sustainability

MDPI

Article

Sustainable Development of a Mobile Payment Security Environment Using Fintech Solutions

Yoonyoung Hwang [1], Sangwook Park [1,*] and Nina Shin [2,*]

[1] School of Business, Seoul National University, Seoul 08826, Korea; bangyy247@snu.ac.kr
[2] School of Business, Sejong University, Seoul 05006, Korea
* Correspondence: sangpark@snu.ac.kr (S.P.); ninashin@sejong.ac.kr (N.S.)

Abstract: Financial technology (fintech) services have come to differentiate themselves from traditional financial services by offering unique, niche, and customized services. Mobile payment service (MPS) has emerged as the most crucial fintech service. While many studies have addressed the essential role of security when service providers and users choose to engage in financial transactions, the relationship between users distinct perceptions of security and MPS success determinants are yet to be examined. Thus, this study primarily aims to uncover the distinctive roles of platform and technology security by investigating how users react differently to their varying understandings of the MPS usage environment. This study proposes a research model comprising two security dimensions (platform and technology) and three MPS success determinants (convenience, interoperability, and trust). We evaluated the proposed model empirically by using an online survey of 356 users. The survey accounts users experiences of the selected MPS. The results show that a security driven MPS can essentially enhance or deteriorate users positive perceptions of MPS success determinants while they use it for financial transactions. To further understand how this recent trend of user perception of security affects the overall MPS usage experience, this study provides theoretical insights into the roles of platform and technology securities. Managerial insights on the design strategies of MPS providers are also provided based on the potential implications of users subjective and objective perceptions of MPS security environment.

Keywords: financial technology; fintech; mobile payment service; platform security; technology security; sustainable development; continuous usage intention

Citation: Hwang, Y.; Park, S.; Shin, N. Sustainable Development of a Mobile Payment Security Environment Using Fintech Solutions. *Sustainability* **2021**, *13*, 8375. https://doi.org/10.3390/su13158375

Academic Editor: Yi-Shun Wang

Received: 25 June 2021
Accepted: 22 July 2021
Published: 27 July 2021

1. Introduction

By using the emerging technological developments in infrastructure, big data, data analytics, and mobile devices, financial technology (fintech) services have come to differentiate themselves from traditional financial services. Of the various fintech services, mobile payment service (MPS) is the most crucial service as it is able to rapidly acquire customers at lower costs and is one of the fastest moving services in terms of innovation and adoption of new payment capabilities [1]. Mobile payment refers to the process of performing at least one phase of transaction via the use of mobile devices such as mobile smartphones, tablets, or any wireless-enabled devices that are capable of safely handling financial transactions over a mobile network, or via various wireless technologies (e.g., NFC, Bluetooth, RFID, etc.) [2]. Given that mobile payments empower users to confirm electronic transactions in a fast, versatile, and convenient manner both anywhere and anytime, they are considered the next-generation payment system [3,4]. This is supported by a recently published article that reported that the mobile payment market is expected to reach 5399 billion USD by 2026, which was otherwise valued at 1499 billion USD in 2020 and grow at a CAGR of 24.5% over the forecast period of 2021–2026 [5]. Thus, along with emerging technologies (e.g., Blockchain, cryptocurrencies, internet of things (IoT), near field communication (NFC), crowdfunding, artificial intelligence (AI), etc.), MPS has become a lucrative market with significant growth potential [6].

With regard to its enormous potential in the financial sector and its key role in the success of customers, many researchers have investigated the adoption of mobile banking and payment services by customers [3,4,7]. The technology acceptance model (TAM) [8], the unified theory of acceptance and use of technology (UTAUT) model [9], and the diffusion of innovations (DOI) model were used as theoretical frameworks in the context of mobile payment adoption. In the research stream, despite there being many scholars that have called for the provision of security to service providers and users within the MPS context [10–15], the relationship between users distinct perception of security and MPS success determinants such as convenience, interoperability, and trust are yet to be examined.

Specifically, the security driven MPS could essentially enhance or deteriorate users positive perceptions of the MPS qualities used for financial transactions. Thus, this study primarily aims to uncover the distinctive roles of platform and technology security by investigating how users react differently to their varying understandings of the MPS usage environment. For example, existing literature on radical innovation and fintech- enabled services distinguish the term 'platform', as the hub where structured and unstructured data are shared, from the term 'technology', as an enablement of digital transformation processes, service productivity, and users engagement in the digital economy [16–19].

This study confirms and expands two theoretical insights with regard to MPS security: the role of platform security as subjective security and the role of technology security as objective security. Considering the different values held by users of technology and platform securities, this study makes theoretical contributions and offers practical insights on the design strategies of MPS providers.

The organization of this study is as follows: In the next section, the general backgrounds of fintech payment services, MPS operation success determinants, and security dimensions are discussed. In Section 3, a research model is proposed and the hypotheses and research methods, including the procedures for instrument development and data collection, are presented. In Section 4, the results of the data analysis are presented. Lastly, in Section 5, the theoretical and managerial insights are discussed.

2. Literature Review

2.1. Fintech-Enabled Mobile Payment Services

Financial technology, known as *fintech*, refers to the use of new and innovative technology to deliver financial services [20]. The technological developments in infrastructure, big data, data analytics, and mobile devices have enabled fintech industries to differentiate themselves from traditional financial services via the offering of unique, niche, and customized services [1]. Of late, we have come to witness a variety of fintech services (e.g., mobile payments, digital banking, financing, asset management, crowdfunding, insurance, and others) provided by a variety of organizations, including device manufacturers, IT distributors, IT service providers, banks, and credit card companies [6].

A variety of fintech services offer cost-effective platforms as an alternative to traditional financial services and strengthen the user experience via the use of easy and convenient service functions [6]. Some of the major contributions of fintech are reduction of transaction costs, improvement of service quality, and preparation of innovative measures to offer financial services [20,21]. To be precise, MPS enables users to easily purchase goods and services by just entering their passwords, PINs, and biometric authentications, with there being no stress to insert personal information for each of the transactions [22–24]. Table 1 provides a list of the characteristics of the most commonly used MPSs in Korea [25].

Table 1. Characteristics of fintech-embedded mobile payment services (MPSs).

