The Impact of Security and Payment Method On Consumers' Perception of Marketplace in Saudi Arabia

(Case Study on Noon)

Mdawi Alqahtani[1]
Department of Business, Umm Al Qura University
P.O. Box 715, Mecca, Saudi Arabia

Marwan Ali Albahar[2]
Department of Science, Umm Al Qura University
P.O. Box 715, Mecca, Saudi Arabia

***Abstract*—Digital transformation has been accelerated in recent years, and COVID-19 has resulted in a rise in overall internet spending. Businesses must take measures in order to ensure that customers have a safe and enjoyable online purchasing experience. In this paper, customers' security perceptions regarding the most popular e-commerce applications in Saudi Arabia are explored. Surveys were distributed online via Google Form to 200 participants in total as part of a cross-sectional research design using quantitative methodology. The main findings were related to confirming eight main hypotheses of the research that were related to testing if some factors were important to forming perceived trust by customers. Five factors (trust, security, reputation, benefits, and convenience) were found to have a positive effect, and the remaining three were not (familiarity, size, and usefulness). Finally, this study recommends various actions for practitioners and policymakers to take in order to improve customer perceptions of payment methods and security in Saudi Arabia.**

Keywords—Payment security; digital strategy; digital transformation; user security

I. Introduction

E-commerce is a type of business transaction where goods and services are bought, sold, and given away over the internet. This includes both business-to-business (B2B) and business-to-consumer (B2C) deals. Consumer behavior has changed because of today's fast-paced market and the fierce competition between businesses [1]. Because of this, e-commerce has become a good choice for many businesses. Classified ads, C2C marketplaces, shopping malls, B2C stores, and social media-based online stores are all examples of e-commerce business models in Saudi Arabia, where people buy and sell things online. Because so many people in Saudi Arabia use mobile devices all the time, Noon is one of the best websites for shopping at e-commerce stores in the country [2, 3]. The Noon website sells merchandise. Noon's goal in Saudi Arabia is to provide a new shopping experience as well as simple sales, secure payment, and integrated logistics. As a result, it is critical for the application system to keep data secure and to have a method to ensure that the transaction records it generates are correct because it will be used to address many threats to the payment system [4]. Consumers must have faith in the security of personal data protection for online remittances for this to happen. Increasingly, people are using smartphones and tablets to do things like make payments and transfer money because they are easy to use and easy to move around. Traditional financial transactions are thought to be more time-consuming and inefficient than mobile financial transactions [5,6].

Customers' perceptions of their personal information and the security of their financial transactions have shifted dramatically in recent years. Mobile applications with a good reputation for security and privacy are used to maintain security and privacy. Customers of mobile applications are concerned about malicious code and unauthorized access infiltrating their applications. They're also worried about others spying on their online activities and stealing their credit card information. Customers' willingness to buy and sell products through mobile commerce applications has been shown to be influenced by privacy and security concerns [6,7,8,9]. Customers are less likely to use an online platform if they are concerned about its security. To better engage with their customers, businesses must first understand how they perceive security and safety when they are online. Because social and cultural factors vary by country, it is critical to investigate customers' perceptions of online platform security and privacy across cultures [10,11]. User behavior shifts in the presence of cybersecurity threats, according to the Protection Motivation Theory (PMT), making it critical for social commerce platforms to protect their customers' personal information and data. As a result, we concentrate our research on customers in Saudi Arabia to investigate if the payment methods used have a positive impact on customer perceptions of security.

Saudi Arabia is widely regarded as a major online shopping market. People buy products using a variety of payment methods and applications all over the world. They are also concerned about the correlation between security, privacy, and payment methods [12, 13]. This motivates us to study the importance of security and privacy for Saudi buyers when it comes to mobile commerce. The objective of this study is to examine Saudi consumers' perspectives on security and privacy concerns when it comes to a popular e-commerce app, namely Noon in Saudi Arabia (KSA). This study used quantitative methodology to determine whether the payment methods that are used have a positive impact on customers' perceptions of security. We used the most popular e-commerce website in Saudi Arabia, which is Noon. Multiple factors are made up of several sub-factors that helped us analyze the user experience of this e-commerce website. As a result, the main contribution of this research is to better understand customer perceptions of the payment methods and security in Saudi Arabia to improve customer perceptions that can be applied to other countries.

