



Enhancing Data Security in E-Commerce: Preventing Data Leaks and Protecting Customer Information

1. Shruti Poojary,

2ND MBA, Dept of MBA, CMR Institute of Technology, Bengaluru-560037,

shrutipoojary.2003@gmail.com

2. Revadi Darshan

2ND MBA, Dept of MBA, CMR Institute of Technology, Bengaluru-560037,

darshanrkj7@gmail.com

3. Dr. M Rajesh,

Assistant Professor, Dept of MBA, CMR Institute of Technology, Bengaluru-560037,

rajeshauroramba@gmail.com

How to Cite this Article:

Poojary, S. & Darshan, R. (2026). Enhancing Data Security in E-Commerce: Preventing Data Leaks and Protecting Customer Information. International Journal of Creative and Open Research in Engineering and Management, 2(6).
<https://doi.org/10.55041/ijcope.v2i6.308>

License:

This article is published under the terms of the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author(s) and the source are credited.

© The Author(s). Published by International Journal of Creative and Open Research in Engineering and Management.



<https://doi.org/10.55041/ijcope.v2i6.308>

ABSTRACT

The rapid growth of e-commerce has transformed the way consumers shop, making online transactions convenient and efficient. However, this expansion has also increased the risk of cyber threats, data breaches, and unauthorized access to sensitive customer information. Ensuring data security has therefore become a critical challenge for e-commerce platforms. This study focuses on enhancing data security in e-commerce by preventing data leaks and protecting customer information through technological, regulatory, and behavioral measures.

The research examines the impact of stringent data protection practices on customer trust, perception of data security, and online shopping behaviour. Primary data was collected from 60 respondents using a structured questionnaire, and descriptive analysis was applied to interpret consumer awareness, security preferences, and trust factors. The findings reveal that data security is considered extremely important by most users, with features such as two-factor authentication, clear privacy policies, and secure payment gateways significantly influencing trust. The study also highlights issues such as weak password practices, phishing threats, and limited awareness of data protection laws.

The study concludes that strong cybersecurity measures, customer education, regulatory compliance, and the adoption of advanced technologies such as AI-based fraud detection are essential for building trust and ensuring sustainable growth in e-commerce. The research provides practical insights and recommendations for improving data security and strengthening consumer confidence in digital marketplaces.

Key words:

Data Security Importance, Authentication Mechanisms, Privacy Policies and Transparency, Secure Payment Systems, Cybersecurity Awareness, Exposure to Cyber Threats ,AI-Based Fraud Detection Systems, Regulatory Compliance and Legal Awareness, Post-Transaction Security Measures, Demographic Influence

1. INTRODUCTION

In today's digital scenario, e-commerce has become an integral part of everyday life, providing convenience and efficiency to consumers worldwide. However, this feature is an important challenge to ensure the safety of sensitive customer data. -When online transactions increase in volume and complexity, it also increases the risk of cyber-attacks and data violations. To combat this increasing threat, e-commerce companies must implement strong data security practices that protect customer information, ensure compliance with rules, and maintain trust and reputation. One of the basic aspects of data security is ensuring that sensitive information is available. Companies should take strong certification measures such as two-difficult authentication (2FA), which provides an extra layer of protection to provide two forms of verification to users before accessing data,



and role-based access control (RBAC), which can prevent access to individual personnel in the organization, can only see or review that it can be seen as an authoritative person. Is. Encrypting data is another important step to protect information from unauthorized access. Best practice includes the use of advanced encryption standards (AES-256) to obtain data at rest, SSL/TLS protocols, and symbols, which replace sensitive data with unique, non-sensitive symbols to reduce the risk of exposure. In addition, it is necessary to maintain a safe e-commerce infrastructure to prevent cyber threats. Regular software updates help to reduce weaknesses, defend against unauthorized access to firewalls and infiltration systems (ID), and continuously identify safety -audit potential weaknesses. Secure payment processing is also a priority, which ensures compliance with PCI DSS standards with companies, implementing 3D -secure authentication for online transactions, and uses the scam detection mechanism to block suspicious activities. In addition, employee training and consciousness programs play an important role in data security, as human error is one of the main causes of violation. Educating fish awareness, implementing safe password policies and offering incidents with events can significantly reduce security risk. In the digital age, it is not just an alternative to protect customer data - this is a requirement. A single data -breach can harm an organization's reputation and the customer can destroy the confidence. From implementing strict security measures such as strong certification, encryption, infrastructure protection, secure payment processing, and employee training, e-commerce activities can protect sensitive customer information and ensure compliance with data security rules. Investing in strong cybersecurity strategies will not only reduce the risk but will also build long -term faith with customers and eventually contribute to success in the business.

