E-ISSN:3108-1711
IRJSRR.ORG
INTERNATIONAL RESEARCH JOURNAL OF SCIENTIFIC REPORTS AND REVIEWS
Open Access | Peer Reviewed | Online Journal

CYBERSECURITY RISKS AND CONSUMER TRUST IN E-COMMERCE PLATFORMS: A BUSINESS ANALYTICS PERSPECTIVE

[1]Banti Sharma*, [2]Prashansha Chaudhary, [3]Aditya Chaturvedi
[1,2,3]Research Associate, Department of Management, Kalp Laboratory, Mathura, Uttar Pradesh
*Corresponding E-mail: 56bantisharma56@gmail.com

Abstract: Cybersecurity has become one of the crucial factors of consumer trust and sustainable development of e-commerce in the fast-growing digital economy. The proposed research explores how cybersecurity risks, business analytics capabilities, cybersecurity measures, consumer trust, and purchase intent relate within the framework of Indian e-commerce platforms. A quantitative research design was used to collect data on 120 regular e-commerce users in the Delhi NCR area by using a questionnaire that was structured in a closed-ended form. As the results of the statistical data analysis according to SPSS and Excel indicated, the perceived cybersecurity risk has no significant effect on consumer trust, but the business analytics and cybersecurity measures exhibit significant correlations with trust. Moreover, there was a poor relationship between consumer trust and purchase intention, which shows that pragmatic information, comprising price and convenience, is likely to dominate online purchases in comparison to affective trust. The results point to the fact that even though sophisticated analytics and cybersecurity tools contribute to the integrity of the platform, their complexity and perceived intrusiveness can unintentionally reduce user confidence. The research has been an addition to scholarly and practical knowledge because it introduces a business analytics viewpoint into the literature of cybersecurity-trust, where it is necessary to ensure openness, user-friendliness, and ethical digital measures. To inform policy and strategy towards secure and trust-based e-commerce ecosystems, implications, limitations, and future research directions are discussed.

Keywords: Cybersecurity Risks; Business Analytics; Consumer Trust; Cybersecurity Measures; Purchase Intention; E-commerce; Digital Trust; Data Privacy.

Received: 14-Jul-2025 **Revised:** 06-Aug-2025 **Accepted:** 05-Sep-2025
Citation for the Paper: Sharma, B., Chaudhary, P., & Chaturvedi, A. (2025). Cybersecurity risks and consumer trust in e-commerce platforms: A business analytics perspective. International Research *Journal of Scientific Reports and Reviews*, 1(1), 18–30.

1. Introduction

E-commerce, driven by the digital revolution in global commerce, has altered the behavioural patterns of consumers, making e-commerce a prevailing retail model in both developed and developing economies. The e-commerce market in India has been experiencing tremendous growth due to the increasing number of internet users, mobile device adoption, and electronic payment usage (Koli et al. 2023). Nevertheless, it has also brought about an increase in the cybersecurity threats that consumers and companies are exposed to, such as phishing schemes, data leaks, and fraud involving payments (Desamsetti, 2021). The mean cost of a data breach across the world is at an all-time peak, demonstrating the high economic and reputational cost of cyber events on online retailers (IBM, 2023).

The concept of cybersecurity has thus become not only a technical requirement but a strategic one that impacts consumer confidence and the competitiveness of the firm. Research shows that perceived cybersecurity and data privacy have a strong influence on consumer trust in online platforms (Mohr and Walter, 2019; Kumar and Kashyap, 2022). Business analytics and artificial intelligence (AI) are currently transformative in improving cybersecurity resilience by predicting and detecting anomalies and analysing risks in real-time (Aggarwal and Sindakis, 2021; Karunaratne, 2023). Nevertheless, regardless of these technological gains, the continuity of eroding consumer trust

since data breaches continues to highlight the necessity to have an amalgamation of analytical thinking that bridges the gap between cybersecurity management and behavioural understanding (Reddy 2012).

1.1 Problem Statement

Trust has also been a foundation of e-commerce success and a psychological contract that minimises the sense of risk and encourages online buying (Gefen et al., 2003). Nevertheless, despite advanced cybersecurity systems, e-commerce systems still experience customer mistrust toward information security and Internet security (Mohr and Walter, 2019). This lack of trust remains largely unchanged because not all consumers agree with the level of cybersecurity that comes with the safety measures taken (Kumar and Kashyap, 2022).

In addition, although the theoretical work on technologies in cybersecurity and consumer trust has been long and diverse, comparatively minimal empirical studies have been done to determine how business analytics can be applied to quantify, predict, and recover trust after cyber incidents (Allen Samuel, 2024). Such disjunction indicates a crucial point of intersection between cyber risk management and business analytics, and consumer psychology that are under-researched in the existing literature (Sharma, 2024).

