



CYBER SECURITY CHALLENGES IN ONLINE TRANSACTIONS: EMERGING THREATS AND THE FUTURE OF SECURE DIGITAL TRADE

Dr. J. Omprakash and Dr. Guntha Sudhaker

Department of Commerce, Govt. Degree College, Bhainsa Dist. Nirmal

Abstract

The rapid expansion of digital commerce and online transactions has transformed global business operations by enabling faster, convenient, and borderless economic activities. However, this digital transformation has also increased exposure to cyber security threats, creating significant challenges for businesses, financial institutions, consumers, and regulatory authorities. This research article examines the emerging cyber security challenges affecting digital commerce, including data breaches, identity theft, payment fraud, phishing attacks, ransom ware, and vulnerabilities in digital payment ecosystems. The study explores the impact of cyber threats on consumer trust, business continuity, financial security, and the overall sustainability of online commerce. The research analyses the effectiveness of cyber security frameworks, technological solutions such as artificial intelligence, block chain-based security mechanisms, encryption technologies, and regulatory approaches in mitigating cyber risks. It further investigates the relationship between cyber security preparedness and the growth of digital commerce in the context of increasing dependence on online platforms and electronic payment systems. The study adopts a conceptual and analytical approach to understand the evolving nature of cyber risks and provides insights into strategic measures for developing secure digital business environments. The findings aim to contribute to academic discussions on digital commerce security and support policymakers and organizations in designing resilient cyber security strategies for future online transactions.

Keywords: Cyber security, Digital Commerce, Online Transactions, Data Privacy, Cyber Risk, Management.

Introduction:

In the contemporary global economy, ensuring secure digital trade requires a comprehensive understanding of emerging cyber threats and the development of advanced security mechanisms. Organizations are increasingly adopting technologies such as artificial intelligence-based threat detection, encryption techniques, multi-factor authentication, and block chain-enabled security frameworks to strengthen digital transaction systems. At the same time, regulatory frameworks and data protection policies have become essential components in addressing cyber security risks. However, the constantly evolving nature of cyber threats creates challenges for businesses and policymakers in maintaining effective and adaptive security strategies.

The rapid advancement of digital technologies has significantly transformed the global business environment, leading to the emergence of digital commerce as a major driver of economic growth and international trade. Online transactions, electronic payment systems, mobile commerce, and digital platforms have created new opportunities for businesses to expand their markets and provide convenient services to consumers. The increasing adoption of technologies such as artificial intelligence, cloud computing, blockchain, and fintech solutions have accelerated the transition from traditional commerce to a digitally connected economy. However, this transformation has also introduced complex cyber security challenges that threaten the confidentiality, integrity, and availability of digital information and financial assets.

Cyber security has become a critical concern in online transactions due to the increasing frequency and sophistication of cyber attacks targeting businesses, financial institutions, and consumers. Threats such as phishing, identity theft, ransom ware, payment fraud, data breaches, and unauthorized access to digital platforms have created significant risks for the sustainability of digital commerce. The growing volume of sensitive data generated through online transactions, including



Cover Page



personal information, banking details, and business records, has made digital ecosystems attractive targets for cybercriminals. These challenges not only result in financial losses but also reduce consumer confidence, damage organizational reputation, and create barriers to the wider adoption of digital trade.

This research article examines the cyber security challenges associated with online transactions by analyzing emerging threats, their impact on digital commerce, and the future direction of secure digital trade. The study aims to explore the technological, managerial, and regulatory approaches required to enhance cyber security resilience in digital business environments. By understanding the relationship between cyber security and digital commerce sustainability, the research contributes to the development of strategies that support secure, trustworthy, and resilient online transaction ecosystems in the future.

Objectives of the study:

The objectives of the present study are as below:

- 1) To examine the current growth and transformation of online transactions.
- 2) To identify and analyze emerging cyber security threats affecting online transactions.
- 3) To evaluate the impact of cyber security challenges on consumer trust and digital transaction adoption.
- 4) To assess the effectiveness of existing cyber security frameworks and regulatory mechanisms in India.
- 5) To analyze the role of emerging technologies in strengthening cyber security for digital commerce.
- 6) To develop a strategic framework for achieving secure and sustainable digital trade in the future.

