

Chapter 10

Emerging Technologies in E-Commerce Security

Bhavisha Ahuja

*Chitkara University Institute of Engineering and Technology, Chitkara
University, Punjab, India*

Chander Prabha

 <https://orcid.org/0000-0002-2322-7289>

*Chitkara University Institute of Engineering and Technology, Chitkara
University, Punjab, India*

Gunjan Garg

*Chitkara University Institute of Engineering and Technology, Chitkara
University, Punjab, India*

ABSTRACT

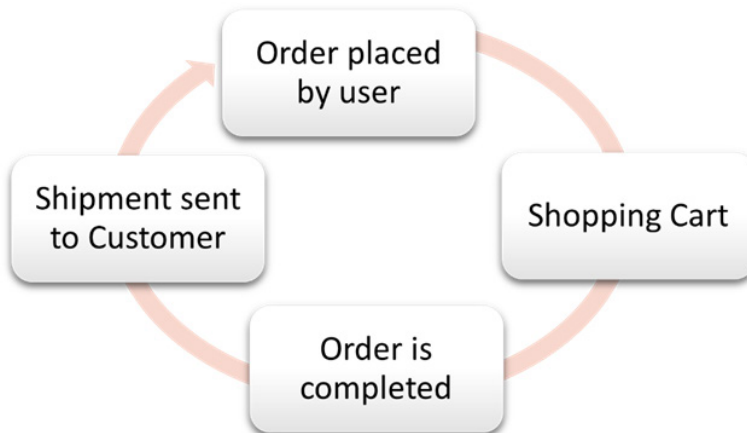
Protecting and Securing the privacy of customers is the most crucial factor for E-commerce companies' growth, since, most transactions occur via online channels. Unfortunately, hackers cause data breaches by getting access to E-commerce platforms and by taking advantage of loopholes in systems and networks. These fissures violate customer privacy and compromise data integrity, thus, leading to mistrust among consumers and retailers. To inactive and reduce these risks to some extent or all; organizations are adopting advanced technologies to enable fraud protection and threat reduction in real-time. Many secure payment gateways are established to protect financial transactions. The encryption of data protects sensitive data. In addition to the above, security layers are added by Multi-Factor Authentication (MFA), and susceptibilities and vulnerabilities are reduced by regular software upgrades and patches. User privacy rules and regulatory compliance also improve security and build customer trust. The chapter explores the emerging technologies for securing E-Commerce in brief.

DOI: 10.4018/979-8-3693-5718-7.ch010

1. INTRODUCTION

Digital technology has changed dramatically in recent years. The term “e-commerce” can be used to represent any online business, it often refers to the sale or purchase of goods online. Although E-Commerce is a familiar concept, however more inclusive than products. It refers to businesses with online banking, online shopping, and other online financial services (Kumain et al., 2020). Online shopping mechanisms include product browsing on e-commerce websites or applications, virtual cart creation, and safe payment gateway completion. Customer feedback, order monitoring, inventory management, and user identification are all part of this procedure, which guarantees customers a simple, easy, and safe online purchasing experience. Figure 1 presents the mechanism for online shopping.

Figure 1. Online shopping mechanism



E-commerce businesses are vulnerable to many security threats that put their lives at risk and lose customer trust, loyalty, and interest. Security issues have increased problems for global e-commerce companies (Shyna, & Vishal, 2017). Because e-commerce impacts consumers through everyday financial transactions with businesses, high-quality security features are essential (Kumar et al., 2020).

Security has become one of the main issues in the modern online world. A few frequent dangers to this online E-Business process include phishing, credit/debit card fraud, money theft, and user data misuse (Saluja, et al. 2022). Table 1 presents various kinds of issues and attacks while using E-Commerce.

24 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/emerging-technologies-in-e-commerce-security/356679

Related Content

A Study on Data Sharing Using Blockchain System and Its Challenges and Applications

Santosh Kumar Smmarwar, Govind P. Gupta and Sanjay Kumar (2023). *Research Anthology on Convergence of Blockchain, Internet of Things, and Security* (pp. 88-107).

www.irma-international.org/chapter/a-study-on-data-sharing-using-blockchain-system-and-its-challenges-and-applications/310441

A Case Study of Effectively Implemented Information Systems Security Policy

Charla Griffy-Brown and Mark W.S. Chun (2008). *Information Security and Ethics: Concepts, Methodologies, Tools, and Applications* (pp. 1727-1740).

www.irma-international.org/chapter/case-study-effectively-implemented-information/23189

Image Encryption Algorithm Based on a Novel 4D Chaotic System

Sadiq A. Mehdi (2021). *International Journal of Information Security and Privacy* (pp. 118-131).

www.irma-international.org/article/image-encryption-algorithm-based-on-a-novel-4d-chaotic-system/289823

Using Statistical Texture Analysis for Medical Image Tamper Proofing

Samia Boucherkha and Mohamed Benmohamed (2008). *International Journal of Information Security and Privacy* (pp. 18-27).

www.irma-international.org/article/using-statistical-texture-analysis-medical/2484

Cross-Layer Based Intrusion Detection and Prevention for Network

Reema Kumari and Kavita Sharma (2018). *Handbook of Research on Network Forensics and Analysis Techniques* (pp. 38-56).

www.irma-international.org/chapter/cross-layer-based-intrusion-detection-and-prevention-for-network/201603