





## Article

# An Empirical Study of Mobile Commerce and Customers Security Perception in Saudi Arabia

Hina Gull <sup>1</sup>, Saqib Saeed <sup>2</sup>, Sardar Zafar Iqbal <sup>1</sup>, Yasser A. Bamarouf <sup>1</sup>, Mohammed A. Alqahtani <sup>1</sup>, Dina A. Alabbad <sup>3</sup>, Madeeha Saqib <sup>1,\*</sup>, Saeed Hussein Al Qahtani <sup>1</sup> and Albandary Alamer <sup>1</sup>

- <sup>1</sup> Department of Computer Information Systems, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia; hgull@iau.edu.sa (H.G.); saiqbal@iau.edu.sa (S.Z.I.); yabamarouf@iau.edu.sa (Y.A.B.); maqhtani@iau.edu.sa (M.A.A.); shaqhtani@iau.edu.sa (S.H.A.Q.); amalamer@iau.edu.sa (A.A.)
- <sup>2</sup> Saudi Aramco Cybersecurity Chair, Department of Computer Information Systems, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia; sbsaed@iau.edu.sa
- <sup>3</sup> Department of Computer Engineering, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia; daalabbad@iau.edu.sa
- \* Correspondence: mssaheed@iau.edu.sa

**Abstract:** Digital transformation of businesses has seen tremendous growth recently, moreover, COVID-19 has increased online shopping. However, it is important for businesses that customers' online shopping experience is secure and joyful. In this paper, customers' security perception regarding some leading mobile commerce applications in Saudi Arabia is explored. Our survey questions focused on three aspects, namely: Consumer rating, trustworthiness, and credit card security. The results highlight that consumers perceive that mobile commerce applications in Saudi Arabia need further improvement in security. In this work, a model to improve customers' security perception in Saudi Arabia is presented. This model can be generalized to other geographical regions as well. The model outlines different actions for practitioners and policymakers that help in improving security infrastructure, authentication mechanisms, and trustworthiness.

**Keywords:** mobile commerce; security; digital strategy; digital transformation; user security



**Citation:** Gull, H.; Saeed, S.; Iqbal, S.Z.; Bamarouf, Y.A.; Alqahtani, M.A.; Alabbad, D.A.; Saqib, M.; Al Qahtani, S.H.; Alamer, A. An Empirical Study of Mobile Commerce and Customers Security Perception in Saudi Arabia.

*Electronics* **2022**, *11*, 293.

<https://doi.org/10.3390/electronics11030293>

electronics11030293

Academic Editors: Cristina Alcaraz, Noemí de Castro García, Manuel A. Serrano and David G. Rosado

Received: 13 November 2021

Accepted: 11 January 2022

Published: 18 January 2022

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**Copyright:** © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

Mobile applications have become an integral part of our lives and have dominated almost all sectors such as health, entertainment, marketing, communication, and commerce. Mobile computing offers low-cost and extensive functionalities that are best adopted by businesses. Therefore, it can be termed as a disruptive technology that has become a valuable facilitator for businesses, allowing them to reach out to worldwide clients in a cost-effective and efficient manner [1]. In most recent years, mobile commerce, known also as m-commerce, has become a core component of the entire supply chain of business organizations [2]. Social, legal, economic, political, and technological aspects influence the digital transformation of businesses as well as customers [3]. The acceptability of e-commerce is further influenced by disparities in technological accessibility, skill levels, security concerns, buying behavior, purchasing power, cultural differences, and regulation [4]. As a result, corporate digital transformation has not been consistent across the world. There has been an increasing trend in online shopping after the COVID-19 global pandemic. In order to achieve business continuity, many businesses have launched online outlets as customers around the world faced lockdown [5]. With the boom in online shopping, the security and privacy of the mobile application industry have also become an important issue. Customers are now more concerned about the privacy of their data and the security of their financial communication. This leads to the use of only those mobile applications that provide more

security and privacy and have a positive perception. Customers are concerned about the exposure of mobile applications to malicious codes and unauthorized access. They are also afraid of third parties tracking their activities and stealing credit card information. Both privacy and security issues have shown to have a profound impact on customers' willingness to buy and sell products using m-commerce applications [6–9]. If customers have concerns about the security aspects of an online business, this will deter them to use that particular platform. Therefore, it is very important for businesses to understand customer perception and security to improve their online platforms for better customer engagement. Since social and cultural factors vary across countries, it is significantly important to explore customers' perceptions across different cultures to understand security and privacy concerns with online platforms [10,11]. Furthermore, Protection Motivation Theory (PMT) highlights that user behavior changes in the presence of cybersecurity threats while online [12], so it is critical for social commerce platforms to ensure the safety of platforms to their customers. Keeping this in view, our study focused on customers in Saudi Arabia.

Saudi Arabia is considered a big market for online shopping. People use different payment methods and multiple applications to buy products across the globe. In the same way, they are also concerned about the security and privacy of these mobile applications [13]. Considering the importance of security and privacy for Saudi buyers related to m-commerce, a study is conducted to analyze Saudi consumers' perspective of security and privacy concerns regarding popular m-commerce applications in the Kingdom of Saudi Arabia (KSA). In this study, a survey was conducted in which 1500 respondents took part to provide their perspective of security and privacy of seven popular m-commerce applications in the KSA. The survey was based on three important factors: Trustworthiness, use of credit card concern, and consumer rating of different factors. Each of these factors are based on multiple sub-factors that helped us to analyze the user view of these m-commerce applications. This study concluded that respondents have depicted several factors that are important for different m-commerce applications (details are given in Section 3). Although many earlier studies have focused on e-commerce adoption practices by businesses and users in Saudi Arabia (given in Section 2), none have focused on customer security perception. So, the core contribution of this work is to understand the customer security perception of mobile commerce applications in Saudi Arabia and provide a model to improve customer security perception, which can be generalized to other geographic regions as well.

The rest of the paper is structured as follows: Section 2 discusses the related work followed by material and methods in Section 3. Section 4 discusses the results followed by the discussion and conclusion in Sections 5 and 6, respectively.

## 2. Related Work

There have been numerous studies showing the importance of the security and privacy of m-commerce applications. M-commerce applications offering better security and privacy lead to customers' readiness to buy and sell products using these applications. Hidayat et al. [14] have carried out an empirical study in Indonesia and found that trust is an important factor for Indonesian consumers to carry out online shopping. Saprikis & Avlogiaris [15] have carried out an empirical study to identify the factors influencing consumers to indulge in shopping from social media applications. The results highlighted that convenience, reward, and security (ICT facilitators of the UTAUT model) have a significant impact on consumers' direct buying from social applications. Customer satisfaction is considered an important factor for customer loyalty, therefore, in another empirical work, Taherdoost and Madanchian [16] have validated the e-service satisfaction model in the context of e-commerce. Their findings highlighted trust, security, performance, and usability as core elements for achieving customer satisfaction. Harris et al. [17] have identified various factors that affect the privacy and security of mobile applications that lead them to install and use these mobile applications. Their study results indicate the relationship between security and privacy i.e., the consumers that perceive more security have greater

trust and reduced risks. Ghayoumi [18] relates six factors of e-commerce security that are also related to m-commerce. These factors are integrity, non-repudiation, authentication, confidentiality, privacy, and availability. According to their study, these factors play an important role in achieving security in m-commerce applications.

The study by Mahmoud et al. [19] aims to illustrate the growing use of m-commerce by the adoption of modern devices and fast internet and the potential challenges of privacy and security. The study focused on providing recommendations to tackle the potential challenges of privacy and security that have been on the rise with the use of m-commerce, and further focused on three main websites Amazon, Ali Baba, and eBay to analyze the user perspective on trust in m-commerce. A deductive approach and mono research method have been adopted in the study. Moreover, a random sample of 100 respondents has also been used to gain insight into the data. The author concluded that the privacy of an e-commerce environment is a bit different than the m-commerce environment, further explaining that the trust level in m-commerce systems is still low considering the privacy and security paradigm. This study further concludes the concerns of data communication concerning privacy and integrity, authentication about security, and highlights that significant room is available for improvement in tackling such challenges.

Kumar et al. [20] studied the status of using m-commerce applications in India. According to the study, users in India are hesitant to use m-commerce applications because of several reasons. One of the main identified reasons is security and payment problems in these m-commerce applications. Users believe that threats of hacking, phishing, and identity theft are always issues for them, and they cannot trust all m-commerce applications to use their credit cards and even personal information. They are also reluctant to use these apps because while making payments they must use third-party websites, which they do not trust. Venkatesh et al. [21] has also studied customer concerns about privacy with online purchases. Their study also included recommendations from different sources such as retailers and other customers' preferences, product relatedness, and discount. Analysis of survey study found a medium effect of recommendations and product relatedness on online purchases. The study found that product relatedness did not improve the effect of privacy enablers on online purchase intentions.

Similarly, Gurung et al. [22] have studied the security and privacy concerns of consumers for e-commerce. They believe that these concerns increase the risk assessment of consumers. They also investigated the association between privacy and security using the concept of organized conduct. The results suggest that privacy and security matters influence risk assessment and awareness. Trust is considered to have a major effect, followed by privacy and security disquiets. Moreover, risk awareness and trust viewpoints have effects on the mindset of people. Ali et al. [23] also investigated the role of privacy as an interpreter of security perceptions in mobile applications. Vărzaru et al. [24] have used a modified technology acceptance model to determine the antecedents on behavioral intention and consumer satisfaction in the post-COVID period. They found a positive influence of perceived usefulness and perceived ease of use on consumer intention. Similarly, D'Adamo et al. [7] have investigated the European consumers to understand their security considerations in online buying in the post-pandemic era. The study highlights that consumers from different European countries have varying sensitivity levels against cybersecurity for e-commerce applications. Hussien et al. [25] have developed a prototype to serve as an agent software among customers and electronic marketplace, where security is implemented in this agent software on the client-side to improve the performance of marketplace systems. Chen et al. [26] have proposed a forensic model which will help to recognize suspicious system behavior.