The rest of this paper is organized as follows. Section II presents recent related works on the impact of security and payment methods on consumers' perceptions. We present the problem formulation in Section III. Section IV introduces our proposed methodology in detail. Section V discusses the study setting and participants. Section VI presents the results and findings and some limitations. Finally, we conclude the paper and discuss some directions for future work in Section VII.

II. Literature Review

Numerous studies have shown that security and privacy are critical in mobile commerce applications. Customers are thus more likely to use mobile commerce applications that provide enhanced security and privacy. According to a study conducted in Indonesia by Hidayat et al. [14], trust is a critical factor for Indonesian customers when shopping online. Saprikis and Avlogiaris [15] conducted an empirical study to ascertain the factors that influence consumers' social media shopping behavior. The findings indicate that convenience, reward, and security all play a significant role in consumers' direct purchases via social applications (ICT facilitators of the UTAUT model). Customer satisfaction, according to Taherdoost and Madanian [16], is a critical factor in customer loyalty, which is why they validated an e-service satisfaction model in an e-commerce context. Customer satisfaction is determined to be most strongly influenced by trust, security, performance, and usability. According to Harris et al. [17], a variety of factors contribute to people installing and using mobile applications that violate their privacy and security. In their study, they discovered a correlation between customer trust and perceived security, indicating that customers who perceive more security have both increased trust and a lower perceived risk. According to Ghayoumi [18], m-commerce is also affected by six security factors. Integrity, non-repudiation, authentication, confidentiality, privacy, and availability are some of these factors. According to the study's researchers, security in m-commerce applications is contingent upon these factors. Mahmoud and colleagues [19] attempted to demonstrate the growing popularity of mobile commerce by highlighting the security risks associated with the use of modern devices and high-speed internet. While the study's primary objective was to make recommendations on how to address potential privacy and security concerns raised by the growing use of mobile commerce, it also examined user perceptions of trust in mobile commerce on three major websites: Amazon.com, AliBaba.com, and eBay. The study takes a deductive approach and employs only one method of research. Additionally, the data was analyzed using a 100-respondent random sample. Although an e-commerce environment is more private than a mobile commerce environment, the author asserts that trust in mobile commerce systems remains low due to the privacy and security paradigm. Additionally, this study demonstrates that there is considerable room for improvement in terms of privacy and integrity, authentication, and security. According to Kumar and colleagues' research [20], while m-commerce applications are gaining popularity in India, users remain wary of them for a variety of reasons. Security and payment issues with these mobile commerce applications have been cited as significant factors. Consumers believe that mobile commerce applications are constantly vulnerable to hacking and phishing attacks and that they cannot trust any of them with their credit cards or even personal information. They are wary of using these apps because they lack trust in third-party websites to process their payments. Venkatesh et al. [21] also investigated customers' privacy concerns when making online purchases. It was discovered that among the recommendations included in the study were retailers' and other customers' preferences for products that were related to one another. According to a survey, online purchases are moderately influenced by recommendations and product-relatedness. Closely associated products with privacy enablers did not affect online purchase intentions. As Gurung et al. [22] discovered when they investigated online shoppers' security and privacy concerns. These concerns, they believe, influence customers' perceptions of risk. The relationship between privacy and security was also examined using organized conduct. The study's findings indicate that privacy and security concerns may influence risk assessment and awareness. Privacy and security concerns rank second, with trust ranking first. Additionally, individuals' mental states are affected by their perceptions of risk and trust. Ali et al. [23] also examined privacy to determine whether it could be used to deduce users' attitudes toward mobile app security. Vărzaru et al. [24] used a reworked version of the technology acceptance model to deduce the factors influencing post-COVID behavioral intention and consumer satisfaction. According to the researchers, consumer intention was positively influenced by perceived usefulness and ease of use. D'Adamo and colleagues [7] discovered that in the post-pandemic era, European consumers are concerned about online security. According to the findings of this study, consumers in Europe have varying levels of concern about e-commerce security. According to Hussien et al. [25], customers and electronic marketplaces can benefit from agent software that provides client-side security to improve marketplace performance. For example, Chen et al. [26] proposed a forensic model that may aid in detecting abnormal system behavior. Numerous studies on e-commerce in Saudi Arabia have been conducted. Between 2013 and 2016, a long-term study by Miao & Tran [27] discovered a significant difference between SMEs' initial adoption of e-commerce and their intention to institutionalize it. Nachar [28] asserts that an e-commerce platform's ease of use and usefulness are statistically significant predictors of customers' willingness to shop online. According to Al-Empirical in Ayed's study [29], customer care, product selection, convenience, personality, and website customization all contribute to e-commerce customer loyalty. Saeed [30] conducted an empirical study of Saudi Arabian expats' adoption of e-commerce and discovered to enhance user interface usability, it is necessary to take cultural differences into account during the technical design stage. Alotaibi [31] found no significant differences in m-commerce customer loyalty by gender, age, or prior experience.