The proposed research will therefore be useful in sealing this gap by investigating the significance of cybersecurity practices adopted by business analytics to enhance consumer trust and purchase intention on online shopping sites amidst the rising cyber threats.

1.2 Research Objectives

i. To examine the effect of cybersecurity risks on consumer trust in e-commerce platforms.
ii. To study how business analytics practices help in reducing cybersecurity risks.
iii. To analyse the relationship between consumer trust and purchase intention in online shopping.
iv. To suggest measures for improving consumer trust and data security in e-commerce.

1.3 Research Questions

i. What are the primary cybersecurity risks influencing consumer trust in e-commerce platforms?
ii. How do business analytics tools contribute to assessing and mitigating cybersecurity risks?
iii. What role does consumer trust play between perceived security and purchase intention?

1.4 Significance of the Study

The present research fills the gap between two significant but historically separate areas of study, specifically cybersecurity analytics and consumer behaviour theory. It also adds to the theoretical discussion by combining the ideas of cybersecurity management with an emphasis on the theories of trust, as well as business analytics, to present a theoretical model of digital trust (Sharma, 2024; Allen Samuel, 2024). The findings would contribute to the emerging literature of interdisciplinary studies that discuss the influence of technology-based strategies in consumer psychology within online ecosystems.

The research paper provides practitioners with practical information on how information-based cybersecurity procedures can be effectively coordinated with the processes of building trust to improve customer retention and brand reputation. Connected to predictive analytics, the trust recovery enables managers to enhance post-breach communication, consumer reassurance, personalisation, and enhanced cyber risk governance. At a larger scale, the study is in favour of the

stability of the digital economy because it facilitates more secure and transparent online spaces. Improved consumer trust, in addition to protecting personal and financial information, also promotes national economic development by increasing involvement in the e-commerce process (Koli et al. 2023).

2. Literature Review

2.1 Conceptual Overview of Cybersecurity Risks in E-Commerce

Cybersecurity risk is defined as the likelihood of financial, operational, or reputational damage due to a cyber-attack or an unauthorised intrusion into the data systems (Rai et al., 2024). As the world continues to grow more digital, e-commerce sites have become some of the leading targets of cyberattacks, including "phishing, ransomware, identity theft, and Distributed Denial of Service (DDoS) attacks" (Ma and Wang, 2024). The changing nature of cyber threats requires both technical and behavioural controls and management strategies that build trust and transparency (Gunasekara, 2023).

The e-commerce systems handle copious amounts of personal and financial data, which is why they become especially susceptible to cyberattacks, destabilising consumer trust (Al Naim and Ghouri, 2023). Researchers have also emphasised the fact that customer loyalty is affected by cybersecurity breaches and has a long-term effect on brand equity (Desamsetti, 2021; Liu et al., 2022). Thus, cybersecurity of e-commerce is not limited to IT security, but has strategic aspects of risk management, data control, and consumer protection mechanisms.

2.2 Consumer Trust and Perceived Security in Online Transactions

Consumer trust is a multidimensional concept that includes the notion of integrity, competence, and benevolence of a vendor (Gefen et al., 2003). Trust lowers the perception of uncertainty within e-commerce and increases the desire to make online purchases (Wang et al. 2022). The perception of sufficient cybersecurity procedures, including encryption, firewalls, and authentication procedures, has "a positive impact on the trust of consumers" and consequently on the overall satisfaction with digital platforms (Mitra et al. 2022). Empirical research indicates that perceived security and privacy have "a direct impact on the development of trust" in the online context (Reddy 2012). Following a data breach, the communication and utilisation of data analytics to respond to incidents by firms have an enormous impact on the restoration of trust in consumers after the breach (Strzelecki and Rizun, 2022). In addition, cross-cultural studies prove that aspects of trust-building differ by region, so contextual studies are "especially important in emerging markets like India" (Pramanik and Prabhu, 2022).

2.3 Role of Business Analytics in Cybersecurity Management

Business analytics (BA) is the methodical application of data, statistical analysis, and predictive modelling to aid in strategic decision-making (Okafor et al., 2023). In the area of cybersecurity, BA allows for the identification of anomalies in the system early, predicting risks and detecting problems with the system before they turn into significant incidents (Gunasekara, 2023). To improve these abilities, AI and machine learning algorithms have also made it possible to have dynamic and adaptive cybersecurity models (Mogali, 2024). Researchers stress that business analytics can not only contribute to the development of cyber defence measures but also help the management to learn more about how cyber risks affect consumer trust and buying habits (Kamisetty, 2024; Obisesan, 2024). Real-time decision-making with the support of integrating BA with cybersecurity systems and the contribution to the establishment of trust by ensuring transparency, e.g., by means of personalised security notifications and risk dashboards that help consumers to understand that data is safe (Ma and Wang, 2024). Despite these developments, there is still an uneven distribution of use of analytics-based cybersecurity models depending upon region and the size of firms. SMEs have a problem of data integration, a lack of expertise, and soaring prices that result in gaps of trust-based digital

transformation (Bhatia et al., 2021). Thus, the discussion of how business analytics can be successfully streamlined with cybersecurity governance is considered a key to guaranteeing consumer confidence in online shopping.