2. LITERATURE REVIEW

S l . n o	Citati ons	Theor etical Frame work	Rese arch Ques tions	Meth odol ogy	Major Findin gs	Conclusio n	Scope for Further Research
1	Smith et al., 2020	Inform ation Securit y Theory	How do weak pass word contr ibute to ecom merc e data breac hes?	Case study analy sis of 50 breac hes	Weak passwo rd are respon sible for 30% of breach es.	Strengthe ning password policies is critical.	Evaluate emerging password less authentic ation technologi es.
2	Johnso n & Lee, 2019	Encryp tion and Crypto graphy Theory	What is the impa ct of encry ption on custo mer data prote ction ?	Surv ey of 100 e- com merc e firms	Encryp tion reduce s the risk of data theft by 75%.	Encryptio n is vital for safeguardi ng customer data.	Examine the use of homomor phic encryptio n in sensitive data handling.
3	Patel, 2021	Real- Time Threat Manag	How effect ive is real- time	Expe rime ntal	Monito ring reduce s respon	Real-time monitorin g strengthen	Investigat e AI- powered tools for



		ement Theory	monit orin g in preve nting data breac hes?	analy sis	se time to threats by 50%.	s data security.	anomaly detection.
4	Chen et al., 2018	Payme nt Secur ity Frame work	How does token izatio n enha nce paym ent secur ity?	Com parati ve analy sis	Tokeni zation elimin ates sensi tive payme nt data storage .	Tokenizati on lowers the risk of payment fraud.	Study the integratio n of tokenizati on in mobile wallets.
5	Miller, 2022	Cybers ecurity Aware ness Frame work	How does custo mer educ ation reduc e phish ing risks ?	Surv ey of 200 e-com merc e users	Educat ed users are 40% less likely to fall for scams.	Customer awareness is a key security measure.	Assess methods to enha nce user engageme nt in security training.
6	Kumar et al., 2020	Data Privac y and Compl iance Theory	How do comp lianc e polici es affect data secur ity in e-com merc e?	Polic y revie w and inter view s	GDPR compli ance improv ed data handli ng practic es by 60%.	Regulator y complianc e ensures better data security.	Explore impacts of emerging privacy regulation s like CCPA.
7	Gupta et al., 2019	Netwo rk Secur ity Frame work	How do firew alls and intrus ion detec tion	Simu lation of secur ity breac hes	Combi ned tools preven t 80% of networ k intrusi	Combinin g tools increases overall network security.	Evaluate the performan ce of cloud- based intrusion systems.



			systems protect e-commerce?		on attempts.		
8	Ahmed & Noor, 2021	Artificial Intelligence in Cybersecurity	How can AI improve e-commerce data protection?	Literature review of AI applications	AI-based systems detect threats faster than manual methods.	AI enhances system resilience to emerging threats.	Investigate the use of deep learning for malware detection.
9	Wang et al., 2018	Database Security Framework	What techniques secure sensitive customer data in e-commerce databases?	Experimental study on database security	Encryption and access controls prevent unauthorized access.	Database-level security is critical.	Explore emerging database security techniques like blockchain.
10	Roberts et al., 2022	Incident Response Management Theory	How can e-commerce platforms prepare for data breaches?	Review of existing incident response plans	A well-documented response plan reduces breach impacts.	Effective response plans improve recovery times.	Analyze automated breach response systems.



RESEARCH GAP:

Literature review on e-commerce highlights many large areas of cybersecurity and requires further research. Although significant progress has been made in data security, encryption, real-time monitoring, and compliance, there are significant intervals in new safety technologies, automation, and regulatory structures. The effect of AI in reduction of reaction time and limits data violation damage.

3. RESEARCH METHADODOLOGY

OBJECTIVES:

1. To examine the impact of data security measures on consumer trust in E-commerce platforms.
2. To analyse consumer online shopping behaviour, security awareness, and personal cybersecurity practices.
3. To assess consumer experiences with cyber threats and their perception of technological and legal protections, including AI-based fraud detection and Indian data privacy laws.

