



The Role of Supervised Learning Algorithms in Fraud Detection for Financial Risk Management: A literature review

Hasna EL MEKKI*¹ and SI Mohamed BOUAZIZ²

*¹ PhD Candidate of Management Sciences. The Faculty of Legal, Economic and Social Sciences of Agadir, Morocco. hasnaelmekki@gmail.com

² Higher Education Professor. The Faculty of Legal, Economic and Social Sciences of Agadir, Morocco. m.bouaziz@uiz.ac.ma

Abstract. Fraud detection is a major challenge in financial risk management, with direct implications for corporate stability and profitability. The application of supervised machine learning algorithms has significantly improved the efficiency of this process. This article examines the roles of various supervised learning methods, such as random forests (RF), support vector machines (SVMs) and artificial neural networks (ANN), on the identification and management of financial risks and the prevention of fraudulent activities. By mining a range of data and identifying complex patterns, these algorithms not only enable faster and more accurate fraud detection, but also significantly reduce financial losses. The article also discusses the challenges of integrating these models into existing systems, and highlights the potential for continuous improvement through machine learning. In conclusion, the adoption of these supervised learning algorithms for fraud detection represents an important step towards proactive and intelligent management, improving organizations' ability to anticipate and manage risk.

Keywords: Fraud Detection, Financial Risk Management, Supervised Learning Algorithms.

1 Introduction

In a highly digitalized economic environment marked by complexity and the constant evolution of threats, both large institutions and small and medium-sized enterprises (SMEs) are increasingly exposed to financial risks, particularly through fraud. According to the Association of Certified Fraud Examiners (ACFE), businesses lose an average of 5% of their annual revenue due to fraudulent activities (ACFE, 2022). Financial fraud is a critical issue in the field of risk management, taking various forms such as accounting manipulation, tax fraud, embezzlement, false financial statements, and fraudulent transactions.

These fraudulent practices can lead to significant financial losses and severely undermine the stability of businesses and financial institutions. Research indicates that the scope of fraud continues to expand due to the increasing sophistication of techniques

© The Author(s) 2025

A. O. Abdellah et al. (eds.), *Proceedings of the International Conference on Multidisciplinary Research in Management and Economics (ICMRME 2025)*, Advances in Economics, Business and Management Research 356,

https://doi.org/10.2991/978-94-6463-892-9_2

used by fraudsters and the growing digitization of financial transactions (Bolton & Hand, 2002; West & Bhattacharya, 2016). In response to this threat, traditional detection approaches, based on manual audits and classical statistical models, have shown their limitations in terms of speed and efficiency (Ngai et al., 2011).

Transformative advances in artificial intelligence, particularly in machine learning, have revolutionized traditional approaches, enabling the development of new, automated, and highly effective technologies that offer more precise tools for identifying and preventing fraudulent activities. Machine learning has profoundly reshaped financial fraud detection strategies (West & Bhattacharya, 2016). In particular, supervised learning algorithms play a crucial role, as they leverage labeled historical data to develop models capable of detecting fraud patterns with high accuracy. Unlike traditional approaches, these models can adapt to emerging forms of fraud by learning from historical data and adjusting their predictions in real time (Baesens et al., 2015). In the context of financial risk management, fraud detection represents a major challenge, relying on the ability to reliably distinguish legitimate transactions from suspicious ones. In this regard, supervised learning algorithms, which utilize labeled historical datasets to classify new transactions, emerge as a promising solution, offering significant potential to enhance the accuracy and efficiency of fraud detection systems. However, several key questions remain unanswered:

- Which supervised learning algorithms are the most effective in detecting financial fraud?
- How does supervised learning represent an advancement in fraud risk management?
- What are the main challenges associated with implementing supervised learning models in financial risk management systems?

The objectives of this study are manifold. This review aims to provide a state-of-the-art analysis of academic research focusing on the role of supervised learning algorithms in financial fraud detection. More specifically, the study first seeks to present the concepts of financial fraud and risk management, along with the fundamentals of machine learning. These technologies offer various possibilities for fraud detection by enabling models to automatically classify suspicious transactions based on patterns learned from labeled historical data, thereby improving the accuracy and speed of fraud identification (West & Bhattacharya, 2016). Supervised learning models, such as random forests and boosting models, can be particularly useful in enhancing the detection of accounting fraud by reducing false positive rates and identifying suspicious behaviors more effectively (Perols, 2011). Additionally, machine learning aids in real-time transaction analysis, allowing for the detection of abnormal behaviors.

This article also aims to conduct an in-depth evaluation of the primary supervised learning paradigms used in fraud detection by highlighting their mechanisms, performance, and practical applications. According to Carcillo et al. (2019), the application of supervised learning techniques improves fraud detection accuracy while reducing false positive rates, making prevention systems more effective and responsive.