	Kakao Pay	**Samsung Pay**	**Payco**	**Naver Pay**
Launch year	September 2014	September 2015	August 2015	June 2015
Estimated users (RU = registered users; MAU = monthly active users)	30 million (RU) 19 million (MAU)	20 million (RU) 12 million (MAU)	9 million (RU) 4 million (MAU)	30 million (RU) 11 million (MAU)
On/offline pay market (market share)	9%	37%	10%	44%
Mobile pay market (market share)	16%	12%	10%	30%
Key services (Top 5)	Simple payment service (QR, bar-code) Transfer service Kakao pay certification service Billing credit inquiry Certified asset management Insurance	Simple payment service (MST, NFC) Transfer service ATM deposit and withdrawal Fund transfer Transportation card function	Simple payment service (QR, bar-code, MST, NFC) Transfer service ATM deposit and withdrawal Charging point system Local tax payment	Simple payment service (QR, bar-code) Transfer service Offline store booking Small business loan Insurance
International transaction availability	Yes	Yes	Yes	Yes
International transaction (currency) coverage	Japan	International card: 24 countries across six continents Domestic card: Most of the areas where NFCs are installed (i.e., US, UK, Russia, Australia, etc.)	Japan	Japan (i.e., 1.6 million franchises through the subsidiary "LINE")
Strategic positioning	Blockchain based payment service Extensive customer data	Securing franchises with low commission	User-focused service Forms partnerships with various retail stores without any bias toward any specific platform	Online and offline link services based on Naver-shopping to 0.3 million online merchants

2.2. Mobile Payment Service (MPS) Success Determinants

Among various factors that are required for a successful payment service, Kang [22] has emphasized that the various organizations offering MPS should satisfy the following requirements to be considered a successful service: convenience, mobile payment infrastructure, and security.

Convenience is defined as a users' belief that the use of MPS can save time and effort [26–28]. Since mobile payment is categorized as a service, rather than a product, a service-oriented interpretation (viewing convenience as a consumers perceptions of time and effort in relation to the buying or using of a service) can be adopted [11,29]. Pousttchi [30] classified convenience into three domains, namely the operating sequence (e.g., easy handling and fast processing), the initialization phase before the first use, and the coverage of the procedure. Accordingly, the construct of convenience can be understood as the ease and speed of the system, easy learnability of the payment procedure [30,31], and simplicity in conducting financial transactions [32].

Interoperability, or also often referred to as mobile infrastructure, includes all the wire networking, storage, and computing elements necessary to offer modern user experiences in smart mobile devices [33]. Mobile payment infrastructure is mandatory for MPS as the objective of the service is to enable users to make desired payments with mobiles anywhere and anytime [22,34]. Without a mobile payment infrastructure based on IT, MPS cannot be used even if a mobile payment service has a superior function [22]. If an operation infrastructure exists and it supports the use of mobile payments, then the willingness to adopt mobile payments will increase [35]. By linking IT with the existing financial institutions, MPS facilitates payments independently from the financial institution system, providing more versatile services than the traditional payment services [22]. In addition, following the registering of card information on a mobile, payments can be made through the mobile without the use of actual cards [36]. As MPS currently operates in complex, multidimensional networks with shared common infrastructures [37], mobile payments can be made through various platforms and applications [38].

Security, in general, refers to the extent secured from the possible losses obtained due to the uncertainty in the use of mobile payments. The losses include adverse consequences to users, such as financial loss, invasion of privacy, dissatisfaction, anxiety, or discomfort [39]. Studies that shed light on the relationship that exists between perceived security and a user's intention to use mobile payments have a consistent view that perceived security has a significant effect on the intention to adopt MPS [35,40–43]. Whenever users find transactions via the use of mobile devices to be less secure and have concerns regarding privacy [44], information loss, and monetary transactions [31,45], they will be reluctant to adopt MPS. Thus, the providers of MPS must consider security to analyze its impact on a user's intention to accept mobile payments [46].

2.3. Security of Mobile Payment Services

The most imminent challenges of security development for fintech-enabled MPS include mutual authentication, authorization, integrity, privacy, atomicity, and availability. Kang [22] contended that the challenges of security should be solved to sustain the MPS development processes. For example, fintech service security can be classified as a multi-dimensional factor such as services, platforms, networks, and devices [6]. Services create new value for the use of IoT services, platforms play an important role in the value chain of IoT as an interface to connect the services and devices, networks are the wired and wireless communications necessary for the use of fintech services, and devices are objects that are equipped with various sensors [47].

This study proposes that security facilitators should mainly possess two dimensions: platform security regarding the service element of the MPS and technology security regarding the device element of MPS.

Platform security refers to the extent to which people believe that their property and personal information are safe when making mobile payments [40]. E-commerce platforms offer users a variety of business services components, such as trading information services and completion of the transaction process, if they are authenticated and authorized. As the entire set of the business process consists of a variety of services from different vendors based on independent services, these service-oriented heterogeneous systems face a variety of security threats and security vulnerabilities [48]. In this respect, mobile payment platforms manage personal information in real time, operate the system without any problems, and maintain the systems periodically to elevate the security level [49]. Since mobile users access a wide range of non-secure wireless networks and download applications from free sources, the security level of the wired and wireless networks to be used for fintech services should be high in order to protect users systems from harmful viruses and malware [6,50].

Technology security refers to the extent to which people believe in the level and variety of security technologies that protect their personal information and financial transaction records [51]. To feel secure while conducting financial transactions with mobile technologies it is important to minimize the concerns around the use of technology for mobile payments [35,52]. Users are concerned about the security of their payments because of viruses, which reduce their trust in mobile payments and thus can affect their usage behaviors and intentions [13]. E-commerce researchers found that users holding devices with high security related to technology are likely to adopt e-banking systems and use e-commerce platforms [12]. Thus, in this sense, mobile payment providers adopt state-of-the-art encryption methods, while also supporting the most up-to-date authentication methods such as fingerprint recognition through dedicated sensors available on mobile devices [53]. MPS providers have introduced hidden technology, anonymous technology, encryption, and decryption to protect the personal information of users and secure it from the risk of an unauthorized third-party invasion [51]. In addition, MPS providers have come to develop an interface design technology so that users can tailor their security settings to improve the protection of their personal information via the customization of their security settings [49]. Technology security can be beneficial depending on how often

an attack occurs, how much damage is caused through an attack's occurrence, and how effective it is in mitigating the damage caused by the attack [54].

3. Hypotheses Development

3.1. Platform and Technology Securities and MPS Success Determinants

Mobile payment platform is an IT channel where users interact with electronic vendors [55] and carryout payments. The concept of platform security is defined as the extent to which people think that their property and personal information are safe when making mobile payments [40]. In order to enhance platform security, MPS providers manage the personal information in real time, maintain the platform periodically [49], and identify the security and connectivity of the wired and wireless networks [6]. Platform security is specifically different from security that is solely enabled by technology. In addition to technologically integrated security, service providers must offer a user-friendly MPS environment, support users connectedness to service representatives, and provide a high level of customer service [56]. Moreover, the development process of platform security can be more complex than technology security. MPS that is built on the existing platform (i.e., Naver Pay from Naver) have already established a high level of customer service based on its existing service delivery platform, independent from financial institutions linkages, giving benefits to users for using the service. However, despite the early launch year of the service, MPS that is built on fintech-enabled financial transaction services such as Kakao Pay and Samsung Pay may struggle in satisfying security requirements by the customers beyond its technological environment [20].