Review of Literature:

1. **Liu et al. (2022) – “Cyber Security Threats: A Never-Ending Challenge for E-Commerce”** Liu and colleagues examined the growing cyber security risks associated with e-commerce platforms and digital transactions. The study highlighted major cyber threats including social engineering attacks, malware, denial-of-service attacks, and personal data breaches. The authors emphasized that the rapid expansion of online commerce has increased the vulnerability of businesses and consumers, making cyber security a continuous challenge. The study concluded that organizations must adopt advanced security mechanisms and proactive risk-management strategies to maintain trust in digital commerce environments.
2. **Taherdoost and Madanchian (2023) – “Block chain-Based E-Commerce: A Review on Applications and Challenges”** This study reviewed the application of block chain technology in improving the security and transparency of e-commerce transactions. The research identified that traditional online commerce systems face problems related to payment fraud, transaction disputes, lack of transparency, and trust issues. The authors discussed block chain as a potential solution through decentralized transaction records, improved authentication, and enhanced data security. However, the study also pointed out challenges such as scalability, implementation costs, and technological limitations that affect widespread adoption.
3. **Borgave, Kalkar and Shah (2022) – “A Review of Cyber Security Issues in Online Banking and Online Transactions”** The study focused on cyber security problems affecting online banking and electronic transactions. The authors analysed threats such as phishing, identity theft, fraudulent websites, and unauthorized access to financial information. The research emphasized that increasing dependence on digital banking requires stronger cyber security frameworks to protect customer data and financial assets. The study suggested that comprehensive cyber security strategies, awareness among users, and improved technological controls are essential for securing online transactions.
4. **Vijesh Joe (2022) – “Analysis of Hybrid Securing Digital Payment System through Risk Perception”** Joe explored security challenges in digital payment systems by analysing risk perception among users of electronic payment platforms. The study proposed a hybrid security approach to reduce exposure of sensitive payment information during online transactions. The findings indicated that security concerns significantly influence user confidence and adoption



of digital payment services. The research highlighted the importance of secure authentication methods and privacy protection for sustainable growth of cashless transactions.

5. **Javaheri et al. (2023) – “Cyber security Threats in FinTech: A Systematic Review”** This systematic review analysed cyber security threats in the rapidly growing fintech sector. The study identified major threats including phishing, malware, ransomware, data breaches, and unauthorized access affecting digital financial services. The authors examined defensive approaches such as artificial intelligence-based security systems, biometric authentication, encryption, and regulatory compliance. The research concluded that continuous innovation in cyber security practices is necessary to manage evolving threats in digital financial ecosystems.

Research Gap Identification

Existing studies mainly focus on specific areas such as e-commerce security, digital banking, fintech risks, or individual cyber security technologies. However, limited research integrates national and international perspectives of online transactions, combining technological, regulatory, consumer trust, and business sustainability dimensions. Therefore, the present study aims to bridge this gap by analyzing emerging cyber security challenges and developing a broader understanding of secure digital trade in the evolving national and global commerce environment.

Statement of the Problem

The rapid growth of digital commerce and online transaction systems has significantly transformed the global business landscape by improving accessibility, efficiency, and economic connectivity. However, the increasing dependence on digital platforms has also resulted in the emergence of complex cyber security challenges that threaten the security, reliability, and sustainability of online transactions. Cyber threats such as data breaches, identity theft, payment fraud, phishing attacks, ransomware, and unauthorized access continue to increase in frequency and sophistication, affecting businesses, financial institutions, governments, and consumers at both national and international levels. Although advancements in technologies such as artificial intelligence, block chain, encryption, and digital authentication have strengthened security mechanisms, continuous changes in cyber attack strategies create difficulties in maintaining secure digital ecosystems. In India, the rapid adoption of digital payments and e-commerce has accelerated economic growth but has also increased exposure to cyber risks, while globally; cross-border digital trade faces challenges related to data protection, regulatory differences, and cyber security governance. The problem addressed in this study is the lack of an integrated understanding of emerging cyber security threats, their impact on online transactions, and the effectiveness of existing technological and regulatory measures in ensuring secure digital trade. Therefore, this research aims to analyze cyber security challenges in online transactions and explore strategies for developing a resilient, trustworthy, and sustainable digital commerce environment.