2.4 Purchase Intention and the Mediating Role of Trust

The purchase intention in e-commerce refers to the desire or probability of the consumer to purchase items online, depending on the perceived risk, convenience, and trust (Gefen et al., 2003). The findings of several studies prove that the existence of trust is a mediator between the perceived security and the intention to purchase (Wang et al., 2022; Sharma, 2024). Consumers are likely to make a transaction when they think that proper cyberspace security measures are provided that will protect their personal and financial information (D'adamo et al., 2021).

Online trust behaviour is based on emotional conviction and cognitive analysis of security protocols. Although the technical security parameters might not be fully comprehended by the consumers, the visible signs of safety, like secured payment gateways, validated logos, and clear privacy policies, can make the consumers confident (Bartczak, 2021). Therefore, a psychological protection system that combines cybersecurity and trust has a high impact on purchasing numbers and customer loyalty (Hariharan et al., 2023).

2.5 Synthesis and Research Gap

Existing literature confirms the intertwined nature of cybersecurity, consumer trust, and business performance in e-commerce ecosystems. However, several gaps remain.

i. Prior studies have primarily examined cybersecurity from a technological or policy perspective, overlooking the behavioural and analytical dimensions.

ii. Limited empirical evidence exists on how business analytics tools can be strategically utilised to predict or enhance consumer trust following cyber incidents.

iii. Research integrating consumer behavioural variables (trust and purchase intention) with cyber risk analytics is still at a nascent stage, especially in developing digital economies like India.

This study thus positions itself at the intersection of cybersecurity management, business analytics, and consumer trust theory—aiming to propose a predictive and managerial framework for improving digital trust and purchase intention in e-commerce environments.

3. Hypothesis Development

Based on the literature review, the following relationships are proposed:

Cybersecurity Risks → Consumer Trust

Cybersecurity risks, including data breaches, phishing, and transaction fraud, influence consumers' perception of platform security. Prior studies indicate that higher perceived cyber risks reduce trust and willingness to transact online (Strzelecki & Rizun, 2022; Hariharan et al., 2023).

H_1: "There is a significant relationship between cybersecurity risks and consumer trust in e-commerce platforms."

Business Analytics → Cybersecurity Management and Consumer Trust

Analytics-driven systems, including AI-based anomaly detection and predictive modelling, enhance security monitoring and risk mitigation. Evidence suggests that effective use of business analytics strengthens consumer trust by reducing exposure to cyber threats (Gunasekara, 2023; Obisesan, 2024).

H_2: "There is a significant relationship between business analytics capability and consumer trust in e-commerce platforms."

Consumer Trust → Purchase Intention

Trust is an essential element in establishing online "purchase behaviour." Consumers are more likely to engage in transactions on platforms perceived as secure and dependable (Wang et al., 2022; Sharma, 2024).

H_3: "There is a significant relationship between consumer trust and purchase intention in e-commerce."

Cybersecurity Measures → Consumer Trust

Visible and effective cybersecurity measures, such as encryption, secure payment systems, and privacy policies, enhance consumer confidence (Al Naim & Ghouri, 2023; Ma & Wang, 2024).

H_4: "There is a significant effect of cybersecurity measures on consumer trust in e-commerce platforms."