Given that mobile payment is a service rather than a product, the concept of convenience is adopted based on a service-oriented interpretation of Berry et al.'s definition [29], viewing convenience as a user's perceptions of time and effort in relation to the use of a service. When users' personal information and operating systems are cyclically controlled by MPS providers, users confirm their expectation that the payment service is stable to be used for mobile payments [6]. Hence, the level of platform security impacts convenience such as ensuring there is no psychological burden to users when they undergo the transaction process [10].

A high level of platform security, namely users understanding of the payment provider's ability to secure the personal information of users, enhances the level of a mobile payment infrastructure [28]. It is expected that people believe their payments to be independent of the financial institution system [22] and are able to purchase without the use of actual cards [36]. Thus, the security of the platform environment provided by the industry enhances the level of the mobile payment interoperability.

Trust is the willingness to expect that the payment platform will perform the transactions accurately and fulfill their obligations regardless of a user's ability to monitor or control the behavior of the mobile payment platform [57]. Mu and Lee [55] defined trust as something that reduces the scruple of users and verifies the security of the transaction process as far as possible. When MPS providers manage the payment transaction process securely and have no communication problems with users, user trust in MPS increases [23]. Thus, the level of platform security is expected to positively influence trust.

Hypothesis 1a. *An increased level of perceived platform security will lead to a higher level of perceived convenience in using MPS.*

Hypothesis 1b. *An increased level of perceived platform security will lead to a higher level of perceived interoperability of MPS.*

Hypothesis 1c. *An increased level of perceived platform security will lead to a higher level of perceived trust in using MPS.*

Advances in mobile technology have led to the reduction of technical barriers while carrying out mobile payments and communications with other individuals or systems

anytime and anywhere [4,58]. Technology security is defined as the extent to which people believe that the level and the variety of the security technologies are protecting their personal information and financial transaction records [51]. MPS providers have introduced state-of-the art technology, encryption, and decryption to secure the systems of users from the risk of an unauthorized third-party invasion.

From a security engineering perspective, previous studies have suggested the existence of a potential conflict between security and convenience, implying that security improvements are generally accompanied by increased complexity. However, thanks to rapidly advanced technologies, convenience has not necessarily had to be sacrificed to enhance security in a few cases [15]. In this sense, when MPS providers develop technology security, payment services become convenient as there will be less technical errors and security problems during the process, faster processes to upload data, and simple registration processes [10]. Thus, the level of technology security impacts the convenience of users.

Interoperability enables the use of MPS through mobiles anywhere and anytime. With a high level of technology security, namely an advanced technology protecting the personal information of users, users verify their expectation of the payment service being secure [55]. In this regard, it is expected that people would engage in mobile payments and even use various platforms and applications regardless of the location [22,59]. Hence, technology security has an influence on the level of the mobile payment interoperability.

Trust is important in the context of mobile technologies where there is a clear relinquishing of control (accepting vulnerability) based on the belief that the anticipated payment service will be provided (positive expectation) [11]. According to Fan et al. [40], the security of technology protects users information and property security, reduces their concerns of privacy exposure and financial fraud, and thus increases their trust in MPS [4]. Thus, it is believed that technology security is highly related to trust.

Hypothesis 2a. *An increased level of perceived technology security will lead to a higher level of perceived convenience in using MPS.*

Hypothesis 2b. *An increased level of perceived technology security will lead to a higher level of perceived interoperability of MPS.*

Hypothesis 2c. *An increased level of perceived technology security will lead to a higher level of perceived trust in using MPS.*

3.2. MPS Success Determinants and Continuous Usage Intention

To investigate the influence of MPS success determinants on continuous usage intentions, a second research model is investigated in this section. Continuous intention to use mobile payment services refers to a situation wherein users who have the experience of using mobile payment services intend to continuously use mobile payment services [6].

Intentions have been extensively reviewed by prior studies on mobile-based payments [60–63]. The expectation-confirmation model (ECM) [64] is one of the most widely used theories to focus on the cognitive beliefs and factors that influence users continuous intention [62,65,66]. The ECM has hypothesized as to how perceived usefulness and satisfaction affect the IS continuance intention. ECM and its reformation have been extensively applied to various IT products and services [66]. For example, Oghuma et al. [67] have shown how perceived service quality and usability significantly affect the satisfaction and continuance intention of users to use mobile instant messaging, which underlies the relations of the ECM. Similarly, Susanto et al. [68] used the ECM and amended it to include perceived security and privacy, trust, and self-efficacy to demonstrate the intention to continue the use of smartphone banking services.

In this sense, this study anticipates the positive association of convenience with continuous intention, as well as that of interoperability with continuation intention. This implies that convenience and interoperability may reinforce the positive aspects of MPS, causing users to carry on using the service.

Hypothesis 3. *The degree of perceived convenience positively influences users intention to continue using MPS.*

Hypothesis 4. *The degree of perceived interoperability positively influences users intention to continue using MPS.*

Trust in the virtual environment is a major means of social control, and trust in the virtual environment is more important than trust in the physical environment. In particular, trust is a significant factor in the development of mobile payment services that are directly related to money [69]. In this study, trust is defined as a subjective belief that users will recognize that the new mobile payment service will fulfill its obligations and functions. Users who provide personal and financial information during mobile payments may expect the service providers to handle their information securely [39]. Previous research has identified trust to be an important antecedent for individuals to continue making mobile payments [70]. For instance, Zhou's [71] investigation found users trust in MPS to have a significant impact on their intention to continue using the service. That is, when users perceive that MPS provides a trustworthy system and service, users intentions to continue using MPS will be enhanced. Hence, this study suggests the following hypothesis:

Hypothesis 5. *The degree of perceived trust positively influences users intention to continue using MPS.*

4. Research Design and Analyses

4.1. Instrument Development

A two-part questionnaire was utilized to collect users empirical data: (1) the demographic information and general information concerning MPS usage; and (2) six constructs measured by multiple items (Table 2). The primary goal of the development of an instrument containing measurement items was to achieve the content validity of latent constructs. To ensure that generated measurement items covered the content domain of a latent construct, literature reviews and consultation with academic and industrial experts were generally adopted [72]. For this study, the items were adopted from previous studies and revised to fit the MPS context. To generate measurement items for each construct, 10 items were created for two components of security, 15 items were created for three components of MPS success determinants, and three items were created to measure user's continuous intention of the MPS usage. A seven point Likert scale ranging from one (strongly disagree) to seven (strongly agree) was adopted to quantitatively measure the items within the latent constructs.

The initial measurement items were developed in English, which then were translated into Korean for the survey of MPS users. Specifically, Samsung Pay, Naver Pay, and Kakao pay, who are three of the largest MPS providers in Korea. To ensure the validity of the questionnaire, Korean questionnaires were translated back into English to compare them to the original English measurement items. This process enabled the authors to confirm that the translated word selections reflected the essence and the intention of the original survey that was initially developed.

