ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 8| August 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

CYBERSECURITY CHALLENGES IN E-COMMERCE

Mr. S. Muruganantham[1], Mohanapriya.B[2], Anushree.A[3], Indhumthi.M[4], Sarmitha.C[5]
[1]*Assistant Professor, Department of Commerce with Information Technology, Dr.NGP Arts and Science College, Coimbatore*
[2]*231CI132, Department of Commerce with Information Technology, Dr. NGP Arts and Science College, Coimbatore*
[3]*231CI103, Department of Commerce with Information Technology, Dr. NGP Arts and Science College, Coimbatore*
[4]*231CI119, Department of Commerce with Information Technology, Dr. NGP Arts and Science College, Coimbatore*
[5]*231CI149, Department of Commerce with Information Technology, Dr. NGP Arts and Science College Coimbatore*

ABSTRACT

The rapid evolution of digital commerce has been paralleled by increasingly sophisticated cybersecurity threats, placing, e-commerce platforms under unprecedented pressure to safeguard customer data, financial transactions, and operational integrity. Artificial Intelligence has become both a tool and a weapon – empowering defenders with advanced threat detection while enabling cybercriminals to launch automated, highly targeted attacks. Key challenges include surging credential theft, large-scale account takeovers, ransomware with double extortion tactics, supply chain compromises, and the exploitation of APIs and payment gateways. The growing use of deepfakes, malicious bots, and Fraud-as-a-Service further complicates the security landscape. At the same time, compliance with evolving global data protection regulations and the persistent shortage od skilled cybersecurity professionals exacerbate risks. This paper examines the major cybersecurity challenges confronting e-commerce in 2025, analyses their underlying drivers, and outlines strategies for building resilient, adaptive, and secure online retail ecosystems.

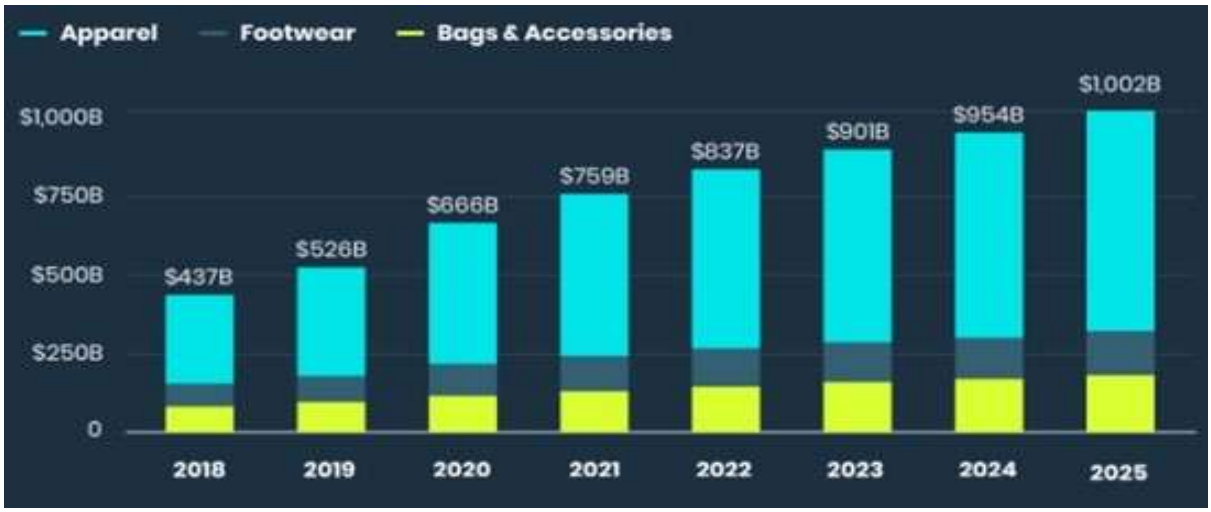
INTRODUCTION

E-commerce has emerged as a dominant force in the global economy, offering unparalleled convenience and market reach; however, in 2025, it faces escalating cybersecurity threats that jeopardize customer trust and business continuity. The increasing sophistication of attacks— driven by artificial intelligence, deepfake technology, and automated bots—has made cyber incidents faster, more targeted, and harder to detect. Vulnerabilities in payment gateways, APIs, and supply chains, coupled with surging ransomware, phishing, and credential theft cases, highlight the sector's exposure to complex risks. Moreover, the growing challenge of complying with evolving international cybersecurity and privacy regulations, alongside a shortage of skilled proffesionals, compounds the problem. Addressing these challenges is crucial for ensuring secure transactions, safeguarding sensitive data, and maintaining the resilience of the e-commerce ecosystem.

