Humanities & Social Sciences Communications

ARTICLE

https://doi.org/10.1057/s41599-024-03585-2 OPEN

Security matters: Empowering e-commerce in Sri Lanka through customer insights

Ruwan Jayathilaka[1]✉ & Isuri Udara[2]

In the fast-paced, post-COVID digital world, e-commerce presents promising prospects for significant advancement. However, customers often feel uncertain due to persistent concerns about the robustness of security measures safeguarding e-commerce platforms. The primary objective of our study was to identify factors affecting the security of e-commerce platforms based on the perceptions of Sri Lankan customers. This research was conducted using data collected from Sri Lankan e-commerce users via both online and offline surveys. An ordered probit regression model was utilised, demonstrating that transaction security, privacy, vendor system security, and platform quality positively impact the perceived security of e-commerce. The e-commerce industry in Sri Lanka is expected to see growth and an increased user penetration rate. The findings of this study are anticipated to assist e-commerce business owners and policymakers in addressing critical security issues, namely vulnerabilities in transactional security, low privacy, inadequate system security, and poor e-commerce platform quality. These improvements are expected to build trust and credibility among consumers, maximising e-commerce success.

[1] Sri Lanka Institute of Information Technology, Malabe, Sri Lanka. [2] University of Kelaniya, Kelaniya, Sri Lanka. ✉email: ruwan.j@sliit.lk

Introduction

The growth of e-commerce, accompanied by increased security concerns, significantly affects customers and e-commerce stakeholders, including owners and vendors. Given the rising security threat, the e-commerce industry has yet to achieve its true potential, as customers require more confidence and trust in purchasing via digital platforms. Hence, to reap the benefits of e-commerce, customer concerns regarding the security of e-commerce platforms should be proactively addressed. Understanding how customers perceive the security of an e-commerce platform will benefit e-commerce owners and vendors by allowing them to assess their platforms' security levels and adopt appropriate measures.

The global platform for buying and selling products and services over the Internet, termed electronic commerce, has revolutionised how businesses operate. Insider Intelligence predicts that the USD 5.717 trillion worldwide retail e-commerce sales in 2022 will grow to USD 8.148 trillion by 2026, with retail purchases expected to increase to 24% by 2026, leading to a USD 8.1 trillion global market share (Baluch, 2023). These statistics reveal that the e-commerce industry is rapidly ascending while making a significant contribution to global economic growth. However, the e-commerce industry remains one of the most susceptible sectors, facing 32.4% of cyber-attacks (Behani, 2019). Cybercrime has risen by 600% since the COVID-19 pandemic, costing one percent of the Global Gross Domestic Product (GDP) (PurpleSec, 2021). The primary security risks faced by e-commerce platforms include financial fraud (credit card fraud and fake return and refund scams), phishing, spamming, Distributed Denial of Service attacks, malware, Structured Query Language (SQL) injection, Cross-site scripting (XSS), brute force attacks, man-in-the-middle attacks, and e-skimming. With the growth of online transactions, USD 41 billion was lost due to e-commerce fraud, and this figure is expected to increase to USD 48 billion in 2023 (Baluch, 2023). When data is compromised during these attacks, 42% of the compromised data includes payment information, and 41% contains personally identifiable data (PurpleSec, 2021). Poor security has been a significant challenge for customers and businesses since the inception of e-commerce. Post-Covid, there is a new window of opportunity for increased internet penetration and security vulnerabilities.

In Sri Lanka, with a population of 21.92 million, approximately 12.34 million people are internet users; the internet penetration rate is 56.3% (Kepios, 2024). With the increase in internet penetration, the e-commerce market in Sri Lanka is anticipated to experience a 20.2% growth in 2023, contributing to the global growth rate of 17.0% in the same year. Currently, Sri Lanka is the 54th largest e-commerce marketplace with a predicted revenue of USD 2,442.4 million by 2024. The revenue is expected to show a compound growth rate of 5.4%, resulting in a projected market volume of USD 3,017.8 million by 2028 (eCommerceDB, 2022). It is evident that internet penetration and the accessibility of smart devices have fuelled the growth of Sri Lanka's digital economy contributing to over 5% of the GDP. Moreover, this increase has been driven by commercial banks offering electronic services and the commitment to increased use of online applications for government services (International Trade Administration 2024b). By 2027, it is projected that Sri Lankan e-commerce users will reach 10.19 million, with the user penetration rate, which stands at 37.8% in 2023, anticipated to increase to 46.1% by 2027 (Statista, 2022). These statistics speak volumes about the promising future of the e-commerce marketplace in Sri Lanka.

The behaviour of Sri Lankan e-commerce users coincides with that of users in most developing countries. According to Sri Lanka's latest report on digital consumers, with 2,703 respondents, 41.86% of online users purchase at least once a month, and the most frequently purchased item category is clothes and accessories, accounting for 49.03%. Additionally, 83% mentioned that their purchases are influenced by the reviews and recommendations of their close circle, and more than half of the shoppers are influenced by price discounts, which is 56.29%. Furthermore, 48.23% of online shoppers expressed a preference for Cash on Delivery payment. This emphasises that Sri Lankan consumers are price-sensitive and still prefer the traditional physical payment method (The Asia Pacific Institute of Digital Marketing and Department of Marketing Management, 2024). Similarly, the e-commerce markets in Bangladesh, Pakistan, and Indonesia are also moving in a positive direction, yet shoppers prefer the Cash on Delivery payment model 90%, 95%, and 57%, respectively, and most of these transactions are related to the purchase of apparel and fashion accessories (International Trade Administration 2024a). These statistics validate that the study of e-commerce and its future growth is an essential area of study.

However, the Statista survey states that 90% of online consumers have at least one primary concern regarding data privacy, and 70% to 80% of customers lost money in online shopping scams from 2015 to 2022 (Statista, 2022). In 2020 online shopping scams accounted for 38% of all reported scams worldwide, and losses from online payment fraud totalled more than USD 40 billion in 2022. Victims who suffered financial losses have consistently remained above 70%, resulting in seven out of ten global e-commerce users not sharing their data with merchants (Statista, 2022). Therefore, adopting suitable measures is an essential accelerator of the e-commerce growth trend, as continuous downfalls in security will create a lack of trust in customers and hinder the success of online providers.

In parallel to the growth of the e-commerce marketplace, there is a competitive increase in the threats targeted at the e-commerce sector. Therefore, developing a sophisticated framework is crucial in ensuring the triumph and long-term sustainability of the e-commerce industry in the digital age. In the increasingly digitised post-Covid world, e-commerce businesses must improve their awareness of risks and safeguards. Safeguarding against fraud could be a catalyst for increased e-commerce adoption (Statista, 2022). Sri Lanka is a cash-based economy, where Sri Lankans show low confidence in e-commerce and e-payments. Although pre-payment is the most preferred payment option by e-commerce vendors, Sri Lankans mostly prefer post-payment via cash on delivery. This was further emphasised by Daraz, stating that "When it comes to purchasing merchandise, Sri Lankan people still prefer the traditional buying method of touch and feel" (Daily News, 2024). Moreover, regarding submitting personal and payment information to e-commerce platforms, there is a preference for online shopping via direct messaging to social media pages and getting the products through a human connection rather than trusting an automated e-commerce platform. Hence, the outcomes of e-commerce never peak in a country like Sri Lanka due to its citizens' wary perception.

