9 Security Vulnerabilities in Online Retail Platforms: Examining the Legal System and Preventive Measures

Dr. Hemant Verma[1*] & Dr. Priyanka Arora [2]

[1,2]Assistant Professor, Department of ICT, Ch. Bansi Lal University, Haryana, India.

*Corresponding Author: hemantverma21@cblu.edu.in

Abstract

Business operations in India have been completely transformed by the digital revolution, and e-commerce is now a major player in the retail industry. E-commerce platforms are now primary targets for cyber threats in the quickly changing digital landscape, offering serious hazards to both consumers and businesses. Due to the wide variety of its user base, varying degrees of digital literacy, and the constantly evolving strategies of cybercriminals, India's e-commerce industry faces an especially complex risk landscape. Almost every industry, including government, banking, healthcare, and transportation, now heavily relies on cybersecurity due to our growing reliance on technology and the internet. In order to detect possible threats, evaluate risks, and stop or lessen the effects of cyber-attacks, cybersecurity involves using a variety of methods, instruments, and procedures. This study examines the common cybersecurity risks that E-Commerce faces and explores the latest developments in these risks. Phishing attacks, malware, data breaches, and insider threats are among the major danger categories identified by the report. These threats are all becoming more complex and destructive. The report also highlights the inadequacies of the current enforcement tools and the need for continuous policy changes in response to the changing cyber threat scenario.

Keywords: E-Commerce, Cyber Security, Cyber Attacks, Phishing.

Introduction

Online retail platforms have transformed the global marketplace by enabling fast, convenient, and personalized shopping experiences. Business operations in

India have been completely transformed by the digital revolution, and e-commerce is now a major player in the retail industry. By 2025, there will be more than 900 million internet users worldwide. Online purchases, digital payments, and virtual marketplaces have all increased dramatically in India. Nowadays, almost anything can be accessed with a single click, from high-tech devices to regular groceries. As e-commerce continues to expand, businesses increasingly rely on digital systems to manage transactions, store sensitive customer information, and support large-scale operations. However, this rapid digitalization has also made online retail platforms a prime target for cyber threats. Protecting sensitive data and preserving the integrity of online transactions are made more difficult by the growing sophistication of cyberattacks and the changing types of threats. Cyber threats like phishing attacks, which trick users into disclosing personal information; malware, which can corrupt systems and steal data; and data breaches, where unauthorized access compromises confidential information, are a constant threat to e-commerce platforms, which range from big international retailers to small online businesses. Security vulnerabilities—ranging from weak authentication and insecure payment gateways to software flaws and poor data handling practices—pose significant risks to both businesses and consumers. Cybercriminals exploit these weaknesses to conduct attacks such as data breaches, identity theft, financial fraud, and unauthorized system access. As a result, ensuring the security and integrity of online retail systems has become a critical concern. Understanding the nature, causes, and implications of these vulnerabilities is essential for developing robust security strategies that protect digital assets, maintain customer trust, and ensure the smooth functioning of e-commerce ecosystems. E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. E-Commerce sites are exposed to threats and attacks to a great extent, and it is now the top-prioritized platform for the purchase and sale of commodities and services. It offers B2B, B2C, C2C, C2B, C2G, and G2C transaction features; therefore, the quantity of data stored and accessed via the internet is large.

Dimensions of E-Commerce Security

E-commerce security is built on several core dimensions that ensure safe, reliable, and trustworthy online transactions. These dimensions protect data, users, and business systems from unauthorized access, misuse, and cyber threats. The major dimensions include:

- **Confidentiality**

Confidentiality ensures that sensitive information—such as personal details, passwords, and payment data—is accessible only to authorized users. Techniques like encryption, secure communication protocols (HTTPS), and access controls help maintain confidentiality.

- **Integrity**

Integrity ensures that data remains accurate, consistent, and unaltered during storage or transmission. It prevents unauthorized modification of information such as order details, financial records, and user data. Digital signatures, hashing, and checksums are commonly used tools.