In the context of Saudi Arabia, there have also been many studies focusing on e-commerce. Miao & Tran [27] carried out a long-term study and found a notable difference between initial e-commerce adoption and intention for e-commerce institutionalization in small and medium enterprises (SMEs) between 2013 and 2016. Nachar [28] has found that perceived e-commerce platform ease of use and perceived e-commerce platform usefulness

are statistically significant in predicting customers' desire to adopt online purchasing. Al-Ayed [29] has carried out an empirical study and found that website interactivity, customer care, product choice, convenience, character, and customization of the website as key factors to foster loyalty in e-commerce customers. Saeed [30] conducted empirical research on expatriate e-business adoption in Saudi Arabia. The study highlights the need of taking cultural variations into account during the technical design stage to make user interfaces more effective. Alotaibi [31] highlighted that in terms of m-commerce consumer loyalty, there were no major variations across gender, age, or experience. Razi et al. [32] have found that students are actively engaged in social commerce activities, which impact their purchase intentions and behavior positively.

By reviewing the literature, it can be inferred that geographical and cultural environment, have an impact on users' behavior towards online shopping [10,11]. However, there is no detailed study focusing on online customers in Saudi Arabia. Since technological adoption is heavily dependent on users' motivation and perception, there exists a knowledge gap regarding how consumers in Saudi Arabia perceive security aspects of social commerce applications. Keeping this in view, this study focuses on m-commerce consumers in Saudi Arabia to understand the factors influencing their security and privacy perception. The findings of the study will help researchers and practitioners to improve customer perception by improving social commerce applications.

### 3. Materials and Methods

Our main research is based on investigating the customer perception of security and privacy of m-commerce applications in Saudi Arabia and we have used protection motivation theory as a framework. The original protection motivation theory was based on three constructs, namely the perceived threat severity, perceived threat vulnerability, and perceived efficacy of response. Those parameters were used to construct the model. In our model, perceived threat severity is evaluated based on consumer rating of the protection against fraudulent transactions, authentication of users by the vendor, authentication of the vendor by users, and secure communication channel provision as sub-factors. Perceived threat vulnerability refers to trustworthiness, where the presence of logos of well-known brands, product pictures, privacy and security seal on the website, as well as enabling the search facility on the website can increase or decrease trustworthiness. The third construct of PMT-perceived efficacy of response is modeled as credit card usage concerns, where if concerns are limited, it means that preventive measures are adequately in place. The following three hypotheses were established for the research based on the constructs of PMT constructs, as shown in Table 1.

**Hypothesis 1 (H1).** *Consumer rating of different perceived security threats to mobile commerce applications affects the security and privacy perception of customers in Saudi Arabia.*

**Hypothesis 2 (H2).** *Trustworthiness of mobile commerce applications, which is determined by perceived vulnerabilities, affects the security and privacy perception of customers in Saudi Arabia.*

**Hypothesis 3 (H3).** *Adoption of preventive measures such as secure payment mechanisms by mobile commerce applications enhances the security and privacy perception of customers in Saudi Arabia.*

To validate our hypotheses, we selected the seven most popular m-commerce applications in Saudi Arabia [33] to explore customers' insight into various factors related to the security and privacy of these applications. Furthermore, we also intended to explore which factors are considered most important for the customer when it comes to using m-commerce applications. For our study, we conducted a cross-sectional quantitative study and rolled out our survey from October 2020–December 2020. The survey questions were based on previously validated questions by Furnell et al. [34]. The survey focused on three major factors related to security and privacy: Trustworthiness, credit card usage

concerns, and consumer rating. The questionnaire was created on Google forms. Social media applications like WhatsApp, Twitter, and Instagram were used to spread the survey link and all participants were volunteers. We decided to apply the snowball sampling method [35], which started with 25 people as a referral and were asked to roll out the survey to their connections. A total of 1500 respondents took part in the survey of which 1400 valid responses were collected (200 for each m-commerce application). The first question was related to respondents' prior experience with mobile commerce applications, which was an eligibility criterion for a valid response. All responses with no experience were discarded. Based on our informal social media review, we identified the seven most popular mobile commerce applications in Saudi Arabia. At the start of the survey, the users have the option to select the application for which they would like to fill the survey. A limit of 200 valid responses for each application was set, and once the limit was achieved the relevant application became inactive for further responses. The majority of the respondents were female (65.1%), aged between 18 and 25 and single (69.2%). Data were analyzed using the partial least square method [36] using SmartPLS [37], and path models were developed for each application to understand the causal relationship among several factors.

**Table 1.** Keys for factors in the model.

Protection Motivation Theory (PMT) Constructs	Factors	Key
Perceived Security of the Threat	Consumer Rating (CR)	
	Protection against fraudulent transactions	CR1
	Authentication of users by the vendor	CR2
	Authentication of the vendor by users	CR3
	Secure Communication Channel provision	CR4
Perceived Vulnerability of the Threat	Trustworthiness (TR)	
	Logo of well-known brands presence	TR1
	Presence of product pictures	TR2
	Presence of privacy seal on the website	TR3
	Enabling of the search facility on the website	TR4
Perceived Response Efficacy of Preventive Measures	Presence of security seal on the website	TR5
	Credit Card Usage Concerns (CC)	
	Application security perception	CC1
	Network deficiency perception	CC2
	Operating system security concerns	CC3
	Unauthorized transactions concerns	CC4

As shown in Table 1, application security perception, network deficiency perception, operating system security concerns, and unauthorized transactions concerns are considered sub-factors for this construct. In the beginning, we developed a path for Amazon KSA considering all three factors and their sub-factors. The details of subfactors are listed in Table 1.

Figure 1 shows the basic model, which was tested using SmartPLS on the data of Amazon KSA. It was observed that indicators related to consumer rating showed negative values that also made the final consumer rating negative. Based on observed facts, this factor was removed to reconstruct the model shown in Figure 2. A similar pattern was applied on all applications as initial models were developed and tested to find any negative correlation among factors. Later models were reconstructed to conclude. The following parameters were used to test the reliability and quality of the factors used in the models: Average Variance Extraction (AVE) > 0.5, Cronbach's alpha ( $\alpha$ ) > 0.7, and composite reliability > 0.7 [38].

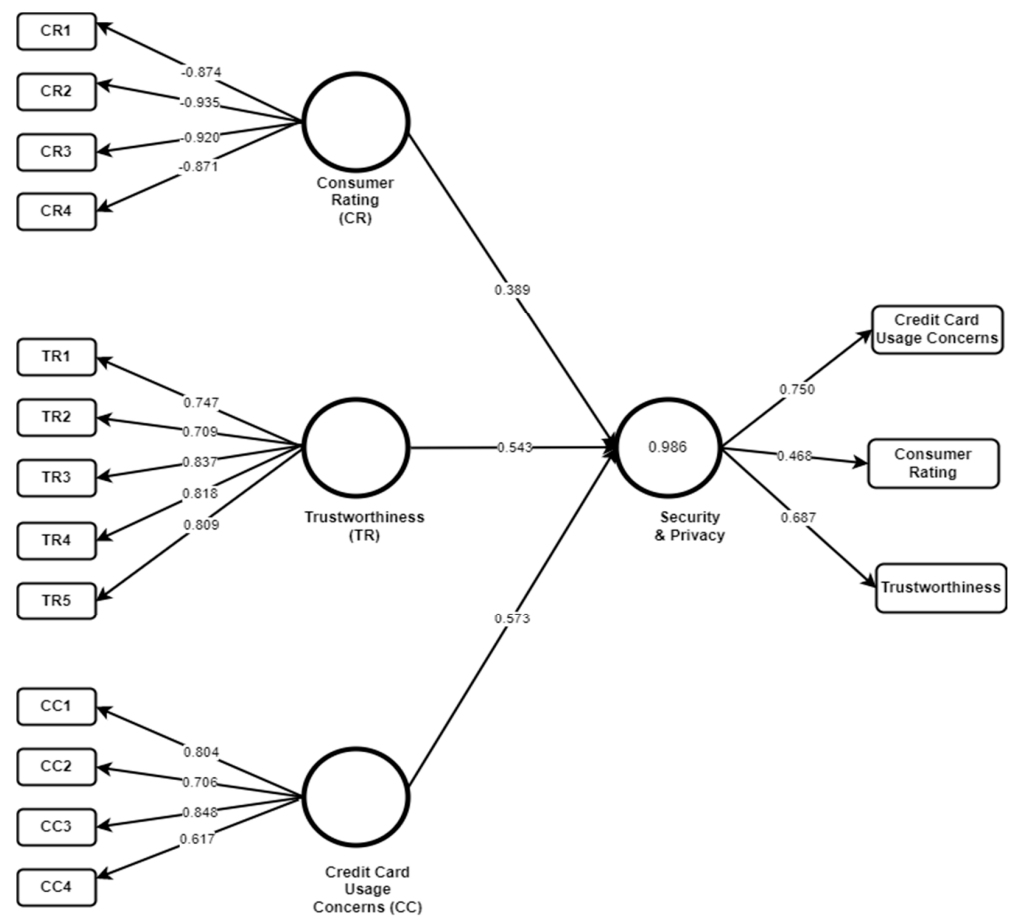


Figure 1. Amazon KSA-Model 1.