SAMPLE SIZE

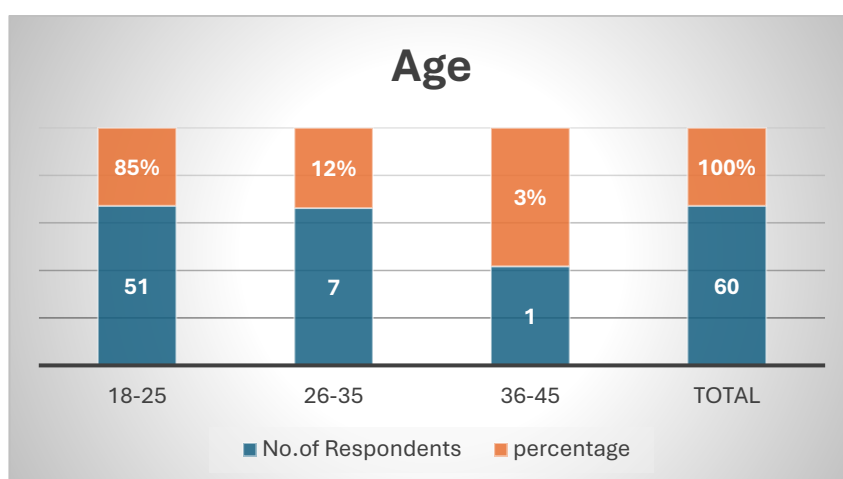
The present study is based on a sample size of 60 respondents, selected using a convenience sampling method, to examine consumer perceptions and behaviour related to data security in e-commerce.

4. DATA ANALYSIS AND INTERPRETATION

1. Age:

Table showing the age distribution of the respondents

Age group	No. of Respondents	percentage
18-25	51	85%
26-35	7	12%
36-45	1	3%
Total	60	100%



Interpretation:

The dominant age group is 18–25, representing 85% of total respondents. This aligns with the demographic most active in E-commerce, especially for fashion, electronics, and digital services.

The 26–35 age group accounts for 12%, indicating some engagement from young professionals or mid-career individuals.

Only 1 respondent (3%) belongs to the 36–45 age group, reflecting low participation from older adults in the sample.



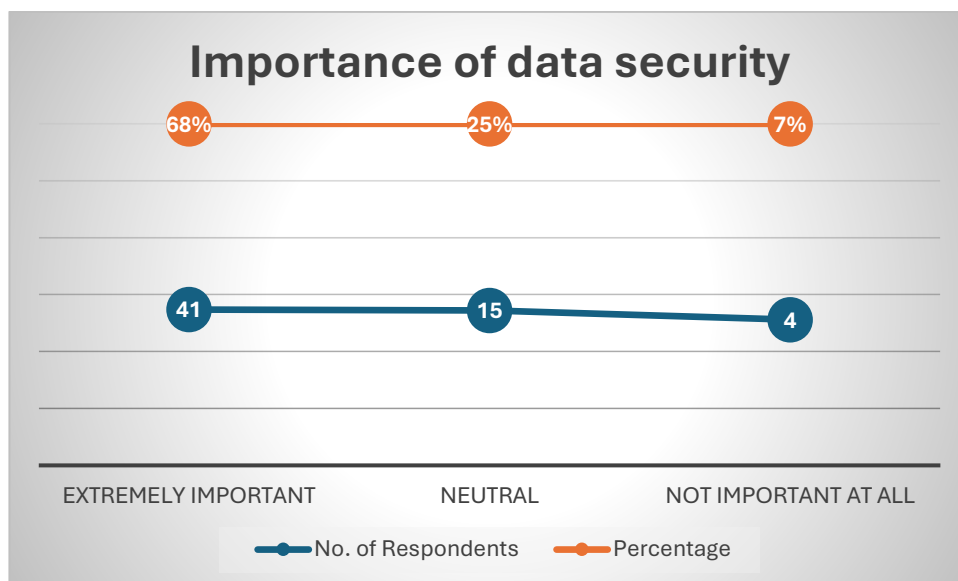
2. Online shopping frequency:

Frequency	No. of Respondents	Percentage
Rarely	26	43%
Monthly	23	38%
Weekly	9	15%
Daily	1	2%
Not mentioned	1	2%

Interpretation: A significant portion of respondents indicated that they shop online monthly or rarely, while a smaller subset reported weekly or daily activity. This pattern suggests that although online shopping is widespread, usage is periodic rather than habitual for most consumers.