According to Razi et al. [32], participation in social commerce by students has a beneficial effect on purchase intentions and behavior.

According to a review of the literature, geographical and cultural factors influence users' attitudes toward online shopping. However, no comprehensive study of online customers has been conducted in Saudi Arabia. Due to the importance of user motivation and perception in technological adoption, there is a knowledge gap regarding how Saudi consumers perceive the security aspects of e-commerce applications.

III. Problem Formulation

Certain studies focus exclusively on the relationship between factors influencing marketplace trust, and only infrequently do they examine the relationship between factors influencing payment system trust in developing countries. In the end, a study by Kim et al. [33] looks at whether trust is affected by factors like reputation, privacy, size, security, benefits, and convenience. It also looks at how this trust affects purchases made with EPS, credit cards, or cash on delivery (COD). It is regarded as user-friendly and useful. Security, usability, trustworthiness, interoperability, common issues, and extra services all affect how well electronic payment systems work. These six factors all affect how well electronic payment systems work. Mutual trust between merchants and customers is required when conducting online shopping, based on the six factors listed above. In [34], the author asserts that the value of security and trust cannot be overstated. Privacy refers to the right to keep one's personal information private. Additionally, privacy is defined as the capacity to manage personal information that is required and used by third parties [35]. If you want to buy something on the internet, you must be willing to give out your personal information before you do so [35]. When it comes to interpersonal relationships, humans prefer to maintain their privacy.

In e-commerce, privacy refers to how willing people are to give out personal information over the internet before they buy something [35]. The term "internet privacy" includes a lot of different things, like data, choices, and sharing with e-commerce service providers. As Belanger stated [36], consumers also want to know that the information they give is safe and lawful. The right to privacy of individuals is extremely well protected. When customers shop online, they provide sellers with extremely detailed information. Consumers who place a high value on privacy often give internet service providers inaccurate or incomplete information. It is possible to take advantage of the privacy settings on a website. In other words, the more confident a user is in a website's ability to protect their information, the greater their trust on the website.

A. Hypothesis

Trust is significantly influenced by people's perceptions of their reputation, privacy, size, security, benefits, website usability, and convenience.

- According to [33], a payment system's perceived user friendliness and usefulness is critical. Security, usability, trustworthiness, interoperability, common issues, and additional services are all factors that have an impact on the performance of electronic payment systems. It's important to think about safety first. As shown by the preceding six factors, online shoppers and merchants need to put in a lot of work to build trust in one another.