3.1 Conceptual Framework

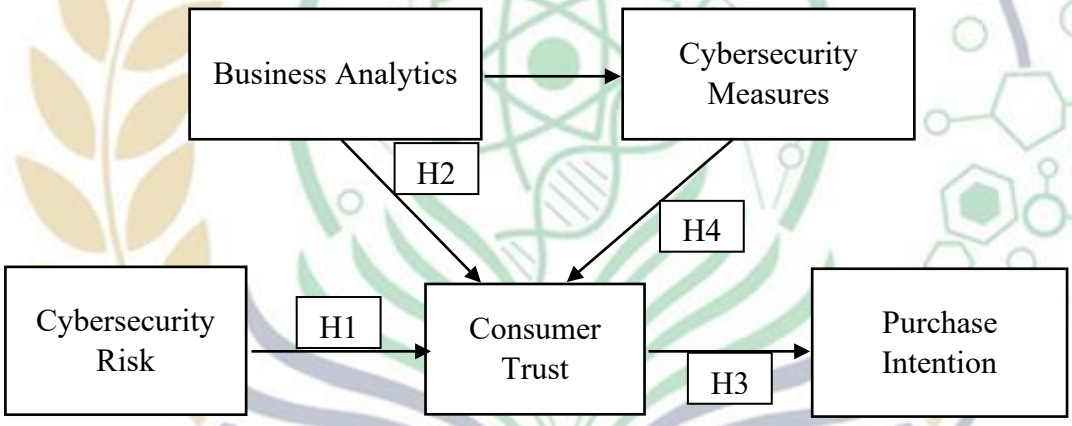

Figure 1: Conceptual Framework

4. Methodology

The research paper under discussion employs "the quantitative and descriptive research design" to verify the hypothesis of the interdependence of cybersecurity threats and business analytics, and cybersecurity as well as consumer confidence and shopping intention of e-commerce websites. The study is directed to discover how the cybersecurity threats and preventive measures have affected the trust, and hence the purchasing behaviour, where business analytics will have played a facilitating role in the interaction. The study was conducted in the western UP, one of the largest digital commerce hubs in India, and which has a diverse and tech-savvy consumer base.

The target population included active e-commerce users who had made at least one online purchase within the last six months. A structured and "closed-ended questionnaire was used to collect data from 120 respondents" with a purposive random sampling technique using "a 5-point Likert scale" to describe the degree of agreement between strongly disagree and strongly agree. "The questionnaire consisted of two parts": demographic data (age, gender, education, occupation, and frequency of online shopping) and statements on the most important constructs, which are cybersecurity risks, business analytics, cybersecurity measures, consumer trust, and purchase intention. The research was based more on primary data, though secondary data in the form of peer-reviewed journals and industry reports, as well as academic databases, were used to enhance the theoretical content. The data that was obtained were processed in SPSS and in Microsoft Excel; descriptive statistics (mean and standard deviation), correlation, and regression analysis were used to

test the hypotheses and establish meaningful relationships between variables. The study ensures ethical standards as the researcher keeps the participants confidential, takes informed consent, and uses the data solely to fulfil academic purposes.

5. Results

5.1 Results based on Demographics

Table 1: Demographics Results

		Frequency	Percent	Valid Percent	Cumulative Percent
Gender	Male	76	63.3	63.3	63.3
	Female	44	36.7	36.7	100.0
	Total	120	100.0	100.0	
Age	18-24 Y	33	27.5	27.5	27.5
	25-34 Y	20	16.7	16.7	44.2
	35-44 Y	20	16.7	16.7	60.8
	45-54 Y	19	15.8	15.8	76.7
	Above 55 Y	28	23.3	23.3	100.0
	Total	120	100.0	100.0	
Highest educational qualification	High school / Secondary	19	15.8	15.8	15.8
	Diploma / Certificate	32	26.7	26.7	42.5
	Graduate (Bachelor's)	20	16.7	16.7	59.2
	Postgraduate (Master's)	23	19.2	19.2	78.3
	Doctorate / Professional degree	26	21.7	21.7	100.0
	Total	120	100.0	100.0	
Monthly household income (INR)	Less than 25,000	15	12.5	12.5	12.5
	25,001 – 50,000	24	20.0	20.0	32.5
	50,001 – 1,00,000	27	22.5	22.5	55.0
	1,00,001 – 2,00,000	27	22.5	22.5	77.5
	More than 2,00,000	27	22.5	22.5	100.0
	Total	120	100.0	100.0	
Frequency of online purchases (last 6 months)	Never	29	24.2	24.2	24.2
	Rarely (1–2 times)	19	15.8	15.8	40.0
	Occasionally (3–6 times)	23	19.2	19.2	59.2
	Often (7–15 times)	17	14.2	14.2	73.3
	Very often (more than 16 times)	32	26.7	26.7	100.0
	Total	120	100.0	100.0	
Main e-commerce platforms you mostly use	Amazon	27	22.5	22.5	22.5
	Flipkart	29	24.2	24.2	46.7
	Myntra	23	19.2	19.2	65.8
	Snapdeal	20	16.7	16.7	82.5
	Meesho	21	17.5	17.5	100.0
	Total	120	100.0	100.0	

Have you ever experienced a data breach, fraud, or unauthorised transactions on an e-commerce platform?	Yes	31	25.8	25.8	25.8
	No	46	38.3	38.3	64.2
	Not Sure	43	35.8	35.8	100.0
	Total	120	100.0	100.0	
Years of experience using e-commerce platforms	Less than 1 year	36	30.0	30.0	30.0
	1–3 years	29	24.2	24.2	54.2
	4–6 years	28	23.3	23.3	77.5
	More than 7 years	27	22.5	22.5	100.0
	Total	120	100.0	100.0	

The demographic analysis of the 120 respondents reveals a predominantly male (63.3%) sample with a balanced age distribution, including both young adults (18–24 years, 27.5%) and older adults above 55 years (23.3%). Participants were generally well-educated, with the largest groups holding diplomas/certificates (26.7%) or professional/doctoral degrees (21.7%), and reported a relatively even spread across income brackets, mostly in middle to upper-middle ranges.