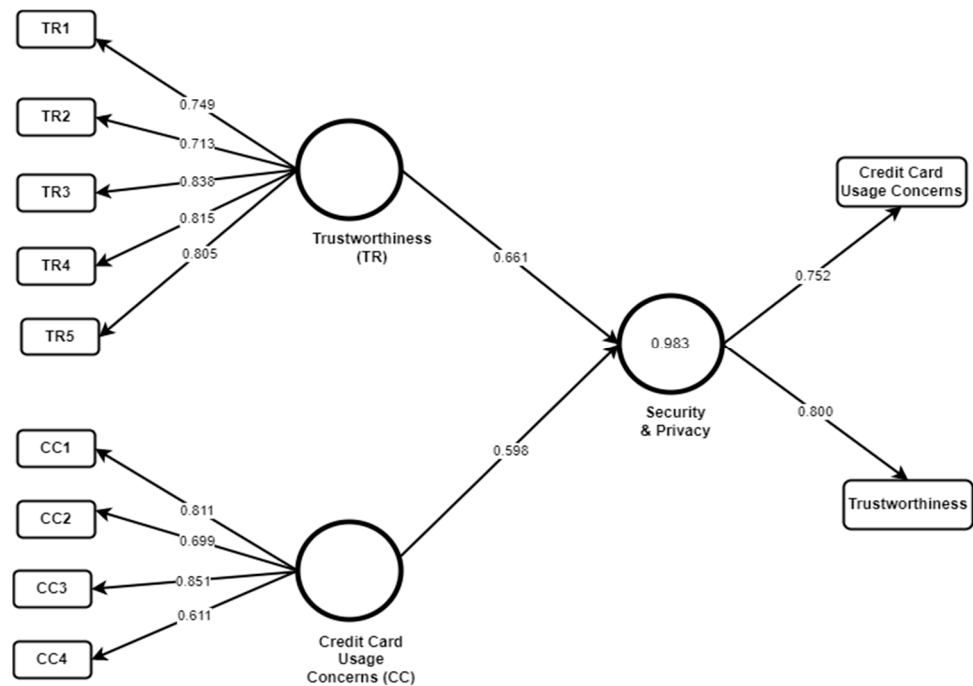


Figure 2. Amazon KSA Model 2.



## 4. Results

This section presents the results of our findings for each of the mobile commerce applications under study.

### 4.1. Amazon KSA

Figure 2 shows the revised structural model for Amazon KSA. The customer perspective of security and privacy is based on trustworthiness and credit card concerns only. After partial square application  $R^2$ , the value for the latent variable Security and Privacy was 0.983, which is a substantial value according to Hair et al. [39]. Therefore, these findings highlight that there is a direct correlation of security and privacy with these two factors. Furthermore, bootstrapping was conducted for the level of path coefficients analysis with about 5000 subsamples. Results show that trustworthiness and credit card concern are considered important for the security and privacy of this application. ( $p < 0.01$  where  $\beta$  (Trustworthiness) = 0.598 and  $\beta$  (Credit Card Usage Concerns) = 0.661). It indicated that both trustworthiness and Credit Card Concerns are significant factors to foster security and privacy.

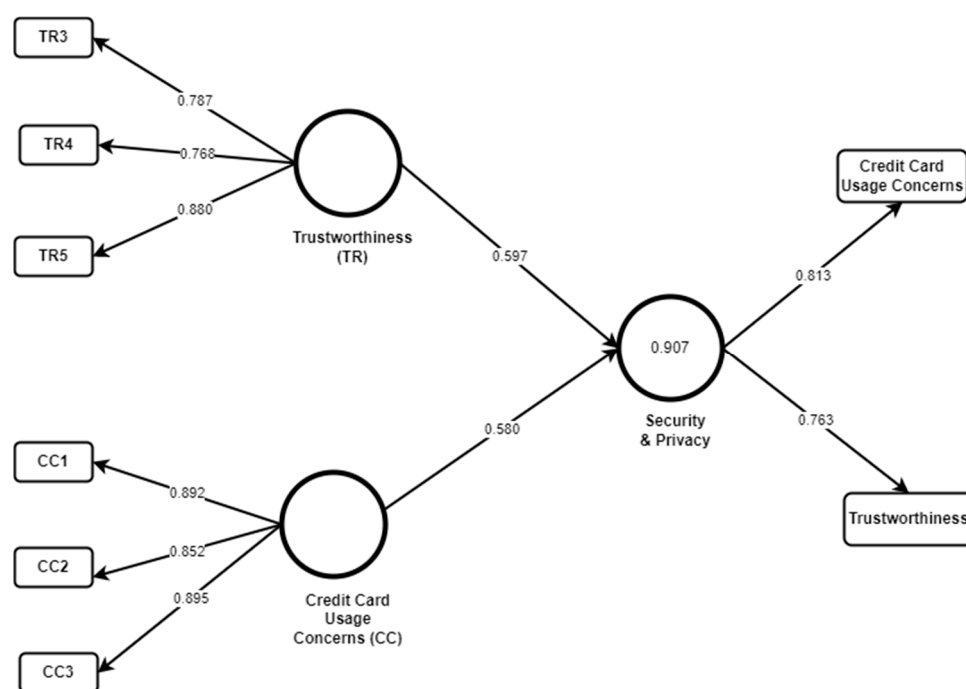
Predictive relevance is used to analyze the model's ability to foresee each latent variable or factor. Predictive relevance ( $Q^2$ ) was calculated by applying blindfolding using the omission distance of  $D = 7$ . Blindfolding results give  $Q^2 = 0.573$  which is greater than 0, indicating that the model has predictive relevance. As far as the quality and reliability of factors are concerned, the Amazon model shows AVE (credit card usage concerns) as 0.561 and AVE (trustworthiness) as 0.617, which are above the threshold value of 0.5. It shows that both factors have shown high levels of convergent validity. Similarly, as shown in Table 2, Cronbach's alpha and composite reliability of both factors are above the threshold of 0.7 showing the reliability of these factors.

**Table 2.** Predictive relevance of model factors for Amazon KSA.

Factors	$\beta$ Value	$Q^2$ ( $=1 - SSE/SSO$ )	Average Variance Extraction (AVE)	Cronbach's Alpha ( $\alpha$ )	Composite Reliability
Credit Card Usage Concerns	0.661	-	0.561	0.736	0.834
Trustworthiness	0.598	-	0.617	0.844	0.889
Security and Privacy	-	0.573	-	-	-

### 4.2. CenterPoint

Figure 3 shows the structural model for CenterPoint. The model was first developed considering all three factors, out of which customer rating shows the negative value and has been removed from the path model. Moreover, the indicators that had a value less than 0.7 were removed as they were not significantly contributing to the latent variable. After partial square application  $R^2$ , the value for the latent variable security and privacy was 0.907, which is a substantial value according to Hair et al. [39]. Therefore, these findings highlight that there is a direct correlation of security and privacy with these two factors.



**Figure 3.** CenterPoint model.

These models clearly state that all factors related to customer rating have been given a low rating by the customers, while factors having trustworthiness and a credit card are considered the most important issues for this application. Furthermore, bootstrapping was conducted for the level of path coefficients analysis with about 5000 subsamples. As shown in Table 3, results show that trustworthiness and credit card concern are considered important for the security and privacy of this application ( $p < 0.01$  where  $\beta$  (Trustworthiness) = 0.597 and  $\beta$  (Credit Card Usage Concerns) = 0.580). It indicated that both trustworthiness and Credit Card Concerns are significant factors to foster security and privacy for the customers of the application. Predictive relevance ( $Q^2$ ) was calculated by applying blindfolding using the omission distance of  $D = 7$ . Blindfolding results gives  $Q^2 = 0.551$  which is greater than 0, showing that the model has predictive relevance. Average Variance Extraction (AVE) values for Credit Card Usage Concerns (0.755) and Trustworthiness (0.661) are above the target values showing the high level of convergent reliability in the factors. Moreover,  $\alpha$  and composite reliability values also indicate the factor's reliability for Center Point as shown in Table 3.

**Table 3.** Predictive relevance of model factors for CenterPoint.

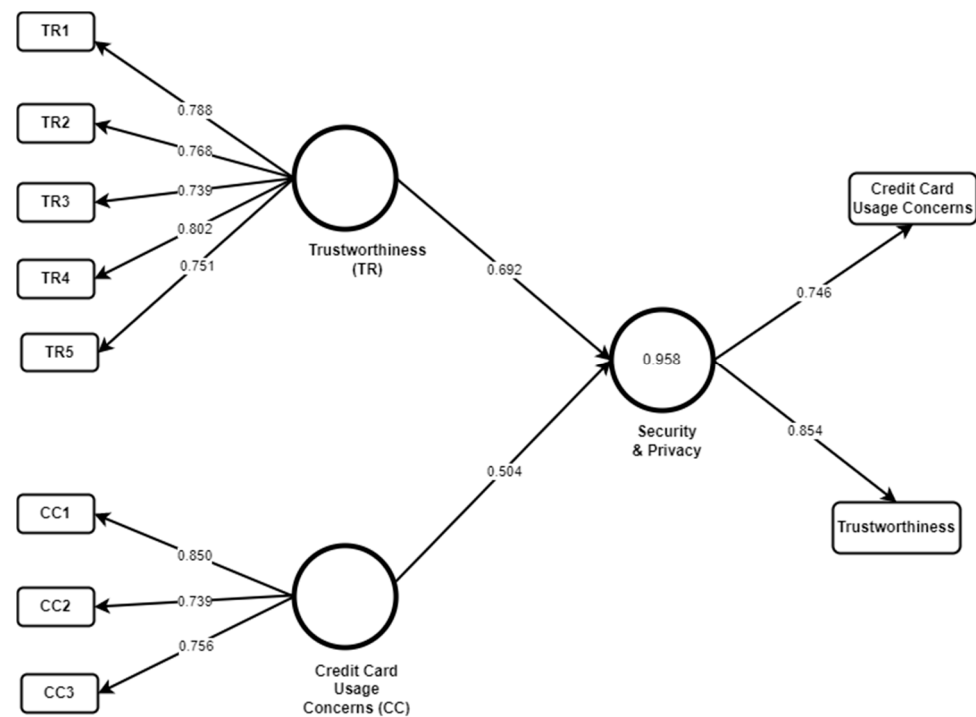
Factors	$\beta$ Value	$Q^2$ ( $=1 - SSE/SSO$ )	Average Variance Extraction (AVE)	Cronbach's Alpha ( $\alpha$ )	Composite Reliability
Credit Card Usage Concerns	0.580	-	0.775	0.854	0.912
Trustworthiness	0.597	-	0.661	0.741	0.854
Security and Privacy	-	0.551	-	-	-

