

# **IoT and Cybersecurity: Innovations and Applications**

**Editors :**

**Dr. Rajesh Kumar**

Associate Professor, Department of Physics  
Government Degree College Nanauta,  
Saharanpur (U.P.), India

**Dr. Krishan Kumar**

Assistant Professor, Department of Computer Science  
Gurukul Kangri (Deemed to be University)  
Haridwar (U.K.), India



**Sahitya Sansthan**

Ghaziabad (U.P.) India

ISBN : 978-93-89882-99-5

© : Editors

Price : 1120/-

Accepted Date : 20 August 2025

Publication Date : 05 September 2025

First

Edition : 2025

Publisher : Sahitya Sansthan  
E-10/660 Uttaranchal Colony  
(Near Sangam Cinema),  
Lony Border,  
Gaziabad-201102, India  
Mobile- 09968047183  
email-fatehchand058@gmail.com

**Disclaimer :**

*The responsibility for facts stated, opinion expressed or conclusions reached and plagiarism, if any in this book is entirely that of the author. Neither the publisher nor the editor will be responsible for them whatsoever.*

Lazer : Muskan Computers, Delhi-110094

Printer : Pooja Printers  
Jagatpuri Vistaar, Delhi-110093

---

IoT and Cybersecurity: Innovations and Applications  
Edited By Dr. Rajesh Kumar, Dr. Krishan Kumar

### 3

## **Cyber Security in E-commerce**

---

**Dr. Rajdeep Singh<sup>1</sup>, Dr. Sunil Kumar<sup>2</sup>, Dr. Amit Bhatnagar<sup>3</sup>**

<sup>1,2,3</sup> Assistant Professor, School of Computer Science  
and Applications,

IFTM University, Moradabad, U.P, India.

E-mail: singh.rajdeep1@gmail.com

### **ABSTRACT**

An E-commerce security framework is a comprehensive strategy designed to protect online businesses from cyber threats. It includes the implementation of security protocols, measures, and best practices to safeguard customer data, financial transactions, and overall business operations. As many are aware, weak cyber security is a major contributor to financial losses and a decline in consumer trust within the e-commerce sector. E-commerce refers to the buying and selling of goods and services over the internet, encompassing a range of online commercial transactions. It relies on various technologies, including mobile commerce, internet marketing, online transaction processing, electronic funds transfer, supply chain management, electronic data interchange (EDI), inventory management systems, and automated data collection. Cyber security challenges in e-commerce are growing increasingly severe. For instance, compared to 2022, the rate of cyber attacks on desktop and mobile platforms surged by 35% in 2023. This rise in threats results in diminished customer loyalty and additional costs associated with recovering from the impact of cyber attacks. E-commerce threats typically arise from malicious use of the internet, with the intent to steal, commit fraud, or breach security. These threats can be intentional, accidental, or the result of human error. Common security risks include vulnerabilities in electronic payment