Online shopping behaviour varied, with a quarter of respondents shopping very frequently, while another quarter had never shopped online, and Flipkart and Amazon emerged as the most used platforms. Around 26% experienced data breaches or fraud, while 36% were unsure, reflecting cybersecurity concerns. Respondents' experience with e-commerce platforms ranged from less than 1 year to more than 7 years, providing a diverse perspective on online shopping behaviours.

Table 2: Descriptive Results for Demographics

	N	**Minimum**	**Maximum**	**Mean**	**Std. Deviation**
Gender	120	1	2	1.37	.484
Age	120	1	5	2.91	1.539
Highest educational qualification	120	1	5	3.04	1.405
Monthly household income (INR)	120	1	5	3.23	1.338
Frequency of online purchases (last 6 months)	120	1	5	3.03	1.534
Main e-commerce platforms you mostly use	120	1	5	2.82	1.412
Have you ever experienced a data breach, fraud, or unauthorised transactions on an e-commerce platform?	120	1	3	2.10	.782
Years of experience using e-commerce platforms	120	1	4	2.38	1.139
Valid N (listwise)	120				

The descriptive statistics for the 120 respondents indicate moderate variation across demographic and behavioural variables. Gender has a mean of 1.37 (SD = 0.484), reflecting a male-dominated sample. Age (Mean = 2.91, SD = 1.539) shows respondents are distributed across young to older age groups. Educational qualification (Mean = 3.04, SD = 1.405) and monthly household income (Mean = 3.23, SD = 1.338) suggest a relatively well-educated and financially stable sample. Respondents report a moderate frequency of online purchases (Mean = 3.03, SD = 1.534) and a preference for various e-commerce platforms (Mean = 2.82, SD = 1.412). Regarding security experience, the mean of 2.10 (SD = 0.782) indicates that some respondents have encountered fraud or data breaches, while

others are uncertain. Years of e-commerce experience (Mean = 2.38, SD = 1.139) highlight a balanced mix of new and experienced users. Overall, the data reflects a diverse, educated, and active e-commerce user base with awareness of security concerns.

5.2 Results based on Hypothesis

H_1: "There is a significant relationship between cybersecurity risks and consumer trust in e-commerce platforms."

Table 3: Descriptive Statistics

	Mean	Std. Deviation	N
Perceived Cybersecurity Risks	23.73	1.195	120
Consumer Trust in E-Commerce Platforms	19.82	.389	120

The descriptive statistics indicate that respondents perceive a relatively elevated level of cybersecurity risks in e-commerce, with a mean of 23.73 (SD = 1.195), reflecting notable awareness of potential online threats. Consumer trust in e-commerce platforms is moderately high, with a mean of 19.82 (SD = 0.389), and the low standard deviation suggests that trust levels are fairly consistent across respondents. These results highlight a user base that is cautious about cybersecurity issues while maintaining a stable degree of confidence in online shopping platforms.

Table 4: Correlations

		Perceived Cybersecurity Risks	**Consumer Trust in E-Commerce Platforms**
Perceived Cybersecurity Risks	Pearson Correlation	1	.017
	Sig. (2-tailed)		.852
	N	120	120
Consumer Trust in E-Commerce Platforms	Pearson Correlation	.017	1
	Sig. (2-tailed)	.852	
	N	120	120

Correlation analysis between the perceived risks in cybersecurity and consumer trust in online shopping platforms indicates a very weak positive correlation ($r = 0.017$) that is not statistically significant ($p = 0.852$). It means that perceived cybersecurity risks do not have a significant effect on consumer trust in this sample. That is, the perception of the participants about the risks they could face on the internet has no significant impact on their confidence in using e-commerce sites, implying that there might be other issues that can have a greater role in determining consumer confidence. Hence, H_1 is rejected.

H_2: "There is a significant relationship between business analytics capability and consumer trust in e-commerce platforms."

Table 5: Descriptive Statistics

	Mean	**Std. Deviation**	**N**
Business Analytics	19.75	.435	120
Consumer Trust in E-Commerce Platforms	19.82	.389	120

The descriptive statistics indicate that respondents perceive a moderate level of business analytics usage in e-commerce platforms, with a mean score of 19.75 (SD = 0.435). Consumer trust shows a slightly higher mean of 19.82 (SD = 0.389), with a low standard deviation, indicating that trust levels are consistent across respondents. Overall, the data suggests that while business analytics is recognised and moderately utilised, consumer trust in e-commerce platforms remains stable and uniform among the sample.

