Cyber security issues in E-commerce in India: exploring Legal framework and preventive strategies

Dr. Nanda Indulkar
Assistant Professor in Commerce
Smt. Parmeshwaridevi Durgadatt Tibrewala Lions Juhu College of Arts Commerce And Science,
J. B. Nagar, Andheri East, Mumbai -59

***Abstract*- The swift growth of e-commerce in India has provided remarkable convenience for consumers and unprecedented opportunities for businesses.. This paper investigates the cybersecurity challenges confronting the Indian e-commerce sector and evaluates the current legal and regulatory frameworks aimed at addressing these risks. The study also points out the shortcomings in existing enforcement mechanisms and the necessity for ongoing policy revisions in response to the evolving landscape of cyber threats. Additionally, the paper discusses practical preventive measures that e-commerce platforms can implement, such as strong encryption protocols, employee training, consumer awareness initiatives, and incident response strategies. By integrating legal perspectives with technological and organizational best practices, this research seeks to offer a holistic approach to enhancing cybersecurity and building consumer confidence in India's digital economy.**

***Index Terms*- E-commerce, Cyber security, IT Act, Data Protection, Phishing, Identity theft**

I.INTRODUCTION

The digital transformation in India has revolutionized business operations, with e-commerce becoming a leading force in the retail sector. As the number of internet users is projected to exceed 900 million by 2025[1], India has experienced an extraordinary increase in online transactions, digital payments, and virtual marketplaces. From everyday groceries to high-tech gadgets, virtually everything is now accessible with a simple click. Nevertheless, this significant expansion in e-commerce has also given rise to numerous cybersecurity challenges, jeopardizing the security of sensitive personal and financial information and eroding consumer confidence. Cybersecurity in the realm of e-commerce encompasses the protective strategies and protocols established to shield online platforms and their users from unauthorized access, data breaches, fraud, identity theft, and various cyber threats. In India, the e-commerce sector contends with a particularly intricate risk landscape due to the vast diversity of its user base, differing levels of digital literacy, and the continuously advancing tactics of cybercriminals. Common threats include phishing scams, ransomware, data leaks, malware injection, and exploitation of payment gateways. These risks not only threaten consumer data but can also lead to significant reputational and financial damage for e-commerce enterprises. In light of these escalating issues, India has introduced several legal frameworks and regulations aimed at enhancing cybersecurity and safeguarding digital consumers. The Information Technology Act of 2000 serves as the foundation of cyber law in India, detailing legal provisions concerning electronic governance, data protection, and penalties for cyber offenses. Over time, this act has been augmented by sector-specific guidelines and regulations, such as the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules of 2011, which require organizations to implement strong data protection measures. More recently, the introduction of the Digital Personal Data Protection Bill has further strengthened these efforts.

II.RESEARCH METHODOLOGY

This research employs a qualitative and exploratory framework to investigate the cybersecurity issues confronting the Indian e-commerce industry, assess the efficacy of the prevailing legal structure. The design is oriented towards acquiring a comprehensive understanding of actual cybersecurity threats and responses specific to the Indian legal and business environment so the data has been collected with the help of secondary sources like Newspapers, government reports, DSCI reports, legal texts and regulations in India etc.

Objectives of the Study

To pinpoint significant cybersecurity threats affecting Indian e-commerce platforms.

To suggest effective practices and preventive strategies utilized by e-commerce enterprises.

Legal framework For E-commerce business In India

1. The cornerstone of India's legal framework for e-commerce is the Information Technology Act, 2000 (IT Act)[2]. Enacted to provide legal recognition to electronic transactions, the IT Act plays a pivotal role in facilitating digital commerce. Key features include:

    - Legal Recognition of Electronic Contracts: Section 10A of the IT Act provides legal validity to contracts formed through electronic means.
    - Digital Signatures: It permits the use of digital signatures to authenticate electronic records.
    - Cybercrimes: The Act includes provisions to address cybercrimes, identity theft, hacking, and data breaches.
    - Intermediary Liability: Section 79 protects online platforms (intermediaries) from liability for user-generated content, provided they follow due diligence.

2. Consumer Protection Act, 2019

The Consumer Protection Act, 2019 superseded the previous 1986 Act and considerably improved consumer rights in the digital realm. Key highlights include:

- E-Commerce Rules, 2020[3]: These regulations pertain to all products and services purchased or sold through digital or electronic platforms.
- Duties of E-commerce Entities: Businesses are required to reveal seller details, guarantee fair pricing, refrain from misleading promotions, and set up a complaint resolution system.
- Product Liability and Unfair Trade Practices: The Act offers solutions for faulty products, inadequate services, and deceptive actions by e-commerce entities.