1) Perceived privacy has a positive effect on trust: According to the authors in [8], privacy is a method of protecting one's identity. The ability to retain one's personal information is defined as "privacy" in this definition. Also included in the definition of privacy is an individual's ability to control the extent to which their personal information is required and used by third parties [35]. Privacy online can be defined as consumers' willingness to share personal information before making a purchase [35]. Humans, like other people, have a standard for how much privacy they want. In e-commerce, privacy is defined as consumers' willingness to provide information via the internet before making a purchase [35]. Concerns about privacy on the internet include "spam," "data," "choices," and e-commerce service providers sharing information. Customers also want assurances that the information they provide will be restricted and regulated by the person concerned [36]. Everyone has a right to have their personal information kept private. Customers in the e-commerce industry are extremely picky about the information they divulge to merchants. Internet service providers are more likely to receive incomplete information from consumers who care about their privacy. When you give your personal information to a website, you run the risk of it being misused. The more trust is placed in an address's ability to protect personal information, the more confident that person is in that address's ability to protect that information.

2) In general, security increases when people feel safe: Security is a significant control issue for businesses that conduct e-commerce. When consumers are involved in electronic transmission, data relating to e-commerce, such as buyer and seller data, must be kept confidential. Additionally, the transmitted data must be safeguarded against modification or alteration by anyone other than the sender [36]. According to [37], security can be defined broadly as the absence of danger. This understanding is comprehensive and encompasses an individual's sense of protection against both intentional and unintentional crimes, such as natural disasters. A security threat is defined as a situation, condition, or event that poses a risk of causing damage to data or networks, which can take the form of data destruction, leakage, alteration, or misuse. Consumer security concerns can be addressed in e-commerce using protection technology. When these technologies are used, they are classified as security features. According to [9], security can be classified into four categories based on security holes: physical security (physical security), personnel security (personnel security), data security (data security), and media and communication techniques (communications). Security in operations refers to the policies and procedures that govern the establishment and management of security systems, as well as post-attack recovery procedures. The management of the online payment system's security can be viewed through the lens of risk management. Authors in [37] recommended employing the "Risk Management Model" when confronted with threats (managing threats). Risk consists of three components: assets, vulnerabilities, and threats. E-commerce network security that incorporates features such as guarantees, contracts, or other procedures ensures the existence and proper operation of payment security. Someone who has a high perception of structural assurance will fervently believe that internet technology (e.x. data encryption) protects in such a way that online transactions are safe. Consumers are protected from financial and personal loss through encryption, legal protection, and technological safeguards. In addition, the authors in [37] stated that security guarantees could be integrated into e-commerce sites through collaboration with third parties with a strong reputation in network security and who provide internet security assurance standards via web assurance seals. Consumers who feel secure in the online environment are more likely to trust websites that offer electronic commerce services than those who believe the internet is unsafe because they do not believe e-commerce sites offer adequate protection.

3) Perceived benefits are considered when trust is enhanced: According to [36,37], usefulness is the likelihood that a specific application will be used by potential users to make their work tasks easier. Results will be obtained more quickly and satisfactorily as a result of the product's simplified performance when used in conjunction with the new technology. Internet banking services can boost productivity by increasing people's perceptions of the benefits these services provide. Increased productivity, improved performance, and improved process efficiency can all be used to determine what people think about the benefits of technology.

4) Consumer trust in a website is increased as a result of familiarity with it: MAQABLEH et al. [39] study and observe consumer behavior and perceptions of security and trust in e-payment systems based on the proximity of the customer to the website. In addition, the authors in [39] identified a slew of determining factors. There was also a tendency to trust, as well as internet experience, personal innovation, and habit. Third-party involvement, payment system intention, enjoyment, risk aversion, and trustworthiness can all be found by looking at the variables that connect them. According to investigation made in [33], after a customer's first visit to a company's website, the level of consumer confidence in that company's website was measured. According to the findings of the investigation, consumers' perceptions of the company's reputation and willingness to improve products and services have a direct impact on consumer confidence. In addition to the other factors, it is thought that controls for usability, ease of use, and security have a big impact on trust.