The final instrument was transferred to a leading nationwide market research provider to carry out the following rigorous listing procedure: initial listing of the eligible survey respondents, screening of the listed respondents to ensure that users have both on- and off-line financial transaction experience with the selected MPSs, and conducting the survey. An initial cross-section list of the respondents was created, and of the total respondents, 356 matched the screening specifications and completed the survey. A summary of the demographic information of respondents in the sample is given in Table 2.

Table 2. Sample description.

Variable	Sample	Percentage
Sex		
Male	170	47.75
Female	186	52.25
Age		
Below 29	107	30.06
30–39	105	29.49
40–49	100	28.09
50 and above	44	12.36
Frequently used mobile payment service		
Kakao Pay	94	26.40
Naver Pay	148	41.57
Samsung Pay	73	20.51
Other	41	11.52
Monthly transaction frequency		
Below 5	88	24.72
5–9	154	43.26
10–19	65	18.26
20 and above	49	13.76
Monthly transaction amount ($1 = 1000 KRW)		
Below $100	90	25.28
$100–$199	106	29.78
$200–$399	78	21.91
$400–$599	47	13.20
$600–$799	15	4.21
$800–$999	12	3.37
$1000 and above	8	2.25

4.2. Measurement Model Analysis

Prior to the testing of the hypothesized structural model, the measurement model was evaluated for its reliability, convergent validity, discriminant validity, collinearity, and model fit.

As Table 3 indicates, the Cronbach's alpha values for all the measurement items ranged from 0.713 to 0.939 and collectively exceeded 0.7, indicating a high reliability of the measurement items [73]. Furthermore, the factor loading, composite reliability (CR), and average variance extracted (AVE) values of each of the latent constructs exceeded 0.7, 0.8, and 0.5, respectively, depicting a satisfactory convergent validity.

Discriminant validity was then tested by comparing the square root of AVE with the correlation coefficient of the latent constructs to examine if each of the latent constructs were distinct [74]. Table 4 confirms a plausible discriminant validity by confirming that the square root value, the depicted value in the diagonal, is greater than the inter-construct correlation coefficient.

Finally, the model fit was tested using a confirmatory factor analysis. The model fit indices, including the normed chi-square (χ^2) (<3.0), comparative fit index (CFI) (>0.70), Tucker–Lewis index (TLI) (>0.90), and the root mean square error of approximation (RMSEA) (<0.10) were evaluated based on the statistical values recommended by Hair et al. [75]. The model fit of the measurement model showed a good fit with the values of $\chi^2/df = 2.590$, $p < 0.001$, CFI = 0.946, TLI = 0.939, and RMSEA = 0.067.

Table 3. Measurement instruments.

Latent Constructs	Measurement Items	Loadings	
Platform Security [6,62,76]	PS 1	I believe that important personal information and transaction records can be safely shared by using this MPS	0.850
	PS 2	This MPS provides a high level of security by operating a regular maintenance and repairing schedule	0.874
	PS 3	This MPS safely manages personal information in real time	0.915
	PS 4	This MPS operates and processes my transactions without problems	0.818
	PS 5	This MPS provides a high security level of wired and wireless networks	0.900
Technology Security [41,49,51,77]	TS 1	I believe that this MPS has a variety of security technologies at an advanced level to protect my important personal information and transaction records	0.920
	TS 2	This MPS provides a variety of authentication methods at a high level prior to make transactions	0.873
	TS 3	This MPS provides a high level of confidentiality, that is hidden technology, anonymous technology, and encryption and decryption are adopted to protect the security of personal information	0.906
	TS 4	This MPS enables customization to adequately tailor security settings to improve the protection of personal information	0.851
	TS 5	This MPS has a high level of firewall technology to prevent the intrusion of unverified systems	0.895
Convenience [11,31,32]	CON 1	This MPS requires minimal time and effort to use payment services	0.934
	CON 2	This MPS provides a high level of learnability in the payment procedure	0.818
	CON 3	This MPS provides a high level of ease of use while using mobile payment services	0.796
	CON 4	This MPS provides a high level of simplicity while conducting financial transactions	0.839
Interoperability [22,36,38,43]	INT 1	This MPS provides a high level of intangibility while making mobile payments without the use of actual cards	0.785
	INT 2	This MPS provides a high level of independence from financial institutions when making mobile payments	0.829
	INT 3	This MPS provides a high level of easy payment service whenever required	0.854
	INT 4	If I register my card information on my mobile, this MPS allows me to pay through a mobile without the use of a physical card	0.737
	INT 5	This MPS provides a high level of interoperability, wherein mobile payments can be made through various platforms and applications	0.778
Trust [65,78]	TRST 1	I believe this MPS ensures that all of the involved third parties retain the entire encrypted transactional data and not use the information for their own benefit	0.835
	TRST 2	I believe this MPS has a high level of integrity, that is the service adheres to the relevant policies and provides reliable services	0.907
	TRST 3	I believe this MPS has the skills to render excellent services	0.807
	TRST 4	I believe this MPS will act in its users best interests	0.713
	TRST 5	I believe that when an unauthorized transaction occurs, this MPS will solve the problem or compensate	0.782
	TRST 6	I believe this MPS processes individual transactions accurately and in a timely manner	0.803
Continuous Intention [79,80]	COI 1	I plan to use MPS in the future	0.925
	COI 2	I intend to continue using MPS in the future	0.937
	COI 3	I expect my use of MPS to continue in the future	0.939

Table 4. Results of the reliabilities and discriminant validity.

	CR	AVE	PS	TS	CON	INT	TRST	COI
Platform security (PS)	0.941	0.761	0.872					
Technology security (TS)	0.950	0.791	0.913	0.889				
Convenience (CON)	0.911	0.720	0.414	0.313	0.848			
Interoperability (INT)	0.897	0.636	0.613	0.491	0.727	0.798		
Trust (TRST)	0.919	0.656	0.878	0.893	0.399	0.575	0.810	
Continuous intention (COI)	0.953	0.872	0.518	0.483	0.563	0.651	0.615	0.934

4.3. Structural Equation Model Analysis

As shown in Figure 1 and Table 5, the results show that platform security (H1) has a positive and significant influence on MPS success determinants and that continuous intention for future transactions with *p*-value is less than 0.01. Technology security (H2) has a negative and significant impact on convenience ($\beta = -1.573$, $p < 0.01$) and interoperability ($\beta = -1.446$, $p < 0.01$), while having a positive and significant impact on trust ($\beta = 0.307$, $p < 0.01$). Users perceived degree of convenience, interoperability, and trust have positive and significant impacts on their intention (H3, H4, H5) to continue using MPS ($\beta = 0.244$, 0.292, and 0.308, respectively, with $p < 0.01$).