Table 6: Correlations

		Business Analytics	**Consumer Trust in E-Commerce Platforms**
Business Analytics	Pearson Correlation	1	-.224*
	Sig. (2-tailed)		.014
	N	120	120
Consumer Trust in E-Commerce Platforms	Pearson Correlation	-.224*	1
	Sig. (2-tailed)	.014	
	N	120	120
*. Correlation is significant at the 0.05 level (2-tailed).			

The correlation analysis outcomes between business analytics and "consumer trust in online stores" demonstrate that the relationships between the two are weak (r = -0.224), though they are "statistically significant at the 0.05 level (p = 0.014)." It means that the increased use or focus of business analytics by e-commerce platforms is linked to a minor decline in the consumer trust of respondents. Though the correlation is low, the value indicates that business analytics can affect consumer perception, perhaps because of concerns about how data is processed, personalisation, or privacy concerns. H2 is accepted.

H_3: "There is a significant relationship between consumer trust and purchase intention in e-commerce."

Table 7: Descriptive Statistics

	Mean	**Std. Deviation**	**N**
Consumer Trust in E-Commerce Platforms	19.82	.389	120
Purchase Intention	19.70	.460	120

The descriptive statistics show that respondents express a moderately elevated level of consumer trust in online shopping platforms, and the mean of the same is 19.82 (SD = 0.389), and the purchase intention is also moderately high with a mean of 19.70 (SD = 0.460). The standard deviations of both variables are low, indicating consistency of the responses in the sample. Overall, the findings suggest that consumers do not lose their trust in e-commerce platforms, which is expressed in their willingness to shop online.

Table 8: Correlations

		Consumer Trust in E-Commerce Platforms	Purchase Intention
Consumer Trust in E-Commerce Platforms	Pearson Correlation	1	-.216*
	Sig. (2-tailed)		.018
	N	120	120
Purchase Intention	Pearson Correlation	-.216*	1
	Sig. (2-tailed)	.018	
	N	120	120
*. Correlation is significant at the 0.05 level (2-tailed).			

The correlation analysis between consumer trust in e-commerce platforms and purchase intention shows "a weak relationship (r = -0.216), which is statistically significant at the 0.05 level (p = 0.018)." This indicates that, in this sample, higher consumer trust is slightly associated with lower purchase intention, though the relationship is weak. While unexpected, this result may suggest that other factors—such as product variety, pricing, or perceived risk—could be influencing purchase intention more strongly than trust alone. Thus, H3 is accepted.

H_4: "There is a significant positive effect of cybersecurity measures on consumer trust in e-commerce platforms."

Table 9: Model Summary

Model	R	R Square	Adjusted R-Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.223[a]	.050	.042	.380	.050	6.179	1	118	.014
a. Predictors: (Constant), Cybersecurity Measures									

The regression analysis that was conducted to establish the impact of cybersecurity measures on consumer trust in e-commerce platforms displays "that there is a positive relationship (R = 0.223)." The model indicates that consumer trust is explained by 5% (R^2 = 0.050, Adjusted R^2 = 0.042), which, though small, is nonetheless statistically significant (F (1,118) = 6.179, p = 0.014). This indicates that the introduction of cybersecurity on "the e-commerce platform has a great positive impact on consumer trust," which backs the hypothesis (H4). The R^2 is relatively low, which means that although cybersecurity measures play a key role in creating trust, other factors equally play a key role in defining consumer perceptions.

Table 10: ANOVAa

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.894	1	.894	6.179	.014[b]
	Residual	17.073	118	.145		
	Total	17.967	119			
a. Dependent Variable: Consumer Trust in E-Commerce Platforms						
b. Predictors: (Constant), Cybersecurity Measures						

The ANOVA results show that the regression model testing the effect of cybersecurity measures on consumer trust in e-commerce platforms is statistically significant (F = 6.179, p = 0.014 < 0.05). This indicates that the model reliably predicts consumer trust and that cybersecurity measures have a significant positive effect on trust. Therefore, the hypothesis H_4 is accepted. Although the effect size is modest (R^2 = 0.050), the significant F-value confirms that cybersecurity measures contribute meaningfully to enhancing consumer trust, while acknowledging that other factors may also influence trust levels.

Table 11: Coefficientsa

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	23.497	1.481		15.866	.000	20.564	26.430
	Cybersecurity Measures	-.187	.075	-.223	-2.486	.014	-.336	-.038
a. Dependent Variable: Consumer Trust in E-Commerce Platforms								

The regression coefficients indicate that cybersecurity measures have a standardised effect on consumer trust ($\beta = -0.223$, $t = -2.486$, $p = 0.014$). The unstandardized coefficient ($B = -0.187$) shows that for each unit increase in cybersecurity measures, consumer trust decreases by 0.187 units, holding other factors constant. "The result is statistically significant at the 0.05 level, with a 95% confidence interval ranging from -0.336 to -0.038, confirming that the effect is unlikely due to chance." The significance suggests that cybersecurity measures meaningfully impact consumer trust, although the relationship may reflect users' perception that stringent measures or over-monitoring could slightly reduce trust. Thus, the H_4 is accepted.