3. Draft E-Commerce Policy
    - India's Ministry of Commerce and Industry published a Draft National E-Commerce Policy[4], which suggests a comprehensive regulatory framework for digital commerce. The main goals include:
    - Data protection and localization
    - Consumer protection
    - Prevention of anti-competitive practices
    - Promotion of Indian digital businesses
    - The finalized version is anticipated to establish thorough regulations regarding data ownership, cross-border data flow, and grievance redressal.
4. Data Protection Laws
    - While the IT Act includes certain aspects concerning data protection, India is progressing toward a stronger framework via the Digital Personal Data Protection Act, 2023[5]. This Act intends to:
    - Protect personal information of users
    - Outline responsibilities of data fiduciaries (e-commerce entities)
    - Create a Data Protection Board for supervision
    - This will greatly influence the ways in which e-commerce platforms gather, manage, and retain user data.

In addition to this, Government of India has taken into consideration of new strategies to control the E-commerce issues by making amendments to the GST Act, Companies Act as well as Foreign Direct Investment policy etc.

Challenges faced In Indian E-commerce

As companies increasingly rely on online platforms for transaction management, customer engagement, and data storage, they become attractive targets for cybercriminals who seek to exploit vulnerabilities for personal or financial gain. One of the most urgent cybersecurity threats is data breaches. E-commerce platforms gather and retain extensive amounts of personal information, including names, addresses, contact numbers, and payment information. Cybercriminals frequently target this sensitive data

to perpetrate identity theft or sell it on the dark web. Insufficient data encryption, lax access controls, and outdated systems often facilitate attacker's ability to infiltrate these platforms.

Phishing attacks represent another significant issue. These attacks typically involve fraudulent emails or websites that imitate legitimate brands to deceive users into divulging confidential information such as login credentials or credit card details. Given that many Indian consumers are still relatively inexperienced with digital platforms and may lack awareness of online scams, they are particularly susceptible to these tactics.

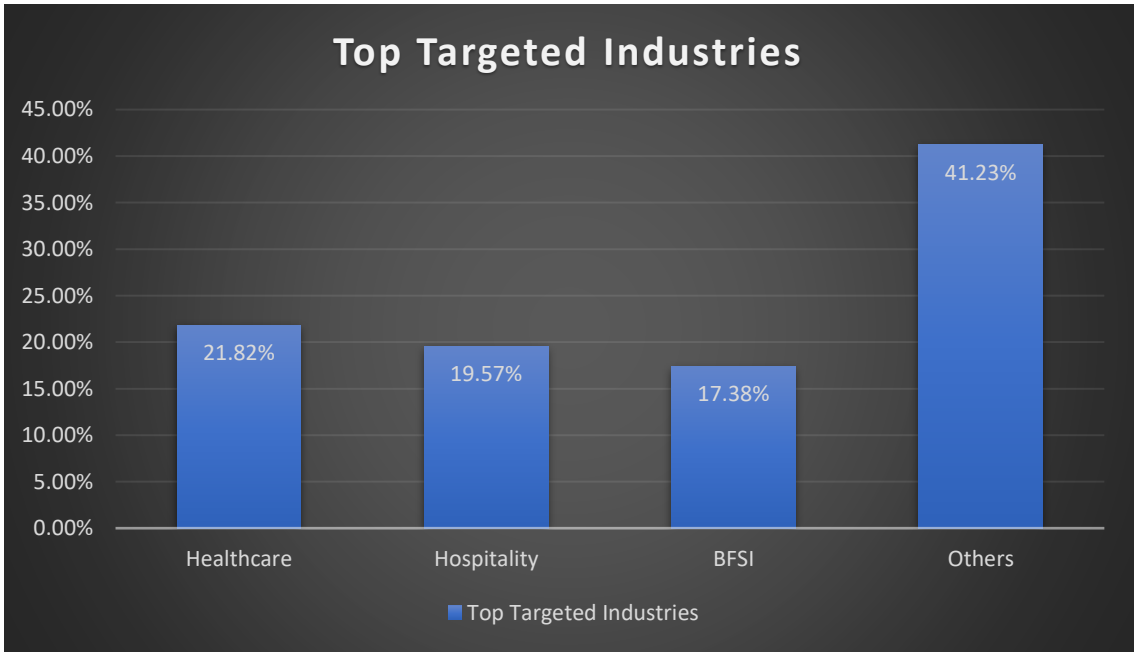
Ransomware also presents an escalating threat. In such attacks, hackers encrypt essential business data and demand payment to restore access. E-commerce platforms, particularly small and medium-sized enterprises, often lack the technical resources necessary to defend against these sophisticated attacks or to recover from them without causing substantial disruption to their services. Payment fraud and fake transaction scams are also widespread. Cybercriminals may exploit vulnerabilities in payment gateways, manipulate discount codes.