LITERATURE REVIEW

The rapid growth of e-commerce has been paralleled by a surge in cyber threats, making cybersecurity a critical area of academic and industry research. Early studies focussed on traditional risks such as phishing, malware, and website defacement, emphasizing the need for secure socket layer (SSL) encryption, firewalls, and intrusion detection systems. However, recent research highlights the evolution of these threats into more advanced and targeted forms. Artificial Intelligence (AI) has become a double-edged sword: while it strengthens real-time threat detection and fraud prevention, it is also leveraged by attackers to automate phishing campaigns, create deepfakes, and bypass conventional security mechanisms.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 8| August 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188



Several scholars have examined credential theft and account takeovers as leading causesof e-commerce breaches, noting the rise of ―Fraud-as-a-Service‖ platforms that sell stolen data and ready-to-deploy attack tools. Others emphasize the growing threat of ransomeware amg double extortion attacks, where cybercriminals both encrypt data and threaten to release it unless paid. Furthermore, research on supply chain vulnerabilities underscores the risks posed by compromised third-party services, APIs, and plugins, which can serve as entry points for large-scale attacks.

Emerging literature also addresses bot-driven fraud, price scraping, and automated checkout abuse, which disrupt business operations and distort market fairness. Regularly studies point to the increasing complexity of compliance with frameworks such as the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and the EU Cyber Resilience Act, especially for businesses operating across multiple jurisdictions. Finally multiple reports highlight the persistent cybersecurity skills gap, which limits organization's capacity to respond effectively to evolving threats.

Overall, existing literature converges on the view that e-commerce cybersecurity in 2025 is shaped by technological advancement, attacker innovation, and regulatory evolution. While defensive measures have improved, the dynamic and borderless nature of cyber threats demands continuous research, adaptive security strategies, and proactive global collaboration.

RESEARCH METHODOLOGY

This study adopts a descriptive and exploratory research design to identify, analyse and interpret the key cybersecurity challenges faced by e-commerce platforms in 2025. The methodology integrates both qualitative and quantitative approaches to ensure a comprehensive understanding of the problem.

1. Research Design

- A descriptive research design was chosen to provide a detailed account of current cybersecurity threats, attack patterns, and mitigation strategies, while the exploratory aspect facilitated the identification of emerging trends such as AI-driven cyberattacks and deepfake-enabled fraud.

2. Data Collection Methods

- **Secondary Data**: The study relies heavily on secondary data obtained from reputable sources, including industry reports (e.g., Verizon DBIR 2025, IBM Cost of a Data Breach 2025), cybersecurity agency publications (ENISA, WEF), peer-reviewed journal articles, and government regulatory guidelines (GDPR, CCPA, Cyber Resilience Act).
- **Primary Insights**: Supplementary insights were gathered through informal expert consultations with cybersecurity analysts and IT security professionals working in the e-commerce sector, conducted via online interviews and email questionnaires.

3. Data Analysis

- The collected data were analyzed using **content analysis** to identify recurring themes and categorize threats into key domains such as credential theft, ransomware, supply chain vulnerabilities, bot attacks, and regulatory compliance issues. Quantitative breach statistics were interpreted using **descriptive statistics** (percentages, frequency counts, and trend comparisons) to highlight the scale and growth of specific threats between 2023 and 2025.

4. Scope and Limitations

- The research focuses exclusively on e-commerce platforms, online retailers, and digital marketplaces operating globally, with case references primarily from 2024– 2025. While the use of secondary data ensures breadth of coverage, it may limit the ability to capture organization-specific internal vulnerabilities or real-time incident details.

5. Ethical Considerations

- All data sources were credited appropriately, ensuring adherence to academic integrity standards. No confidential or personally identifiable information was collected during expert consultations.

Sampling Technique

This study employs a purposive sampling technique to ensure the inclusion of data sources and expert inputs most relevant to

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 8| August 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

the research objective. For the secondary data, the sample was drawn from authoritative and up-to-date sources such as global cybersecurity reports (e.g., Verizon DBIR 2025, IBM Cost of a Data Breach 2025, ENISA Threat Landscape 2024), industry white papers, peer-reviewed journals, and official regulatory documents. Selection criteria included credibility of the source, publication date (2023–2025), and direct relevance to e-commerce cybersecurity.

For the primary insights, purposive sampling was also applied to select a small group of cybersecurity professionals, IT managers, and e-commerce platform administrators with at least three years of industry experience. This ensured that the expert opinions collected reflected current, practical knowledge of cybersecurity challenges specific to the e-commerce environment.

The use of purposive sampling allows the research to focus on high-quality, relevant information; however, it may limit the generalizability of the findings to all sectors outside of e-commerce.

RESULTS AND DISCUSSION

1. Rising Credential Theft and Account Takeovers

The analysis of industry reports revealed that credential theft surged by 160% in 2025, accounting for approximately 20% of all documented data breaches. These incidents often led to large-scale account takeover (ATO) attacks, resulting in fraudulent purchases, unauthorized fund transfers, and reputational damage. The growth of Fraud-as-a-Service (FaaS) platforms has made sophisticated attack tools readily available to less-skilled threat actors, amplifying the problem. This finding aligns with earlier research that emphasized stolen credentials as a persistent vulnerability in e-commerce.