5) Perceived convenience has a positive effect on trust: According to [37,38], ease of use can be defined as the extent to which a person believes that using technology will be free of effort on his or her part. As implied by the definition, ease perception is a belief about the decision-making process that is experienced by the individual. Using an information system is more likely to occur if a consumer believes it is simple to use and understand. As identified by [36-37-38], the dimensions of perceived ease are as follows: ease of learning (easy to learn), ease of use (easy to use), clear and understandable (straightforward and easy to understand), and the ability to become skillful (becoming skilled).

6) Perceived trust has a positive impact on purchase intention when EPS is employed: Consumers' online behavior is heavily influenced by their level of trust in the companies they do business with, which is why trust is such an important consideration in electronic commerce. One's social standing rises as a result, and one can spend money in the market. According to [8-34-35-36], trust is based on the trustworthiness of the parties involved in the transaction, specifically electronic payments and cross-border trade. Trust in other parties and the use of regulatory control mechanisms were found to be the most important factors in determining the level of trust in transactions. Both variables have objective and subjective components. A lack of trust is a direct indicator of attitude and behavior because of the dynamic nature of cyberspace's high uncertainty and constant change. Trust can also be defined as a person's belief in the ability of others to be trusted, which is based on perceived integrity, benevolence, and competence. The most basic definition of trust is the belief that others will not take advantage of you and that the vendor will deliver on what they have promised. Online shopping relies heavily on trust, which is a significant factor in e-commerce. For e-commerce to work properly, trust and security are two of the most critical constructs, customers tend to have a higher level of trust in e-commerce websites with higher quality content. In a developing country, establishing trust in a new environment is a challenging task that is essential to influencing consumer attitudes [4,5,30,31,33].

7) Perceived trust influences cash on delivery (or/and) credit card purchases: Tsiakis and Sthephanides [40] argued that trust and security are two of the most important factors to consider when developing an electronic payment system. According to Kim et al. [33], user convenience and usefulness are important factors to consider when choosing a payment system for their needs. In fact, the ability to feel safe and confident in a company's products and services is critical to attracting and retaining customers.

IV. Proposed Method

This study's quantitative design collects data from a pool of participants one at a time. Customers of the Saudi Arabian online shopping platform Noon were chosen as the population and sample for this study based on the researchers' judgment of what they should buy. Hair et al. [41] stated that the number of samples in PLS-SEM research must be five times the number of questions in the questionnaire. As a result, this study's questionnaires contain 5 x 40 questions, yielding a total of 200 respondents. The research questionnaire had closed questions with one of five measurement scales for each variable (Likert). This is done using Google Form and explains what will be done to respondents via social media such as WhatsApp, Instagram, and other social media.

The components of this study were adapted from Maqableh et al. [39] findings on trust behavior and online shopping payment methods for shoppers in Saudi Arabia. The Likert scale was used to measure all constructs in this study, with 1 representing "strongly disagree" and 5 representing "strongly agree." Table I summarizes the results of the fittest for the overall PLS-SEM model. With the Good of Model Fit (GOM) metric, the structural model testing phase can be done as follows:

TABLE I. MODEL FIT GOODNESS

Goodness Model of Fi	Original Value (Saturated Model)	Estimated Model	Note
d_ULS	4.23	9.378	Model Fit
SRMR	0.05	0.088	Model Fit
d_G	1.63	1.80	Model Fit

The Standardized Root Mean Square Residual (SRMR) graph illustrates the amount of error associated with predicting the independent variable's effect on the dependent variable in question. According to the definitions of d_ULS and d _G, a representative research model must have a value greater than 0.05 (if the 95 percent confidence interval is used) or greater than 0.01 for the study's smaller initial estimate (if using a 99 percent confidence interval). In other words, the research model's residual distribution is quite small. Validity is established when the square root of the average variance (AVE) value has a loading factor greater than 0.5, and reliability is established when the composite reliability value is greater than 0.7 or when Conbach's Alpha has a loading factor of 0.6.

