

# Chapter 14

## Strategic Feature Selection Techniques for E-Commerce Application and Data Protection in AI and ML

**Vipin Kumar**

 <https://orcid.org/0000-0002-4610-218X>

*Lovely Professional University, India*

**Mohammad Suleman Quraishi**

*Acharya University, Uzbekistan*

**Vipin Kumar Chaudhary**

*Lovely Professional University, India*

### **ABSTRACT**

*E-commerce applications are widely used in shopping, money transfers, and other purposes. These applications store the user data to provide good results and recommend new products to the user. The user data saved on the server are critical and must provide proper security, safety, and availability. Any attack on these data may damage users' privacy. Machine learning can analyze and detect any attack on these data and applications. A machine learning model uses high-impact features to make a good model and effective prediction. Selecting the most critical data attributes is known as feature selection. Effective feature selection is a vital component in the process of developing a model with a high level of accuracy. This chapter explains the feature selection process and compares different feature selection techniques.*

DOI: 10.4018/979-8-3693-5718-7.ch014

Copyright © 2025, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

*This chapter analyzes filter-matched, wrapper-matched, and embedded methods and their variations. This chapter discussed the essential features concerning the security of e-commerce applications and e-commerce data.*

## **1. INTRODUCTION**

In recent years, the use of the Internet and online shopping has grown significantly, and the usage of other Internet-based resources has become increasingly vital. The company acquired user data through its website. Unfortunately, websites that serve as platforms for e-commerce are among the most appealing targets for cybercriminals. This is because these websites are responsible for the processing of payments and the acquisition of personal information. Several high-profile data breaches have occurred over the many years that have passed. Many diverse methods have been utilized to bring about these breaches. As a straight consequence, the security of websites employed for online commerce has developed into a significant concern for every platform and corporation. If there is a breach in security, the company's brand may suffer damage that cannot be undone, and the faith of the company's customers may be irreversibly lost. Both of these outcomes are possible. Customers believe the corporation will assume responsibility for assuring their safety without any questions or reservations. At the same time that the number of cybercrimes is increasing, there is also a growth in the number of new security threats posed to organizations that carry out their operations online. However, this is a sword with two edges. Online websites facilitating online commerce are responsible for collecting and storing significant user data and information regarding online transactions. These websites gather and store this information, which is responsible for their acquisition. These materials will be of considerable interest to anyone who is participating in activities that are considered to be illegal. The sector saw the most attention if cyber-attacks were carried out against the retail business. This conflict never resolves and is constantly developing in new ways because it is continuous. The reason behind this is that new assault tactics that are both more sophisticated and more advanced are continually being created. This is the reason why situations are the way they are. In addition, the organization is responsible for ensuring the safety and security of the website itself and the safety and security of anybody who uses the website. Implementing reliable security procedures is a precondition that must be met before anything else can be considered when building robust security protocols.

Behavioral analysis is a technique used in cybersecurity that entails monitoring the activities within a system to differentiate between conventional behavior and unusual or abnormal behavior and to discover potential dangers. Traditional ap-

24 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: [www.igi-global.com/chapter/strategic-feature-selection-techniques-for-e-commerce-application-and-data-protection-in-ai-and-ml/356683](http://www.igi-global.com/chapter/strategic-feature-selection-techniques-for-e-commerce-application-and-data-protection-in-ai-and-ml/356683)

## Related Content

---

### Are the Payments System and e-Banking in India Safer than in other SAARC Members?

Rituparna Das (2016). *International Journal of Information Security and Privacy* (pp. 11-25).

[www.irma-international.org/article/are-the-payments-system-and-e-banking-in-india-safer-than-in-other-saarc-members/154985](http://www.irma-international.org/article/are-the-payments-system-and-e-banking-in-india-safer-than-in-other-saarc-members/154985)

### Cryptography-Based Authentication for Protecting Cyber Systems

Xunhua Wang and Hua Lin (2011). *Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering* (pp. 32-51).

[www.irma-international.org/chapter/cryptography-based-authentication-protecting-cyber/46237](http://www.irma-international.org/chapter/cryptography-based-authentication-protecting-cyber/46237)

### A Network Security Transmission Model Based on Improved Sparrow Search Algorithm

Alimire Maimaiti Tuxun and Qingrui Guo (2024). *International Journal of Information Security and Privacy* (pp. 1-17).

[www.irma-international.org/article/a-network-security-transmission-model-based-on-improved-sparrow-search-algorithm/356350](http://www.irma-international.org/article/a-network-security-transmission-model-based-on-improved-sparrow-search-algorithm/356350)

### A Mark-Up Language for the Specification of Information Security Governance Requirements

Anirban Sengupta and Chandan Mazumdar (2011). *International Journal of Information Security and Privacy* (pp. 33-53).

[www.irma-international.org/article/mark-language-specification-information-security/55378](http://www.irma-international.org/article/mark-language-specification-information-security/55378)

### A Retrospective on the Development of Web Service Specifications

Shrideep Pallickara, Geoffrey Fox, Mehmet Aktas, Harshawardhan Gadgil, Beytullah Yildiz, Sangyoon Oh, Sima Patel, Marlon Pierce and Damodar Yemme (2008). *Securing Web Services: Practical Usage of Standards and Specifications* (pp. 22-49).

[www.irma-international.org/chapter/retrospective-development-web-service-specifications/28513](http://www.irma-international.org/chapter/retrospective-development-web-service-specifications/28513)