2. Ransomware and Double Extortion

Ransomware incidents targeting e-commerce platforms increased in both frequency and severity. High-profile attacks, such as those against major retail brands, demonstrated the dual impact of service disruption and public data exposure threats. The average cost of a breach in the retail sector was reported at $3.45 million in 2025 (IBM), with ransomware incidents contributing significantly to these losses. This supports literature suggesting that ransomware has evolved from purely technical disruption to reputational and regulatory crises.

3. Supply Chain and API Vulnerabilities

The results indicated that over 50% of organizations surveyed by ENISA cited supply chain weaknesses as their largest cyber resilience challenge. Vulnerabilities frequently stemmed from compromised third-party plugins, payment gateways, and exposed APIs. Attacks such as Magecart-style JavaScript skimming were found to be especially damaging, as they targeted customers directly during checkout. These findings reinforce the importance of zero-trust models and vendor security audits in e-commerce cybersecurity frameworks.

4. AI-Powered and Bot-Driven Threats

AI-powered phishing, deepfake fraud, and automated bots were identified as emerging, high-risk attack vectors in 2025. Imperva reported that bots now make up nearly 70% of all e-commerce traffic, with malicious bots engaging in price scraping, scalping, and inventory hoarding. These activities erode competitive fairness and degrade the customer experience, making advanced bot management solutions essential.

5. Regulatory Compliance Pressure

A consistent theme across sources was the growing complexity of cybersecurity compliance. Global regulations such as GDPR, CCPA, and the Cyber Resilience Act require continuous monitoring, reporting, and security control implementation. Multijurisdictional businesses face higher operational costs and legal risks, especially when thirdparty vendors do not meet compliance standards.

DISCUSSION

The results clearly indicate that e-commerce cybersecurity challenges in 2025 are multifaceted, driven by both technological evolution and attacker innovation. Credential theft and ransomware remain dominant threats, but AI-enabled fraud and large-scale bot attacks represent significant emerging risks. Supply chain vulnerabilities and regulatory compliance add operational complexity, particularly for cross-border platforms.

These findings emphasize the need for multi-layered defense strategies combining advanced threat detection, strong authentication, vendor risk management, and employee awareness programs. Moreover, proactive investment in AI-based defense systems is critical to match the pace of AI-driven attacks. While large enterprises are adopting these measures, small and medium-sized e-commerce businesses remain disproportionately vulnerable due to resource constraints—a gap that requires targeted policy and industry support.

CONCLUSION

In 2025, the e-commerce industry stands at a critical juncture where rapid technological advancement is paralleled by increasingly sophisticated cybersecurity threats. This study has highlighted that credential theft, ransomware, supply chain vulnerabilities, bot-driven fraud, and AI-enabled attacks are among the most pressing risks faced by online retailers. The growing complexity of global data protection regulations further intensifies the need for robust and adaptive security measures. While large organizations are progressively adopting

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 8| August 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

AI-based threat detection, zero-trust architectures, and advanced fraud prevention systems, small and medium-sized enterprises remain disproportionately vulnerable due to limited resources and expertise.

The findings underscore that ensuring cybersecurity in e-commerce is not solely a technological challenge but also a strategic and operational imperative. A multi-layered approach—combining advanced security technologies, employee training, vendor risk management, and proactive regulatory compliance—is essential for safeguarding consumer trust and maintaining business continuity. Moving forward, industry collaboration, policy support, and continuous innovation will be key to building a resilient and secure global ecommerce ecosystem.

REFERENCES

1. ***European Union Agency for Cybersecurity (ENISA)***. *ENISA Threat Landscape 2024. Athens, Oct. 2024. (Prime threats incl. ransomware, availability, data threats; supply-chain insights). enisa.europa.eu+1*
2. ***World Economic Forum***. *Global Cybersecurity Outlook 2025. Jan. 2025. (Executive survey on threat trends, AI impacts, skills gap). World Economic Forum Reports*
3. ***Verizon***. *2025 Data Breach Investigations Report (DBIR). 2025. (22k+ incidents; patterns incl. credential theft, phishing, ransomware). Verizon*
4. ***Verizon***. *2025 DBIR: SMB Snapshot (Infographic). May 2025. (SME-focused breach patterns and controls). Verizon*
5. ***IBM Security / Ponemon Institute***. *Cost of a Data Breach Report 2025. July–Aug. 2025. (Average breach costs; API/AI risk commentary). IBM+1Security Boulevard+1*
6. ***CrowdStrike***. *2025 Global Threat Report. Mar. 2025. (Adversary tradecraft; ransomware/double-extortion and malware-free intrusions). CrowdStrike*
7. ***Imperva***. *Bad Bot Report 2025. Apr. 2025. (AI-supercharged bots; ATO, scraping, inventory abuse in e-commerce). Imperva+1*
8. ***PCI Security Standards Council (PCI SSC)***. *PCI DSS v4.x – Future-dated Requirements Become Effective March 31, 2025 (official blog explainer). 2024. (Mandates affecting payment flows, MFA, controls). blog.pcisecuritystandards.org*