The main research question formulated by translating the problem statement is: 'What are the factors affecting the security of e-commerce platforms in Sri Lanka?' To answer this question; clear, measurable, and verifiable research objectives were formulated. The main objective of this study is to identify the factors affecting the security of e-commerce platforms in Sri Lanka. This main objective was achieved with the aid of the following specific research objectives: to identify the impact of transactional security on the security of the e-commerce platform, to identify the impact of privacy on the security of the e-commerce platform; to identify the impact of customer perceived vendor's system security on the security of the e-commerce platform; and to identify the impact of customer perceived e-commerce vendor's platform quality on the security of the e-commerce platform. Four hypotheses were derived based on the above objectives and the literature review. These hypotheses tested whether the four variables transactional security, privacy, vendor's system security, and vendor's platform quality have a positive impact on the overall e-commerce platform security. This study aims to identify the factors affecting the perceived security of e-commerce platforms from the Sri Lankan customer's point of view to address the critical issues of vulnerabilities in transactional security, low privacy, low system security, and low e-commerce platform quality thereby building trust and credibility in the minds of consumers.

This research differs from existing studies by bridging the literature gap in five ways. First, prior research on e-commerce in Sri Lanka mainly studies consumer behavioural aspects and facets of technology adoption rather than security perception. Even in the research on technology adoption in e-commerce, the studies revolve around the technology adoption framework without considering the security factor. Therefore, more research needs to be conducted to determine the security implications of e-commerce platforms from the customers' viewpoint. Second, limited research discusses how e-commerce customers perceive the security of the unseen e-commerce platform. The e-commerce platform owners' or vendors' system lateral has yet to be a major researched area. Hence, the influence of system security provided by the vendor and how a customer perceives its importance in determining the use of a specific e-commerce platform has ample opportunity for research. Third, this study draws attention to developing a framework well attuned to the local Sri Lankan context, which implies the perception of security in a cash-based developing country with a low to mid digital literacy population. Fourth, this study will assist academic researchers conducting similar studies by drawing on this research framework for other developing countries with low digital literacy. Finally, this study will guide policymakers to align consumer protection and digital acts to uplift the e-commerce ecosystem in Sri Lanka and help e-commerce business owners harness better revenue.

Therefore, it is evident that this research addresses critical gaps in the existing literature on e-commerce security in Sri Lanka by focusing on several key areas. Prior studies have largely concentrated on consumer behaviour and technology adoption overlooking the security aspects. Additionally, the impact of vendor's system security and its influence on customer trust and usage remains underexplored. This showcases the importance of a concise framework to improve the security of the driver of a country's digital economy, which in turn can be utilised by similar economies, assisting policymakers in ensuring consumer rights and strengthening the economy.

The conceptual framework was tested with four hypotheses using the ordered probit model, and the results highlighted that the impact of transactional security is low as shoppers are heavy users of cash-based transactions, whereas the other hypotheses were accepted. These results correspond with research in similar economic landscapes. Since few studies have focused on incorporating customer perceived security of e-commerce platforms, the results offer important theoretical and practical contributions for e-commerce vendors on how to improve their platforms. This can be used as an eye-opener for policymakers to establish solid policies and acts on securing consumers when exposing personal and financial data online.

The remaining sections are organised as follows "Literature Review", which focuses on extant literature; "Data and Methodology", presenting the data and methodology utilised; "Results and Discussion", evaluating the empirical results and the discussion; and "Conclusion and Policy Implications", presenting the recommendations and conclusion, respectively.

Literature review

For this empirical investigation, the researcher referred to studies related to e-commerce published between 2013 and 2023. To access relevant literature in English, the researcher utilised well-regarded electronic research databases such as Emerald Insight, Springer, Science Direct, JSTOR, SAGE Premier, Wiley Online, Research Gate, and IEEE. The search strategies led to the identification of full-text publications available online. The selection process involved examining both titles and abstracts to choose articles suitable for the study, while irrelevant articles were excluded, leading to a final selection of 23 articles for the current investigation. Figure 1 depicts the literature search flow diagram incorporating the search strategies.

Past research in this area highlights numerous factors that impact the secure adoption of e-commerce platforms from the customer's viewpoint. These factors differ based on each country's population's usage and digital literacy level. The proposed research framework addresses the specific factors influencing the secure adoption of e-commerce from the perspective of customers in Sri Lanka.

Customer's transactional security. Transactional security in e-commerce refers to "a secure non-fraudulent transfer of monetary value from the payer to the payee via electronic means, which links the exchanged data to an economic real-world value" (Kuruwitaarachchi et al. 2019). This process asserts that all transactions should be secure by its definition—the research on e-commerce transaction security encompasses the security of the e-payment system and payment data security. In a research study conducted in the United Kingdom (UK), it was revealed that 86.3% of respondents strongly agreed that e-commerce vendors must have a secure online payment system, and 67.6% of respondents did not agree to provide payment details to local e-commerce vendors (Alshehri and Meziane, 2017). Similarly, research in Bahrain supported the idea that trust in online payment systems is a crucial predictor of the acceptance of e-commerce and data security of e-payments plays a significant role in establishing the security of a transaction (Albastaki et al. 2022). Moreover, a study conducted in Pakistan concluded that customers' credit card usage and data security are significant in the customer's perception of the security of the transaction (Saeed, 2023). Furthermore, research also revealed that credit card information usage directly correlates to the transaction field's security(Gull et al. 2022). Considering the above facts, customers are more concerned about the safety of their payments and payment information via electronic platforms. Therefore, transactional security can be viewed as a crucial explanatory variable in determining an e-commerce platform's security from a customer's perspective.

Customer's privacy. Online privacy also known as "Internet privacy," and it is the "individual's right to access and control their personal information concerning its collection, use, and transfer over the Internet" (Alharbi et al. 2013). The literature on privacy mainly discusses the collection and use of customer data. Research shows that online customers are comfortable providing general and vague information on personal choices and preferences but are not comfortable providing personal identification and payment card details as they are considered sensitive information (El Haddad et al. 2018). Studies indicate that consumers need to overcome privacy concerns as their primary obstacle because the main hindrance that prevents customers from engaging in e-commerce transactions is when they are required to share personal information (Gurung and Raja, 2016). Further research also states that the rising anxieties