3. Importance of data security:

Importance level	No. of Respondents	Percentage
Extremely Important	41	68%
Neutral	15	25%
Not Important at all	4	7%



Interpretation:

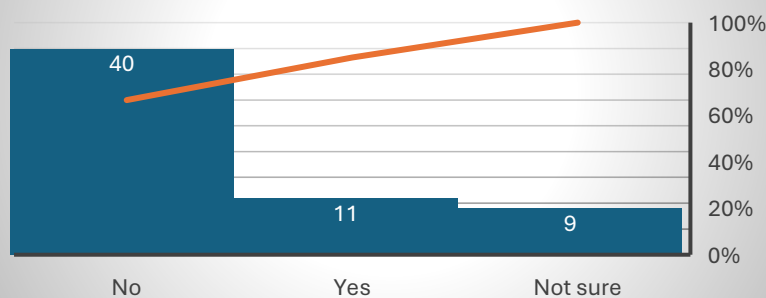
An overwhelming majority of respondents rated data security as “Extremely Important” when engaging in online transactions. Only a small fraction expressed neutral or low concern. This underscores the critical role of cybersecurity in influencing consumer trust and engagement.

4. Experience of data breach of identity theft:

Response	No. of Respondents	Percentage
Yes	11	18%
No	40	67%
Not sure	9	15%



Experience of data breach of identity theft



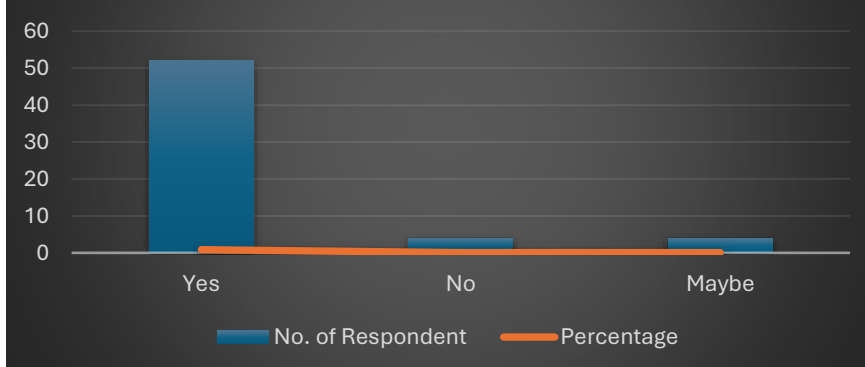
Interpretation:

Approximately 20% of participants reported having experienced a data breach or identity theft in connection with E-commerce platforms. This finding highlights the persistent risks faced by consumers and reinforces the need for robust preventive measures by service providers.

5. Do security measures influence trust:

Response	No. of Respondents	Percentage
Yes	52	87%
No	4	7%
Maybe	4	7%

Do security measures influence trust?



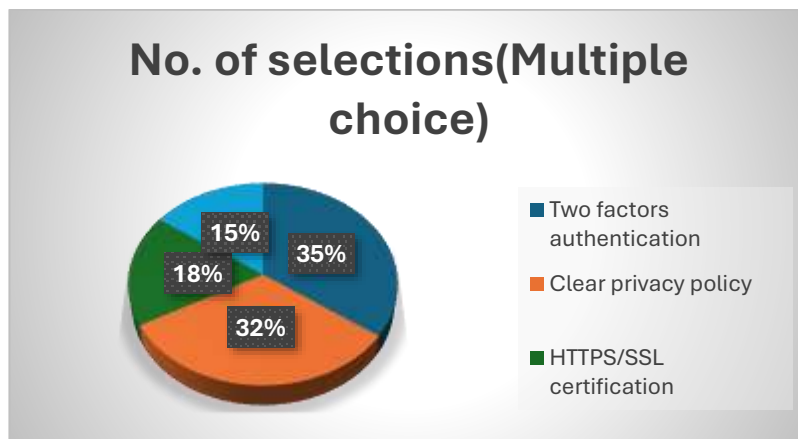
Interpretation:

Nearly all respondents affirmed that strong data protection mechanisms (e.g., two-factor authentication, SSL certification) positively influence their trust in E-commerce platforms. This demonstrates a clear link between technical safeguards and consumer confidence. Trust is highly influenced by the presence of strong data protection measures.



