context. *Span. J. Mark. -ESIC* **2017**, *21*, 131–145. [CrossRef]

45. Jin, N.; Line, N.D.; Merkebu, J. The impact of brand prestige on trust, perceived risk, satisfaction, and loyalty in upscale restaurants. *J. Hosp. Mark. Manag.* **2016**, *25*, 523–546. [CrossRef]

46. Pappas, N. Marketing strategies, perceived risks, and consumer trust in online buying behaviour. *J. Retail. Consum. Serv.* **2016**, *29*, 92–103. [CrossRef]

47. Wang, S.; Wang, J.; Li, J.; Wang, J.; Liang, L. Policy implications for promoting the adoption of electric vehicles: Do consumer's knowledge, perceived risk and financial incentive policy matter? *Transp. Res. Part A Policy Pract.* **2018**, *117*, 58–69. [CrossRef]

48. Wang, S.; Wang, J.; Lin, S.; Li, J. Public perceptions and acceptance of nuclear energy in China: The role of public knowledge, perceived benefit, perceived risk and public engagement. *Energy Policy* **2019**, *126*, 352–360. [CrossRef]

49. Ariffin, S.K.; Mohan, T.; Goh, Y.-N. Influence of consumers' perceived risk on consumers' online purchase intention. *J. Res. Interact. Mark.* **2018**, *12*, 309–327. [CrossRef]

50. Lee, M.-C. Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit. *Electron. Commer. Res. Appl.* **2009**, *8*, 130–141. [CrossRef]

51. Copeland, A.L.; Peltier, M.R.; Waldo, K. Perceived risk and benefits of e-cigarette use among college students. *Addict. Behav.* **2017**, *71*, 31–37. [CrossRef] [PubMed]

52. Cho, S.-H.; Ali, F.; Manhas, P.S. Examining the impact of risk perceptions on intentions to travel by air: A comparison of full-service carriers and low-cost carriers. *J. Air Transp. Manag.* **2018**, *71*, 20–27. [CrossRef]

53. Biemans, W. *Managing Innovation within Networks*; Routledge: Abingdon, UK, 2018; Volume 7.

54. Shuen, A. *Web 2.0: A Strategy Guide: Business Thinking and Strategies behind Successful Web 2.0 Implementations*; O'Reilly Media: Sebastopol, CA, USA, 2018.

55. Selwyn, N. *Education and Technology: Key Issues and Debates*; Bloomsbury Publishing: London, UK, 2016.

56. Nicholls, A. *Managing Educational Innovations*; Routledge: Abingdon, UK, 2018.

57. Hartley, J. *Communication, Cultural and Media Studies: The Key Concepts*; Routledge: Abingdon, UK, 2019.

58. Perse, E.M.; Lambe, J. *Media Effects and Society*; Routledge: Abingdon, UK, 2016.

59. Lai, P. The literature review of technology adoption models and theories for the novelty technology. *JISTEM-J. Inf. Syst. Technol. Manag.* **2017**, *14*, 21–38. [CrossRef]

60. Flodgren, G.; O'Brien, M.A.; Parmelli, E.; Grimshaw, J.M. Local opinion leaders: Effects on professional practice and healthcare outcomes. *Cochrane Database Syst. Rev.* **2019**. [CrossRef]

61. Van Aken, J.E.; Berends, H. *Problem Solving in Organizations*; Cambridge University Press: Cambridge, UK, 2018.

62. Dwivedi, Y.K.; Rana, N.P.; Jeyaraj, A.; Clement, M.; Williams, M.D. Re-examining the unified theory of acceptance and use of technology (UTAUT): Towards a revised theoretical model. *Inf. Syst. Front.* **2019**, *21*, 719–734. [CrossRef]

63. Buttle, F.; Maklan, S. *Customer Relationship Management: Concepts and Technologies*; Routledge: Abingdon, UK, 2019.

64. Charter, M.; Polonsky, M.J. *Greener Marketing: A Global Perspective on Greening Marketing Practice*; Routledge: Abingdon, UK, 2017.

65. Berry, F.S.; Berry, W.D. Innovation and Diusion Models in Policy Research. In *Theories of the Policy Process*; Routledge: Abingdon, UK, 2018; pp. 263–308.

66. Ikenberry, G.J. The International Spread of Privatization Policies: Inducements, Learning, and "Policy Bandwagoning". In *The Political Economy of Public Sector Reform and Privatization*; Routledge: Abingdon, UK, 2019; pp. 88–110.

67. Landsverk, J. *Beyond Common Sense: Child Welfare, Child Well-Being, and the Evidence for Policy Reform*; Routledge: Abingdon, UK, 2017.

68. Islam, A. The role of perceived system quality as educators' motivation to continue e-learning system use. *AIS Trans. Hum. -Comput. Interact.* **2012**, *4*, 25–43. [CrossRef]

69. Lee, S.; Cho, M. Social media use in a mobile broadband environment: Examination of determinants of Twitter and Facebook use. *Int. J. Mob. Mark.* **2011**, *6*, 71–87.

