Chapter 4
Advancing E-Commerce Security:
Strategic Innovations and Future Directions in AI and ML

L. A. Anto Gracious
https://orcid.org/0000-0003-2386-9182
R.M.K. College of Engineering and Technology, India

L. Sudha
SRM Institute of Science and Technology, India

B. Chitra
Panimalar Engineering College, India

Gaganpreet Kaur
https://orcid.org/0000-0002-3322-1315
Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India

V. Sathya
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, India

P. Kabitha
Sathyabama Institute of Science and Technology, India

R. Siva Subramanian
https://orcid.org/0000-0002-7509-9223
R.M.K. College of Engineering and Technology, India

ABSTRACT

The research carried out in this study aims at analyzing the role that AI as well as ML can play in enhancing the approaches to e-commerce data security. It concentrates to basic AI and ML strategies such as anomaly detection, predictive analysis, and advanced threat detection strategies especially in minimizing cyber risks. This

DOI: 10.4018/979-8-3693-5718-7.ch004

paper also covers privacy preservation, legal issues, and pertinent issues of data quality, interpretability, and scalability. Challenges for the future of e-commerce security are explored as the areas of reinforcement learning, federated learning, and utilizing the block chain as the main directions for the future development in this field. The need to emphasize ethical practice in artificial intelligence is demonstrated for the sustenance of equity and open practices. In conclusion, the research clearly identifies AI and ML as critical strategic assets needed to advance secure e-commerce platforms while building and maintaining customers' trust in today's fast-developing environment.

1. INTRODUCTION

1.1 Overview of E-commerce and Data Security Challenges

E-commerce has greatly transformed the business market for consumers where one can easily purchase goods and services via the internet (Gupta, 2014). The increase in technological innovation and the use of the internet in buying and selling processes has significantly expanded the concept of E-commerce all over the world. However, as growth occurs, lots of complexities arise and this is especially true with issues on data security (Taher, 2021). Due to the nature of business that is conducted, including purchase of goods and services, and exchange of personal and financial information, E-commerce platforms are major targets for hackers. E-commerce possibly has several data security meanings that involve the safe guarding of the customer details, protection of transaction data, and guaranteeing that customers get an uncompromised quality shopping from the online platform. Risks to E-commerce platforms include hacking, identity theft, phishing, and DDoS attacks (Sharma et al., 2019). For example, the criminal may be able to crack into the firm's website and procure confidential information from the customers thus resulting to compromise that leads to loss of substantial money and reputation. Among them, it is possible to distinguish the following one: Ever evolving nature of cyber threats. When it comes to the protection of their websites, most e-commerce firms are tightening their belts and introducing more protective measures every year, however, the hackers learn how to get around such measures every new year. Moreover, the growth of other innovative technological areas, such as mobile payments, the use of the Internet of Things (IoT), also added new types of threats. Risk management is important and tricky in e-commerce because of the employments of sites for payments, globalization, and, the conflict between ease of use and security. In addition, the legal requirements or which govern data protection are continually tightening. Controlling possibilities are regulated under legal acts such as GDPR in Europe or concerning