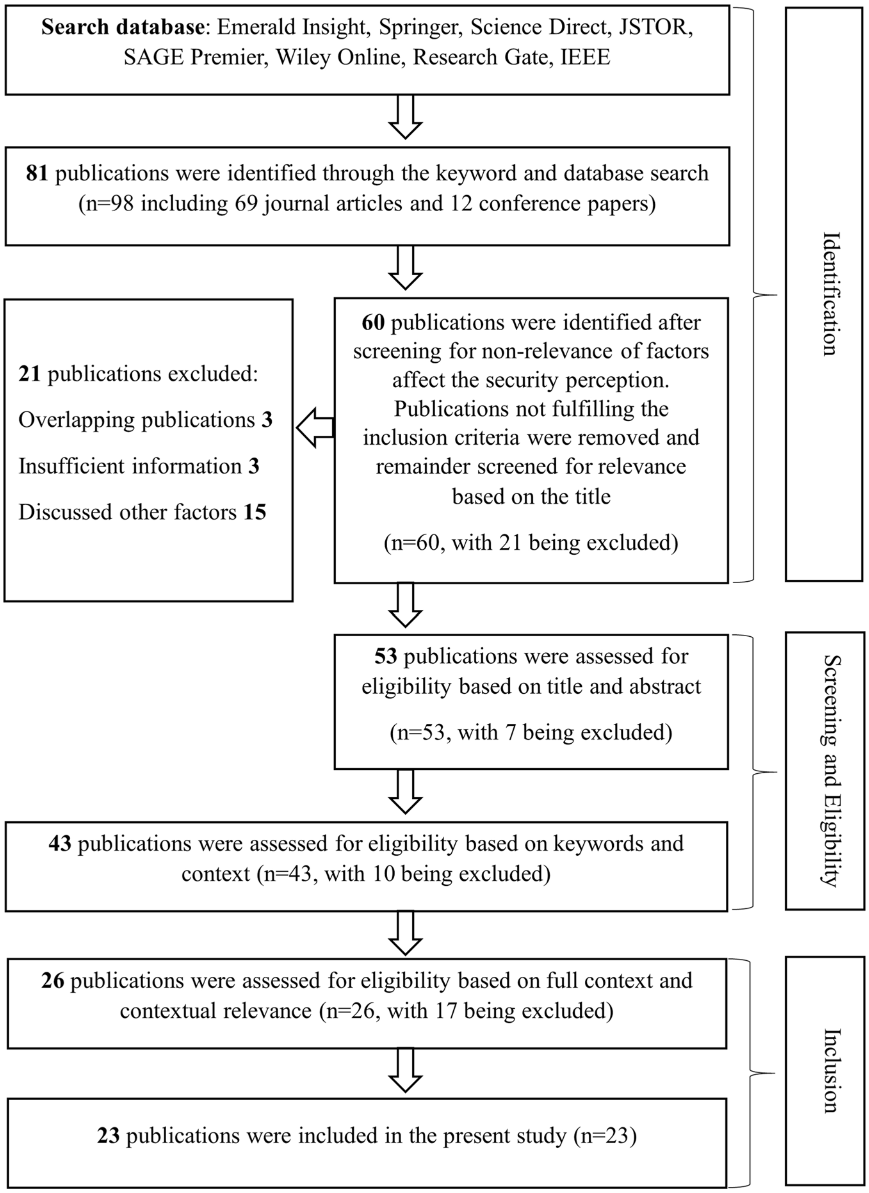
Search database: Emerald Insight, Springer, Science Direct, JSTOR, SAGE Premier, Wiley Online, Research Gate, IEEE
81 publications were identified through the keyword and database search (n=98 including 69 journal articles and 12 conference papers)
60 publications were identified after screening for non-relevance of factors affect the security perception. Publications not fulfilling the inclusion criteria were removed and remainder screened for relevance based on the title
(n=60, with 21 being excluded)
21 publications excluded:
Overlapping publications 3
Insufficient information 3
Discussed other factors 15
53 publications were assessed for eligibility based on title and abstract
(n=53, with 7 being excluded)
43 publications were assessed for eligibility based on keywords and context (n=43, with 10 being excluded)
26 publications were assessed for eligibility based on full context and contextual relevance (n=26, with 17 being excluded)
23 publications were included in the present study (n=23)
Identification
Screening and Eligibility
Inclusion

Fig. 1 Literature search. Source: Authors' compilation based on the literature.

about privacy and security cause customers to offer restricted, partial, or incorrect information on websites to safeguard their data (Alharbi et al. 2013).

Additionally, research proves that customers are worried about the exchange of personal information between them and e-commerce platforms, as well as how these platforms handle their data (Hong and Thong, 2013). Therefore, the level of trust an e-commerce vendor earns regarding their ability to safeguard personal information directly correlates with the customer's confidence in that vendor's capability to protect sensitive data. A study conducted in Saudi Arabia revealed that privacy has a significant positive impact on security (Alqahtani and Albahar, 2022). Controversially, Gurung and Raja (2016) conclude that privacy outweighs security. The literature stated above signifies that privacy is a significant concern in the hearts of customers, as they believe they have no control over their data once it is submitted to an e-commerce platform. Therefore, customers have practised the tendency to provide incorrect information in all possible fields, causing e-commerce vendors and platform owners to analyse and interpret inaccurate data. Hence, to address the menace of privacy concerns in using e-commerce, customer privacy can be considered an imperative influence in determining the perceived security of an e-commerce platform.

Customer perceived vendor's system security. System security is a significant attribute of concern for e-commerce vendor's as it mainly focuses on the availability and security of the web server and the database. Customers do not see the backend of an e-commerce operation; therefore, how they asses the availability factor is based on extended loading times, delays, breakdowns, and unusual activities at the customer's interface (Kuruwitaarachchi et al. 2019). Moreover, platform failure, inaccessibility, non-adaptability, delay, and insecurity are the indicators of e-service quality. Such factors negatively impact the e-service quality of an e-commerce platform (Tan et al. 2016). Some literature discusses the vendor's system security perceived by customers as e-service quality as it is the service that customers can assess the providing system. The central factors that negatively influence the growth of e-commerce are the inadequate security on e-commerce web servers and the security vulnerabilities in customer devices (Singh, 2014). The threats reaching the customer can be minimised when adequate security is available on customers' devices.

Further, any information leakage via a system failure can harm the customers in the eyes of the e-commerce vendor (Girsang et al. 2020). It was identified that there is literature on cybercrimes in e-commerce. Yet, the number of pieces of literature that discussed the system security of the e-commerce vendor from the customer perspective could have been much higher. The research contribution on the significant importance of ensuring system security of the e-commerce platform provider is limited, yet it is an explanatory variable, in determining the perceived security of an e-commerce platform.

Customer perceived vendor's platform quality. Platform quality in e-commerce refers to the design excellence, usability, and availability of the playing field of an e-commerce customer as it enables customers to purchase products and services online. The lack of any of the above attributes will negatively impact e-commerce and is considered a form of online service failure (Amsl et al. 2023). The e-commerce platform quality can be positively influenced when the design problems, navigational problems at the site, and website purchasing process confusion are solved through the design (Roy et al. 2022). E-commerce users prefer platforms where they can absorb the platform rapidly, go from page to page with straightforward navigation, search for products, and purchase expeditiously. When the above elements are detailed, trust builds, and the fear of being misled is curbed.

Moreover, based on the empirical findings from Vietnam, customers' perception of design, positively correlates with their perceptions of reliability, privacy, customer service, and purchase intention concerning the e-commerce platform (Dang and Pham, 2018). Based on the above findings, it ensures that the look and feel of an e-commerce platform can build a sense of security. Therefore, platform quality can be considered an influential variable for the security of e-commerce platforms.

The comprehensive literature review paved the way to identify the theoretical and practical gaps in past studies. Most research on e-commerce has used the Technology Acceptance Model (TAM) coupled with privacy concerns and trust as the key attributes of study. Yet, there is no framework that incorporates security as a key variable under e-commerce. Therefore, this research models a conceptual framework by considering the security of the e-commerce platform as the dependent variable to study the impact of four factors that are separately considered in past literature. Moreover, the research found insights that a single framework to address the security needs of e-commerce is not yet present. Therefore, it enhances the attractiveness of this research and its contribution to developing a distinct security framework for online business. Four independent variables have been identified during the literature review, and each variable is investigated extensively to unveil an accurate picture of the security of e-commerce platforms. S1 Appendix presents a summary of the selected literature including the authors, paper title, year of publication, methodology, data collection methods, and findings.

Data and methodology

This study utilised the waterfall approach and was conducted in twelve phases. As shown in Fig. 2 the study commenced with the initial background research on e-commerce and various security threats faced by its users. This highlighted the need for further research on the security aspects of e-commerce specifically in the Sri Lankan context. Subsequently, the research problem was defined, leading to the formulation of a solid research question and clear objectives. Next, a thorough literature review was conducted across well-regarded research databases to assess the extent of current studies and to identify theoretical gaps. Additionally, expert opinion was elicited from special e-commerce users and academics. These activities led to identifying the variables of study and the development of the conceptual framework. Next, the questionnaire was designed covering all the variables and was tested by ten experts in the pilot study, which further refined the instrument. Data was then collected both online and offline and was analysed using STATA. The analysis derived useful information to confirm the hypotheses of the study. These findings were discussed under the results and discussion, drawing comparisons with similar studies. Finally, the study concluded with identifying the practical implications, contributions to policy development, and potential future work.