#### 4.3. Hunger Station

Figure 4 shows the structural model for Hunger Station. The model was first developed considering all three factors, out of which customer rating shows the negative value and has been removed from the path model. Moreover, the indicators having a value less than



0.7 were removed as they were not significantly contributing to the latent variable. After partial square application  $R^2$ , the value for the latent variable Security and Privacy was 0.958, which is a substantial value according to Hair et al. [39]. Therefore, these findings highlight that there is a direct correlation of security and privacy with these two factors. These models clearly state that all the factors related to customer rating have been given a low rating by the customers, while factors having trustworthiness and a credit card are considered as the most important issues for this application.



**Figure 4.** Hunger Station model.

Furthermore, bootstrapping was conducted for the level of path coefficients analysis with about 5000 subsamples. Results show that Trustworthiness and Credit Card Concern are considered important for the security and privacy of this application ( $p < 0.01$  where  $\beta$  (Trustworthiness) = 0.692 and  $\beta$  (Credit Card Usage Concern) = 0.506). It indicated that both Trustworthiness and Credit Card Concerns are significant factors to foster security and privacy for customers of the application. Like other applications, blindfolding was applied to examine predictive relevance ( $Q^2$ ). Blindfolding gives  $Q^2 = 0.592$  which is greater than 0, showing that this model also has predictive relevance. As shown in Table 4, Average Variance Extraction (AVE), Cronbach's alpha, and composite reliability values above the minimum threshold value indicate that both factors are reliable for Hunger Station.

**Table 4.** Predictive relevance of model factors for Hunger Station.

Factors	$\beta$ Value	$Q^2$ ( $=1 - SSE/SSO$ )	Average Variance Extraction (AVE)	Cronbach's Alpha ( $\alpha$ )	Composite Reliability
Credit Card Usage Concerns	0.506	-	0.613	0.712	0.826
Trustworthiness	0.692	-	0.593	0.828	0.879
Security and Privacy	-	0.592	-	-	-

#### 4.4. Namshi

Figure 5 shows the structural model for Namshi. The model was first developed considering all three factors, out of which credit card concern shows a negative value and has been removed from the path model. Moreover, the indicators having a value less than 0.7 were removed as they were not significantly contributing to the latent variable. After partial square application  $R^2$ , the value for the latent variable Security and Privacy was 1, which is a perfect fit value according to Hair et al. [39]. Therefore, these findings highlight that there is a direct correlation of security and privacy with these two factors. These models clearly state that all factors related to credit card concerns have been given a low rating by customers, while factors with trustworthiness and customer rating are considered as the most important issues for this application.

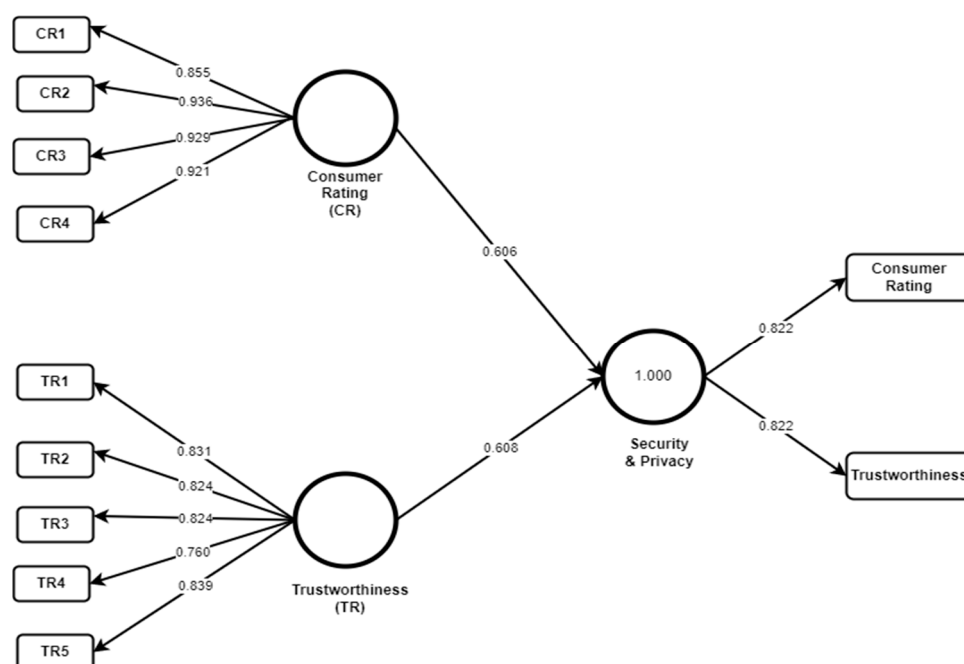


Figure 5. Namshi model.

Furthermore, bootstrapping was conducted for the level of path coefficients analysis with about 5000 subsamples. Results show that trustworthiness and credit card concern are considered important for the security and privacy of this application ( $p < 0.01$  where  $\beta$  (Trustworthiness) = 0.608 and  $\beta$  (Customer Rating) = 0.606). It indicated that both Trustworthiness and Customer Rating are significant factors to foster security and privacy for customers of the application. Blindfolding with omission distance  $D = 7$  results gives  $Q^2 = 0.653$  which is greater than 0, indicating that the model has predictive relevance. As shown in Table 5, the reliability of factors (Consumer Rating and Trustworthiness) can be proved by the AVE,  $\alpha$ , and composite reliability values given as below. All these values are above the threshold.

Table 5. Predictive relevance of model factors for Namshi.

Factors	$\beta$ Value	$Q^2$ (=1 – SSE/SSO)	Average Variance Extraction (AVE)	Cronbach's Alpha ( $\alpha$ )	Composite Reliability
Consumer Rating	0.606	-	0.83	0.931	0.951
Trustworthiness	0.608	-	0.666	0.874	0.909
Security and Privacy	-	0.653	-	-	-

#### 4.5. NOON

Figure 6 shows the structural model for NOON. The model was first developed considering all three factors, out of which customer rating shows a negative value and has been removed from the path model. Moreover, the indicators having a value less than 0.7 were removed as they were not significantly contributing to the latent variable. After partial square application  $R^2$ , the value for the latent variable Security and Privacy was 0.953, which is a substantial value according to Hair et al. [39]. Therefore, these findings highlight that there is a direct correlation of security and privacy with these two factors. These models clearly state that all the factors related to customer rating have been given low ratings by the customers, while factors relating to trustworthiness and a credit card are considered as the most important issues for this application.

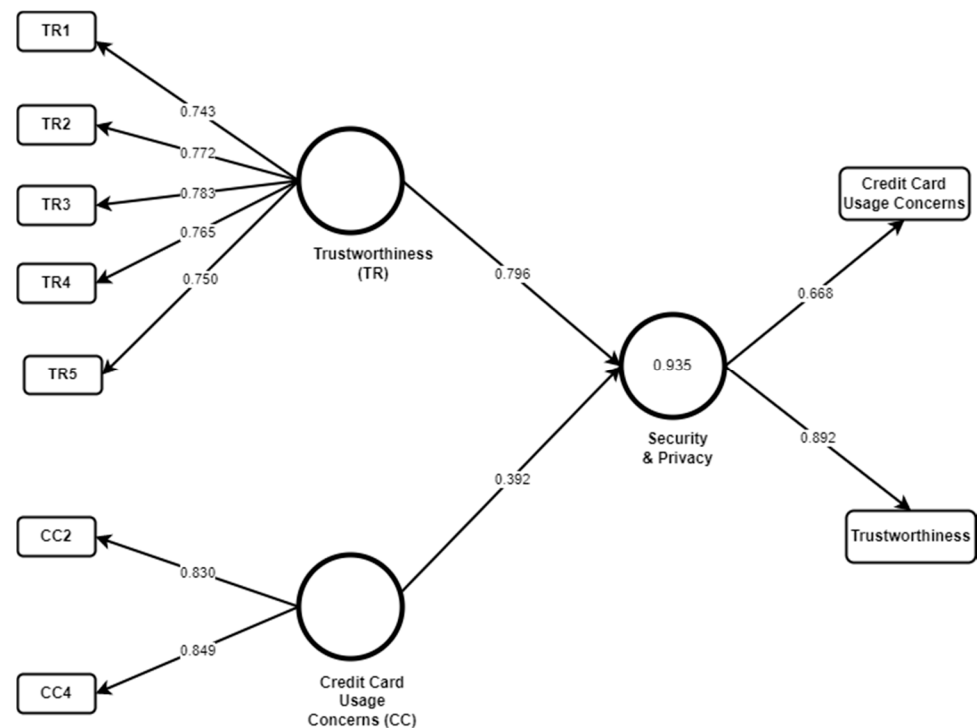


Figure 6. NOON Model.