70. Smith, E.R.; Mackie, D.M.; Claypool, H.M. *Social Psychology*; Psychology Press: Philadelphia, PA, USA, 2000.

71. King, A.J.; Lazard, A.J.; White, S.R. The influence of visual complexity on initial user impressions: Testing the persuasive model of web design. *Behav. Inf. Technol.* **2019**, *39*, 1–14. [CrossRef]

72. King, R.C.; Schilhavy, R.A.; Chowa, C.; Chin, W.W. Do customers identify with our website? The effects of website identification on repeat purchase intention. *Int. J. Electron. Commer.* **2016**, *20*, 319–354. [CrossRef]

73. Das, S.; Mishra, A.; Cyr, D. Opportunity gone in a flash: Measurement of e-commerce service failure and justice with recovery as a source of e-loyalty. *Decis. Support Syst.* **2019**, *125*, 113130. [CrossRef]

74. Chen, J.; Shen, X.-L. Consumers' decisions in social commerce context: An empirical investigation. *Decis. Support Syst.* **2015**, *79*, 55–64. [CrossRef]

75. Kim, D.J.; Ferrin, D.L.; Rao, H.R. A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decis. Support Syst.* **2008**, *44*, 544–564. [CrossRef]

76. Yoo, C.W.; Sanders, G.L.; Moon, J. Exploring the effect of e-WOM participation on e-Loyalty in e-commerce. *Decis. Support Syst.* **2013**, *55*, 669–678. [CrossRef]

77. Anderson, R.E.; Swaminathan, S. Customer satisfaction and loyalty in e-markets: A PLS path modeling approach. *J. Mark. Theory Pract.* **2011**, *19*, 221–234. [CrossRef]

78. Gefen, D. Customer loyalty in e-commerce. *J. Assoc. Inf. Syst.* **2002**, *3*, 2. [CrossRef]

79. Gefen, D.; Straub, D.W. Consumer trust in B2C e-Commerce and the importance of social presence: Experiments in e-Products and e-Services. *Omega* **2004**, *32*, 407–424. [CrossRef]

80. Fornell, C.R.; Lacker, D.F. Two structural equation models with unobservable variables and measurement error. *J. Mark. Res.* **1981**, *18*, 39–50. [CrossRef]

81. Wold, S.; Sjöström, M.; Eriksson, L. PLS-regression: A basic tool of chemometrics. *Chemom. Intell. Lab. Syst.* **2001**, *58*, 109–130. [CrossRef]

82. Chin, W.W.; Marcolin, B.L.; Newsted, P.R. A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study. *Inf. Syst. Res.* **2003**, *14*, 189–217. [CrossRef]

83. Marakas, G.; Johnson, R.; Clay, P.F. The evolving nature of the computer self-efficacy construct: An empirical investigation of measurement construction, validity, reliability and stability over time. *J. Assoc. Inf. Syst.* **2007**, *8*, 2. [CrossRef]

84. Loch, K.D.; Straub, D.W.; Kamel, S. Diffusing the Internet in the Arab world: The role of social norms and technological culturation. *IEEE Trans. Eng. Manag.* **2003**, *50*, 45–63. [CrossRef]

85. Gaskin, J.; Godfrey, S. Successful System-Use: It's Not Just Who You Are, But What You Do. *AIS Trans. Hum.-Comput. Interact.* **2018**, *10*, 57–81. [CrossRef]

86. Podsakoff, P.M.; Organ, D.W. Selfreports in Organizational Research: Problems and Prospects. *J. Manag.* **1986**, *12*, 531–544.

87. Podsakoff, P.M.; MacKenzie, S.B.; Lee, J.-Y.; Podsakoff, N.P. Common method biases in behavioral research: A critical review of the literature and recommended remedies. *J. Appl. Psychol.* **2003**, *88*, 879. [CrossRef]

88. Podsakoff, P.M.; MacKenzie, S.B.; Podsakoff, N.P. Sources of method bias in social science research and recommendations on how to control it. *Annu. Rev. Psychol.* **2012**, *63*, 539–569. [CrossRef] [PubMed]

89. Nunnally, J.C. *Psychometric Theory 3E*; Tata McGraw-Hill Education: New York, NY, USA, 1994.

90. Kline, E.; Wilson, C.; Ereshefsky, S.; Tsuji, T.; Schiffman, J.; Pitts, S.; Reeves, G. Convergent and discriminant validity of attenuated psychosis screening tools. *Schizophr. Res.* **2012**, *134*, 49–53. [CrossRef]

91. Henseler, J.; Ringle, C.M.; Sarstedt, M. A new criterion for assessing discriminant validity in variance-based structural equation modeling. *J. Acad. Mark. Sci.* **2015**, *43*, 115–135. [CrossRef]

92. Patel, V. Airport Passenger Processing Technology: A Biometric Airport Journey. Available online: https://commons.erau.edu/cgi/viewcontent.cgi?article=1384&context=edt (accessed on 4 May 2020).