International Journal of Global Research Innovations & Technology (IJGRIT)
ISSN : 2583-8717(Online), Impact Factor: 6.972, Volume 03, No. 04, October-December, 2025, pp 163-168

Cyber Security Issues and Challenges in E-Commerce

Dr. Neelam Kapoor*

Department Commerce, PGDAV Evening College, Delhi University.

*Corresponding Author: neelamkapoor@pgdave.du.ac.in

Citation: Kapoor, N. (2025). Cyber Security Issues and Challenges in E-Commerce. International Journal of Global Research Innovations &amp; Technology, 03(04), 163–168.

ABSTRACT

E-commerce, or electronic commerce, refers to buying and selling goods or services and transferring information or assets over electronic networks, primarily the internet. These transactions can occur in different models such as business-to-business (B2B), business-to-consumer (B2C), consumer-to-consumer (C2C), or consumer-to-business (C2B). E-commerce relies on digital tools like computers, smartphones, fax machines, barcode scanners, credit cards, and ATMs, eliminating the need for paper documents or physical visits to stores. It covers activities such as procurement, order processing, payment, authentication, inventory management, order fulfillment, shipping, and customer support. Even simple credit card payments using a magnetic stripe reader are part of e-commerce. E-commerce security is a crucial part of information security, focusing on protecting e-commerce systems and data from unauthorized access, misuse, alteration, or destruction. While e-commerce provides significant opportunities, especially in the financial sector, it also introduces new risks such as cyberattacks, fraud, and hacking. Therefore, implementing strong security measures is essential for safe and efficient online transactions. With the growth of mobile computing and communication technologies, e-commerce has expanded across all product segments, from groceries to electronics and vehicles. However, cyber fraud and identity theft remain major challenges, with hackers exploiting vulnerabilities in websites and user systems. Strengthening security protocols for both servers and users is critical for supporting the continued growth and reliability of e-commerce. This study provides guidance for enhancing e-commerce security, ensuring that online transactions are safe, efficient, and trustworthy. The advent of the digital era has led to rapid growth in e-commerce, driven by the combined influence of technological advancement, commercial expansion, and active customer participation. Despite these benefits, e-commerce faces serious challenges, particularly the increasing threat of cyber risks, which undermine trust, security, and the overall stability of online business platforms. This paper critically examines the growing impact of cyber threats on e-commerce, analyzes their consequences, and proposes comprehensive solutions. Major cyber threats such as data breaches, spear phishing, payment fraud, malware, and ransomware pose significant risks to online businesses. Data breaches result in the exposure of sensitive customer information, leading to financial losses and erosion of consumer trust. Spear phishing attacks deceive individuals into disclosing confidential data, thereby violating user privacy and damaging system reliability. Payment fraud, including credit card theft and manipulation of chargeback systems, directly disrupts financial transactions. In addition, malware and ransomware attacks can paralyze business operations and corrupt valuable consumer databases. E-commerce systems face complex cybersecurity challenges due to their reliance on interconnected networks, third-party service providers, and extensive supply chains. Human factors such as user errors, weak security practices, and insider threats further increase vulnerability. The study highlights the urgent need for proactive cybersecurity strategies involving e-commerce businesses, policymakers, and cybersecurity professionals to protect digital trade. Furthermore, in view of the continuously evolving cyber threat landscape and the expanding e-commerce economy, cybersecurity regulations must adapt dynamically to ensure sustainable and secure online commerce.

***Keywords**: E-commerce, Electronic Networks, Inventory Management, Consumer Trust, Cybersecurity.*

Introduction

E-commerce security is about protecting online business systems and customer data. It is very important because people use e-commerce to make payments through credit/debit cards, PayPal, e-money, and other digital methods. A strong and reliable system is needed to keep these transactions safe.

With the rise of mobile commerce, security has become even more important. Users often worry about privacy, identity theft, and fraud, which affects their trust in online services. Companies are slowly improving their security, but many customers still need guidance on safe online practices.

Viruses, worms, and Trojan programs are common threats that can bypass security systems. Privacy issues are also a concern, making the protection of customer data a top priority.

Cybercrime and online fraud are growing more sophisticated, targeting weaknesses in technology, processes, and human behavior. Successful attacks can harm company reputation and cause financial losses.

To maintain trust and safety, businesses must secure their systems and protect customer information. A company-wide security model focusing on customer safety is essential for successful e-commerce.

Security is a major concern in e-commerce, affecting both customers and businesses. Protecting online transactions is key to the growth of e-commerce.

This includes B2C (business-to-consumer) and C2C (consumer-to-consumer) websites. Security strategies focus on technology and system improvements to make e-commerce safer.