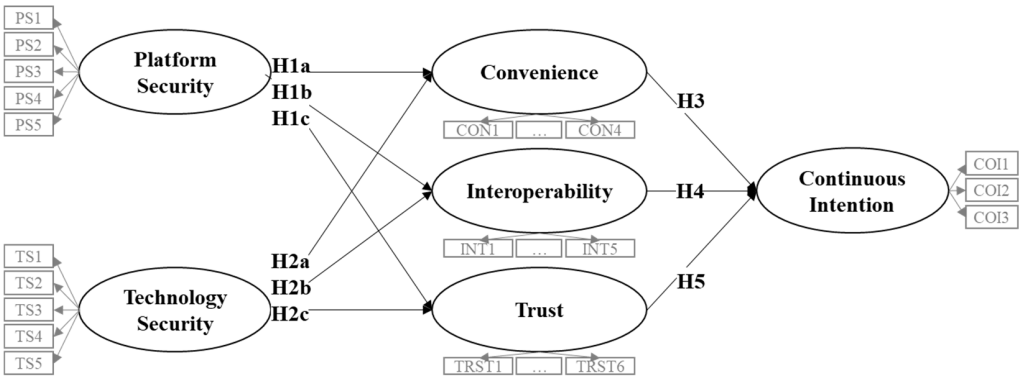

Figure 1. Hypothesized roles of the platform, and technology, securities in the MPS use model.

Table 5. Summary of research results.

	Hypothesized Relationship	Path Coefficients	*p*-Value
H1a	An increased level of platform security will lead to a higher level of perceived convenience in using MPS	1.955	0.001
H1b	An increased level of platform security will lead to a higher level of perceived interoperability of MPS	1.982	0.001
H1c	An increased level of platform security will lead to a higher level of perceived trust in using MPS	0.658	0.001
H2a	An increased level of technology security will lead to a higher level of perceived convenience in using MPS	−1.573	0.001
H2b	An increased level of technology security will lead to a higher level of perceived interoperability of MPS	−1.446	0.001
H2c	An increased level of technology security will lead to a higher level of perceived trust in using MPS	0.307	0.001
H3	The degree of perceived convenience positively influences users intention to continue using MPS	0.244	0.001
H4	The degree of perceived interoperability positively influences user intention to continue using MPS	0.292	0.001
H5	The degree of perceived trust positively influences user intention to continue using MPS	0.308	0.001

5. Conclusion and Discussions

5.1. Theoretical Insights

Security is one of the key considerations of service providers and users when they choose to engage in financial transactions. To this end, this study confirms and expands two theoretical insights with regard to MPS security: the role of platform security as subjective security and the role of technology security as objective security.

Firstly, this study shows how a higher level of platform security leads to users having a positive perception of convenience, interoperability, and trust with regard to MPS (Hypotheses 1a, 1b, 1c). This finding is in alignment with the various studies that find platform management and its equipped level of security to contribute towards a higher perception level of platform requirements [37,80,81]. For example, Fan et al. [81] emphasized that, with an effective cooperation between the retailers and the third-party payment platform, the supply chain can collectively reduce users price sensitivity and even stimulate market demand by facilitating the consumptions patterns of users. Similarly, platform security is also regarded as users subjective evaluation of MPS security [80]. It is only when a user's perceived feeling of security exceeds a certain expectation that they will have a positive outlook on overall MPS success determinants from the standpoint of convenience, interoperability, and trust perspectives.

Secondly, an interesting finding of this study is that technology security has a rather negative impact on the convenience and interoperability of MPS (Hypotheses 2a, 2b). In alignment with Taherdoost's [80] view on security from two different perspectives, i.e., objective and subjective, this study empirically validates the roles and differing outcomes of these two different perspectives. Objective security includes the following aspects of the service: "authentication, authorization, integrity, confidentiality and non-repudiation" [70] (p. 536). For a higher level of security, users are often requested to complete two or more authentication processes (i.e., passcode, fingerprint, phone call confirmation, SMS confirmation). However, the more MPS is equipped with technological security verification and protection such as anti-virus add-on installation, the more are the chances of a user's perceived level of convenience significantly decreasing. For example, convenience is commonly measured based on a user's perceptions of time and effort in relation to the making of financial transactions [11]. Despite the benefit of a high level of security supported by technological advancements, this study shows how users might perceive an inconvenience when rather unnecessary value-adding activities are added to existing MPS interoperability.

In general, service providers and security technology developers may expect that a higher level of security would create an absolute value-adding experience to a user's MPS interaction. This study recommends that such generalizations can be misleading. This study emphasizes and highlights the previous implications related to user perceptions of security and its role in the overall usage environment. Jun et al. [32] noted that, when there are excessive complications in the technology security process, these can create an uneasy learning environment for users. Moreover, Iman [37] noted that technology-driven applications could potentially create complexities and burdens to the firms that use either a shared infrastructure or the service platform. In sum, the distinctive roles of platform and technology securities hinge on how differently users react to their own subjective and objective understandings of the MPS usage environment. This carries significant implications to the management of service operations, quality, and marketing as existing MPS studies are limited to the investigation of the information, system, and service aspects of the MPS environment. Thus, there is a need to investigate the impact of user interaction methods with platform and technology from a distinct perspective.

5.2. Managerial Insight

Security-driven MPS can significantly enhance or deteriorate users positive perceptions of convenience, interoperability, and trust while using MPS for financial transactions. Based on the understanding that users form subjective and objective perceptions of the

MPS security environment, both servers as well as service providers must make strategic plans to develop their overall MPS design.

For example, the difference between platform security and technology security can be delineated through the source and the provider of the security. The ecosystem of MPS mainly includes server providers, third party payment providers, and service providers [3,82]. Based on the involvement of technology, or platform, providers, the methodologies used for payment, authentication, and enabling for retailers can significantly differ. MPS providers must develop platform design strategies in alignment with marketing strategies as users predominantly place different values on technology, and platform, securities.

Additionally, overall user perceptions of MPS convenience, interoperability, and trust are significantly determined by the level of security. Prior to the expansion of the scope of technology security, firms should evaluate as to how such efforts can (i) strengthen (or weaken) the overall privacy and security of users information, (ii) accelerate (or dampen) the ease and speed of service usage, and (iii) enable (or disables) higher level of MPS use preference in the future in comparison with the traditional payment service.

Finally, of the various MPS characteristics, trust also plays an imperative role in the banking and financial payment service sector [83,84]. Trust can effectively mitigate user uncertainty pertaining to the outcome of financial transactions, and thereby increase the likelihood of future engagement [85]. The results of this study reveal that many of users intend to continuously use MPS in the presence of trust, instead of the traditional payment system. Firms are recommended to strategically strengthen the overall trust level to develop an irreplaceable MPS that alleviates the concerns of users while they make financial transactions.