Data. This study investigates the factors affecting the perceived e-commerce platform security based on the customer's perspective in Sri Lanka. The SLIIT Business School and the SLIIT Ethical Review Board reviewed and approved the study. The research followed a cross-sectional deductive approach, gathering quantitative data from an online and offline survey using a structured questionnaire. The population of this research includes all the internet users in Sri Lanka. As of February 2024 there are 12.34 million internet users in Sri Lanka (Kepios, 2024). The recommended sample size for this population was 307 based on

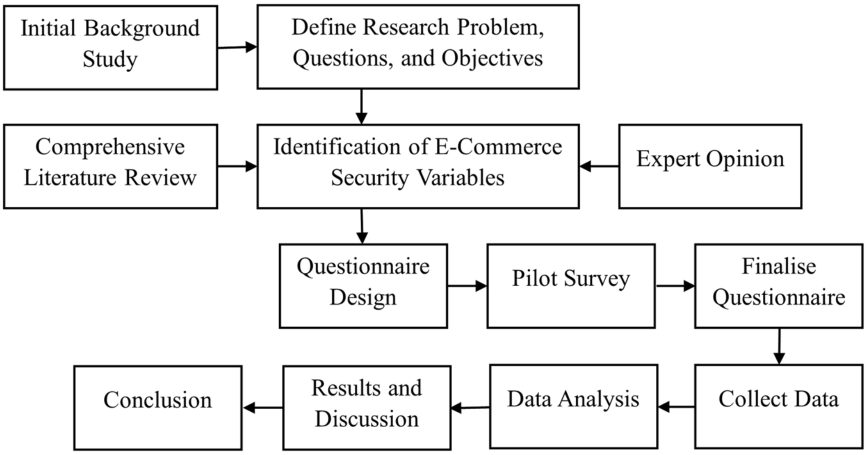

Fig. 2 Research flow diagram. Source: Authors' compilation.

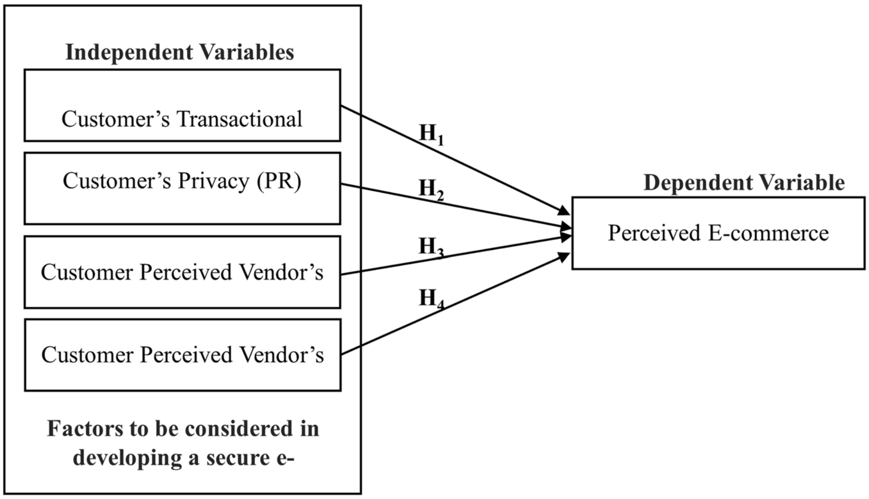

Fig. 3 Conceptual research framework. Source: Authors' compilation based on the literature.

the Krejcie and Morgan table (Krejcie and Morgan, 1970). However, the researchers were able to collect a sample of 306 data points. The sample size was determined at a 95% confidence level and 5.6% margin of expected error. The significance level considered in the study was α = 0.05.

Questionnaire Design. The questionnaire was aligned with the research objectives and the study's conceptual framework, incorporating existing models adopted in previous research studies as referenced in the literature review. The questionnaire was designed with simple, understandable questions in the English language to elicit data from all participants. It was divided into six sections. Section one focused on the respondents' demographic details, and sections two to six concentrated on identifying the factors affecting the perceived e-commerce platform security in Sri Lanka. A five-point Likert scale ranging from "Strongly Disagree" (1) to "Strongly Agree" (5) was used in sections two to six. The questionnaire is presented in S2 Appendix. Moreover, the questionnaire incorporated open-ended questions to list the leading e-commerce platforms and the negative experiences encountered while using e-commerce. The survey was conducted from mid-August 2023 to early October 2023 in Sri Lanka, and the primary data were tested for validity and reliability.

The questionnaire design involved two phases. Initially, a pilot survey was conducted offline with ten participants from different demographic profiles. Based on their feedback, ambiguities in the questionnaire were resolved, resulting in a more understandable version.

Research framework and hypothesis. Figure 3 presents the conceptual framework, developed from the literature review, led to the formulation of the following hypothesis:

Hypothesis 1: There is a positive impact of customer's transaction security on e-commerce platform security.

Hypothesis 2: There is a positive impact of customer's privacy on e-commerce platform security.

Hypothesis 3: There is a positive impact of perceived e-commerce vendor's system security on e-commerce platform security.

Hypothesis 4: There is a positive impact of perceived vendor's platform quality on e-commerce platform security.

The framework identifies the factors affecting customer-perceived security of an e-commerce platform. Table 1 in the study presents the constructs and measurements for these variables.

Methodology. Internal reliability of the responses was assessed using Cronbach's alpha, and descriptive statistics were computed for the four independent variables and the dependent variable. The ordered probit regression model, introduced by Aitchison and Silvey in 1957, was used as the primary data analysis technique to model the categorical data (Aitchison and Silvey 1957).

The ordered probit regression provides a generalised approach for conducting regression analysis on ordinal dependent variables with more than two outcomes (Aitchison and Silvey 1957). Ordered probit model is a regression framework that uses maximum likelihood estimation and is used to include multiple predictor variables to analyse relationships similar to other techniques. But this method differs from other regression techniques from four main ways. First, is its suitability for ordinal data unlike linear regression, which assumes continuous outcome, and logistic regression, which is designed for binary outcomes. Second, the model estimates threshold parameters that delineate boundaries between different categories of the ordinal variable, which can aid in providing insights into how changes in variables influence the probability of moving from one category to another. Third, this model assumes does not require the assumption of equal distances between categories, which helps to accurately reflect the nature of ordinal data. Finally, it assumes that the error term is normally distributed influencing the interpretation and the fitness of the model.

The selection of the ordered probit model for this study is justified by the following five reasons. First, the ordered probit model can aid in analysing ordinal data with categories with or without equal intervals. Therefore, the model eases to categorise the perceived security of e-commerce platforms based on the probability of being a low-secure or high-secure platform. Second, the interpretable coefficients emphasise the effect of each independent variable on the likelihood of moving from one category to another, enabling us to understand the impact of predictors. Third, the ordered probit model accommodates different types of ordinal responses such as the Likert scale, which is the central question style in the questionnaire of this study. Fourth, the model offers an array of goodness-of-fit measures, enabling the assessment of how well the model fits the data. Finally, The ordered probit model was chosen for its ability

Table 1 Operationalisation Table.