Using third-party services adds extra security challenges because applications need to coordinate with external services and users over the internet.

While e-commerce brings great opportunities, it also creates risks like data breaches and fraud. Protecting customer data and online payments is essential, and this requires careful planning, technical solutions, and proper management.

E-commerce security is about protecting online business assets from unauthorized access, misuse, changes, or destruction. Customers worry about losing their financial information, while e-commerce sites are concerned about financial losses caused by security breaches or hacks.

There are several key organizational and human issues in e-commerce security:

- **Organizational processes:** Companies need proper risk management, security policies, separation of duties, access control, and regular security checks.
- **Human factor:** Employees or users are often the weakest link, rather than technology itself. People may store passwords insecurely or share them with outsiders.
- **Software management:** How security technologies are deployed and maintained also affects safety.

Types of Security Threats:

- **Unauthorized Access:** This happens when someone illegally accesses systems or data.
- **Passive access:** The hacker only observes communications to gather sensitive information.
- **Active access:** The hacker changes or manipulates information to cause harm.
- **Denial of Service (DoS):** Attackers try to overload systems or networks to make them unavailable.
- **Spamming:** Sending a huge number of emails to a target system.
- **Distributed DoS (DDoS):** Using multiple compromised computers to flood a target with requests.
- **Viruses and worms:** Malicious programs that replicate and damage systems.
- **Trojan Horses:** Programs disguised as safe software that trick users into running them.
- **Theft and Fraud:** Hackers steal or modify sensitive data, including credit card information and personal details. Theft can also involve illegal copying of software or stealing hardware. Merchant servers, databases, and third-party processing centers are common targets for such attacks.

Overall, e-commerce security involves protecting both technology and people to ensure safe online transactions and prevent financial and data losses.

Conceptual Framework

The e-commerce environment is laden with cybersecurity threats that significantly endanger both businesses and consumers. These threats jeopardize sensitive information and undermine trust in digital commerce platforms. Recognizing the types, instances, and effects of these threats is essential for creating effective defenses.

- ****Data Breaches****

Data breaches present a serious risk within the e-commerce industry, involving unauthorized access to customers' sensitive information, including personal and financial details. A notable example occurred in 2018 when a major online retailer suffered a data breach, compromising millions of individuals' personal information. The immediate and long-term economic repercussions of such breaches can be extensive, ranging from immediate financial losses to ongoing identity theft and damage to brand reputation. Consequently, e-commerce organizations must protect vast amounts of data from increasingly sophisticated cybercriminals, while facing the challenge of rising identity theft incidents and a lack of effective preventive measures.

- ****Phishing Attacks****

E-commerce scams often deceive customers into disclosing valuable information, including payment details and passwords. For instance, a customer might receive an email from a seemingly reputable e-commerce site, instructing them to update their account information via a phishing link. This can lead to immediate financial loss and further criminal activity. The impact on e-commerce websites can be profound, as consumer trust diminishes, and legal repercussions loom. These attacks erode the fragile connection between customers and online businesses, undermining the essential security foundation needed for the online economy's success.

- ****Payment Fraud****

Payment fraud in e-commerce can take many forms, from unauthorized transactions using stolen credit and debit card information to hackers manipulating online transactions. A common type of payment fraud is credit card fraud, where stolen card information is used for unauthorized purchases. Chargeback fraud, known as “friendly fraud,” occurs when a customer purchases a product online and then falsely claims to their bank that they never made the purchase. This type of fraud results in immediate financial losses for merchants and additional operational costs as businesses implement stronger security measures and more careful dispute resolution processes. Unfortunately, the issues related to payment fraud disrupt business resources and compel companies to reassess how they deliver customer service and detect fraud in an ever-changing digital marketplace.

- ****Malware and Ransomware****

Malware and ransomware are particularly dangerous threats due to their stealthy nature. Malware can infiltrate vulnerable systems and leak personal data, while ransomware encrypts critical information, demanding payment for the decryption key—often from the organization that has been compromised. A well-known online retailer that suffered a ransomware attack exemplifies the severity of this issue, as the attack significantly disrupted their operations. Given the potential for substantial legal consequences resulting from such attacks, e-commerce businesses must take proactive measures to guard against both malware and ransomware.

- ****Underlying Factors****

The intricate infrastructure of e-commerce platforms—comprising numerous interconnected services and third-party integrations—has exacerbated cybersecurity risks. While these integrations are essential for providing key services like payment processing and customer relationship management, they also create multiple vulnerabilities. Integration points linking e-commerce systems to financial software and other applications can become access points for attackers. The complexity of these technologies is compounded by human factors, where errors or malicious actions by employees or customers can introduce additional risks. This interplay of complex system architectures and human error creates frequent opportunities for attacks. An effective cybersecurity strategy is necessary, combining advanced technological defenses with comprehensive training to minimize risks.