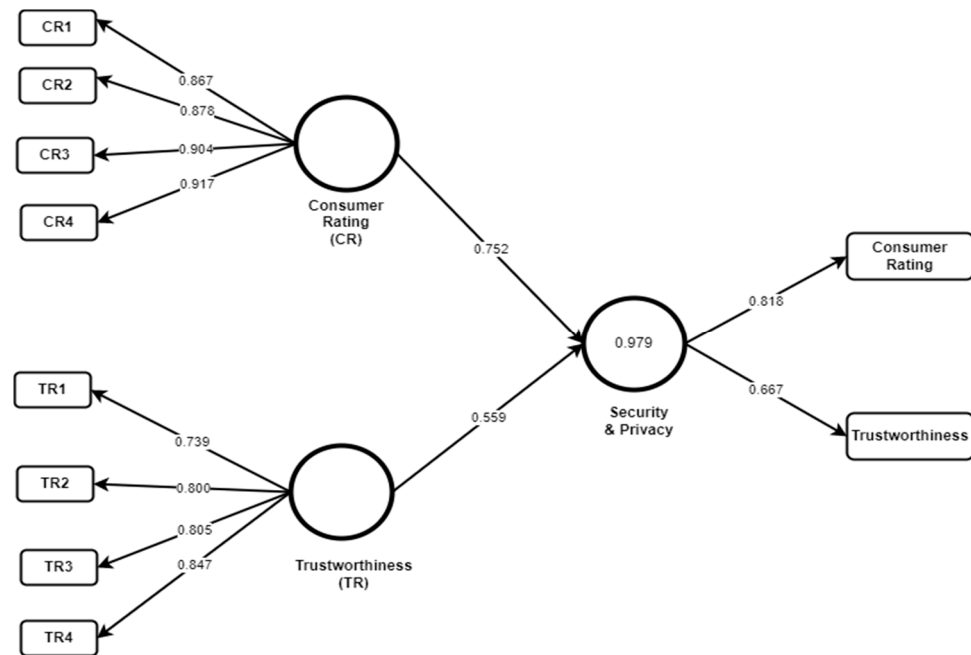
Furthermore, bootstrapping was conducted for the level of path coefficients analysis with about 5000 subsamples. Results show that trustworthiness and credit card concern are considered important for the security and privacy of this application ( $p < 0.01$  where  $\beta$  (Trustworthiness) = 0.678 and  $\beta$  (Credit Card Usage Concerns) = 0.560). It indicated that both trustworthiness and Credit Card Usage Concerns are significant factors to foster security and privacy for the customers of the application. Predictive relevance ( $Q^2$ ) was calculated by applying blindfolding. Blindfolding with omission distance  $D = 7$  results gives  $Q^2 = 0.581$  which is greater than 0, showing that this model also has predictive relevance. As shown in Table 6, both the factors Credit Card Usage Concerns and Trustworthiness are considered as reliable for NOON, as all of these values are above the target value for NOON, except for Cronbach's alpha ( $\alpha$ ) value of Credit Card Usage Concerns, which is a little lower.

**Table 6.** Predictive relevance of model factors for NOON.

Factors	$\beta$ Value	$Q^2$ ( $=1 - SSE/SSO$ )	Average Variance Extraction (AVE)	Cronbach's Alpha ( $\alpha$ )	Composite Reliability
Credit Card Usage Concerns	0.560	-	0.705	0.581	0.827
Trustworthiness	0.678	-	0.582	0.82	0.874
Security and Privacy	-	0.581	-	-	-

#### 4.6. OUNAS

Figure 7 shows the structural model for OUNAS. The model was first developed considering all three factors, out of which the use of credit cards shows a negative value and has been removed from the path model, which shows that people do not trust OUNAS to use their credit card information. Moreover, many indicators with a value less than 0.7 were removed as they were not significantly contributing to the latent variable. After partial square application  $R^2$ , the value for the latent variable Security and Privacy was 0.979, which is a substantial value according to Hair et al. [39]. Therefore, these findings highlight that there is a direct correlation of security and privacy with these two factors.

**Figure 7.** OUNAS model.

These models clearly state that all factors related to a credit card have been given a low rating by the customers, while factors having trustworthiness and customer rating are considered as the most important issues for this application. Furthermore, bootstrapping was conducted for the level of path coefficients analysis with about 5000 subsamples. Results show that trustworthiness and credit card concern are considered important for the security and privacy of this application ( $p < 0.01$  where  $\beta$  (Trustworthiness) = 0.559 and  $\beta$  (Customer Rating) = 0.752). It indicated that both trustworthiness and Credit Card Usage Concerns are significant factors to foster security and privacy for the customers of the application. Here, likewise other applications, we also intend to examine the predictive relevance of the model by applying blindfolding. The results give  $Q^2 = 0.506$ , which is greater than 0, showing that the model has predictive relevance. As shown in Table 7,

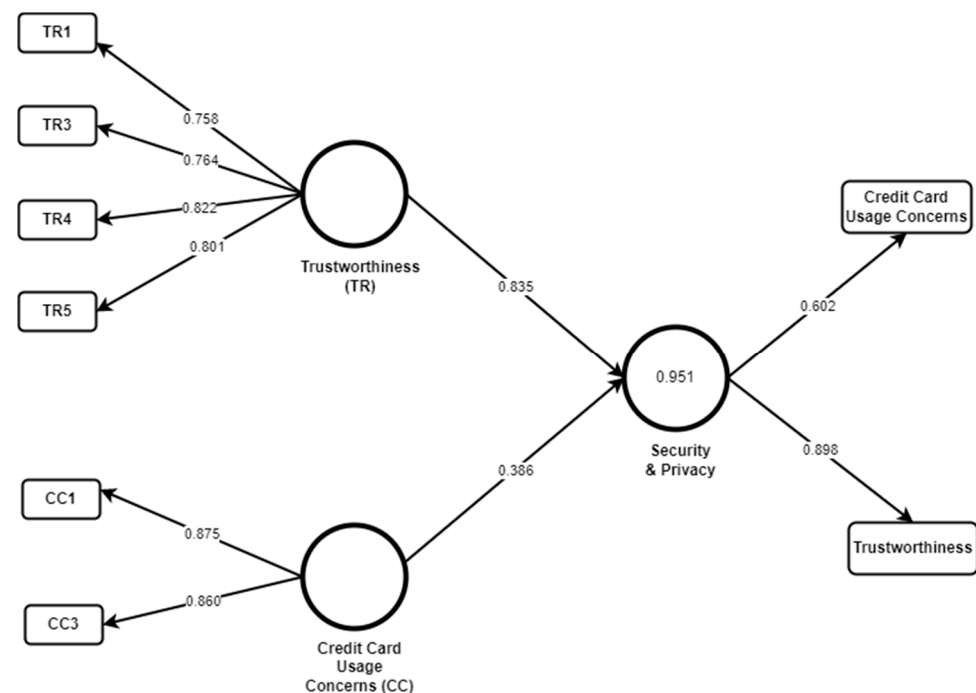
Average Variance Extraction (AVE), Cronbach's alpha, and the composite reliability factor values for OUNAS indicate reliability as all values are above the recommended values.

**Table 7.** Predictive relevance of model factors for OUNAS.

Factors	$\beta$ Value	$Q^2$ (=1 – SSE/SSO)	Average Variance Extraction (AVE)	Cronbach's Alpha ( $\alpha$ )	Composite Reliability
Consumer Rating	0.752	-	0.795	0.914	0.939
Trustworthiness	0.559	-	0.578	0.816	0.872
Security and Privacy	-	0.506	-	-	-

#### 4.7. SHEIN

Figure 8 shows the structural model for SHEIN. The model was first developed considering all three factors, out of which customer rating shows the negative value and has been removed from the path model. Moreover, the indicators with a value less than 0.7 were removed as they were not significantly contributing to the latent variable. After partial square application  $R^2$ , the value for the latent variable Security and Privacy was 0.951, which is a substantial value according to Hair et al. [39]. Therefore, these findings highlight that there is a direct correlation of security and privacy with these two factors.



**Figure 8.** SHEIN model.

These models clearly state that all factors related to customer rating have been given a low rating by the customers, while factors regarding trustworthiness and a credit card are considered as most important issues for this application. Furthermore, bootstrapping was conducted for the level of path coefficients analysis with about 5000 subsamples. Results show that Trustworthiness and Credit Card Concern are considered important for the security and privacy of this application ( $p < 0.01$  where  $\beta$  (Trustworthiness) = 0.835 and  $\beta$  (Credit Card Usage Concern) = 0.386). It indicated that both Trustworthiness and Credit Card Concerns are more significant factors to foster security and privacy for the customers of the application. Like other applications, Blindfolding with omission distance  $D = 7$  results

gives  $Q^2 = 0.504$  which is greater than 0, showing that the model has predictive relevance. As shown in Table 8, Average Variance Extraction (AVE) and composite reliability values are higher than the threshold. These results indicate that both factors are considered reliable for SHEIN.