Type of Variable	Variable Name	Indicators	Measurement (Likert Scale)	Question Items	References
Independent Variable	**Customer's Transaction Security**	■ Online payment system ■ Trust ■ Payment information storage ■ Refund and return	1 = Strongly Disagree 2 = Disagree 3 = Neutral 4 = Agree 5 = Strongly Agree	[Q1 -Q17]	■ (Alshehri and Meziane, 2017) ■ (El Haddad et al. 2018) ■ (Pramanik and Prabhu, 2022)
	Customer's Privacy	■ Information collected ■ Information storage ■ Information usage ■ Trust	1 = Strongly Disagree 2 = Disagree 3 = Neutral 4 = Agree 5 = Strongly Agree	[Q18 -Q30]	■ (Gurung and Raja, 2016) ■ (Akour et al. 2022) ■ (Pramanik and Prabhu, 2022)
	Customer Perceived Vendor's System Security	■ Availability ■ Authentication process ■ Security certificates ■ Cyber attacks	1 = Strongly Disagree 2 = Disagree 3 = Neutral 4 = Agree 5 = Strongly Agree	[Q31 - Q47]	■ (Belanger et al. 2002) ■ (Kumar and Gupta, 2021) ■ (Amsl et al. 2023)
	Customer Perceived Vendor's Platform Quality	■ Information quality ■ Platform design ■ E-service quality	1 = Strongly Disagree 2 = Disagree 3 = Neutral 4 = Agree 5 = Strongly Agree	[Q47-Q62]	■ (Belanger et al. 2002) ■ (Dang and Pham, 2018) ■ (Amsl et al. 2023)
Dependent Variable	**Perceived E-commerce Platform Security**	■ Internet security ■ Web security ■ Security seals ■ Integrity	1 = Strongly Disagree 2 = Disagree 3 = Neutral 4 = Agree 5 = Strongly Agree	[Q63-Q74]	■ (Belanger et al. 2002) ■ (El Haddad et al. 2018) ■ (Saeed, 2023)

Source: Authors' compilation based on the literature.

Table 2 Categorical groups for the ordered probit model.

Group	Category	Interpretation
Group 01	Deficient security	Mean value of perceived e-commerce platform security is less than or equal to 2.25
Group 02	Low security	Mean value of perceived e-commerce platform security is greater than 2.25 and less than or equal to 2.75
Group 03	Moderate security	Mean value of perceived e-commerce platform security is greater than 2.75 and less than or equal to 3.2
Group 04	High security	Mean value of perceived e-commerce platform security is greater than 3.2 and less than or equal to 3.5
Group 05	Very high security	Mean value of perceived e-commerce platform security is greater than or equal to 5

Source: Authors' compilation.

to analyse ordinal data with unequal intervals, interpret coefficients, accommodate Likert scale responses, offer goodness-of-fit measures, and its previous use in similar research objectives (Weerasena and Jayathilaka, 2023).

In this study, the researcher will categorise the respondent's perception of e-commerce platform security into five possibilities: deficient security, low security, moderate security, high security, and very high security. Consequently, the ordered probit model will be formulated with five categorical groups ($k = 5$). Table 2 presents the five definite groups and their interpretation.

Accordingly, five categorical groups were based on respondent's perceptions, and the grouping was based on dividing samples into five equal categories with a variation of plus or minus ten samples.

The ordered probit model used in the research is specified in Eq. 1.

$$SECURITY(1,2,3,4,5) = X_i(\beta_0 + \beta_1 TS + \beta_2 PR + \beta_3 SS + \beta_4 PQ) + \varepsilon_i \quad (1)$$

SECURITY stands for perceived e-commerce platform security, and TS, PR, SS, and PQ stand for customer transaction security, privacy, vendor system security, and vendor platform quality, respectively. Table 3 below describes the dependent and four independent variables of the study.

The table above depicts the expected positive impact of each variable on e-commerce platform security based on past empirical studies. STATA software was used for statistical analysis, and Word Cloud was used to analyse responses to the open-ended questions in the survey.

Results and discussion

Reliability was assessed using Cronbach's approach for internal consistency. The study's five variables, encompassing four independent variables and one dependent variable, underwent testing to compute Cronbach's alpha. The reliability statistics, as presented in Table 4, indicate that the collected data are reliable, with the reliability coefficient surpassing 0.8.

The Table outlines the study's variables, observation sample size, the number of questionnaire items covered by each variable's indicators, Cronbach's alpha, and the average interitem covariance reflecting the items' average variance.

S3 Appendix presents descriptive statistics for the five variables, including four independent variables and one dependent variable. The research's estimated outcomes were derived using

Table 3 Summary of variables.

Variable	Description	Expected sign
SECURITY	Dummy variable to denote the perceived security of e-commerce platforms where very low is denoted as 1, low as 2, moderate as 3, high as 4, and very high as 5	+
TS	Five-point Likert scale variable with extremes “Strongly Disagree-1” to “Strongly Agree-5” to measure the impact from customer’s transaction security	+
PR	Five-point Likert scale variable with extremes “Strongly Disagree-1” to “Strongly Agree-5” to measure the impact from customer’s privacy	+
SS	Five-point Likert scale variable with extremes “Strongly Disagree-1” to “Strongly Agree-5” to measure the impact from perceived vendor’s system security	+
PQ	Five-point Likert scale variable with extremes “Strongly Disagree-1” to “Strongly Agree-5” to measure the impact from perceived vendor’s platform quality	+

Source: Authors’ compilation based on the literature.

Table 4 Internal Consistency.

Item	Observations	Number of items	Cronbach’s alpha	Average interitem covariance
SECURITY	306	12	0.8312	0.273514
TS	306	17	0.8397	0.1861721
PR	306	13	0.8582	0.3000944
SS	306	16	0.8189	0.1821492
PQ	306	16	0.8808	0.2969432

Source: Authors’ calculation.

the ordered probit regression model aimed at understanding the variables’ impact on perceived e-commerce platform security in Sri Lanka.

The survey data utilised for estimation was collected from 306 internet users in Sri Lanka. Figure 4 illustrates the distribution of Likert scores for the dependent and four independent variables using a violin plot.

The distribution of the dependent variable appears relatively symmetrical around 3, suggesting an average perception close to neutral. Among the four independent variables, system security exhibits a higher density, indicating a tendency towards a positive perception, while platform quality is skewed towards 4 and 5, signifying a generally favourable view.

The initial ordered probit model was estimated using the four independent variables. Table 5 provides the results, goodness-of-fit statistics, adjusted log-likelihood index ratio, and the number of observations. Marginal effects were calculated to interpret the substantive effect of each independent variable separately across various security levels.

The study’s results are consistent with findings in existing literature. The subsequent section delineates the outcome of the four hypotheses evaluated.

Impact of customer’s transactional security. The impact of customer transactional security is evident in the marginal effects observed. A one percent increase in transactional security correlates with a reduction in the probability of an e-commerce platform being categorized as low-security, by 0.03 and 0.04 percentage points for the deficient security and low-security groups, respectively. Conversely, transactional security enhances the probability of a platform being perceived as secure by 0.01, 0.04, and 0.01 percentage points for the moderate, high, and very high-security groups. This indicates that perceived e-commerce platform security improves across low to high security levels.

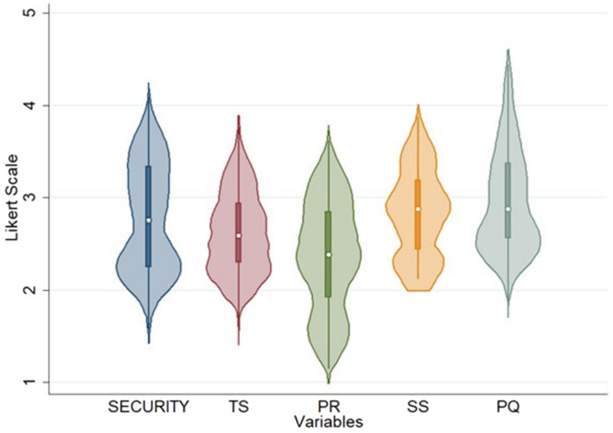

Fig. 4 Distribution of dependent and independent variables. Source: Authors’ compilation based on Likert scores.

Transactional security emerges as a crucial determinant of perceived e-commerce platform security, albeit with a significance level that is relatively low. These findings align with previous research in developing countries, where consumers exhibit reluctance towards digital payment methods. Cash on delivery remains the preferred mode due to perceived security threats, credibility concerns, trust issues, and apprehensions regarding privacy invasion (Khan et al. 2023; Muniraju and Hariprasad, 2019).