In summary, cybersecurity threats in e-commerce are diverse and multifaceted. Each type of attack has unique methods and consequences. Data breaches expose personal identification and financial information, leading to customer distrust and regulatory scrutiny. Phishing schemes trick individuals into compromising their own security, resulting in unauthorized access and economic losses. Payment fraud undermines trading integrity and adversely affects e-commerce companies. Additionally, malware and ransomware disrupt operations while threatening the confidentiality, availability, and integrity of information. The intricate nature of e-commerce ecosystems, coupled with financial policies and human factors, further complicates these challenges.

Research Objectives

- To analyse the significance of E-commerce security.
- To analyse and examine the purpose of Security in E-commerce.
- To identify the involvement of outsider hazard in Online Shopping.

Literature Review

- **E-Commerce Trust and Security**

In traditional commerce, trust usually refers to a customer's confidence in a salesperson. In e-commerce, trust extends to the website, the products, and other users. It is often described as a consumer's willingness to be vulnerable, their expectations, or their belief that the e-commerce site and related parties will act honestly.

E-commerce website owners focus on attracting customers and making them feel secure while shopping online, while users want to know how safe a site is and how to protect themselves. Every step of an online transaction involves security measures to keep data safe.

- **Common Threats**
  - **Viruses and Trojans:** These programs can bypass security measures like password protection or encryption because they capture data before it is encrypted.
  - **Identity Theft and Fraud:** Media reports of these issues have made users wary, and many refuse to shop online due to fear for their personal information. Online transactions require users to share sensitive data, increasing risk if trust is low.

Understanding and building consumer trust is essential for the growth of e-commerce.

Technologies for Transaction Security

- **Encryption:** Converts readable data (plain text) into unreadable form (cipher text) to protect stored data and data in transmission. Only the sender and receiver can decode it.
- **Secure Socket Layer (SSL):** A common method to secure communication over the Internet. SSL provides data encryption, server authentication, optional client authentication, and message integrity to prevent eavesdropping, tampering, or forgery.
- **Secure Hypertext Transfer Protocol (S-HTTP):** Secures individual messages sent over HTTP. It can encrypt, sign, or authenticate each message to make web communication safer.
- **Digital Signature:** A unique electronic signature that verifies a document's authenticity. It is linked to the data, so any changes invalidate the signature. Typically, it uses a hash of the message encrypted with the sender's private key.
- **Secure Electronic Transaction (SET):** Ensures secure credit card and payment transactions online. SET authenticates cardholders and merchants, keeps payment information confidential, and allows different systems and software to work together safely.
- **Digital Certificate:** Issued by a trusted Certification Authority (CA), a digital certificate contains information about the organization or individual, their public key, and the CA's signature. It verifies the authenticity of websites and users.

Overall, e-commerce trust and security depend on protecting data, authenticating users, and using technologies that ensure safe online transactions.

Discussion and Findings

Cybersecurity remains mostly the responsibility of engineers and IT professionals, while many other employees are unaware of the risks or how to respond. Many organizations use a mix of old, outdated, and new technology, so updating new systems does not fix vulnerabilities in older ones. Additionally, companies often focus more on production and profits rather than investing time, money, and staff into cybersecurity.

Cybersecurity is a growing problem across industries, as attacks can severely damage businesses or even individuals. Malware is increasing rapidly every year. By 2021, cybercrime losses were expected to reach $6 trillion annually, and cybersecurity spending worldwide exceeded $1 trillion between 2017 and 2021. Hackers attack every 39 seconds, affecting about one in three Americans each year. Yet, only 38% of organizations worldwide feel fully prepared to handle advanced cyberattacks. In 2017, 7 out of 10 companies reported that their security risks had increased, and 54% suffered one or more successful attacks compromising data or IT infrastructure. About 77% of these attacks used fileless techniques, which are harder to detect.

India faces similar challenges, and there is an urgent need to strengthen the country's cyber infrastructure. Payment gateways, banks, and other financial services must be fully secure. Reports on Indian cybersecurity show various weaknesses in the current system. E-commerce platforms have a primary responsibility to protect customer data and maintain cybersecurity. Failing to do so can lead to both civil and criminal liability. There is a pressing need for a regulatory framework in India that mandates disclosure of cyber breaches to safeguard the rights and interests of consumers.