**Table 8.** Predictive relevance of model factors for SHEIN.

Factors	$\beta$ Value	$Q^2$ ( $=1 - SSE/SSO$ )	Average Variance Extraction (AVE)	Cronbach's Alpha ( $\alpha$ )	Composite Reliability
Credit Card Usage Concerns	0.386	-	0.574	0.625	0.801
Trustworthiness	0.835	-	0.568	0.81	0.867
Security and Privacy	-	0.504	-	-	-

The results are summarized in Tables 9–11. Table 9 highlights that consumers think that Namshi and Ounas applications have positive ratings for all four factors, whereas all other applications scored negatively for these factors. As shown in Table 10, in the context of trustworthiness, Amazon, Namshi, and Noon applications received a positive ranking in all parameters, whereas Ounas and Hunger station applications received a negative ranking in all parameters. Centerpoint application received negative ratings for the presence of logo and product pictures and SHEIN applications received negative ranking only for product pictures. As shown in Table 11, in the case of credit card security, none of the applications received a positive ranking for all parameters. Namshi and Ounas applications received negative rankings for all parameters. CenterPoint and Hunger Station received positive ratings for application security, network, and operating system security. Amazon KSA and SHEIN applications received positive ratings only for application and operating system security parameters. In the case of the NOON application only network security and unauthorized transaction preventions secured positive ratings. Overall, the results highlight that there is a need for improving the customer security perception in the Saudi Arabian e-commerce sector. As shown in Table 9, five out of seven applications did not receive a positive rating for any of the factors, therefore our hypothesis “Consumer rating of different perceived security threats to mobile commerce applications affects the security and privacy perception of customers in Saudi Arabia” is approved as results show that customers are not satisfied with the majority of social commerce applications in Saudi Arabia. The issues like provision of fraudulent protection, secure communication, and authentication can help in improving customer perception of security and privacy.

**Table 9.** Customer rating summary.

Application	Against Fraudulent Protection	Authentication of Vendor	Authentication by Customer	Secure Communication
Amazon KSA	-	-	-	-
CenterPoint	-	-	-	-
Hunger Station	-	-	-	-
Namshi	Y	Y	Y	Y
NOON	-	-	-	-
OUNAS	Y	Y	Y	Y
SHEIN	-	-	-	-



**Table 10.** Trustworthiness summary.

Application	Logo of Brand	Picture of Product	Privacy Seal	Security Seal	Search Facility
Amazon KSA	Y	Y	Y	Y	Y
CenterPoint	-	-	Y	Y	Y
Hunger station	-	-	-	-	-
Namshi	Y	Y	Y	Y	Y
NOON	Y	Y	Y	Y	Y
OUNAS	-	-	-	-	-
SHEIN	Y	-	Y	Y	Y

**Table 11.** Credit Card Security summary.

Application	App_Security	Network Deficiency	OS Security Concern	Unauthorized Transactions
Amazon KSA	Y	-	Y	-
CenterPoint	Y	Y	Y	-
Hunger station	Y	Y	Y	-
Namshi	-	-	-	-
NOON	-	Y	-	Y
OUNAS	-	-	-	-
SHEIN	Y	-	Y	-

As shown in Table 10, there are only two applications that did not receive a positive rating for any of the factors, whereas the other five achieved a positive rating for at least one of the factors. In the case of our second hypothesis, “Trustworthiness of mobile commerce applications, which is determined by perceived vulnerabilities, affects the security and privacy perception of customers in Saudi Arabia” is also approved as the results confirmed that different trustworthiness factors increase/decrease the perceived threat vulnerability. The majority of social commerce applications in Saudi Arabia are seen as trustworthy by consumers.

As shown in Table 11, only two out of seven applications did not receive a positive rating for any of the factors relevant to credit card security, whereas others have at least one positive rating. So, the third hypothesis, “Adoption of preventive measures such as secure payment mechanisms by mobile commerce applications enhances the security and privacy perception of customers in Saudi Arabia” is approved as well, as it was shown that preventive measures increase the perception of security and privacy among customers in Saudi Arabia.

## 5. Discussion

Security risks impact customers’ online behavior [40,41], and our empirical findings highlight that vendors in Saudi Arabia need to improve customers’ security perception to improve e-commerce sales.

### 5.1. Theoretical Implications

Protection Motivation theory [42] has widely been used in the health sector to determine the behavioral changes in patients confronted with higher medical risk. Recently, cybersecurity literature has adopted this to understand the users’ online behavior. Our study contributes to this understanding by exploring customer security perception in Saudi Arabia while engaging in mobile commerce. As the PLS model of different mobile applications suggest that due to the different design of these mobile applications the presence of the factors is varied, which affects the intended customer behavior. The empirical data highlights that security perceptions of customers are different while engaging with different

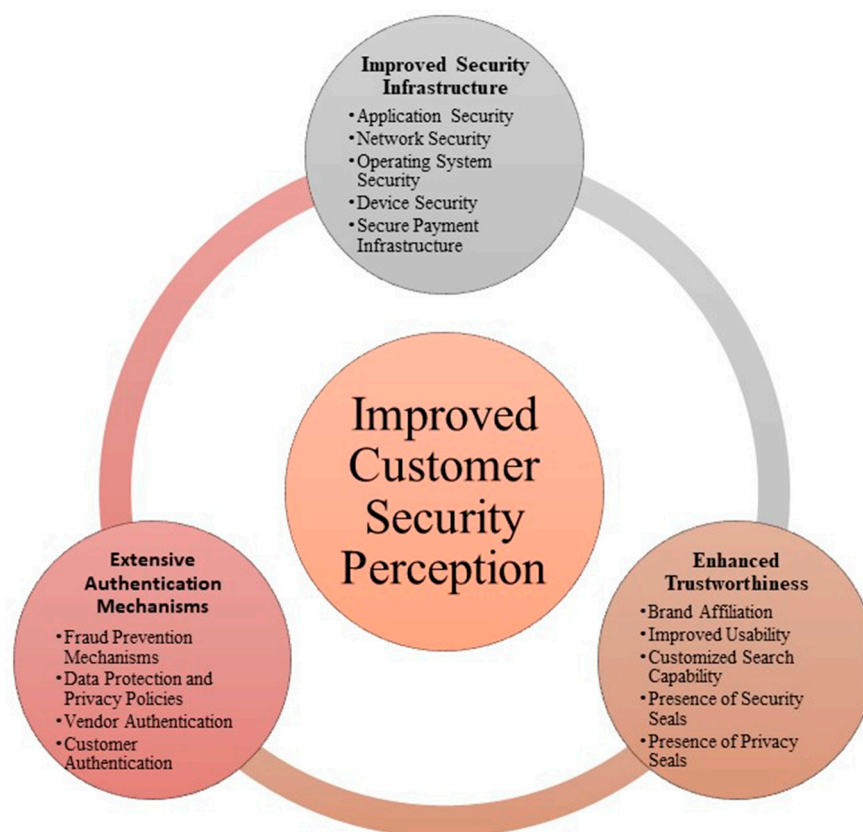
mobile commerce websites, which is inline with the PMT, highlighting that behavior is modeled based on the three specified constructs.

### 5.2. Practical Implications

The design and development of e-commerce applications is a complex task. The results of our studies have practical implications for technology managers. As different social commerce applications are developed by a different set of developers, some features of one platform may be more well designed than some aspects in others. As we have seen, the model for each application had a variety of attributes in the respective model, highlighting only the factors that received a positive rating for that application. The other missing factors received negative ratings, so they were omitted from the model and respective applications need to work on their applications to improve the missing aspects. As shown in Table 2, users rated negatively Amazon KSA, CenterPoint, Hunger Station, NOON, and SHEIN applications, so these applications need not only to improve their technological infrastructure but also raise awareness to end-users regarding their technical competence so that end users can have confidence about the security aspects of these applications. Similarly, Ounas and Hunger Station applications need to improve their usability by providing better search facilities and displaying detailed product information and security seals and certificates. Overall, payment mechanisms were evaluated positively, however, Namshi and Ounas applications need to improve their payment mechanism to secure them. The findings highlight that the designers of social commerce applications need to appropriate their applications as a weakness in one aspect that can negatively affect customers' perceptions.

Therefore, we presented a model shown in Figure 9 to improve customer security perception, which focuses on three important aspects, namely extensive authentication mechanisms, enhanced trustworthiness, and improved security infrastructure. The security of the mobile application is important for customers and there is a need for effective security assurance processes to ensure that the functional logic of mobile e-commerce applications is secure [43,44]. Network security is another important factor where e-commerce vendors need to focus [45,46]. Operating systems are another important source of security vulnerabilities and e-commerce infrastructures need to ensure that operating system vulnerabilities are appropriately handled [47–49]. E-commerce infrastructures need to be robust so that they can identify and respond to malicious activities by customer devices [50]. Payment security is one of the biggest concerns and mobile commerce vendors need to provide a secure payment system to boost customer confidence [51–53]. With the advent of cryptocurrencies, the vendors need to also weigh the possibilities of securely integrating crypto payment mechanisms [54].

Trust in e-commerce applications is another important dimension for e-commerce security acceptance [55]. To enhance the trustworthiness of e-commerce applications, the vendors can affiliate with well-known brands [56] and improve the usability of applications for better navigation [57–60]. Features like customized search and security and privacy seals [61,62] on applications also contribute positively to customers' trust. Therefore, it is important to adopt a customer-centric approach to improve the design of e-commerce applications [63]. The adoption of a sound authentication mechanism is also an important factor to enhance customer satisfaction [64]. E-commerce applications need to have an effective fraud detection mechanism in place [65]. A design of comprehensive data protection and privacy policies will improve customers' understanding of prevailing policies and make them more comfortable in indulging in online shopping [66]. Similarly, vendor authentication and customer authentication procedures are other important factors to improve customer perception [67].