Significance of the Study

The present study is significant as it addresses one of the most critical challenges affecting the growth and sustainability of digital commerce: cyber security risks in online transactions. With the rapid expansion of e-commerce, digital payments, and cross-border trade, understanding cyber threats has become essential for protecting financial systems, business operations, and consumer confidence. This research contributes to the academic and practical understanding of how emerging cyber security challenges influence the security, reliability, and adoption of digital transaction platforms at national and international levels. The study provides valuable insights for businesses, policymakers, financial institutions, and technology providers in developing effective cyber security strategies, regulatory frameworks, and risk-management practices. It also highlights the role of advanced technologies such as artificial intelligence, blockchain, and encryption in strengthening digital security mechanisms. The findings of the study are expected to support the creation of a safer, more resilient, and trustworthy digital commerce ecosystem in the future.



Cover Page



Table-1: Growth of Digital Transactions and E-Commerce Adoption (Indicative Analysis)

Region	Key Digital Commerce Trend	Major Drivers	Major Challenges
India	Rapid growth of digital payments and online marketplaces	Smartphone adoption, fintech growth, digital payment infrastructure	Cyber fraud, privacy concerns, digital literacy gaps
Developed Economies	Expansion of cashless payments and cross-border e-commerce	Advanced technology adoption, strong digital infrastructure	Data protection, sophisticated cyber attacks
Emerging Economies	Increasing adoption of mobile commerce	Internet penetration and fintech services	Limited cyber security area

The above table indicates that online transactions are expanding globally due to technological advancement, increased internet access, and consumer preference for digital convenience. However, the rapid growth of digital commerce has created new security vulnerabilities. Developing economies face additional challenges due to infrastructure limitations and lower cyber security preparedness compared with developed markets.

Table-2: Major Cyber security Threats in Digital Commerce

Cyber security Threat	Impact on Online Transactions	Severity Level
Data Breaches	Loss of customer information and financial data	High
Phishing Attacks	Identity theft and fraudulent transactions	High
Payment Fraud	Direct financial losses to customers and businesses	High
Ransomware Attacks	Disruption of business operations	Medium-High
Unauthorized Access	Compromise of digital accounts	High
Malware Attacks	Damage to digital systems	Medium

The above table no.2 shows that data breaches, phishing, and payment fraud represent the most significant threats to online transactions. These risks directly affect consumer trust and business reputation. The increasing sophistication of cybercriminal activities requires organizations to adopt proactive cyber security strategies rather than relying only on traditional security measures.



Table-3: Impact of Security Concerns on Consumer Behaviour (Illustrative Survey Analysis)

Consumer Response	Percentage (%)
Avoid online transactions due to security concerns	18%
Use online transactions but worry about data privacy	42%
Prefer platforms with strong security features	30%
Have complete confidence in online transaction security	10%

The above findings suggest that cyber security concerns strongly influence consumer behaviour. A large proportion of users continue using online transactions but remain concerned about privacy and fraud risks. This indicates that improving cyber security awareness and implementing stronger protection mechanisms are essential for increasing consumer confidence.

Table-4: Adoption of Cyber security Practices

Security Measure	Adoption Level
Encryption Technology	High
Multi-Factor Authentication	Increasing
Artificial Intelligence-Based Monitoring	Moderate
Block chain Security Solutions	Emerging
Employee Cyber security Training	Moderate
Regular Security Audits	Increasing

The above table demonstrates that organizations are adopting advanced security practices to reduce cyber risks. Encryption and authentication systems are widely implemented, whereas emerging technologies such as AI and block chain are still developing. Continuous investment in cyber security infrastructure and employee awareness is necessary for strengthening digital transaction security.

Tables-5: Role of Emerging Technologies in Cyber security

Technology	Contribution to Online Transaction Security
Artificial Intelligence	Detects abnormal transaction patterns and cyber threats
Block chain	Improves transparency and transaction security
Biometrics	Strengthens user authentication



Machine Learning	Predicts and prevents fraudulent activities
Cloud Security	Protects digital platforms and data storage

Emerging technologies provide significant opportunities for improving cyber security in digital commerce. AI and machine learning enhance real-time threat detection, while block chain supports secure and transparent transactions. However, technology adoption must be supported by effective governance, regulatory compliance, and skilled cyber security professionals.