III.FINDINGS

According to report of Data Security Council of India, the magnitude of cyber threats is astonishing. The identification of more than 369. 01 million security incidents across 8. 44 million endpoints indicates that, on average, there are 702 possible security threats each minute[6]. This surge in attacks illustrates the unyielding nature of contemporary cyber threats and the ongoing strain on security systems.

A particularly significant trend is the notable change in the detection of malware. The rise in behaviour-based detections from 12. 5% to 14. 5% marks a crucial advancement in both offensive and defensive tactics. This shift indicates that attackers are developing increasingly advanced malware that can bypass conventional signature-based detection techniques.

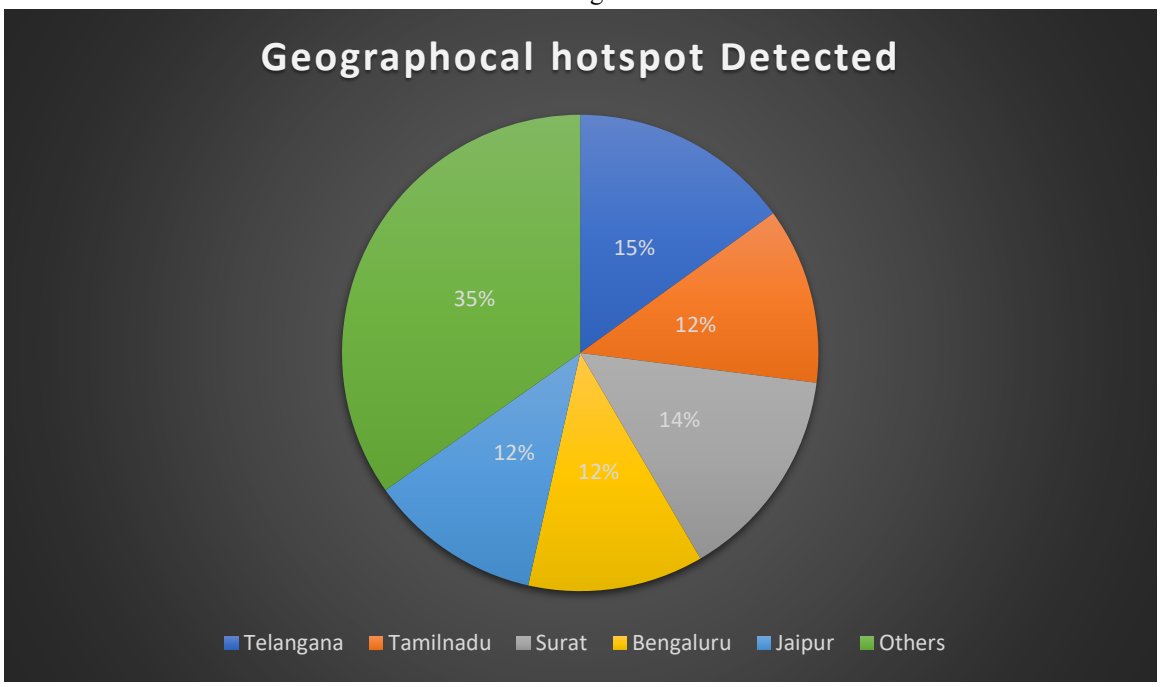
Fig. 1.1



Source: https://www.dsci.in/resource/content/india-cyber-threat-report-2025

In fig.1.1 , it is explained that most of the frauds are executed with the help of major 3 targeted industries. The healthcare sector's status as the most victimized industry (21. 82% of all attacks) is particularly alarming. This is likely indicative of the high worth of medical information and the essential nature of healthcare operations, which may lead organizations to be more inclined to satisfy ransom demands. The considerable targeting of the hospitality (19. 57%) and banking sectors (17. 38%) suggests that attackers concentrate on industries managing substantial amounts of personal and financial information.