5.3. Sustainable Management Inspiration

Strategic integration of platform and technology security can be considered an alternative to designing a sustainable MPS transaction environment. Specifically, service providers may consider the applications of sustainable development to address some of the existing challenges raised by the artificial intelligence environment, such as resource management efficiency, sustainable service design, and network technologies. This study advances the understanding of alternatives to the designing of a sustainable mobile payment service by utilizing appropriate levels of security technologies in the service delivery platform. Service providers may improve their service by providing a higher level of security and may also sustain the wireless network design by eliminating an undesirable level of technology integration while providing service to the end user.

5.4. Future Research Avenues

Based on an in-depth investigation of the relationship between technology advancements and MPS security performance, this study recommends engaging in the following future research opportunities: to identify and understand the rate of technological change in MPS environments and the development of a dynamic strategy with regard to platform design for an overall MPS security improvement; to develop a continuous monitoring process for advanced knowledge of fintech-driven market requirements and of MPS platform and technology security performance; to identify potential security risks and their significance to the overall MPS usage experience from both platform, and technology, management perspectives.

Author Contributions: All authors conceived, developed, analyzed the research model; contributed to the discussion and design of the framework; Y.H. and N.S. wrote the manuscript; S.P. supervised; All authors have read and agreed to the published version of the manuscript.

Funding: The authors wish to thank the Institute of Management Research at Seoul National University for supporting this research. This work was also supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF-2020S1A5A8045955).

Data Availability Statement: Not applicable.

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

References

1. Lee, I.; Shin, Y.J. Fintech: Ecosystem, business models, investment decisions, and challenges. *Bus. Horiz.* **2018**, *61*, 35–46. [CrossRef]
2. Ghezzi, A.; Renga, F.; Balocco, R.; Pescetto, P. Mobile payment applications: Offer state of the art in the Italian market. *Info* **2010**, *12*, 3–22. [CrossRef]
3. Choi, H.; Park, J.; Kim, J.; Jung, Y. Consumer preferences of attributes of mobile payment services in South Korea. *Telemat. Inform.* **2020**, *51*, 101397. [CrossRef]
4. Kim, C.; Mirusmonov, M.; Lee, I. An empirical examination of factors influencing the intention to use mobile payment. *Comput. Hum. Behav.* **2010**, *26*, 310–322. [CrossRef]
5. Intelligence, M. Mobile Payments Market-Growth, Trends, COVID-19 Impact, and Forecasts (2021–2026). Available online: https://www.mordorintelligence.com/industry-reports/mobile-payment-market (accessed on 20 May 2021).
6. Lim, S.H.; Kim, D.J.; Hur, Y.; Park, K. An Empirical Study of the Impacts of Perceived Security and Knowledge on Continuous Intention to Use Mobile Fintech Payment Services. *Int. J. Hum. Comput. Interact.* **2019**, *35*, 886–898. [CrossRef]
7. Tounekti, O.; Ruiz-martínez, A.; Skarmeta-gómez, A.F. Users' evaluation of a new web browser payment interface for facilitating the use of multiple payment systems. *Sustainability* **2021**, *13*, 4711. [CrossRef]
8. Davis, F.D.; Bagozzi, R.P.; Warshaw, P.R. User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. *Manag. Sci.* **1989**, *35*, 982–1003. [CrossRef]
9. Venkatesh, V.; Davis, F.D. Theoretical extension of the Technology Acceptance Model: Four longitudinal field studies. *Manag. Sci.* **2000**, *46*, 186–204. [CrossRef]
10. Indiani, N.L.P.; Fahik, G.A. Conversion of online purchase intention into actual purchase: The moderating role of transaction security and convenience. *Bus. Theory Pract.* **2020**, *21*, 18–29. [CrossRef]
11. Williams, M.D. Social commerce and the mobile platform: Payment and security perceptions of potential users. *Comput. Hum. Behav.* **2018**, 1–12. [CrossRef]
12. Wu, D.; Moody, G.D.; Zhang, J.; Lowry, P.B. Effects of the design of mobile security notifications and mobile app usability on users' security perceptions and continued use intention. *Inf. Manag.* **2020**, *57*, 103235. [CrossRef]
13. Hossain, M.A. Security perception in the adoption of mobile payment and the moderating effect of gender. *PSU Res. Rev.* **2019**, *3*, 179–190. [CrossRef]
14. Lai, P.C. Design and Security impact on consumers' intention to use single platform E-payment. *Interdiscip. Inf. Sci.* **2016**, *22*, 111–122. [CrossRef]
15. Kim, B.C.; Park, Y.W. Security versus convenience? An experimental study of user misperceptions of wireless internet service quality. *Decis. Support. Syst.* **2012**, *53*, 1–11. [CrossRef]
16. Mačiulienė, M.; Skaržauskienė, A. Building the capacities of civic tech communities through digital data analytics. *J. Innov. Knowl.* **2020**, *5*, 244–250. [CrossRef]
17. Liébana-Cabanillas, F.; García-Maroto, I.; Muñoz-Leiva, F.; Ramos-de-Luna, I. Mobile payment adoption in the age of digital transformation: The case of apple pay. *Sustainability* **2020**, *12*, 5443. [CrossRef]
18. Lakshmi, V.; Bahli, B. Understanding the robotization landscape transformation: A centering resonance analysis. *J. Innov. Knowl.* **2020**, *5*, 59–67. [CrossRef]
19. Tiberius, V.; Schwarzer, H.; Roig-Dobón, S. Radical innovations: Between established knowledge and future research opportunities. *J. Innov. Knowl.* **2021**, *6*, 145–153. [CrossRef]
20. Fosso Wamba, S.; Kala Kamdjoug, J.R.; Epie Bawack, R.; Keogh, J.G. Bitcoin, Blockchain and Fintech: A systematic review and case studies in the supply chain. *Prod. Plan. Control.* **2020**, *31*, 115–142. [CrossRef]
21. Aslam, J.; Saleem, A.; Khan, N.T.; Kim, Y.B. Factors influencing blockchain adoption in supply chain management practices: A study based on the oil industry. *J. Innov. Knowl.* **2021**, *6*, 124–134. [CrossRef]
22. Kang, J. Mobile payment in Fintech environment: Trends, security challenges, and services. *Hum. Cent. Comput. Inf. Sci.* **2018**, *8*. [CrossRef]
23. Lim, S.; Hur, Y. An empirical study on the impact of the perceived securities and trust to diffusion of IoT-based smart banking services-focusing on university students. *Insur. Financ. Rev.* **2017**, *28*, 37–65.
24. Nan, D.; Kim, Y.; Park, M.H.; Kim, J.H. What motivates users to keep using social mobile payments? *Sustainability* **2020**, *12*, 6878. [CrossRef]
25. Choi, S. The Evolving Simple Payment Market, the Financial Industry Is Now at War with OO Pay. Available online: https://www.sktinsight.com/122067 (accessed on 24 June 2021).
26. Brown, L.G. Convenience in Services Marketing Convenience: A Topic for the Convenience: A Conceptual. *J. Serv. Mark.* **1990**, *4*, 53–59. [CrossRef]
27. Yoon, C.; Kim, S. Convenience and TAM in a ubiquitous computing environment: The case of wireless LAN. *Electron. Commer. Res. Appl.* **2007**, *6*, 102–112. [CrossRef]
28. Chen, Y.L.; Wu, W.-N. An Exploration of the Factors Affecting User's Satisfaction with Mobile Payments. *Int. J. Comput. Sci. Inf. Technol.* **2017**, *9*, 97–105. [CrossRef]