Conclusion

Online business refers to buying and selling goods and services through electronic networks, mainly the internet. With the rapid growth of e-business and mobile commerce, online retailing has expanded worldwide and continues to attract a large number of users. As this growth increases, ensuring strong e-commerce security has become a major concern. E-commerce security focuses on protecting online assets and information from unauthorized access, misuse, modification, or destruction.

The key elements of e-commerce security include data integrity, which prevents unauthorized changes; non-repudiation, which ensures that parties cannot deny their transactions later; authenticity, which verifies the source of information; confidentiality, which protects data from unauthorized disclosure; and overall security control over data access and sharing. Therefore, both online businesses and customers must identify security risks, evaluate possible technical solutions, and manage these risks effectively.

It is difficult for any system to achieve maximum connectivity, security, and usability at the same time, as improving one often affects the others. Hence, some level of compromise is unavoidable. From a merchant's perspective, protecting sensitive information such as transaction records is crucial, and such data should be stored securely behind firewalls. In addition, unnecessary services and applications should be removed to minimize vulnerabilities.

In conclusion, successful e-commerce depends on maintaining a careful balance between privacy, trust, and security. Technologies such as encryption, verification, and authentication play a vital role in shaping users' perception of security. Ultimately, the online marketplace can function effectively only when customers feel confident and trust the environment in which they conduct transaction.

References

1. Bhattacherjee (2002). Individual trust in online firms: scale development and initial test. Journal of Management Information Systems, 19 (1) (2002), pp. 211–242
2. Adam Jolly (2003). The Secure Online Business: Great Britain and the United States. Kogan Page Limited 2003, pp: 93-118.
3. Anderson, Ross (1994). Why Cryptosystems Fail. Communications of the ACM, 37 (11), 32-40
4. Jarnail Singh (2014). Review of e-Commerce Security Challenges. International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 2, February 2014
5. S. Ba, A.B. Whinston, H. Zhang (2003). Building trust in online auction markets through an Economic incentive mechanism. Decision Support Systems, 35 (3) (2003), pp. 273–286
6. S.E. Beatty, M. Mayer, J.E. Coleman, K.E. Reynolds, J. Lee (1996). Customer–sales associate Retail relationships. Journal of Retailing, 72 (3) (1996), pp. 223–247.
7. Shazia Yasin, Khalid Haseeb (2012). Cryptography Based E-Commerce Security: A Review. IJCSI-Vol. 9, Issue 2, No 1, March 2012.
8. Stuart Feldman (2000). The Changing Face of E-Commerce: Extending the Boundaries of The Possible. IEEE Internet Computing, May -June 2000, pp:82-83.

9. V. Srikanth (2012). Ecommerce online security and trust marks. IJCET ISSN 0976 – 6375, Volume 3, Issue 2, July- September (2012)

10. Borisov, N., I. Goldberg, and D. Wagner (2001). Intercepting Mobile Communications: The Insecurity of 802.1. Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking: 180-189

11. Chaum, David. 1985. Security Without Identification: Transaction Systems to Make Big Brother Obsolete. Communications of the ACM, 28, 1030-1044.

12. Delaigle, J-F., C. De Vleeschouwer, and B. Macq (1996). Digital Watermarking. Proceedings Of the Conference 2659 – Optical Security and Counterfeit Deterrence Techniques, 99-110.

13. DonalO.Mahony, Michael Peirce Hitesh Tewari (2001). Electronic Payment Systems for ECommerce. Artech House computer security Series-Boston 2001, Second Edition, pp: 19-69.

14. E. Brynjolfsson, M. Smith (2000). Frictionless commerce? A comparison of Internet and Conventional retailers. Management Science, 46 (4) (2000), pp. 563–585

15. JOSE A. ONIEVA (2008). Multiparty Nonrepudiation: A Survey. ACM Computing Surveys, Vol. 41, No. 1, Article 5, December 2008, pp:5.1-5.42

16. Mohit Kabra Chief Financial Officer, MakeMyTrip.in Future of e-Commerce: Uncovering Innovation page no.27.

17. Peter C. Chapin, Christian Skalka, and X. Sean Wang (2008). Authorization in Trust Management: Features and Foundations. ACM Computing Surveys, Vol. 40, No. 3, Article 9, August 2008, pp: 9.1-9.48.

18. Pradnya B. Rane, Dr. B. B. Meshram (2012). Transaction Security for Ecommerce Application. IJECSE -ISSN2277-1956. 2012.

19. R.E. Plank, D.A. Reid, E.B. Pullins (1999). Perceived trust in business-to-business sales: a New measure. The Journal of Personal Selling & Sales Management, 19 (3) (1999), pp. 61–71.

20. Randy C. Marchany, Joseph G. Tront (2002). E-Commerce Security. Issues “Proceedings of The 35th Hawaii International Conference on System science 2002