**Figure 9.** Improved customer security perception.

### 5.3. Limitations

Our study relied on quantitative data, so it is vulnerable to inherent weaknesses of the qualitative approach such as finding causal relationships and a representative sample. In our study, we relied on only 200 responses for each application, so these respondents may not reflect the total population characteristics of the entire population of Saudi mobile commerce customers. Furthermore, demographic factors of respondents and imbalanced representation of respondents from the different geographical regions may impact our findings to generalize [68]. On the other hand, investigating causal relationships between empirical data is difficult due to limited details in closed-ended questions, so finding the detailed reasons for user responses was also not possible. Such details require rich descriptive data, so we intend to complement our study with a follow-up qualitative study to understand the detailed reasons, which will help practitioners and researchers to consider these findings in the design process [69].

## 6. Conclusions

Mobile commerce applications have seen a significant increase in their popularity during and after COVID-19. However, to sustain customer loyalty, customers must have a positive perception regarding the security of e-commerce applications. Due to diverse social and cultural implications, each geographic setting pose additional challenges to the adoption of mobile commerce. In this paper, we have taken a representative sample of e-commerce applications in Saudi Arabia to determine the security perceptions of customers. After conducting an empirical survey study, the findings show that the apparent privacy hazard negatively affects the perceived security of mobile applications. Similarly, an effective privacy policy positively influences customer perceptions of mobile application security. The results also highlight that users have different privacy-security perceptions based on the information sensitivity of the mobile application. Our findings are in line with the protection motivation theory, which highlights the perceived severity of the threat,

the perceived vulnerability of threat, and the perceived response efficacy of preventive measures model user behavior. Our study highlights that there is a need to improve customer perception and we have presented a model to improve customer perception. In the future, we can generalize this model by testing it in different geographical and cultural settings.

**Author Contributions:** Conceptualization, S.S. and H.G.; methodology, S.H.A.Q. and A.A.; validation, M.S.; data curation, S.Z.I.; writing—original draft preparation, H.G. and S.S.; writing—review and editing, Y.A.B.; M.A.A. and D.A.A.; supervision, S.Z.I. All authors have read and agreed to the published version of the manuscript.

**Funding:** The authors would like to thank SAUDI ARAMCO Cybersecurity Chair, Imam Abdulrahman Bin Faisal University for funding this project.

**Institutional Review Board Statement:** The study was conducted according to the guidelines of the Declaration of Helsinki, and approved by the Computer Information Systems department of College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University (CIS-009: 13 September 2020).

**Informed Consent Statement:** Informed consent was obtained from all subjects involved in the study.

**Data Availability Statement:** The data presented in this study are available on request from the corresponding author. The data are not publicly available due to privacy.

**Acknowledgments:** The authors would like to thank anonymous reviewers for their valuable comments to improve our manuscript and all subjects in filling our questionnaire.

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

## References

1. Reyachav, I.; Beeri, R.; Balapour, A.; Raban, D.R.; Sabherwal, R.; Azuri, J. How reliable are self-assessments using mobile technology in healthcare? The effects of technology identity and self-efficacy. *Comput. Hum. Behav.* **2019**, *91*, 52–61. [\[CrossRef\]](#)
2. Taneja, B. The Digital Edge for M-Commerce to Replace E-Commerce. In *Emerging Challenges, Solutions, and Best Practices for Digital Enterprise Transformation*; IGI Global: Hershey, PA, USA, 2021; pp. 299–318.
3. Ortiz, J. The global environment through the SLEPT framework. *Int. J. Bus. Glob.* **2010**, *5*, 475–492. [\[CrossRef\]](#)
4. Chaffey, D.; Edmundson-Bird, D.; Hemphill, T. *Digital Business and E-Commerce Management*; Pearson: London, UK, 2019.
5. Saeed, S.; Bolívar, M.P.R.; Thurasamy, R. *Pandemic, Lockdown, and Digital Transformation*; Springer: Berlin/Heidelberg, Germany, 2021.
6. Niranjnamurthy, M.; Kavyashree, N.; Chahar, S.J.D. Analysis of E-Commerce and M-Commerce: Advantages, Limitations and Security issues. *Int. J. Adv. Res. Comput. Commun. Eng.* **2013**, *2*, 2360–2370.
7. D’Adamo, I.; González-Sánchez, R.; Medina-Salgado, M.S.; Settembre-Blundo, D. E-Commerce Calls for Cyber-Security and Sustainability: How European Citizens Look for a Trusted Online Environment. *Sustainability* **2021**, *13*, 6752. [\[CrossRef\]](#)
8. Pabian, A.; Pabian, B.; Reformat, B. E-Customer Security as a Social Value in the Sphere of Sustainability. *Sustainability* **2020**, *12*, 10590. [\[CrossRef\]](#)
9. Fathima, K.; Balaji, D.S. Enhancing Security in M-Commerce Transactions Enhancing Security in M-Commerce Transactions. *Ann. Rom. Soc. Cell Biol.* **2021**, *25*, 3915–3921.
10. Clemons, E.K.; Wilson, J.; Matt, C.; Hess, T.; Ren, F.; Jin, F.; Koh, N.S. Global Differences in Online Shopping Behavior: Understanding Factors Leading to Trust. *J. Manag. Inf. Syst.* **2016**, *33*, 1117–1148. [\[CrossRef\]](#)
11. Mohammed, Z.A.; Tejay, G.P. Examining privacy concerns and ecommerce adoption in developing countries: The impact of culture in shaping individuals’ perceptions toward technology. *Comput. Secur.* **2017**, *67*, 254–265. [\[CrossRef\]](#)
12. Lee, D.; LaRose, R.; Rifon, N. Keeping our network safe: A model of online protection behaviour. *Behav. Inf. Technol.* **2008**, *27*, 445–454. [\[CrossRef\]](#)
13. Alotaibi, A.R.; Faleel, J. Investigating the preferred methods of payment for online shopping by Saudi Customers. *PalArch’s J. Archaeol. Egypt Egyptol.* **2021**, *18*, 1041–1051.
14. Hidayat, A.; Wijaya, T.; Ishak, A.; Catyanadika, P.E. Consumer Trust as the Antecedent of Online Consumer Purchase Decision. *Information* **2021**, *12*, 145. [\[CrossRef\]](#)
15. Saprikis, V.; Avlogiaris, G. Factors That Determine the Adoption Intention of Direct Mobile Purchases through Social Media Apps. *Information* **2021**, *12*, 449. [\[CrossRef\]](#)
16. Taherdoost, H.; Madanchian, M. Empirical Modeling of Customer Satisfaction for E-Services in Cross-Border E-Commerce. *Electronics* **2021**, *10*, 1547. [\[CrossRef\]](#)
17. Harris, M.A.; Brookshire, R.; Chin, A.G. Identifying factors influencing consumers’ intent to install mobile applications. *Int. J. Inf. Manag.* **2016**, *36*, 441–450. [\[CrossRef\]](#)

