Chapter 12
Leveraging AI and ML for Proactive Threat Detection for E-Commerce

Akshay Mudgal
Amity University, Gurugram, India

ABSTRACT

In the fast-paced realm of e-commerce, safeguarding sensitive data is crucial for customer trust and loyalty. Traditional security measures often fall short against evolving cyber threats. Thus, integrating AI and ML technologies enhances data security. AI-powered systems can identify potential breaches in real-time, while ML algorithms improve fraud detection and authentication. AI-driven predictive analytics identify vulnerabilities, and AI-powered chatbots monitor for suspicious activities. Adaptive security frameworks dynamically adjust to evolving threats, ensuring resilience. This strategic collaboration with AI and ML helps e-commerce enterprises secure customer data and maintain a safe digital environment.

1. INTRODUCTION TO ENHANCING E-COMMERCE SECURITY THROUGH AI AND ML

The shift to online transactions is common in this digital era, but e-commerce platforms constantly face scrutiny over data security. AI and ML offer innovative solutions for protecting data integrity. This examination highlights the critical role of data security in e-commerce success. Trust in platforms to safeguard personal and financial data is essential. Data breaches impact more than finances—they affect

DOI: 10.4018/979-8-3693-5718-7.ch012

the platform's reputation and trustworthiness. Data security underpins customer confidence, regulatory compliance, and protection against fraud and identity theft. Robust security mechanisms foster a secure environment, cultivate customer loyalty, and encourage continued engagement (Behgounia & Zohuri, 2020).

1.1. Facts - Data Security in E-commerce

Data security in e-commerce is a complex arena for safeguarding the sensitive data and maintaining trust between consumers and online businesses (Chen, Esperança & Wang, 2022). With cybercriminals such a big threat, e-commerce is one of the areas that targets the most, given the vast amounts of valuable personal and financial information processed daily. A report by the Ponemon Institute states that the average cost of a data breach for businesses, including e-commerce, reached $3.86 million in 2020, emphasizing the financial impact of such attacks.

The domain of e-commerce data security is multi-dimensional, which is quite significant in safeguarding sensitive information and ensuring trust between consumers and online businesses. Here are the highlights of the facts that imprints the importance and complexity of data security in e-commerce:

E-commerce security is crucially guided by regulatory compliance, including GDPR and CCPA, necessitating robust data protection measures and imposing severe penalties for violations. Encryption protocols like SSL and TLS are pivotal for securing data in transit, while Multi-factor Authentication (MFA) adds layers of security for account access. AI and ML technologies play an increasingly significant role in real-time fraud detection, bolstering transaction security. Payment security standards like PCI DSS are mandatory for safeguarding credit card information. Moreover, the damaging impact of data breaches extends beyond financial losses, affecting brand reputation and consumer trust. Regular security audits are imperative to identify and rectify vulnerabilities, while customer education on secure online practices is vital for minimizing breach risks.

An aware understanding of these facts about data security in e-commerce portrays the necessity of a proactive and inclusive approach in protecting sensitive information within the digital marketplace. With the changing cyber threats, strategies will also need to be continuously changed, in order for e-commerce to be safe and trustworthy in consumers worldwide.

The graph presented below demonstrate the drastic increase of online threats and frauds, due to which the online users and shoppers are facing challenges on daily basis.