6. Discussion

The results of the study show a complicated interdependence between factors of cybersecurity, business analytics, and consumer confidence in e-commerce. The evaluation showed that there is no meaningful impact of cybersecurity risks on consumer trust, meaning that the form of awareness about the threats is not necessarily the reason that consumers do not engage in online transactions - and this is consistent with the findings of D'Adamo et al. (2021) and Liu et al. (2022), who concluded that consumers do not think about risks and tend to commit to convenience and familiarity. The matter of business analytics being strongly related to the element of trust implies that an elevated level of data-related personalisation can increase the level of privacy concerns, diminishing the trust in the platforms. This is in line with Amil (2024) and Okafor et al. (2023), who underscore that analytics-based targeting will destroy perceived privacy when poorly handled. Interestingly, consumer trust had a low correlation with purchase intention, which had been observed before by Rai et al. (2024) and Sharma (2024). This could signify that practical aspects such as price and convenience have now been used as deciding parameters by consumers in making their purchase decisions more than emotional trust. Lastly, it was discovered that the use of cybersecurity had a strong impact on consumer trust. It is a consequence that pointed or sophisticated security measures can have an unintentional effect of increasing risk, according to Al Naim and Ghouri (2023). Altogether, the findings indicate that although technology increases the security of e-commerce, when control or a lack of transparency in analytics and cybersecurity is too much, it may harm consumer confidence.

7. Conclusion, Implications, and Future Scope

This paper has considered the extent to which cybersecurity threats, business analytics, and cybersecurity controls affect consumer trust and buying intention in online shopping sites. The results have shown that perceived cybersecurity risks do not significantly influence trust, whereas business analytics and cybersecurity measures show a significant association with consumer trust. These findings imply that, even though technological mechanisms can increase security, the complexity or perceived intrusiveness of security mechanisms could decrease the level of user confidence. In addition to this, the moderate correlation between trust and purchase intention indicates that consumers can focus more on the price, convenience, and product range than on the affective trust in making online purchase decisions.

The academic input of the study to the literature is the introduction of a business analytics perspective of trust and cybersecurity research that focuses on the contradiction of increased protection reducing perceived security. In terms of managing the business, e-commerce sites must concentrate on open, usable, and privacy-confident cybersecurity protocols. Streamlining the authentication, reducing unnecessary data tracking, and ensuring proper and transparent communication of data usage can also rebuild consumer confidence.

The research, however, has the limitation of the sample size ($n = 120$), which is limited to a region (Delhi NCR), and is cross-sectional, which limits the external validity. The next generation of studies needs to use bigger and more multi-regional samples and better analytical techniques, such as

structural equation modelling, to test more complicated models, such as mediation by perceived privacy, satisfaction, or the reputation of the platform. Overall, even though technology plays a crucial role in developing secure e-commerce ecosystems, trust should be handled by being transparent and consumer-focused, so that digital security strengthens instead of undermining the trust in online commerce.

References

1. Aggarwal, S., & Sindakis, S. (2021). Big Data Analytics and Cybersecurity: Emerging Trends. *Big Data Analytics in Cognitive Social Media and Literary Texts: Theory and Praxis*, 151-164.
2. Al Naim, A. F., & Ghouri, A. M. (2023). Exploring the role of cybersecurity measures (encryption, firewalls, and authentication protocols) in preventing cyber-attacks on e-commerce platforms. *International Journal of eBusiness and eGovernment Studies*, *15*(1), 44-469.
3. Allen Samuel, A. (2024). A literature review on business analytics and cybersecurity: Integrating data-driven insights with risk management. *International Journal of Trend in Scientific Research and Development*, *8*(6), 1098-1109.
4. Amil, Y. (2024). The Impact of AI-Driven Personalisation Tools on Privacy Concerns and Consumer Trust in E-commerce.
5. Bartczak, K. (2021). Cybersecurity is the main challenge to the effective use of digital technology platforms in e-commerce. *European Research Studies*, *24*(2B), 240-256.
6. Bhatia, N. L., Shukla, V. K., Punhani, R., & Dubey, S. K. (2021, June). Growing aspects of cybersecurity in E-commerce. In *2021 International Conference on Communication information and Computing Technology (ICCICT)* (pp. 1-6). IEEE.
7. D'adamo, I., González-Sánchez, R., Medina-Salgado, M. S., & Settembre-Blundo, D. (2021). E-commerce calls for cybersecurity and sustainability: How European citizens look for a trusted online environment. *Sustainability*, *13*(12), 6752.
8. Desamsetti, H. (2021). Crime and Cybersecurity as Advanced Persistent Threat: A Constant E-Commerce Challenge. *American Journal of Trade and Policy*, *8*(3), 239-246.
9. Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly*, 51-90.
10. Gunasekara, A. (2023). AI-Driven Big Data Analytics for Transforming Cybersecurity for Zero-Day Vulnerabilities in E-Commerce Supply Chains. *Journal of Advances in Cybersecurity Science, Threat Intelligence, and Countermeasures*, *7*(12), 17-31.
11. Hariharan, J., Sheik, A. T., Maple, C., Beech, N., & Atmaca, U. I. (2023, June). Customers' perception of cybersecurity risks in E-commerce websites. In *International Conference on AI and the Digital Economy (CADE 2023)* (Vol. 2023, pp. 53-60). IET.
12. IBM. (2023). *Cost of a Data Breach Report 2023.* IBM Security.
13. Kamisetty, A. (2024). The Role of Cybersecurity in Safeguarding Cross-Border E-Commerce and Economic Growth. *Asian Business Review*, *14*(2), 85-94.
14. Karunaratne, T. (2023). Machine learning and big data approaches to enhancing e-commerce anomaly detection and proactive defence strategies in cybersecurity. *Journal of Advances in Cybersecurity Science, Threat Intelligence, and Countermeasures*, *7*(12), 1-16.