V. STUDY SETTING AND PARTICIPANTS

Data points from the distribution of questionnaires were collected using Google's non-probability form method, and these data points can be used to generate additional research data. The following are the characteristics of the 200 participants in the survey (see Table II). Noon customers are predominantly female, with 80% of respondents to this study's questionnaire distribution reporting a shopping frequency of more than 19 times per month, according to the results of the study. Customers who are the most active on Noon fall into this category. Using a correlation coefficient, it was discovered that the effects of total reputation perception, privacy perception, scale perception, safeguard perception, perceived usefulness, user-friendly perception, and trust perception were all increased by 74.1%. In EPS, the variable assessing trust perception accounted for 42.4% of the total. Fixed trust perception of factual purchases made with credit cards accounted for 15% of the total, while variable trust perception of factual purchases made with cash-on-delivery accounted for another 24% of the total (see Table III). Finally, after figuring out the coefficients of determination for each parameter, we conduct the experiment to determine the validity of the hypothesis (Fig. 1).

TABLE II. DEMOGRAPHIC INFORMATION OF RESEARCH RESPONDENTS

Type of Characteristic	Characteristic	Total	Percentage
Sex	Male	40	20%
	Female	160	80%
Age	14 – 20 years old	102	51%
	21 – 30 years old	60	30%
	40 – 50 years old	18	9%
	> 50 years old	20	10%
Occupation	Students	100	59,27%
	Public Sector Employees	43	17,34%
	Private Sector Employees	40	18,95%
	Enterprise Employees	17	4,44%
Income	< RS 6,000	124	69,35%
	RS 7,000 – 12,000	50	20,16%
	RS 13,000 – 17,000	15	6,05%
	> RS 20,000	11	4,44%
Shopping Frequency	< 4 times	70	34,68%
	8 times	50	26,21%
	12 times	20	8,06%
	>19 times	60	31,05%
Shopping Cost	< RS 4,000	140	75,40%
	RS 5,000	48	19,76%
	RS 7,000	4	1,61%
	RS 15,000	8	3,23%

TABLE III. COEFFICIENT OF DETERMINATION

Model	R Square
Trust is significantly influenced by people's perceptions of their reputation, privacy	0.74
Purchase with the intention of utilizing EPS	0.428
Purchase made with credit card	0.015
Actual purchase made with on-delivery payment	0.024

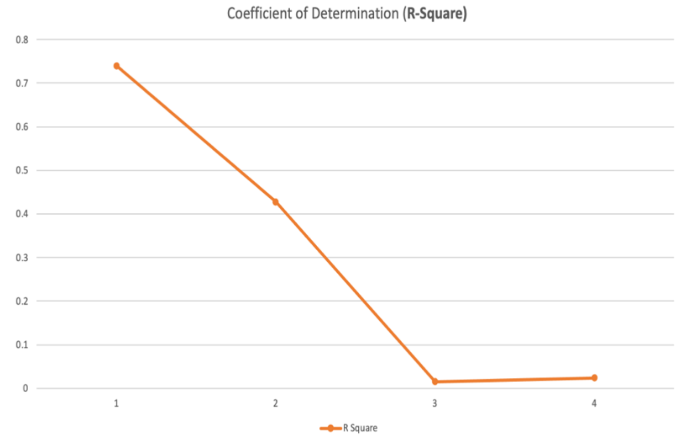

Fig. 1. Coefficient of Determination (R-square).