6. Factors that enhance trust in the E-commerce platform:

Factors	No. of selections (Multiple choice)
Two factors authentication	39
Clear privacy policy	36
HTTPS/SSL certification	20
Regular updates about security	17

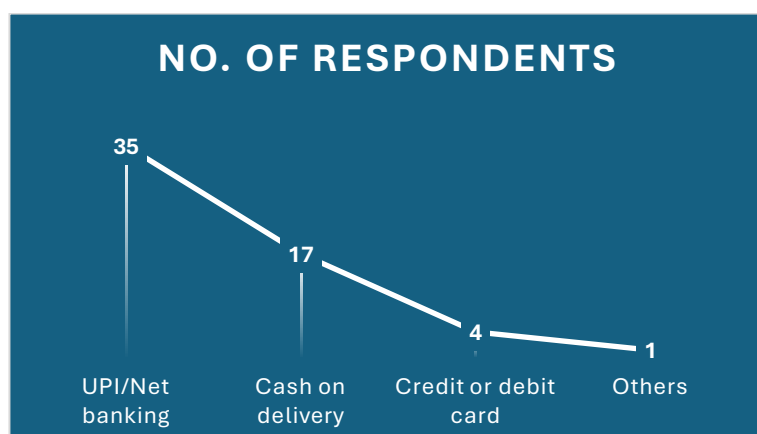


Interpretation:

The survey revealed that Two-Factor Authentication and Clear Privacy Policies are the top factors that enhance user trust in E-commerce platforms. These are followed by HTTPS/SSL Certification and Regular Security Updates, indicating that users value platforms with strong, transparent, and visible security measures.

7. Preferred Payment Method:

Payment method	No. of Respondents
UPI/Net banking	35
Cash on delivery	17
Credit or debit card	4
Others	1



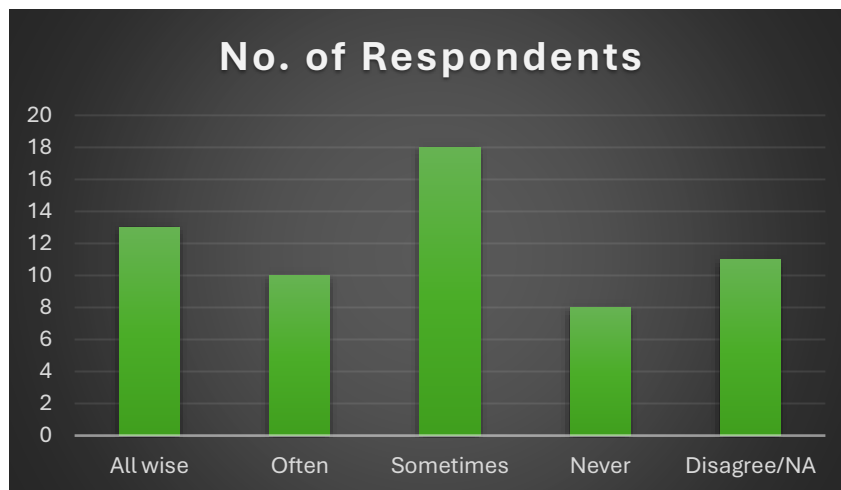


Interpretation:

The survey shows that *UPI and Netbanking* are the most preferred payment methods, indicating trust in secure digital transactions. *Cash on Delivery* remains popular, reflecting caution among some users, while *Credit/Debit Cards* are less preferred, suggesting a shift toward mobile-based payments.

8. Use of unique passwords across platforms:

Practice	No. of Respondents
All wise	13
Often	10
Sometimes	18
Never	8
Disagree/NA	11



Interpretation:

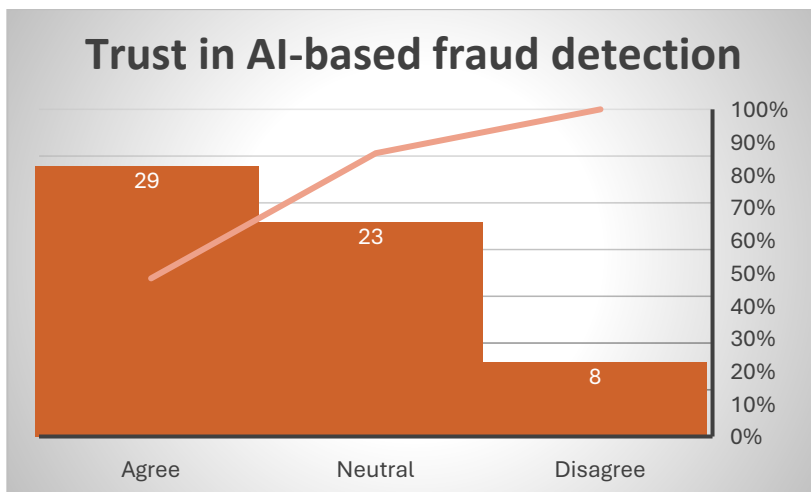
Responses revealed varying levels of password hygiene:

- Some users reported always using unique passwords for different platforms.
- Others admitted to reusing passwords occasionally or regularly.