- **Availability**

Availability ensures that e-commerce services, websites, and systems remain accessible to users at all times. Downtime caused by server failures or cyber-attacks (e.g., DDoS attacks) can disrupt business operations and lead to financial losses.

- **Authenticity**

Authenticity ensures that the parties involved in a transaction are genuine. This involves verifying user identities, merchant legitimacy, and trusted communication channels. Methods include digital certificates, two-factor authentication, and biometrics.

- **Non-Repudiation**

Non-repudiation ensures that parties in a transaction cannot deny their actions. It provides proof of the origin and delivery of information. Digital signatures and transaction logs are commonly used to support non-repudiation.

- **Privacy**

Privacy ensures that user data is collected, processed, and stored responsibly and is not misused or exposed. E-commerce platforms must follow data protection regulations and ensure users' personal information remains secure.

Threat to E-Commerce

E-commerce is the buying and selling of goods and services via the Internet that are accessible to everyone on the planet. Payments for these transactions are made via online payment portals, which facilitate simple, quick, and convenient bank account transfers. Numerous cybersecurity risks, each with distinct traits and possible effects, affect e-commerce systems. Phishing attacks are a common danger in which fraudsters use phony emails or websites to deceive consumers into divulging private information, like bank account information or login credentials. Malware, which includes viruses, worms, and ransomware, can interrupt operations, encrypt data for ransom, and jeopardize system integrity.

Here are the major E-Cash Threats explained clearly and in simple terms:

- **Counterfeiting**

Since e-cash exists in digital form, cybercriminals may attempt to create fake or duplicate digital coins or tokens. Weak encryption or flawed system design can increase the risk of counterfeit e-cash circulating in the system.

- **Double Spending**

  Double spending occurs when a user spends the same digital currency more than once. Unlike physical cash, digital money must be carefully validated to prevent reuse, making it a major challenge for e-cash systems.

- **Unauthorized Access**

  Hackers may gain access to users' e-wallets or payment accounts through malware, phishing, or weak authentication, leading to theft or misuse of funds.

- **Data Interception**

  During transmission, e-cash data can be intercepted if communication channels are not secure. Attackers might steal, modify, or reroute transaction data.

- **Fraudulent Transactions**

  Fake merchants or scam websites can trick users into making payments for non-existent products or services, exploiting the anonymity and speed of e-cash systems.

- **Money Laundering**

  Because some e-cash systems allow anonymous transactions, criminals may use them to hide illegal money transfers or make tracing financial flows difficult.

- **System Failures**

  Technical issues—such as server crashes, software bugs, or network failures—can corrupt e-cash data, disrupt transactions, or cause loss of funds.

- **Privacy Threats**

  If e-cash systems collect excessive user data or lack proper privacy protections, users' financial behaviour and identity may be exposed or misused.

Emerging Threats

E-commerce platforms are increasingly facing new and sophisticated cyber threats as online transactions continue to grow. Modern attackers use advanced tools such as AI-driven phishing, bot attacks, and credential stuffing to steal customer data and gain unauthorized access to accounts. Ransomware and supply chain attacks are rising, targeting payment gateways and third-party plugins. Weak or unsecured APIs in mobile apps also expose sensitive information. Additionally, threats like deep fake-based fraud, synthetic identities, and crypto jacking are becoming common as hackers use AI and automation to bypass traditional security measures. These emerging risks highlight the need for stronger authentication, regular security updates, and continuous monitoring in e-commerce systems.

E-Commerce Security Solutions

Security is very important in online shopping sites. Nowadays, a huge amount is being purchased on the internet, because it’s easier and more convenient. Almost anything can be bought such as music, toys clothing, cars, food and even porn. Even though some of these purchases are illegal we will be focusing on all the item ‘s you can buy legally on the internet.

