International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

# Cyber Security in E-Commerce

**R. Nagalakshmi[1], Dr. P. Yasodha[2]**

[1]Research Scholar, NIFT-Tea College of Knitwear Fashion, Tirupur.
[2]Assistant Professor, NIFT-Tea College of Knitwear Fashion, Tirupur.

**Abstract:**
The cyber security is a crucial aspect of modern society that aims to protect compute system network and sensitive data from unauthorized access.The WWW has become popular to search the information, trading, business and so on. Companies and Various Organizations also employing the web in order to introduce their products oe services around the world. A huge amount of information is generated and stored in the web services.it includes the encryption of protecting data and it is transferred over networks to prevent interception.The uptake of ecommerce has led to associated security threats. In this paper we use techniques security purposes, in detecting preventing and predicting the cyber attack on virtual space.

**Keywords:** Cybercrime, E-commerce, Security, threats, attacks.

## 1. Introduction

E-commerce has grown exponentially over the year. The integrity, privacy, and safety of customers and e-commerce businesses is essential to safeguarding the Cyber security. In this paper we will explore the cyber security challenges faced and discuss some of the best measures that can be adopted to mitigate the e-commerce business. Cyber security is the practice of protecting computer systems, sensitive information and networks from damage, theft or unauthorized access. With the widespread use of digital technology and the internet. Cyber security has become important for individuals, businesses, and government around the world. Cyber threats come in many forms, including viruses, malware, phishing scams, hacking, and denial-of-service attacks. These threats can cause significant damage to computer systems and networks, resulting in data breaches, financial losses, and reputational damage.

It is also important to stay informed about the threats and to regularly software update and system to protect against new vulnerability. To mitigate the risk associated with cyber threats, individuals and organizations need to implement a range of security measures and firewalls, antivirus software, encryption, and strong passwords. Overall, cyber security is a constantly evolving the field that requires attention and vigilance to stay ahead of the latest threats and protect against them effectively.

## 2. Objectives

The research aims to explore the concerns about cyber security threats in e-commerce with a focus on Malware, denial of services and Attacks on Personal Data and provide a managerial solution.

## 3. Ways to enhance the E-commerce security

### Secure payment gateways

Implementing secure & trusted payment gateways is fundamental for protecting financial transactions.

Encryption protocols, such as SSL/TLS, ensure that customer payment details are transmitted securely over the internet, preventing interception by malicious actors.

**Data encryption & tokenization**

Encrypting sensitive data, including customer information & payment details, adds an extra layer of protection. Tokenization reducing the risk associated with storing & transmitting confidential information and replaces sensitive data with unique tokens.

**Multi-factor authentication [MFA]**

MFA adds to appreciate the security of user accounts by requiring multiple forms of verification. This additional layer of authentication helps prevent unauthorised access, beyond passwords, especially to customer accounts containing personal & financial information.

**Regular security audits & vulnerability assessments**

Conducting vulnerability assessments and regular security audits helps identify and address potential weaknesses in the e-commerce infrastructure. It allows businesses to stay ahead of emerging threats and fortify their security measures and proactive approach.

**Employee training & awareness**

Human error is one of the consequences factors in cyber security incidents. Comprehensive training programs recognize phishing attempts and understand their role in maintaining a secure online environment. They ensure that employees are aware of cyber security best practices.

**Incident response plan**

Developing a robust is important for minimizing the impact of a cyber incident. This plan outlines the steps to be taken in the event of a security breach, ensuring a swift & coordinated response and protecting customer data to mitigate damage.

## 4. Challenges of Cyber Security

- Cloud computing has spread widely in recent years. Cloud Service providers now offer their customers a wide array of cloud platforms to reduce costs and maximize efficiency.
- Ransomware is malicious software that can cause irreparable damage to your data and your computer. It revokes your data to access by locking the device itself or encrypting the files stored on it.
- IoT devices are breached to gain access to confidential information and data. These breaches usually involve installing malware on a device, corrupting or damaging the device itself, or using it to access deeper levels of confidential data belonging to the solicitude business.
- Phishing is a form of social engineering frequently employed to pilfer personal information including usernames, passwords, and credit card numbers. This cyber security problem involves a bad actor who masquerades as a reliable entity cold email messages, sending emails, or texts to vulnerable targets.
- This incident exemplifies just how damaging an insider threat can be a single individual can intent seriously maliciously damage its reputation and company in terms of financial standing.

## 5. Overcome the challenges in Cyber Security

Cybersecurity is a task that requires processes and comprehensive strategies that demand continual attention and continuous reinforcement. Employing solutions like two-factor authentication, alerts for

malicious activity, encryption algorithms, and safe password practices will help to keep us safe in cyberspace.

If it looks at the digital landscape and feels overwhelmed by the challenges of cybersecurity, it might bring Sprinto into the world. Sprinto helps you to take the strides to achieve a secure security posture by helping you align your security systems with the global standards defined by compliance frameworks like ISO 27001 and SOC 2. These steps not only help you to achieve compliance but also lay the foundation for a culture that prioritizes security over anything.

**6. Choices of E-commerce Platform**

Statista predicts that global retail ecommerce sales will reach $6 billion for the first time in 2024. However, the growth that breaks records doesn't stop there.