The significance of transactional security could be even higher, considering the low awareness and usage of e-payments among most Sri Lankans. The preference for cash-on-delivery is predominant, as evidenced by the high usage of platforms like Daraz, with 46.4% market share, and other local e-commerce platforms accounting for 16.01%. Notably, 51.63% of users prefer cash on delivery as their primary payment method.

Impact of customer’s privacy. The impact of customer privacy on e-commerce platform security is substantial, as evidenced by the observed marginal effects. A one per cent increase in privacy results in a decrease in the probability of an e-commerce platform being categorized as low-security by 0.05 and 0.07 percentage points for the very low-security and low-security groups, respectively. Conversely, privacy enhances the probability of a platform being perceived as secure by 0.02, 0.07, and 0.02 percentage points for the moderate, high-, and high-security groups. This trend indicates that perceived e-commerce platform security improves across low to high security levels with an increase in privacy.

Table 5 Ordered Probit Regression Results.

Variable	Estimate	Robust SE	Marginal effects (in percentages)				
			Very low (*SECURITY* =)	Low (*SECURITY* = 2)	Moderate (*SECURITY* = 3)	High (*SECURITY* = 4)	Very high (*SECURITY* = 5)
TS	0.2267	0.2472	−0.0314	−0.0434	0.0172	0.0424	0.0152
PR	0.3699[b]	0.2315	−0.0542[c]	−0.0750[c]	0.0297[c]	0.0732[c]	0.0263
SS	0.3147[b]	0.2831	−0.1077[b]	−0.1491[b]	0.0591[b]	0.1455[b]	0.0522[a]
PQ	1.8548[a]	0.2663	−0.2516[a]	−0.3482[a]	0.1379[a]	0.3398[a]	0.1220[a]
Ancillary parameters			Marginal effects				
Very low	6.8582	0.5676	0.0917	0.3361	0.3443	0.1916	0.0364
Low	7.8439	0.5779					
Moderate	9.0048	0.6179					
High	10.0625	0.6586					
Pseudo R^2	0.2720						
Log likelihood	−290.6473						
Observations	306						

Source: Authors' calculation.
[a] Significant at the 1% level;
[b] Significant at the 5% level;
[c] Significant at the 10% level.

Privacy emerges as a crucial determinant of perceived e-commerce platform security, with notable implications for Sri Lankan consumers. Sri Lankans tend to prefer human engagement and utilize social media pages for purchasing products, often without creating accounts. Instead, they provide their name, address, and telephone number directly to the individual managing the page. This preference reflects the lower digital literacy levels among Sri Lankans, who are hesitant to create accounts and share personal details with business organizations due to concerns about information control.

These findings resonate with previous research, highlighting the adverse effects of limited corporate privacy responsibilities and regulatory protection on consumer trust (Bandara et al. 2021; Choi et al. 2018). Thus, privacy plays a significant role in determining e-commerce platform security. Increased control over personal information fosters a higher probability of a platform becoming highly secure, thereby enhancing consumer trust and confidence in e-commerce transactions.

Impact of customer perceived vendor's system security. The perceived system security maintained by vendors significantly influences the security perception of e-commerce platforms, as indicated by the observed marginal effects. A one percent increase in customer-perceived vendor system security results in a decrease in the probability of an e-commerce platform being classified as low-security by 0.1 and 0.14 percentage points for the deficient security and low-security groups, respectively. Conversely, an improvement in vendor system security enhances the probability of a platform being perceived as secure by 0.05, 0.14, and 0.05 percentage points for the moderate, high, and high-security groups. This trend underscores the positive impact of vendor system security across different levels of e-commerce platform security, ranging from low to high.

The findings highlight the critical role of vendors' system security in shaping the perceived security level of e-commerce platforms, particularly in the Sri Lankan consumer context. Vendors' responsibility in providing a secure platform is gauged by their contribution to maintaining system security, encompassing both web and server-side aspects. The study underscores the significance of robust vendor system security, which significantly enhances e-commerce platform security, aligning with previous research (Kuruwitaarachchi et al. 2019). Thus, improving vendor system security is imperative for ensuring very high levels of e-commerce platform security, fostering consumer trust and confidence in online transactions.

Impact of customer perceived vendor's platform quality. The impact of customer-perceived platform quality on e-commerce platform security is substantial, as evidenced by the observed marginal effects. A one percent increase in platform quality results in a decrease in the probability of an e-commerce platform being classified as low-security by 0.25 and 0.34 percentage points for the deficient security and low-security groups, respectively. Conversely, enhancing platform quality increases the probability of a platform being perceived as secure by 0.13, 0.33, and 0.12 percentage points for the moderate-security, high-security, and high-security groups. This indicates that perceived e-commerce platform security is notably improved across various security levels, ranging from low to high, with high-quality platforms.

Platform quality emerges as the most influential variable in determining perceived e-commerce platform security in the local context, underscoring its significance in enhancing security perceptions. Increasing platform quality, through the integration of design elements and enhancing user experience, substantially contributes to elevated e-commerce platform security. These findings resonate with previous research, suggesting that e-commerce platforms prioritizing content quality over technical aspects yield superior security perceptions (Herrada-Lores et al. 2022). Moreover, the results align with studies emphasising that elements such as navigation, search functionality, and design positively influence perceived platform quality (Roy et al. 2022).

This study, grounded in four hypotheses, analyses data collected from Sri Lankan e-commerce users, revealing insights into the impact of various factors on e-commerce platform security. While the impact of transactional security on overall e-commerce platform security is found to be insignificant, privacy demonstrates moderate significance. Notably, customer-perceived vendor system security and platform quality significantly influence e-commerce platform security, highlighting their importance in shaping consumer perceptions.

The utilisation of an ordered probit model tailored for ordinal security outcomes enhances result interpretation, elucidating how independent variables drive transitions between different security levels. These outcomes offer valuable insights for policymakers, enabling precise policy recommendations aimed at strengthening vendor system security and platform quality, given their pivotal

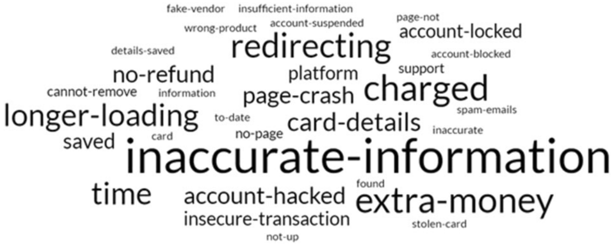

Fig. 5 Word cloud depicting negative experiences faced by e-commerce customers (Labs). Source: Authors' compilation.

role in influencing e-commerce platform security according to customer perceptions.

Furthermore, the questionnaire administered in this study captures the negative experiences encountered by e-commerce users, providing a comprehensive understanding of challenges faced in the local context. Figure 5 depicts these negative experiences through a word cloud, shedding light on prevalent issues impacting e-commerce user experiences.

The predominant negative experiences reported largely centre on discrepancies found within e-commerce platforms, including inaccuracies, insufficiencies, and outdated information. Moreover, users frequently encounter extended page loading times, persistent redirections, and system crashes. Additionally, concerns were raised regarding the storage of card details without the option for removal. Further grievances encompass unexpected charges during checkout, unauthorized deductions, delays in refunds, and payments deducted without authentication. These instances collectively underscore the undesirable encounters faced by customers.

Recent studies predominantly employ the Technology Acceptance Model (TAM), focusing on perceived usefulness, ease of use, and attitude towards usage. While TAM elucidates consumer acceptance and utilisation of e-commerce by highlighting perceived benefits, its scope is somewhat limited. The model's emphasis on ease of use and usefulness fails to encompass contextual factors pivotal to technology acceptance. Addressing this theoretical gap, our research adopts a security-centric perspective in evaluating e-commerce acceptance. Empirical data reveals that while users acknowledge the importance of platform security, their understanding of security assessment remains lacking. Consequently, security perceptions vary greatly based on individual users' digital literacy.