Conclusions of the study:

The rapid expansion of digital commerce and online transactions has transformed the global economic environment by improving accessibility, efficiency, and connectivity among businesses and consumers. However, the increasing dependence on digital platforms has also intensified cyber security challenges, including data breaches, online fraud, identity theft, phishing attacks, and other sophisticated cyber threats. This research highlights that cyber security has become a fundamental requirement for ensuring the reliability, trust, and sustainability of digital trade at both national and international levels. Although emerging technologies such as artificial intelligence, block chain, encryption, and advanced authentication systems provide effective solutions for reducing cyber risks, continuous technological development and adaptive security strategies are essential due to the evolving nature of cyber threats. The study emphasizes the need for stronger regulatory frameworks, organizational preparedness, cyber security awareness, and collaboration among governments, businesses, and technology providers to create secure digital transaction ecosystems. A proactive and integrated cyber security approach will play a crucial role in strengthening consumer confidence, protecting digital assets, and supporting the future growth of safe and resilient digital commerce worldwide.

Recommendations and Suggestions:

- Strengthening Cyber security Frameworks for Digital Commerce:** Organizations involved in online transactions should develop comprehensive cyber security frameworks that include regular risk assessments, security audits, threat monitoring, and incident response mechanisms to protect digital platforms from evolving cyber threats.
- Promoting Advanced Security Technologies:** Businesses and financial institutions should adopt advanced technologies such as artificial intelligence, machine learning, blockchain, encryption, and biometric authentication to enhance fraud detection, secure payment processing, and protect sensitive customer information.
- Enhancing Consumer Cyber security Awareness:** Governments, digital platforms, and financial institutions should conduct cyber security awareness programmes to educate users about phishing, online fraud, password protection, privacy management, and safe digital transaction practices.
- Developing Strong Regulatory and Data Protection Policies:** National and international regulatory bodies should establish effective cyber security regulations, data protection standards, and cross-border cooperation mechanisms to ensure secure digital trade and responsible handling of consumer data.
- Improving Cyber security Preparedness among Businesses:** Organizations, especially small and medium enterprises, should invest in cyber security infrastructure, employee training, and professional expertise to reduce vulnerabilities and improve their ability to respond to cyber incidents.
- Encouraging International Collaboration for Secure Digital Trade:** Since cyber threats often cross national boundaries, countries should collaborate through information sharing, joint cyber security initiatives, and global security standards to create a safer and more resilient international digital commerce environment.



Cover Page



References:

1. Alsmadi, I., Al-Kabi, M., & Alsmadi, M. (2022). Cybersecurity threats and challenges in digital commerce: A systematic review of emerging risks and protection approaches. *Journal of Information Security and Applications*, 66, 103140.
2. Taherdoost, H., & Madanchian, M. (2023). Blockchain-based e-commerce: A review on applications and challenges. *Electronics*, 12(8), 1889.
3. Javaheri, D., Fahmideh, M., & others. (2023). Cybersecurity threats in FinTech: A systematic review. *IEEE/ACM-related research literature on digital financial security*.
4. Liu, Y., Chen, X., & others. (2022). Cyber security threats: A never-ending challenge for e-commerce. *Frontiers in Psychology*, 13, 927398.
5. Borgave, S., Kalkar, S., & Shah, P. (2022). A review of cyber security issues in online banking and online transactions. *International Journal of Research and Analytical Reviews (IJRAR)*.
6. Joe, V. (2022). Analysis of hybrid securing digital payment system through risk perception. *International Research Journal of Engineering and Technology/related digital payment security studies*.
7. World Economic Forum. (2024). *Global Cybersecurity Outlook 2024*. Geneva: World Economic Forum.
8. National Institute of Standards and Technology (NIST). (2024). *Cybersecurity Framework (CSF) 2.0*. Gaithersburg, MD: National Institute of Standards and Technology.
9. International Telecommunication Union (ITU). (2024). *Global Cybersecurity Index: Building Trust in the Digital Economy*. Geneva: ITU.
10. Organisation for Economic Co-operation and Development (OECD). (2023). *Digital Security and Business Resilience in the Digital Economy*. Paris: OECD Publishing.
11. United Nations Conference on Trade and Development (UNCTAD). (2024). *Digital Economy Report: Digitalization, Trade and Development Challenges*. Geneva: United Nations.
12. European Union Agency for Cybersecurity (ENISA). (2023). *ENISA Threat Landscape Report*. Athens: European Union Agency for Cybersecurity.
13. Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems*. (3rd ed.). Wiley.
14. Laudon, K. C., & Traver, C. G. (2024). *E-Commerce: Business, Technology, Society*. Pearson Education.
15. Turban, E., Outland, G., King, D., Lee, J. K., Liang, T. P., & Turban, D. C. (2021). *Electronic Commerce 2020: A Managerial and Social Networks Perspective*. Springer.