VI. RESULT AND FINDINGS

These findings demonstrate that belief-formers have an impact on online shopping on the Noon application in Saudi Arabia, which is decided by factors such as safety, benefits, and convenience, all of which have a statistically significant impact. According to the authors in [12,33], high-quality e-commerce sites have a greater perception of trust from their customers, and the exceptional measures taken to earn the trust of customers will shape consumer attitudes in a developing country.

In this study, the researchers discovered that clients who shop online through the Noon application are more likely to purchase things from Noon when they pay with an electronic funds transfer (EPS). According to the findings of Tsiakis and Sthephanides [40], credence and safeguard are the most important and vital components for electronic payment systems that are used as a tool in financial operations. Furthermore, according to the authors in [34], security and trust play crucial roles in recruiting and retaining customers. Also demonstrated in this study is that the perceived safety, benefits, and convenience of shopping online at Noon in Saudi Arabia have an impact on trust perception, and that using EPS is the most influential factor in trust perception when it comes to purchasing online. As a result, marketplace service providers such as Noon may be able to develop confidence by emphasizing the safety, benefits, and convenience of online shopping. In the long run, service providers may be able to design payment mechanisms that are compatible with EPS. The likelihood of consumers making purchases online at Noon will increase as their degree of confidence increases, as will the likelihood of consumers using EPS payment options (Fig. 2). The online services provided by Noon in Saudi Arabia will be directly recommended to clients who have expressed satisfaction with the company's trustworthiness, security, and convenience of payment (see Table IV).

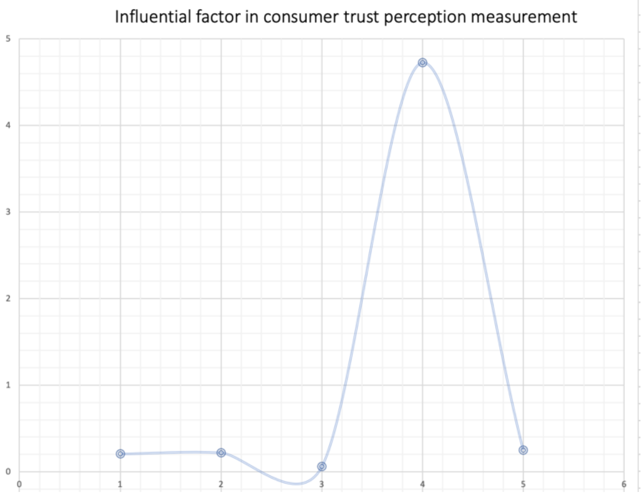

Fig. 2. Influential Factor in Consumer Trust Perception Measurement.

TABLE IV. HYPOTHESIS TEST

Model	Original Sample	Mean of the ample	Standard Deviation	T-Value	P-Value	Note
Reputation, privacy, size, security, benefits, website usability, and convenience all influence trust.	0.155	0.151	0.070	2.224	0.021	significant
A favorable perception of the firm's size increases trust.	0.013	0.002	0.057	0.047	0.951	Not significant
People trust more when they feel safe.	0.411	0.452	0.057	7.749	0.000	significant
Perceived benefits increase trust.	0.112	0.165	0.055	2.560	0.015	significant
Familiarity increases consumer trust in a website.	0.030	0.020	0.083	0.363	0.711	Not significant
Convenience has a positive effect on trust.	0.156	0.182	0.081	2.227	0.039	significant
When EPS is used, perceived trust positively impacts purchase intention.	0.662	0.665	0.031	20.645	0.000	significant
Trust perception affects cash on delivery / credit card purchases	0.127	0.131	0.062	1.986	0.042	significant