Designing e-commerce platforms entails navigating a complex technical landscape. Features deemed effective in one platform may falter in another. Thus, customers' perceptions of security across platforms differ, influenced by varied factors. This study furnishes practical implications for e-commerce vendors. Enhancing system security and platform quality is paramount. Vendors must invest in technological infrastructure, user interfaces, search functionalities, product information clarity, navigation enhancements, and prominent display of security seals and certificates. Moreover, raising awareness among online users regarding technical competencies and security aspects is crucial. Comprehensive privacy and data protection policies should be formulated and communicated transparently. A customer-centric approach is advocated to bolster confidence and drive increased e-commerce sales.

While e-commerce is not novel in urban Sri Lanka, it gained traction among middle-aged to elderly urban dwellers and emerged as a novel concept in rural areas during the Covid-19 pandemic. Despite attracting new customers during the pandemic, e-commerce platforms face trust deficit, hindering customer engagement. This study investigates factors influencing e-commerce platform security based on Sri Lankan users' digital literacy. Improved vendor system security and platform quality, alongside transactional security enhancements, are deemed essential. In the absence of robust governmental measures to address growing security concerns, the e-commerce industry faces stagnation. Policymakers must intervene to ensure adherence to security practices by e-commerce platforms and vendors, thereby fostering user trust and industry growth.

This study advocates the applicability of its conceptual framework as a foundational guide for enhancing e-commerce platform security in regions with varying degrees of digital literacy. Future research can leverage this framework to explore factors affecting platform security from diverse perspectives, including those of customers, platform owners, vendors, and security professionals. The findings can inform policy interventions aimed at bolstering the sustainability of the e-commerce sector.

Conclusion

The primary objective of this research was to identify factors influencing perceived e-commerce platform security based on the customer's perspective in Sri Lanka. Studies undertaken in this ontological area have not yet covered Sri Lankans' perspective, despite the increase in e-commerce adoption since the Covid -19 pandemic. Therefore, this study will provide a new epistemological stance in this domain. This effort will be a green light for e-commerce vendors and related parties to pay more attention to the security concerns of e-commerce users. The findings of this study will be helpful for e-commerce platform owners, vendors, and consumer affairs authorities to address and contribute to significant issues such as low transactional security, low privacy, vulnerable system security, and confusing platform quality. Technology adoption in Sri Lanka is soft, with a lack of trust, low technology literacy, and a negative attitude towards technology.

Along with the low technology literacy of the middle-aged to the elderly population and Sri Lankans in rural areas, they are more vulnerable to adopting e-commerce. The possibilities they get trapped in insecure e-commerce platforms that can trick the customers are high. Moreover, when customers heavily use e-commerce, and when most of their data is available in cyberspace, they also fall into vulnerabilities with time, eventually resulting in a drop in their trust towards e-commerce vendors. The above reasons can result in a negative customer perspective on e-commerce platform security, and the severity of these issues can further deepen with time. The solution to uplift the negative perception of customers in Sri Lanka must be met with a standard plan. The above-discussed situations should be handled separately. Therefore, the significant influencing variables of the study, vendor system security and platform quality, should be considered on an e-commerce business level and technology level. In contrast, the moderately significant variables, transactional security, and privacy, should be considered at a personal level, e-commerce business level, and technology level, where the potential loopholes can be addressed in advance in each of these levels.

Furthermore, the negative perception among the middle-aged to the elderly and rural customers should be handled by e-commerce-owning business entities along with policymakers to address their concerns in a lively manner. Accordingly, the government, the Ministry of Consumer Affairs Authority, and the Information and Communication Technology Agency (ICTA) can develop well-defined policies from this research as a guideline. As a result, consumer trust and adoption of e-commerce will increase, which, in turn, will increase the revenue of e-commerce entities, eventually resulting in an increased contribution to the GDP of Sri Lanka.

Policy implications. Meanwhile, this evidence-based study can be referred to as a guide for government policymakers, ICTA, and authorities on consumer affairs to challenge the status quo, address the growing security concerns in customers' minds, and make data-driven decisions on the operations of e-commerce platforms. Policymakers should take the necessary actions to bring updated policies and rules for e-commerce platform owners and e-commerce vendors and to conduct awareness sessions on acceptable practices. Moreover, the relevant authorities should regularly monitor and evaluate the online presence and operations to maintain reasonable security standards. Notably, e-commerce is an industry with fewer entry barriers; therefore, policymakers should take a stance to maintain proper business operation practices.

The significant exploratory variables of the study can be considered as the factors leading to the determination of the security of an e-commerce platform. Even though security is an ongoing and never-ending concern as cyberspace is a lawn for vulnerabilities, e-commerce, which operates in this cyberspace, is turning into the must-have digital presence of any business entity. Therefore, e-commerce business owners should adhere to relevant policies and acts such as the Electronic Transactions Act 19 of 2006, Computer Crimes Act 24 of 2007, data protection policies and rules in the Information and Communication Act of 2003, Consumer Affairs Authority Act 9 of 2003, and intellectual property act 36 of 2003. Moreover, regular checks on e-commerce platform vulnerabilities should be considered. The relevant countermeasures and mitigation plans can be put forward to strengthen the backbone of e-commerce with the necessary security ingredients. Adhering to appropriate policies and making concerted efforts can increase the security of e-commerce platforms and can be beneficial in driving the digital ecosystem of businesses to reap sales outcomes, business growth, and customer loyalty in return.

Limitations and further research. The research primarily focuses on the factors affecting the security of e-commerce platforms from the customer's point of view in Sri Lanka. One limitation of the study is that the study did not consider the affecting security factors from the perspectives of the e-commerce vendors, platform owners, and security professionals. Therefore, this research area can study the perception of security from the e-commerce owners and vendors lateral and design security policies for e-commerce platforms with the collective input from security professionals. Additionally, the paper's limited generalisability outside Sri Lanka and the absence of a broader analysis should be acknowledged. Future work could extend this research to include comparative studies across similar regions and simulate these findings in natural e-commerce environments.

Data availability

The datasets generated during and analysed during the current study are not publicly available due to containing information that could compromise the privacy of research participants but are available from the corresponding author on reasonable request.

Received: 30 December 2023; Accepted: 12 August 2024;
Published online: 20 August 2024

References

Aitchison J, Silvey SD (1957) The generalization of probit analysis to the case of multiple responses. Biometrika 44(1/2):131–140. https://doi.org/10.2307/2333245

Akour I, Alnazzawi, N, Alshurideh, M, Almaiah, MA, Al Kurdi, B, Alfaisal, RM, et al. (2022) A conceptual model for investigating the effect of privacy concerns on E-commerce adoption: A Study on United Arab Emirates Consumers. Electronics, 11(22). https://doi.org/10.3390/electronics11223648

Albastaki T, Hamdan, A, Albastaki, Y, Bakir, A (2022) Factors Affecting E-payment acceptance by customers: An empirical study in the Kingdom of Bahrain. Compet Rev: Int Bus J, ahead-of-print(ahead-of-print). https://doi.org/10.1108/CR-09-2022-0133

Alharbi MI, Zyngier S, Hodkinson C (2013) Privacy By design and customers' perceived privacy and security concerns in the success of E-commerce. J Enterp Inf Manag 26(6):702–718. https://doi.org/10.1108/JEIM-07-2013-0039

Alqahtani M, Albahar M (2022) The impact of security and payment method on consumers' perception of marketplace in Saudi Arabia. Int J Adv Comput Sci Appl 13(5):81–88. https://doi.org/10.14569/IJACSA.2022.0130511