Having an e-commerce presence is vital for a brand to keep up with the growing number of consumers who choose to purchase online. Creating a successful online store isn't as easy as it sounds, and the online platform you choose is what ultimately determines its success.

The ecommerce platforms available are endless in terms of possibilities. When choosing ecommerce software, it's important to carefully plan how to launch your site and understand your business needs.

Some of the best ecommerce platforms designed for the buying and selling of online goods and services include:

- Bigcommerce
- Adobe Commerce Cloud
- Commercetools
- Shopify
- Salesforce commerce cloud

**7. Best practices to Combat Security Threats in Ecommerce**

- Protect your website with a complex password that can be cracked open by a password.
- Make sure that the website is created using closed-source code.
- Add multilayer security to the website and a trusted firewall, which can be used to install antivirus and antimalware software.
- Use HTTPS for an extra layer of safety on the e-commerce website.

**7.1 Cyber security Awareness**

- Cyber security awareness refers to the understanding and knowledge about potential cyber threats and how to handle them.
- It involves recognizing the various types of cyber threats, such as phishing, malware, ransom ware, and social engineering attacks.
- By being aware of these threats and knowing how to respond to them, individuals and organizations can better protect their sensitive information and systems from being compromised.

**7.2 Cyber security Awareness Training**

- Cyber security mindfulness preparing is an instructive handle outlined to educate people almost the potential cyber dangers and the best hones for moderating these dangers.

- This preparing frequently incorporates subjects such as recognizing phishing emails, making solid passwords, understanding the significance of program overhauls, and recognizing suspicious exercises.
- The objective is to prepare people with the information and aptitudes required to anticipate and react to cyber dangers effectively.

**8. Ways to Safeguard Ecommerce business in Cyber security**

- It protecting customer data such as customer information, financial transactions, name, address and payment details.
- Implementing strong cyber security measures ensures that customer data remains secure and confidential.
- End to end encryption ensures that data is encrypted throughout its entire journey by cyber criminals the data remains unreadable and secure.
- Securing network infrastructure is also essential to prevent unauthorized access and protecting the sensitive data.
- Penetration testing involves simulating cyber attack to identify potential security and weakness in networks and ecommerce system.

**8.1 Case Studies and industry Examples**

Several ecommerce companies have experienced high profile cyber incidents,which have highlighted the require for more grounded cybersecurity measures:

Tata Data Breach(2013) : one of the significant ecommerce data breaches, the target breach exposed the credit card data of millions of customers. This breach exhibit the importance of securing payment systems and monitoring third party sellers for exposure.

Alibaba cybersecurity Efforts: Alibaba, a leading ecommerce platform, has contributed intensely in cyber security which includes the development of AI-based fraud detection system to protect the users and merchants on the platform.

Magento Security Flaws: Magento, a popular e-commerce platform, the target of multiple cyber attacks due to security exposure in the open source code. These underline the need for businesses using open source platform to regular security updates and patches.

**9. Limitations**

The scope of cyber security and e-commerce is comprehensive, and this work is limited to its scope as a perspective work. Explorative, qualitative, and quantitative research with a much broader scope is needed to discover other sides of this study.

**10. Conclusion**

Cyber crimes have started to make a fear in the minds of many people connected to the networks mostly worried to ecommerce technology as its success lies in the internet. The various mechanisms used for securing web based transactions or communication can be grouped into´Authorization, Authentication and Integrity ´Privacy ´ Availability by controlling access In order to safe guard the present success of e-commerce. The IT Act 2000 has to be reviewed in order to save India from Cyber criminals and privacy invaders. Cyber criminals should not take the advantages of browser legislative delay, ignorance, judicial inefficiency,enforcement lapse.

**References**

1. I. Bubanja and M. Vidas-Bubanja, “Managing trade transactions in the covid era: The rise of e-commerce,” Journal of Engineering Management and Competitiveness (JEMC), vol. 12, no. 1, pp. 20–34,2022.
2. Statista, “E-commerce in the united kingdom (uk) – statistics facts,” 2022. [Online]. Available: https://www.statista.com/topics/2333/e-commerce-in-the-united-kingdom/#topicHeader__wrapper
3. F. Firouzi, B. Farahani, M. Weinberger, G. DePace, and F. S.Aliee, Iot fundamentals: Definitions, architectures, challenges, and promises. Springer, 2020, pp. 3–50.
4. S. Kuipers and M. Schonheit, “Data breaches and effective crisiscommunication: a comparative analysis of corporate reputational crises,” Corporate Reputation Review, vol. 25, no. 3, pp. 176–197,2022.
5. S. Luo and T. Choi, “E-commerce supply chains with considerations of cyber-security: Should governments play a role?” Production and Operations Management, 2022.
6. Y. Wang and C. Herrando, “Does privacy assurance on social commerce sites matter to millennials?” International Journal of Information Management, vol. 44, pp. 164–177, 2019.
7. Randy C. Marchany, "Tom Wilson. A Keystroke Recorder Attack on a Client/Server Infrastructure", Proceedings of the Network Security '96 Conference.
8. Patrick Thibodeau, "Privacy Concerns Rankle Industry - In Blow to sites" in FTC pushes for regulation, Computerworld, vol. 34, no. 22.