VII. Conclusion

In recent years, digital transformation has accelerated, and COVID-19 has resulted in an increase in overall internet spending. Businesses must take precautions to ensure that their customers have a safe and enjoyable online shopping experience. This paper investigates customers' security perceptions of the most popular e-commerce applications in Saudi Arabia. As part of a cross-sectional research design employing quantitative methodology, surveys were distributed online via Google Form to a total of 200 participants. The main findings were related to confirming the research's eight main hypotheses, which were related to testing whether some factors were important in forming perceived trust by customers. Five factors were discovered to have a positive effect (trust, security, reputation, benefits, and convenience), while the remaining three did not (familiarity, size, and usefulness). Based on our findings, trust is a multidimensional construct comprised of reputation, privacy, size, benefits, security, benefits, familiarity with the web, and ease. As demonstrated by this result, the p-value does not apply to all indicators with a loading of less than 0.04 on the latent variable. This study suggests several actions that practitioners and policymakers can take to improve customer perceptions of payment methods and security in Saudi Arabia.

References

[1] Reychav, 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.

[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.

[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] Niranjanamurthy, 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.

[8] Pabian, A.; Pabian, B.; Reformat, B. E-Customer Security as a Social Value in the Sphere of Sustainability. Sustainability 2020, 12, 10590.

[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.

[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.

[12] Lee, D.; LaRose, R.; Rifon, N. Keeping our network safe: A model of online protection behavior. Behav. Inf. Technol. 2008, 27, 445–454.

[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.

[15] Saprikis, V.; Avlogiaris, G. Factors That Determine the Adoption Intention of Direct Mobile Purchases through Social Media Apps. Information 2021, 12, 449.

[16] Taherdoost, H.; Madanchian, M. Empirical Modeling of Customer Satisfaction for E-Services in Cross-Border E-Commerce Electronics 2021, 10, 1547.

[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.

[18] Ghayoumi, M. Review of Security and Privacy Issues in e-Commerce. In Proceedings of the International Conference one- 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.

[20] Kumar, U.; Gope, A.K.; Singh, S. Emerging Challenges and Opportunities of Mobile Commerce in India: A Study on Societal Perspective. Comput. Trendz J. Emerg. Trends Inf. Technol. 2016, 6.

[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.

[22] Gurung, A.; Raja, M.K. Online privacy and security concerns of consumers. Inf. Comput. Secur. 2016, 24, 348–371.

[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.

[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.

[30] Saeed, S. Digital Business adoption and customer segmentation: An exploratory study of the expatriate community in Saudi Arabia. ICIC Express Letter. 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] Kim, C., Tao, W., Shin, N. and Kim, K.S. An Empirical Study of Customers' Perceptions of Security and Trust in E-Payment Systems. Electronic Commerce Research and Applications, 9, 84-95. use mobile payment. Computers in Human Behavior, 26, pp.310–32, 2010.

[34] Nuri, H. A Study of Role of the Factors Influencing the Acceptance of E-Banking. No. 3, 521-525, 2014.

[35] Ackerman, S. and Davis, D. T. Jr. Privacy and security issues in e-commerce. In the New Economy Handbook, pages. 911–930. Academic Press/ Elsevier, 2003.

[36] Belanger, F., Hiller, J. S., & Smith, W. J. Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *The Journal of Strategic Information Systems*, *11*(3-4), 245-270,2002.

[37] Liu, L., & Shi, W. Trust and reputation management. *IEEE Internet Computing*, *14*(5), 10-13, 2010.

[38] Montibeller, G., Franco, L. A., & Carreras, A. A Risk Analysis Framework for Prioritizing and Managing Biosecurity Threats. In Risk Analysis (Vol. 40, Issue 11, pp. 2462–2477, 2020).

[39] MAQABLEH, M. *Analysis and design security primitives based on chaotic systems for ecommerce*, 2012. (Doctoral dissertation, Durham University).

[40] Tsiakis, T., & Sthephanides, G. The concept of security and trust in electronic payments. *Computers & Security*, *24*(1), 10-15, 2005.

[41] Hair, F. Jr, Sarstedt, J., Hopkins, M. , L. and Kuppelwieser, G. , V., "Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research", European Business Review, Vol. 26 No. 2, pp. 106-121, 2014. https://doi.org/10.1108/EBR-10-2013-0128, 1989.