29. Berry, L.L.; Seiders, K.; Grewal, D. Understanding service convenience. *J. Mark.* **2002**, *66*, 1–17. [CrossRef]
30. Pousttchi, K. Conditions for Acceptance and Usage of Mobile Payment Procedures. In Proceedings of the 6th Annual Global Mobility Round Table, Los Angeles, CA, USA, 1 June 2007.
31. Park, J.K.; Ahn, J.; Thavisay, T.; Ren, T. Examining the role of anxiety and social influence in multi-benefits of mobile payment service. *J. Retail. Consum. Serv.* **2019**, *47*, 140–149. [CrossRef]
32. Jun, J.; Cho, I.; Park, H. Factors influencing continued use of mobile easy payment service: An empirical investigation. *Total Qual. Manag. Bus. Excell.* **2018**, *29*, 1043–1057. [CrossRef]
33. Bonomi, F. The future mobile infrastructure: Challenges and opportunities. *IEEE Wirel. Commun.* **2010**, *17*, 4–5. [CrossRef]
34. Dahlberg, T.; Mallat, N.; Ondrus, J.; Zmijewska, A. Past, present and future of mobile payments research: A literature review. *Electron. Commer. Res. Appl.* **2008**, *7*, 165–181. [CrossRef]
35. Oliveira, T.; Thomas, M.; Baptista, G.; Campos, F. Mobile payment: Understanding the determinants of customer adoption and intention to recommend the technology. *Comput. Hum. Behav.* **2016**, *61*, 404–414. [CrossRef]
36. Kim, M.; Kim, S.; Kim, J. Can mobile and biometric payments replace cards in the Korean offline payments market? Consumer preference analysis for payment systems using a discrete choice model. *Telemat. Inform.* **2019**, *38*, 46–58. [CrossRef]
37. Iman, N. Is mobile payment still relevant in the fintech era? *Electron. Commer. Res. Appl.* **2018**, *30*, 72–82. [CrossRef]
38. Kazan, E.; Tan, C.W.; Lim, E.T.K. Towards a framework of digital platform competition: A comparative study of monopolistic & federated mobile payment platforms. *J. Theor. Appl. Electron. Commer. Res.* **2016**, *11*, 50–64. [CrossRef]
39. Oh, J.; Kim, W. The Effects of Mobile Payment System on Consumer Attitude and Behavioral Intention. *J. Internet Electron. Commer. Res.* **2020**, *20*, 35–50. [CrossRef]
40. Fan, J.; Shao, M.; Li, Y.; Huang, X. Understanding users' attitude toward mobile payment use: A comparative study between China and The U.S. *Ind. Manag. Data Syst.* **2018**, *118*, 524–540. [CrossRef]
41. Liébana-Cabanillas, F.; de Luna, I.R.; Montoro-Ríosa, F. Intention to use new mobile payment systems: A comparative analysis of SMS and NFC payments. *Econ. Res. Istraz.* **2017**, *30*, 892–910. [CrossRef]
42. Shin, D.H. Towards an understanding of the consumer acceptance of mobile wallet. *Comput. Hum. Behav.* **2009**, *25*, 1343–1354. [CrossRef]
43. Schierz, P.G.; Schilke, O.; Wirtz, B.W. Understanding consumer acceptance of mobile payment services: An empirical analysis. *Electron. Commer. Res. Appl.* **2010**, *9*, 209–216. [CrossRef]
44. Bailey, A.A.; Pentina, I.; Mishra, A.S.; Ben Mimoun, M.S. Mobile payments adoption by US consumers: An extended TAM. *Int. J. Retail. Distrib. Manag.* **2017**, *45*, 626–640. [CrossRef]
45. Yang, K.; Forney, J.C. The moderating role of consumer technology anxiety in mobile shopping adoption: Differential effects of facilitating conditions and social influences. *J. Electron. Commer. Res.* **2013**, *14*, 334–347.
46. Sharma, S.K.; Sharma, H.; Dwivedi, Y.K. A Hybrid SEM-Neural Network Model for Predicting Determinants of Mobile Payment Services. *Inf. Syst. Manag.* **2019**, *36*, 243–261. [CrossRef]
47. Lee, J. A literature review on security for internet of things in Korea based on IoT S-P-N-D-Se ecosystem model. *J. Secur. Eng.* **2015**, *12*, 397–414.
48. Huang, M.; Zhao, Y.; Zhu, L. Research for e-commerce platform security framework based on SOA. In Proceedings of the 2011 4th International Conference on Biomedical Engineering and Informatics (BMEI), Shanghai, China, 15–17 October 2011. [CrossRef]
49. Zhang, J.; Luximon, Y. A quantitative diary study of perceptions of security in mobile payment transactions. *Behav. Inf. Technol.* **2020**, 1–24. [CrossRef]
50. Mala Nabi, R.; Mohammed, R.A.; Mala Nabi, R. Smartphones Platform Security a Comparison Study. *Int. J.* **2015**, *5*, 4–9.
51. Lee, S.H.; Huang, K.W.; Yang, C.S. TBAS: Token-based authorization service architecture in Internet of things scenarios. *Int. J. Distrib. Sens. Netw.* **2017**, *13*. [CrossRef]
52. Salisbury, W.D.; Pearson, R.A.; Pearson, A.W.; Miller, D.W. Perceived security and World Wide Web purchase intention. *Ind. Manag. Data Syst.* **2001**, *101*, 165–177. [CrossRef]
53. Liébana-Cabanillas, F.; Muñoz-Leiva, F.; Sánchez-Fernández, J. A global approach to the analysis of user behavior in mobile payment systems in the new electronic environment. *Serv. Bus.* **2018**, *12*, 25–64. [CrossRef]
54. Butler, S.A. Security attribute evaluation method: A cost-benefit approach. *Proc. Int. Conf. Softw. Eng.* **2002**, 232–240. [CrossRef]
55. Mu, H.-L.; Lee, Y.-C. Examining the Influencing Factors of Third-Party Mobile Payment Adoption: A Comparative Study of Alipay and WeChat Pay. *J. Inf. Syst.* **2017**, *26*, 247–284. [CrossRef]
56. Arcand, M.; PromTep, S.; Brun, I.; Rajaobelina, L. Mobile banking service quality and customer relationships. *Int. J. Bank Mark.* **2017**, *35*, 1066–1087. [CrossRef]
57. Yu, L.; Cao, X.; Liu, Z.; Gong, M.; Adee, L. Understanding mobile payment users' continuance intention: A trust transfer perspective Article information: About Emerald www.emeraldinsight.com Understanding mobile payment users' continuance intention: A trust transfer perspective. *Internet Res.* **2018**, *28*, 456–476.
58. Liébana-Cabanillas, F.; Marinkovic, V.; Ramos de Luna, I.; Kalinic, Z. Predicting the determinants of mobile payment acceptance: A hybrid SEM-neural network approach. *Technol. Forecast. Soc. Chang.* **2018**, *129*, 117–130. [CrossRef]
59. Kazan, E.; Damsgaard, J. Towards a market entry framework for digital payment platforms. *Commun. Assoc. Inf. Syst.* **2016**, *38*, 761–783. [CrossRef]