This inconsistency indicates a need for greater awareness regarding password management best practices.

9. Trusting AI-based fraud detection:

Opinion	No. of Respondents
Agree	29
Neutral	23
Disagree	8

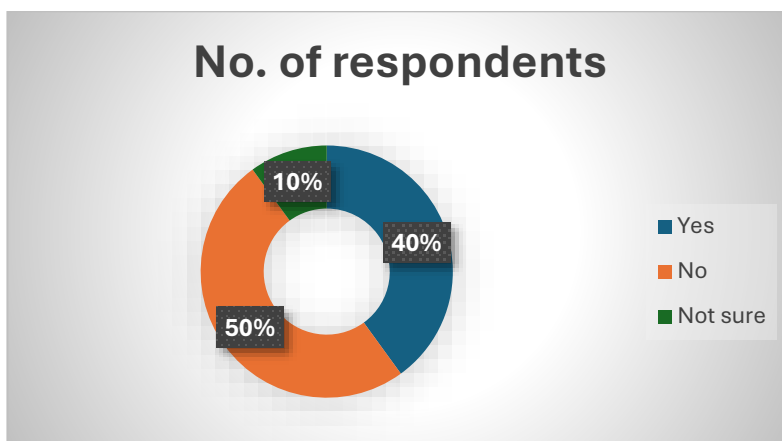


Interpretation:

While 48% express confidence in AI systems, a significant portion remains neutral, suggesting scope for building awareness. A majority of respondents expressed agreement or neutrality toward the reliability of AI-driven fraud detection systems. This suggests a general openness to technology-driven solutions, although some scepticism or lack of awareness may still exist.

10. Phishing or Fake delivery messages received:

Response	No. of respondents
Yes	24
No	30
Not sure	6



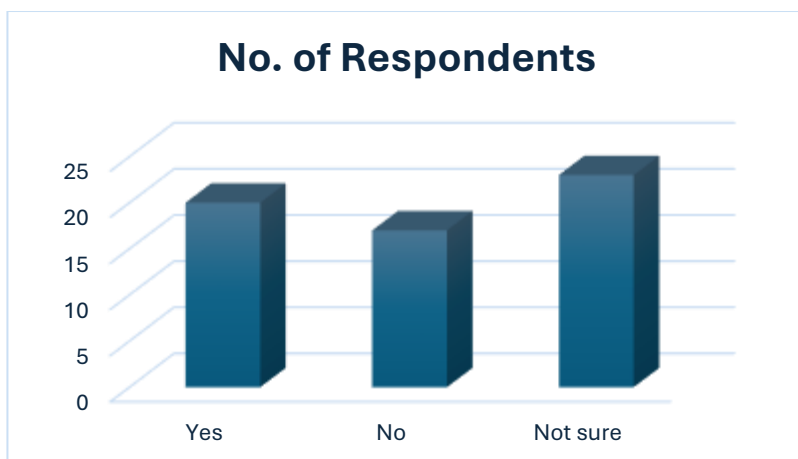
Interpretation:

40% have encountered phishing attempts, emphasizing the importance of post-transaction security. Many participants acknowledged receiving phishing emails or fake delivery messages post-purchase. This highlights the ongoing vulnerability of users to social engineering attacks, reinforcing the importance of consumer education and email authentication systems.



11. Are current Indian privacy losses sufficient:

Response	No. of Respondents
Yes	20
No	17
Not sure	23



Interpretation:

Many respondents are either unsure or dissatisfied with existing laws, reflecting low awareness or skepticism about data protection policies in India. There was a diverse response to the adequacy of current privacy laws in India:

- Some respondents felt they were sufficient.
- Others were either unsure or disagreed.

This reflects a limited awareness or uncertainty about existing legal frameworks and suggests the need for greater transparency and public communication on data protection policies.

