

Recent Innovations in Cyber Security in Retail Sector

Ankur Soni, Associate Professor, Dept. of Management, SunRise University, Alwar, Rajasthan

Abstract

The rapid digital transformation of the retail sector has significantly increased its dependence on e-commerce platforms, cloud computing, mobile applications, Internet of Things (IoT) devices, digital payment systems, and data-driven technologies. While these innovations have improved customer experience and operational efficiency, they have also expanded the cyber-attack surface and created new security challenges. Recent innovations in cybersecurity are therefore becoming essential for protecting customer information, payment data, business systems, and supply-chain networks. Technologies such as artificial intelligence (AI) and machine learning (ML) are increasingly being used to detect abnormal behaviour, identify sophisticated threats, and automate incident response. Zero Trust Architecture provides continuous verification of users, devices, and applications, reducing the risks associated with unauthorized access. Blockchain-based solutions can enhance the integrity and traceability of transactions, while advanced encryption and tokenization help protect sensitive payment and customer data. Additionally, behavioural analytics, biometric authentication, Security Information and Event Management (SIEM), and extended detection and response (XDR) technologies are strengthening real-time threat monitoring. This paper examines recent cybersecurity innovations in the retail sector and discusses their role in addressing emerging threats such as ransomware, phishing, credential theft, payment fraud, and data breaches. It also highlights implementation challenges, including cost, privacy concerns, legacy systems, and the shortage of cybersecurity expertise. The study emphasizes the need for an integrated, proactive, and adaptive cybersecurity framework to ensure secure and resilient retail operations.

Keywords: Cybersecurity, Retail Sector, Artificial Intelligence, Machine Learning, Zero Trust, Blockchain, Data Protection, Cyber Threats, Digital Payments, Ransomware.