Alshehri H, Meziane, F (2017) The Influence of Advanced and Secure E-Commerce Environments on Customers Behaviour: The Case of Saudis in the UK. 12th International Conference for Internet Technology and Secured Transactions (ICITST): 332-337. https://doi.org/10.23919/ICITST.2017.8356411

Amsl S, Watson, I, Teller, C, Wood, S (2023) Presenting Products on Websites – The Importance of Information Quality Criteria for Online Shoppers. International Journal of Retail & Distribution Management, ahead-of-print(ahead-of-print). https://doi.org/10.1108/IJRDM-04-2023-0266

Baluch A (2023). 38 E-Commerce Statistics Of 2023. https://www.forbes.com/advisor/business/ecommerce-statistics/. Accessed 5 2023

Bandara R, Fernando M, Akter S (2021) Managing consumer privacy concerns and defensive behaviours in the digital marketplace. Eur J Mark 55(1):219–246. https://doi.org/10.1108/EJM-06-2019-0515

Behani N (2019) E-commerce Security Infographics- Statistic, Issues, and Solutions for 2022

Belanger F, Hiller JS, Smith WJ (2002) Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. J Strateg Inf Syst 11(3):245–270. https://doi.org/10.1016/S0963-8687(02)00018-5

Choi H, Park J, Jung Y (2018) The role of privacy fatigue in online privacy behavior. Comput Hum Behav 81:42–51. https://doi.org/10.1016/j.chb.2017.12.001

Daily News (2024) E-commerce usage to increase to 5% from current 2% by 2025. Available at: https://www.dailynews.lk/2023/10/27/business/192542/e-commerce-usage-to-increase-to-5-from-current-2-by-2025/

Dang VT, Pham TL (2018) An empirical investigation of consumer perceptions of online shopping in an emerging economy. Asia Pac J Mark Logist 30(4):952–971. https://doi.org/10.1108/APJML-01-2018-0038

eCommerceDB (2022). eCommerce market in Sri Lanka. https://ecommercedb.com/markets/lk/all. Accessed 2023-03-12 2023

El Haddad G, Aïmeur, E, Hage, H (2018). Understanding Trust, Privacy and Financial Fears in Online Payment. 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE): 28-36. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00015

Girsang MJ, Candiwan, Hendayani, R, Ganesan, Y (2020). Can Information Security, Privacy and Satisfaction Influence The E-Commerce Consumer Trust? 2020 8th International Conference on Information and Communication Technology (ICoICT): 1-7. https://doi.org/10.1109/ICoICT49345.2020.9166247

Gull H, Saeed S, Iqbal SZ, Bamarouf YA, Alqahtani MA, Alabbad DA et al. (2022) An empirical study of mobile commerce and customers security perception in Saudi Arabia. Electronics 11(3):293

Gurung A, Raja MK (2016) Online privacy and security concerns of consumers. Inf Comput Secur 24(4):348–371. https://doi.org/10.1108/ICS-05-2015-0020

Herrada-Lores S, Iniesta-Bonillo MÃ, Estrella-Ramón A (2022) Weaknesses and strengths of online marketing websites. Span J Mark - ESIC 26(2):189–209. https://doi.org/10.1108/SJME-11-2021-0219

Hong W, Thong JYL (2013) Internet privacy concerns: an integrated conceptualization and four empirical studies. MIS Q 37(1):275–298

International Trade Administration (2024a). Country Commercial Guides. https://www.trade.gov/country-commercial-guides. Accessed June 15 2024

International Trade Administration (2024b). Sri Lanka - Country Commercial Guide: eCommerce. https://www.trade.gov/country-commercial-guides/sri-lanka-ecommerce. Accessed June 13 2024

Kepios (2024). Digital 2024: Sri Lanka. https://datareportal.com/reports/digital-2024-sri-lanka. Accessed June 20 2024

Khan F, Ateeq S, Ali M, Butt N (2023) Impact of COVID-19 on the drivers of cash-based online transactions and consumer behaviour: evidence from a Muslim market. J Islam Mark 14(3):714–734. https://doi.org/10.1108/JIMA-09-2020-0265

Krejcie RV, Morgan DW (1970) Determining Sample Size for Research Activities. Educ Psychol Meas 30(3):607–610. https://doi.org/10.1177/001316447003000308

Kumar K, Gupta, H (2021) Designing a Security Framework for Enhancement of Electronic Transactions. 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO): 1-5. https://doi.org/10.1109/ICRITO51393.2021.9596545

Kuruwitaarachchi N, Abeygunawardena PKW, Rupasinghe P, Udara I (2019) A systematic review of security in electronic commerce- threats and frameworks. Glob J Comput Sci Technol 19(1):33–39. https://doi.org/10.34257/GJCSTEVOL19IS1PG33

Labs RI Freewordcloudgenerator. https://www.freewordcloudgenerator.com/

Muniraju Y, Hariprasad S (2019) Digital payment: rural web users' perception during online shopping. Int J Soc Econ Res 9(3):147–155

Pramanik R, Prabhu, S (2022) Analysing Cyber Security and Data Privacy Models for Decision Making Among Indian Consumers in an E-Commerce Environment. 2022 International Conference on Decision Aid Sciences and Applications (DASA): 735–739. https://doi.org/10.1109/DASA54658.2022.9765113

PurpleSec (2021) Cyber Security Statistics: The Ultimate List Of Stats Data, & Trends For 2023. https://purplesec.us/resources/cyber-security-statistics/#Cybercrime. Accessed 02-03-2023 2023

Roy V, Vijay TS, Srivastava A (2022) The distinctive agenda of service failure recovery in E-Tailing: Criticality of logistical/non-logistical service failure typologies and E-tailing ethics. J Retail Consum Serv 64:102837. https://doi.org/10.1016/j.jretconser.2021.102837

Saeed S (2023) A customer-centric view of E-commerce security and privacy. Appl Sci 13(2):1020

Singh J (2014) Review of E-commerce security challenges. Int J Innov Res Comput Commun Eng 2:2850–2858

Statista (2022) eCommerce - Sri Lanka. https://www.statista.com/outlook/dmo/ecommerce/sri-lanka. Accessed 2023-03-12 2023

Tan CW, Benbasat I, Cenfetelli R (2016) An exploratory study of the formation and impact of electronic service failures. MIS Q 40:1–29. https://doi.org/10.25300/MISQ/2016/40.1.01

The Asia Pacific Institute of Digital Marketing, Department of Marketing Management (2024). Digital Outlook Sri Lanka 2024. Colombo

Weerasena A, Jayathilaka R (2023) Is the best option still in low adoption? An investigation on factors affecting the adoption of online school education in rural areas in Sri Lanka. Educ Technol Res Dev 71(3):1371–1390. https://doi.org/10.1007/s11423-023-10201-8

Author contributions

I.U.: writing original draft, conceptualization, formal analysis, investigation, data analysis, methodology and writing (review/editing). R.J.: conceptualization, formal analysis, methodology, supervision, validation, writing (review/editing).

Competing interests

The authors declare no competing interests.

Ethical approval

This study was approved by the Sri Lanka Institute of Information Technology, Sri Lanka (RE/MBA/2023/10).

Informed consent

Each individual in this study gave written consent prior to the feedback survey. All consent process was documented. Participants did not receive any incentive for participation. Participant names and any other identifying information were removed from the written transcripts.

Additional information

Supplementary information The online version contains supplementary material available at https://doi.org/10.1057/s41599-024-03585-2.

Correspondence and requests for materials should be addressed to Ruwan Jayathilaka.

Reprints and permission information is available at http://www.nature.com/reprints

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Open Access This article is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License, which permits any non-commercial use, sharing, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if you modified the licensed material. You do not have permission under this licence to share adapted material derived from this article or parts of it. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by-nc-nd/4.0/.

© The Author(s) 2024