Chapter 7
Opportunities, Challenges, and Future Directions of Strategic Innovations of AI and ML for E-Commerce Data Security

Djamel Saba
https://orcid.org/0000-0001-7552-3613
URERMS-EPST CDER, Algeria

Abdelkader Hadidi
URERMS-EPST CDER, Algeria

ABSTRACT

In today's digital landscape, E-commerce has become a dominant force in global commerce. As E-commerce platforms collect vast amounts of sensitive customer information, safeguarding this data against cyber threats is paramount. Integrating machine learning (ML) and artificial intelligence (AI) technology has become a viable strategy for improving e-commerce data security in recent years. This paper presents the opportunities, challenges, and future directions associated with the strategic application of AI and ML in bolstering E-commerce data security. The future directions of strategic innovations in AI and ML for E-commerce data security are multifaceted. One key area of focus involves the development of AI-driven adaptive security systems capable of autonomously adapting to emerging threats. Finally, while significant opportunities exist to leverage these technologies for threat

DOI: 10.4018/979-8-3693-5718-7.ch007

detection and mitigation, overcoming associated challenges and pursuing innovative approaches will be essential for safeguarding the integrity and confidentiality of E-commerce transactions.

INTRODUCTION

AI is a broad field with the goal of automating tasks requiring human intelligence (Abdelkader Hadidi, Saba, & Sahli, 2022; Noble & Noble, 2023). Computers can replicate human behavior and carry out operations that usually require human intelligence (Kumar & Mehta, 2023; Djamel Saba, Sahli, & Hadidi, 2022b). AI has become a revolutionary technology impacting various aspects of life, from data analysis to decision-making (Djamel Saba et al., 2022). However, AI also presents challenges such as privacy, security vulnerabilities, and cybercrimes due to its rapid development alongside technologies like 5G and the Internet of Things (Djamel Saba, Sahli, & Hadidi, 2021; Djamel Saba, Sahli, Maouedj, & Hadidi, 2021). While AI processes information rapidly like computers, it is limited in understanding life solely as information processing, unlike organisms that use processing to create objectives and purpose. Therefore, AI's role is significant but must be used cautiously and in alignment with proper scientific principles to maximize its benefits and mitigate potential risks.

AI's Machine Learning (ML) subset allows computers to learn from data without explicit programming (Mohamed et al., 2023). ML involves algorithms that improve their performance based on past experiences or training examples (Delgado De Molina Rius, 2023). It encompasses various approaches, such as supervised, unsupervised, and reinforcement learning, where machines learn from data to make decisions or predictions (Kataria et al., 2022). ML tools and structures are utilized to acquire information from diverse data sources, with deep learning algorithms being particularly effective for solving specific problems. The field of ML is evolving rapidly, with ongoing investigations focusing on topics like adversarial training and federated learning, providing a broad view of current techniques and advancements in the field.

AI and ML technologies are revolutionizing wearable technology, military systems, Electric Vehicles (EVs), and other industries. EVs apply AI and ML to enhance information security through attack prevention, intrusion detection, and authentication (Djamel Saba, Sahli, Maouedj, Hadidi, & Medjahed, 2021). Wearables are benefiting from AI and ML advancements, facing challenges in networking, computational complexity, and training algorithms (Zincir-Heywood, Mellia, & Diao, 2021). Military systems are exploring AI/ML for predictive capabilities, despite data limitations, by leveraging real-time simulation architectures for engine