60. De Luna, I.R.; Liébana-Cabanillas, F.; Sánchez-Fernández, J.; Muñoz-Leiva, F. Mobile payment is not all the same: The adoption of mobile payment systems depending on the technology applied. *Technol. Forecast. Soc. Chang.* **2019**, *146*, 931–944. [CrossRef]
61. Kalinic, Z.; Marinkovic, V.; Molinillo, S.; Liébana-Cabanillas, F. A multi-analytical approach to peer-to-peer mobile payment acceptance prediction. *J. Retail. Consum. Serv.* **2019**, *49*, 143–153. [CrossRef]
62. Shao, Z.; Zhang, L.; Li, X.; Guo, Y. Antecedents of trust and continuance intention in mobile payment platforms: The moderating effect of gender. *Electron. Commer. Res. Appl.* **2019**, *33*, 100823. [CrossRef]
63. Chen, S.C.; Chung, K.C.; Tsai, M.Y. How to achieve sustainable development of mobile payment through customer satisfaction-The SOR model. *Sustainability* **2019**, *11*, 6314. [CrossRef]
64. Bhattacherjee, A. Understanding Information Systems Continuance: An Expectation-Confirmation Model. *Manag. Inf. Syst.* **2001**, *25*, 351–370. [CrossRef]
65. Talwar, S.; Dhir, A.; Khalil, A.; Mohan, G.; Islam, A.K.M.N. Point of adoption and beyond. Initial trust and mobile-payment continuation intention. *J. Retail. Consum. Serv.* **2020**, *55*, 102086. [CrossRef]
66. Ouyang, Y.; Tang, C.; Rong, W.; Zhang, L.; Yin, C.; Xiong, Z. Task-technology Fit Aware Expectation-confirmation Model towards Understanding of MOOCs Continued Usage Intention. In Proceedings of the 50th Hawaii International Conference on System Science, Waikoloa Village, HI, USA, 4–7 January 2017; pp. 174–183. [CrossRef]
67. Oghuma, A.P.; Libaque-Saenz, C.F.; Wong, S.F.; Chang, Y. An expectation-confirmation model of continuance intention to use mobile instant messaging. *Telemat. Inform.* **2016**, *33*, 34–47. [CrossRef]
68. Susanto, A.; Chang, Y.; Ha, Y. Determinants of continuance intention to use the smartphone banking services: An extension to the expectation-confirmation model. *Ind. Manag. Data Syst.* **2016**, *116*, 508–525. [CrossRef]
69. Lee, J.; Ryu, M.H.; Lee, D. A study on the reciprocal relationship between user perception and retailer perception on platform-based mobile payment service. *J. Retail. Consum. Serv.* **2019**, *48*, 7–15. [CrossRef]
70. Hong Zhu, D.; Ying, L.Y.P.; Chang, L. Understanding the Intention to Continue Use of a Mobile Payment Provider: An Examination of Alipay Wallet in China. *Int. J. Bus. Inf.* **2017**, *12*, 369–390. [CrossRef]
71. Zhou, T. Understanding the determinants of mobile payment continuance usage. *Ind. Manag. Data Syst.* **2014**, *114*, 936–948. [CrossRef]
72. Cao, M.; Zhang, Q. Supply chain collaboration: Impact on collaborative advantage and firm performance. *J. Oper. Manag.* **2011**, *29*, 163–180. [CrossRef]
73. Fornell, C.; Larcker, D.F. Evaluating structural equation models with unobservable variables and measurement error. *J. Mark. Res.* **1981**, *18*, 39–50. [CrossRef]
74. Dehghanpouri, H.; Soltani, Z.; Rostamzadeh, R. The impact of trust, privacy and quality of service on the success of E-CRM: The mediating role of customer satisfaction. *J. Bus. Ind. Mark.* **2020**, *11*, 1831–1847. [CrossRef]
75. Hair, J.F.; Black, W.C.; Babin, B.J.; Anderson, R.E.; Tatham, R.L. *Multivariate Data Analysis*; Prentice-Hall: New Jersey, NJ, USA, 2006.
76. Fan, Y.; Stevenson, M. A review of supply chain risk management: Definition, theory, and research agenda. *Int. J. Phys. Distrib. Logist. Manag.* **2018**. [CrossRef]
77. Milian, E.Z.; De MSpinola, M.; De Carvalho, M. Fintechs: A literature review and research agenda. *Electron. Commer. Res. Appl.* **2019**, *34*. [CrossRef]
78. Thammarat, C.; Kurutach, W. A lightweight and secure NFC-base mobile payment protocol ensuring fair exchange based on a hybrid encryption algorithm with formal verification. *Int. J. Commun. Syst.* **2019**, *32*, 1–21. [CrossRef]
79. Agarwal, R.; Karahanna, E. Time Flies When You're Having Fun: Cognitive Absorption and Beliefs about Information Technology Usage. *MIS Q.* **2000**, *24*, 665. [CrossRef]
80. Taherdoost, H. Understanding of e-service security dimensions and its effect on quality and intention to use. *Inf. Comput. Secur.* **2017**, *25*, 535–559. [CrossRef]
81. Fan, X.; Zhao, W.; Zhang, T.; Yan, E. Mobile payment, third-party payment platform entry and information sharing in supply chains. *Ann. Oper. Res.* **2020**. [CrossRef]
82. Park, S.; Kim, Y.; Chang, H. An empirical study on security expert ecosystem in the future IoT service environment. *Comput. Electr. Eng.* **2016**, *52*, 199–207. [CrossRef]
83. Ahn, K.; Cho, J.-S. Major concerns of FinTech (Financial Technology) services in the Korean market. *J. Bus. Retail. Manag. Res.* **2019**, *14*, 123–133. [CrossRef]
84. Singh, N.; Sinha, N. How perceived trust mediates merchant's intention to use a mobile wallet technology. *J. Retail. Consum. Serv.* **2020**, *52*, 101894. [CrossRef]
85. Singh, N.; Srivastava, S.; Sinha, N. Consumer preference and satisfaction of M-wallets: A study on North Indian consumers. *Int. J. Bank Mark.* **2017**, *35*, 944–965. [CrossRef]