Fig.1.2



Source: https://www.dsci.in/resource/content/india-cyber-threat-report-2025

Fig.1.2 explains the major areas of cyber-attacks in India. The geographical analysis of attacks uncovers an intriguing trend regarding the dissemination of cyber threats throughout India. While prominent tech centres such as Telangana (15. 03% of detections) and Tamil Nadu (12%) continue to be principal targets, there is a notable uptick in incidents in Tier 2 cities. This implies that cybercriminals are broadening their focus beyond established targets, possibly due to weaker cyber defences in smaller urban areas.

Every year new threats are emerging as technology is advancing for e.g. The more people are using AI and advance technology online , they are expose to the risk of AI powered adaptive malware or deepfake-enabled attacks etc.[7] Mobile Phones and other devices are also under threat from the attacks of advance mobile malware, cloud controlled android threats, biometric data exploitation etc. In financial and identity threats, attackers are crating investment platforms frauds, cryptojacking attacks, identity theft campaigns as well as creating fake apps etc.

Cybercriminals have skilfully taken advantage of the government's various apps to spread harmful software. Many cases of these fraudulent messages, allegedly sent with the help of such apps. For E.g. Traffic Police app has been misuse by the attackers to create fraud by sending vehicle owner ticket. Nevertheless, unbeknownst to the recipients, the linked APK file harbours malicious software intended to extract information from Android devices. This infostealer malware silently penetrates devices, jeopardizing sensitive information and committing billing fraud by sending messages to designated phone numbers. There are various such incidents happening all over India and millions are people are under threat of this scams.

Preventive measures to be taken by e-commerce platforms:-

While legal regulations lay the groundwork for compliance, it is crucial to implement proactive and practical preventive measures to safeguard online businesses and their customers against the ever-evolving cyber threats. E-commerce platforms should adopt a comprehensive security strategy that integrates technological, organizational, and human-centric elements. One of the most effective approaches involves establishing a strong cybersecurity framework.

This entails utilizing end-to-end encryption to secure data during transmission and employing secure socket layer (SSL) certificates to create trusted, encrypted connections between users and the platform[8]. Regular updates of firewalls, intrusion detection systems (IDS)[9], and antivirus

software are necessary to identify and mitigate malicious activities before they inflict damage. Keeping all software, plugins, and third-party applications current is also vital, as outdated systems frequently harbour exploitable vulnerabilities.

Furthermore, prioritizing data protection and access control mechanisms is essential. Sensitive customer information, including personal identification and payment details, must be encrypted and securely stored. Role-based access controls should be implemented to ensure that only authorized personnel can access or modify critical data. Additionally, platforms should adopt multi-factor authentication (MFA) to provide an extra layer of security for both consumers and employees accessing the system[10].

Conducting regular security audits and vulnerability assessments is crucial for identifying weaknesses within the system. Penetration testing, or ethical hacking, can replicate real-world cyberattacks to evaluate the system's resilience against intrusion attempts. The results of these assessments should be addressed promptly.

IV.CONCLUSION

In conclusion, as e-commerce expands rapidly in India, the associated cyber security threats also increase. Problems such as data breaches, identity theft, financial fraud, and phishing attacks present considerable dangers to both consumers and businesses. The current legal framework, primarily based on the Information Technology Act, 2000, along with sector-specific guidelines and the forthcoming Digital Personal Data Protection Act, 2023, provides a basis for tackling these threats. However, relying solely on legal measures is inadequate.

There is an urgent requirement for a multi-faceted approach that merges stringent legislative enforcement with proactive preventive strategies. This entails the implementation of advanced cybersecurity technologies, comprehensive data protection measures, consumer awareness campaigns, and ongoing capacity enhancement among stakeholders. By promoting collaboration between government entities, e-commerce platforms, cybersecurity specialists, and consumers, India can develop a safer digital marketplace. A secure and robust e-commerce environment is essential not only for consumer confidence but also for fostering sustainable long-term growth in the digital economy.

REFERENCES

[1]. https://economictimes.indiatimes.com/tech/technology/india-to-cross-900-million-internet-users-this-year-says-iamai-report/articleshow/117290089.cms?from=mdr
[2]. https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf
[3]. https://consumeraffairs.nic.in/theconsumerprotection/consumer-protection-e-commerce-rules-2020
[4]. https://www.epw.in/journal/2022/38/special-articles/national-e-commerce-policy-2019.html
[5]. https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023
[6]. https://www.dsci.in/resource/content/india-cyber-threat-report-2025
[7]. https://www.dsci.in/resource/content/india-cyber-threat-report-2025
[8]. https://www.digicert.com/tls-ssl/tls-ssl-certificates
[9]. https://www.ibm.com/think/topics/intrusion-detection-system
[10]. https://www.sherweb.com/blog/security/multi-factor-authentication/