15. Koli, B., Bhura, P., & Umesh, M. (2023). An analytical review of the growth of e-commerce towards consumers in India. *International Journal of Management, Public Policy and Research*, *2*(3), 19-24.

16. Kumar, A., & Kashyap, A. K. (2022). Understanding the factors influencing repurchase intention in online shopping: A meta-analytic review. *Vision*, 09722629221107957.

17. Liu, X., Ahmad, S. F., Anser, M. K., Ke, J., Irshad, M., Ul-Haq, J., & Abbas, S. (2022). Cybersecurity threats: A never-ending challenge for e-commerce. *Frontiers in psychology*, *13*, 927398.

18. Ma, X., & Wang, Z. (2024). Computer security technology in the E-commerce platform business model construction. *Heliyon*, *10*(7).

19. Mitra, D., Kulkarni, P., Pathak, P., & Natrai, N. A. (2022, November). Importance of coping with cybersecurity challenges in e-commerce business. In *2022 International Interdisciplinary Humanitarian Conference for Sustainability (IIHC)* (pp. 1596-1601). IEEE.

20. Mogali, S. K. (2024). AI and Cloud Technologies in E-commerce: A Novel Strategy for Enhancing Customer Experience and Cybersecurity. *Journal of Computational Analysis & Applications*, *33*(8).

21. Mohr, H., & Walter, Z. (2019). Formation of consumers' perceived information security: Examining the transfer of trust in online retailers. *Information Systems Frontiers*, *21*(6), 1231-1250.

22. Obisesan, S. M. (2024). Integrating Artificial Intelligence and Cybersecurity Frameworks: Challenges and Opportunities in E-commerce Cybersecurity Management. *Available at SSRN 5070108*.

23. Okafor, C., M. Agho, A. Ekwezia, N. Eyo-Udo, and C. Daraojimba. "Utilising business analytics for cybersecurity: A proposal for protecting business systems against cyber attacks." *Acta Electronica Malaysia* 7, no. 2 (2023): 29-39.

24. Pramanik, R., & Prabhu, S. (2022, March). Analysing Cyber Security and Data Privacy Models for Decision Making among Indian Consumers in an e-commerce environment. In the *2022 International Conference on Decision Aid Sciences and Applications (DASA)* (pp. 735-739). IEEE.

25. Rai, R., Rohilla, A., & Rai, A. (2024). Understanding cybersecurity threats in e-commerce. In *Strategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning* (pp. 501-522). IGI Global.

26. Reddy, A. (2012). A study on consumer perceptions of security, privacy, and trust on e-commerce portals. *International Journal of Multidisciplinary Management Studies*, *2*(3), 1-15.

27. Sharma, B. P. (2024). Role of advanced cybersecurity frameworks in safeguarding data integrity and consumer trust in digital commerce and enterprise systems. *Journal of Cybersecurity Research, 12*(3), 211–228.

28. Strzelecki, A., & Rizun, M. (2022). Consumers' change in trust and security after a personal data breach in online shopping. *Sustainability*, *14*(10), 5866.

29. Wang, J., Shahzad, F., Ahmad, Z., Abdullah, M., & Hassan, N. M. (2022). Trust and consumers' purchase intention in a social commerce platform: A meta-analytic approach. *Sage Open*, *12*(2), 21582440221091262.