18. Ghayoumi, M. Review of Security and Privacy Issues in e-Commerce. In Proceedings of the International Conference on e-Learning, e-Business, Enterprise Information Systems, and e-Government, Las Vegas, NV, USA, 25–28 July 2016; p. 156.
19. Mahmoud, M.A.; Khrais, L.; AlOlayan, R.M.; Alkaabi, A.M.; Suwaidi, S.Q.A.; Alghamdi, B.A.; Aljuwaie, H.F. Consumers Trust, Privacy and Security Issues on Mobile Commerce Websites. *Mod. Appl. Sci.* **2019**, *13*, p21. [\[CrossRef\]](#)
20. Kumar, U.; Gope, A.K.; Singh, S. Emerging Challenges and Opportunities of Mobile Commerce in India: A Study on Societal Perspective. *Comput. Trends J. Emerg. Trends Inf. Technol.* **2016**, *6*. [\[CrossRef\]](#)
21. Venkatesh, V.; Hoehle, H.; Aloysius, J.A.; Nikkhah, H.R. Being at the cutting edge of online shopping: Role of recommendations and discounts on privacy perceptions. *Comput. Hum. Behav.* **2021**, *121*, 106785. [\[CrossRef\]](#)
22. Gurung, A.; Raja, M.K. Online privacy and security concerns of consumers. *Inf. Comput. Secur.* **2016**, *24*, 348–371. [\[CrossRef\]](#)
23. Ali, B.J. Impact of COVID-19 on consumer buying behavior toward online shopping in Iraq. *Econ. Stud. J.* **2020**, *18*, 267–280.
24. Vărzaru, A.A.; Bocean, C.G.; Rotea, C.C.; Budică-Iacob, A.-F. Assessing Antecedents of Behavioral Intention to Use Mobile Technologies in E-Commerce. *Electronics* **2021**, *10*, 2231. [\[CrossRef\]](#)
25. Hussien, F.T.A.; Rahma, A.M.S.; Wahab, H.B.A. Design and implement a new secure prototype structure of e-commerce system. *Int. J. Electr. Comput. Eng.* **2022**, *12*, 560–571.
26. Chen, C.-M.; Cai, Z.-X.; Wen, D.-W. Designing and Evaluating an Automatic Forensic Model for Fast Response of Cross-Border E-Commerce Security Incidents. *J. Glob. Inf. Manag.* **2022**, *30*, 1–19. [\[CrossRef\]](#)
27. Miao, J.J.; Tran, Q.D. Study on e-commerce adoption in SMEs under the institutional perspective: The case of Saudi Arabia. *Int. J. E-Adopt. (IJEA)* **2018**, *10*, 53–72.
28. Nachar, M. Factors that Predict the Adoption of Online Shopping in Saudi Arabia. Ph.D. Thesis, Walden University, Columbia, MD, USA, 16 April 2019.
29. Al-Ayed, S. The impact of e-commerce drivers on e-customer loyalty: Evidence from KSA. *Int. J. Data Netw. Sci.* **2022**, *6*, 73–80. [\[CrossRef\]](#)
30. Saeed, S. Digital Business adoption and customer segmentation: An exploratory study of expatriate community in Saudi Arabia. *ICIC Express Lett.* **2019**, *13*, 133–139.
31. Alotaibi, R.S. Understanding customer loyalty of M-commerce applications in Saudi Arabia. *Int. Trans. J. Eng. Manag. Appl. Sci. Technol.* **2021**, *12*, 1–12.
32. Razi, M.J.M.; Sarabdeen, M.; Tamrin, M.I.M.; Kijas, A.C.M. Influencing Factors of Social Commerce Behavior in Saudi Arabia. In Proceedings of the 2019 International Conference on Computer and Information Sciences (ICCIS), Sakaka, Saudi Arabia, 3–4 April 2019; pp. 1–4.
33. Top Apps Ranking. Available online: <https://www.similarweb.com/apps/top/google/store-rank/sa/shopping/top-free/> (accessed on 1 October 2021).
34. Furnell, S.M.; Karweni, T. Security implications of electronic commerce: A survey of consumers and businesses. *Internet Res.* **1999**, *9*, 372–382. [\[CrossRef\]](#)
35. Naderifar, M.; Goli, H.; Ghaljaei, F. Snowball Sampling: A Purposeful Method of Sampling in Qualitative Research. *Strides Dev. Med. Educ.* **2017**, *14*. [\[CrossRef\]](#)
36. Lowry, P.B.; Gaskin, J. Partial Least Squares (PLS) Structural Equation Modeling (SEM) for Building and Testing Behavioral Causal Theory: When to Choose It and How to Use It. *IEEE Trans. Dependable Secur. Comput.* **2014**, *57*, 123–146. [\[CrossRef\]](#)
37. Ringle, C.M.; Wende, S.; Becker, J.-M. SmartPLS. Available online: <https://www.smartpls.com/> (accessed on 1 October 2021).
38. Sargani, G.R.; Jiang, Y.; Zhou, D.; Chandio, A.A.; Hussain, M.; Khan, N. Endorsing Sustainable Enterprises Among Promising Entrepreneurs: A Comparative Study of Factor-Driven Economy and Efficiency-Driven Economy. *Front. Psychol.* **2021**, *12*, 735127. [\[CrossRef\]](#) [\[PubMed\]](#)
39. Hair, J.F.; Sarstedt, M.; Hopkins, L.; Kuppelwieser, V.G. Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research. *Eur. Bus. Rev.* **2014**, *26*, 106–121. [\[CrossRef\]](#)
40. Bangun, C.S.; Handra, T. How Theory of Planned Behavior And Percieved Risk Affect Online Shopping Behavior. *Aptisi Trans. Manag. (ATM)* **2021**, *5*, 169–179. [\[CrossRef\]](#)
41. Habib, S.; Hamadneh, N.N. Impact of Perceived Risk on Consumers Technology Acceptance in Online Grocery Adoption amid COVID-19 Pandemic. *Sustainability* **2021**, *13*, 10221. [\[CrossRef\]](#)
42. Rogers, R.W. A Protection Motivation Theory of Fear Appeals and Attitude Change. *J. Psychol. Interdiscip. Appl.* **1975**, *91*, 93–114. [\[CrossRef\]](#) [\[PubMed\]](#)
43. Nabi, F.; Malhi, M.S.; Farhan, M.; Mahmood, U. Process of Security Assurance Technique for Application Functional Logic in E-Commerce Systems. *J. Inf. Secur.* **2021**, *12*, 189–211. [\[CrossRef\]](#)
44. Zhang, M.; Lin, L.; Chen, Z. Lightweight security scheme for data management in E-commerce platform using dynamic data management using blockchain model. *Clust. Comput.* **2021**, 1–15. [\[CrossRef\]](#)
45. Shakya, V.; Chatterjee, J.M.; Thakur, R.N. Network Security and Its Impact on Business Strategy: A Case Study on E-Commerce Site Daraz. *Com. LBEF Res. J. Sci. Technol. Manag.* **2021**, *3*, 45–60.
46. Xu, Q.; Wang, G. Cross-Cultural Communication of Regional Images Based on Multimodal Discourse Analysis and Network Security. *Mob. Inf. Syst.* **2021**, *2021*, 9956593. [\[CrossRef\]](#)
47. Iqbal, S. A Study on UAV Operating System Security and Future Research Challenges. In Proceedings of the 2021 IEEE 11th Annual Computing and Communication Workshop and Conference, CCWC 2021, Las Vegas, NV, USA, 27–30 January 2021.



48. Asif, R.; Ghanem, K.; Irvine, J. Proof-of-PUF Enabled Blockchain: Concurrent Data and Device Security for Internet-of-Energy. *Sensors* **2021**, *21*, 28. [\[CrossRef\]](#)
49. Šarac, M.; Pavlović, N.; Bacanin, N.; Al-Turjman, F.; Adamović, S. Increasing privacy and security by integrating a Blockchain Secure Interface into an IoT Device Security Gateway Architecture. *Energy Rep.* **2021**, *7*, 8075–8082. [\[CrossRef\]](#)
50. Gull, H.; Iqbal, S.Z. Usability evaluation of e-government websites in saudi arabia by cognitive walkthrough. In *Design Solutions for User-Centric Information Systems*; IGI Global: Hershey, PA, USA, 2017; pp. 297–312. ISBN 9781522519454.
51. Kim, H.-J.; Han, K.-H.; Shin, S.-S. Hash-based SSDP for IoT Device Security. *J. Korea Conver. Soc.* **2021**, *12*, 9–16. [\[CrossRef\]](#)
52. Patel, J. Secured and Efficient Payment Gateways for eCommerce. *Int. J. Res. Publ. Rev.* **2021**, *2*, 575–582.
53. Williams, M.D. Social commerce and the mobile platform: Payment and security perceptions of potential users. *Comput. Hum. Behav.* **2021**, *115*, 105557. [\[CrossRef\]](#)
54. Mujeeb-ur-Rehman; Lakhan, A.; Hussain, Z.; Khoso, F.H.; Arain, A.A. Cyber Security Intelligence and Ethereum Blockchain Technology for E-commerce. *Int. J. Emerg. Trends Eng. Res.* **2021**, *9*, 967–972. [\[CrossRef\]](#)
55. Sim, J.J.; Loh, S.H.; Wong, K.L.; Choong, C.K. Do We Need Trust Transfer Mechanisms? An M-Commerce Adoption Perspective. *J. Theor. Appl. Electron. Commer. Res.* **2021**, *16*, 2241–2262. [\[CrossRef\]](#)
56. Chiu, W.; Cho, H. E-commerce brand: The effect of perceived brand leadership on consumers' satisfaction and repurchase intention on e-commerce websites. *Asia Pac. J. Mark. Logist.* **2019**, *33*, 1339–1362. [\[CrossRef\]](#)
57. Saeed, S.; Wahab, F.; Cheema, S.A.; Ashraf, S. Role of usability in e-government and e-commerce portals: An empirical study of Pakistan. *Life Sci. J.* **2013**, *10*, 8–13.
58. Lee, S.; Koubek, R.J. The effects of usability and web design attributes on user preference for e-commerce web sites. *Comput. Ind.* **2010**, *61*, 329–341. [\[CrossRef\]](#)
59. Hasan, L.; Morris, A.; Proberts, S. A comparison of usability evaluation methods for evaluating e-commerce websites. *Behav. Inf. Technol.* **2012**, *31*, 707–737. [\[CrossRef\]](#)
60. Gul, H.; Iqbal, S.Z.; Saqib, M. Usability Evaluation of an Educational Website in Saudi Arabia. *VAWKUM Trans. Comput. Sci.* **2015**, *8*, 84–92. [\[CrossRef\]](#)
61. Moores, T.T.; Dhillon, G. Do privacy seals in e-commerce really work? *Commun. ACM* **2003**, *46*, 265–271. [\[CrossRef\]](#)
62. Katsikas, S.K.; Lopez, J.; Pernul, G. Trust, privacy and security in e-business: Requirements and solutions. In Proceedings of the 10th Panhellenic Conference on Informatics, Volos, Greece, 11–13 November 2005.
63. Saeed, S.; Reddick, C.G. *Human-Centered System Design for Electronic Governance*; IGI Global: Hershey, PA, USA, 2013.
64. Basu, A.; Muylle, S. Authentication in E-Commerce Commun. ACM **2003**, *46*, 159–166. [\[CrossRef\]](#)
65. Irofti, P.; Pătrașcu, A.; Băltoiu, A. Fraud Detection in Networks. In *Enabling AI Applications in Data Science*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 517–536. [\[CrossRef\]](#)
66. Ciocchetti, C.A. E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors. *Am. Bus. Law J.* **2007**, *44*, 55–126. [\[CrossRef\]](#)
67. Schlaeger, C.; Pernul, G. Authentication and Authorisation Infrastructures in b2c e-Commerce. In Proceedings of the International Conference on Electronic Commerce and Web Technologies, Copenhagen, Denmark, 23–26 August 2005; pp. 306–315.
68. Choy, L.T. The Strengths and Weaknesses of Research Methodology: Comparison and Complimentary between Qualitative and Quantitative Approaches. *IOSR J. Humanit. Soc. Sci.* **2014**, *19*, 99–104. [\[CrossRef\]](#)
69. Saeed, S.; Bajwa, I.S.; Mahmood, Z. *Human Factors in Software Development and Design*; IGI Global: Hershey, PA, USA, 2014.