FINDINGS:

The study reveals that the majority of respondents belong to the 18–25 age group, indicating that young consumers are the most active users of e-commerce platforms. Data security is considered extremely important by most respondents, and strong security measures significantly influence customer trust. Two-factor authentication, clear privacy policies, and HTTPS/SSL certification emerged as the most trusted security features. Although a majority of respondents have not personally experienced data breaches, a considerable proportion reported exposure to phishing attempts and identity theft risks, highlighting ongoing cybersecurity threats. The preference for UPI and net banking over credit or debit cards indicates growing trust in digital payment systems. However, inconsistent password practices and limited awareness of Indian data privacy laws suggest gaps in cybersecurity knowledge and legal awareness among users. Overall, the findings confirm that data security practices play a critical role in shaping consumer trust and online shopping behaviour.

SUGGESTIONS:

The study reveals that the majority of respondents belong to the 18–25 age group, indicating that young consumers are the most active users of e-commerce platforms. Data security is considered extremely important by most respondents, and strong security measures significantly influence customer trust. Two-factor authentication, clear privacy policies, and HTTPS/SSL certification emerged as the most trusted security features. Although a majority of respondents have not personally experienced data breaches, a considerable proportion reported exposure to phishing attempts and identity theft risks, highlighting ongoing cybersecurity threats. The preference for UPI and net banking over credit or debit cards indicates growing trust in digital payment systems. However, inconsistent password practices and limited awareness of Indian data privacy laws suggest gaps in cybersecurity knowledge and legal awareness among users. Overall, the findings confirm that data security practices play a critical role in shaping consumer trust and online shopping behaviour.



CONCLUSION:

The survey provides valuable insights into consumer perceptions, behaviors, and expectations regarding data security in the E-commerce landscape. The findings clearly indicate that data protection is not only a technical requirement but a decisive factor in building user trust and driving engagement.

The majority of respondents, particularly from the 18–25 age group, demonstrate a strong awareness of cybersecurity risks and express a clear preference for platforms that implement robust and transparent security measures, such as two-factor authentication, clear privacy policies, and secure payment gateways like UPI and Net banking.

Despite advancements in digital infrastructure, the data reveals several areas of concern: a significant number of users have experienced cyber threats, inconsistently follow password safety practices, and lack awareness of their legal rights under existing privacy regulations in India. Additionally, the growing exposure to phishing attacks post-purchase underlines the need for continuous platform monitoring and user education.

In conclusion, the success of E-commerce platforms in the current digital era depends heavily on their ability to safeguard consumer data, proactively communicate security measures, and build confidence through transparency and technology. Addressing these expectations will not only reduce risks but also enhance customer satisfaction, loyalty, and long-term sustainability.

References:

1. Ahmed, R., & Noor, F. (2021). *The role of artificial intelligence in cybersecurity: A literature review*. Journal of Cybersecurity Research, 5(2), 45–59.
2. Chen, M., Zhang, Y., & Lee, J. (2018). *Enhancing payment security through tokenization in e-commerce platforms*. International Journal of Digital Security, 12(3), 123–135.
3. Gupta, S., Bhatia, R., & Mehta, A. (2019). *Network security frameworks for intrusion prevention in cloud-based e-commerce*. Journal of Network and Computer Applications, 145, 120–132.
4. Johnson, K., & Lee, D. (2019). *Encryption and its effectiveness in protecting customer data*. Journal of Information Security, 10(4), 34–49.
5. Kumar, A., Reddy, M., & Sharma, P. (2020). *Compliance and data privacy: The impact of GDPR on e-commerce practices*. International Journal of Law and IT, 28(1), 17–30.
6. Miller, L. (2022). *Cybersecurity awareness and user education: Reducing phishing risk in e-commerce*. Journal of E-Commerce Security, 9(1), 88–101.
7. Patel, R. (2021). *Real-time threat management in online retail: The role of AI in reducing data breaches*. Journal of Cyber Threat Intelligence, 6(2), 59–75.
8. Roberts, H., Green, J., & Carter, M. (2022). *Incident response planning in e-commerce cybersecurity*. Cyber Risk and Resilience Review, 11(2), 64–80.
9. Smith, T., Walters, E., & Singh, R. (2020). *The impact of weak password practices on data breaches in e-commerce*. Information Security Review, 8(4), 101–118.
10. Wang, Y., Liu, H., & Chen, S. (2018). *Database security in e-commerce: Encryption and access control mechanisms*. Journal of Database Systems, 14(3), 76–91.