- **Firewall**

In order to stop attacks, firewalls thoroughly examine incoming traffic using pre-established rules and filter traffic from unreliable or questionable sources (Nife, 2020). Firewalls protect data at the ports, or entry points, of a computer. Firewalls prohibit access using ports other than 80 and 443 in order to defend web servers against assaults. Firewalls can be physical or software-based. A software firewall is a program installed on every computer that regulates traffic via port numbers and programs, whereas a physical firewall is a piece of hardware positioned between your network and gateway. It is good to have both. A web application firewall (WAF) helps protect an organization's web applications by analyzing and filtering traffic between each web application and the internet.

- **Secure Sockets Layer (SSL)**

The client and server computers exchange messages during the security "handshake" that SSL offers. It is the standard method for securing an Internet connection and protecting any sensitive data being exchanged between two systems, making it impossible for hackers to read and alter the data. The two systems may be server-to-server or server and client. The majority of contemporary browsers will flag a website as "Not Secure" if it does not employ an SSL certificate. By encrypting the data transit between the visitor's browser and the website, SSL safeguards information. The browser encrypts the data using the website's public key if everything checks out. The public key and a secret private key are then used to decrypt the data once it has been returned to the target server (website). The majority of phishing and man-in-the-middle assaults are stopped by SSL. Additionally, session hijacking—also referred to as cookie hijacking—can be stopped by SSL. By encrypting the data on a website login page, SSL keeps hackers from deciphering the password. This approach works particularly well for banks and online retailers.

- **Digital Signature**

It is based on Asymmetric cryptography, which gives each user a public encryption key and a private decryption key, is the foundation of the digital signature. The most Digital signatures are frequently used for software distribution, financial transactions, and other situations where they are needed to identify tampering and fabrication. There are three primary uses for the digital key:

  - **Authentication:** provides the recipient with evidence that the message was sent by the sender.
  - **Non-repudiation:** You may undoubtedly demonstrate who owns the communication by using the digital backfill.
  - **Integrity:** The digital signature safeguards the message's integrity by keeping it from being changed during its transmission.

- **Be Aware of Cookies and Behavioural Marketing**

Through the use of "cookies," an online tracking mechanism that inserts code into our Internet browsers, online retailers and other websites monitor our purchasing and browsing habits to keep track of the websites we visit when conducting online searches. "Session" cookies expire when you close the browser, whereas "persistent" cookies stay on your machine. Cookies are used by online retailers to identify you and expedite your next purchase. You might be able to configure your browser to reject or disable cookies, but doing so might restrict your online capabilities and possibly make it impossible for you to place an online order. In most cases, to place an order, session cookies must be enabled.

- **Keep Your Password Private**

A lot of online retailers demand that customers log in prior to viewing or placing an order. Typically, the consumer has to supply a password and a username. Never let anyone know your password. When choosing a password, avoid using information that is well known, like your mother's maiden name, your birth date, or the numbers from your Social Security number or driver's license. Avoid reusing the same password on additional websites, especially those connected to private data. The most effective password has at least eight characters, including both letters and numbers.

- **Don't Fall for "Phishing" Messages**

Internet consumers receive a tonne of emails from identity fraudsters requesting that they update their bank, credit card, online payment, or popular shopping account details. The email may advise you that you must give your account information to the company again right away because it has expired, been compromised, or been lost. Links to official-looking websites are frequently included in emails sent as part of these phishing campaigns. In other cases, the emails request that the customer download and fill out an electronic form. Recall that reputable companies never request private information by email. If you receive an email requesting financial information, don't reply. Once more, avoid clicking on any links included in dubious emails and always call the retailer or financial institution to verify your account status before divulging any information.

Conclusion

E-commerce is widely considered the buying and selling of products over the internet, but any transaction that is completed solely through electronic means can be considered e-commerce. Day by day, E-commerce and M-commerce play a very good role in online retail marketing, and people use of this technology day by day increasing all over the world. Security vulnerabilities in online retail platforms pose significant risks to both businesses and consumers, especially as e-commerce continues to expand in scale and complexity. Online consumers who are prone to making careless mistakes are a continual target for fraudsters. Shopping on insecure websites, disclosing too much personal information, and leaving computers accessible to malware are common blunders that leave consumers vulnerable. A multifaceted strategy that combines proactive preventive measures with strict legislative enforcement is desperately needed. This calls for the deployment of cutting-edge cybersecurity technologies, thorough data protection protocols, consumer education initiatives, and continuous stakeholder capacity building. The findings emphasize the need for a multi-layered security approach that integrates robust technical safeguards, strong organizational policies, and continuous user awareness. Furthermore, proactive monitoring and rapid incident response can significantly reduce the impact of security breaches. As cyber threats evolve, online retail platforms must prioritize security as an ongoing process rather than a one-time effort. Future research should focus on emerging technologies—such as AI-driven threat detection, blockchain-based payment systems, and zero-trust frameworks—to strengthen e-commerce resilience. Ultimately, enhancing security in online retail ecosystems is crucial for fostering consumer confidence and ensuring sustainable growth in the digital economy.

References

1. Mohanad Halaweh, Christine Fidler - " Security Perception in Ecommerce: Conflict between Customer and Organizational Perspectives". Proceedings of the International Multiconference on Computer Science and Information Technology, pp. 443 – 449, ISBN 978-83-60810-14-9- 2008- IEEE
2. Yuanqiao Wen, Chunhui Zhou. "Research on E-Commerce Security Issues". 2008 International Seminar on Business and Information Management.
3. Rui Wang, Shuo Chen, "How to Shop for Free Online Security Analysis of Cashier-as-a-Service Based Web Stores". IEEE S&P‘11 proceedings.
4. V.SRIKANTH "ECOMMERCE ONLINE SECURITY AND TRUST MARKS". IJCET ISSN 0976 – 6375, Volume 3, Issue 2, July- September (2012).
5. Shazia Yasin, Khalid Haseeb. "Cryptography-Based E-Commerce Security: A Review". IJCSI-Vol. 9, Issue 2, No 1, March 2012.

6. https://economictimes.indiatimes.com/tech/technology/india-to-cross-900-million- internetusers-this-year-says-iamaireport/articleshow/ 117290089.cms? from=mdr

7. Pan, J.; Paul, S.; Jain, R. A survey of the research on future internet architectures. IEEE Commun. Mag. 2011, 49, 26–36. [Google Scholar] [CrossRef]

8. Safa, N.S.; Von Solms, R.; Furnell, S. Information security policy compliance model in organizations. Comput. Secur. 2016, 56, 70–82. [Google Scholar] [CrossRef]

9. Von Solms, R.; van Niekerk, J. From information security to cyber security. Comput. Secur. 2013, 38, 97–102. [Google Scholar] [CrossRef]

10. Craigen, D.; Diakun-Thibault, N.; Purse, R. Defining cyber security. Technol. Innov. Manag. Rev. 2014, 4, 13–21. [Google Scholar] [CrossRef]

11. Wang, W.; Lu, Z. Cyber Security in the Smart Grid: Survey and Challenges. Comput. Netw. 2013, 57, 1344–1371. [Google Scholar] [CrossRef]

12. Papp, D.; Ma, Z.; Buttyan, L. Embedded systems security: Threats, vulnerabilities, and attack taxonomy. In Proceedings of the 2015 13th Annual Conference on Privacy, Security and Trust, Izmir, Turkey, 21–23 July 2015; pp. 145–152. [Google Scholar]

13. Yaacoub, J.P.A.; Noura, H.N.; Salman, O.; Chehab, A. Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations. Int. J. Inf. Secur. 2021, 21, 115–158. [Google Scholar].

☯☯☯