Another key objective of this study is to analyze the advantages and limitations of adopting machine learning technologies, particularly regarding data quality, model in-

interpretability, and implementation costs. On one hand, these technologies offer significant benefits, such as improved decision-making through more accurate and faster fraud detection, learning from historical data to identify abnormal behaviors, and continuously enhancing system performance to counter emerging fraud patterns (Chong et al., 2017).

On the other hand, their implementation presents major challenges, including data quality and availability, the risk of algorithmic bias, and the difficulty decision-makers face in interpreting complex models (Baesens et al., 2015).

2 Research Methodology

The methodology adopted is exploratory in nature and relies on an in-depth analysis of academic works and recent research regarding the application of supervised learning algorithms in financial fraud detection. The approach is divided into several key steps: a systematic collection of academic publications and a rigorous selection of articles based on their quality, relevance, and impact on the field. Once the literature was gathered, the studies were synthesized and compared to identify the main methods, significant results, as well as challenges and gaps in existing research. This process allowed for the identification of current trends and best practices in fraud detection while also highlighting possible future direction for improving detection systems, particularly by combining supervised and unsupervised learning techniques.

3 Structure of the article

Through this study, we seek to provide a comprehensive and critical perspective on the development of supervised learning algorithms and their use in fraud detection and financial risk management, shedding light on their strengths as well as the challenges that must be overcome for a more beneficial and effective adoption.

Initially, we propose a conceptual review by defining the fundamental notions of financial fraud and financial risk management while presenting the basics of machine learning. Subsequently, we analyze the main supervised learning approaches applied to fraud detection, highlighting their advantages and limitations. We then delve deeper into the study of factors influencing the performance of these algorithms, as well as the challenges inherent in their implementation within an operational framework. Finally, we explore future developments and challenges, identifying key areas for improvement to enhance the effectiveness of supervised learning models in combating fraud.

Through this literature review, our objective is to provide a critical and in-depth analysis of the application of supervised learning algorithms in financial risk management, emphasizing their potential while underscoring the challenges that must be overcome for a more effective and widespread adoption.

4 Conceptual Review

4.1 Financial Fraud

Financial fraud remains one of the major risks that businesses face, potentially leading to significant consequences both financially and in terms of brand image and reputation. In financial risk management, financial fraud detection has been extensively studied and relies on multiple theories and approaches. Among the fundamental theories, anomaly theory plays a key role in identifying unusual behaviors within a financial dataset, where deviations from normal behavior are perceived as anomalies (Chandola et al., 2009).

In the context of fraud detection, an anomaly is defined as a transaction or action that significantly deviates from expected or routine behavior. By nature, fraud is rare and often distinct from the rest of the observed data. The principle of anomaly theory is based on identifying atypical or rare behaviors within a dataset, as these anomalies are considered potential indicators of unusual events, such as fraud (Iglewicz & Hoaglin, 1993). This anomaly-based approach is particularly useful in machine learning systems, which learn from historical data to establish profile of expected behavior. When new data is processed, the algorithm identifies significant deviations from the established profile, thus highlighting anomalies. Models such as random forests (RF) and support vector machines (SVMs) are commonly used to detect atypical transactions.

A second important theory is fraud network theory, which posits that fraud often arises from relationships and collusions between individuals or entities within a network. Fraud is thus considered a web of connections between different actors. Fraud networks provide an innovative approach to detecting complex fraud patterns by analyzing relationships between the involved entities, thereby enhancing the understanding of fraudulent behaviors and identifying anomalies in interconnected contexts (Embrechts et al., 2013).

The central idea of this theory is that fraud does not occur in isolation but rather through intricate interactions and relationships among various actors within a network. The goal is therefore to identify not only suspicious transactions but also the actors and the links connecting them, allowing for a more systemic and integrated fraud detection approach. This method draws from graph theory, where fraudsters are represented as interconnected nodes within a network, and the interactions between these nodes (transactions, communications, affiliations) help detect suspicious relationships and reveal fraudulent behaviors.

The third theory, supervised learning, is based on the idea that models can be trained on labeled data to reliably predict future fraudulent behaviors (Kou et al., 2004). Neural networks and decision trees are machine learning models that have demonstrated effectiveness in fraud detection by accurately classifying legitimate and suspicious transactions.

The theories applied to fraud detection in financial risk management are diverse, designed to address the complexities of fraudulent behaviors. These three approaches, anomaly detection, fraud networks, and supervised learning complement each other and

enhance the robustness of fraud detection systems and financial risk management. By leveraging deep learning techniques and probabilistic models, they provide powerful tools for improving fraud prevention strategies.

4.2 Financial Risk Management

The concept of risk management is not new, and its techniques have existed for a long time (Doherty, 2000). Over time, it has evolved significantly, moving away from traditional insurance, which is now considered a protection tool that competes with and complements various other risk management methods (Dionne, 2013).

Financial risk management is a constantly evolving discipline, as financial risks and organizations develop in parallel. Its primary objective is to manage risks associated with business activities, particularly credit risk, market risk, and operational risk (Hull, 2018), as well as investment-related risks such as price risk, liquidity risk, and counterparty risk. According to Dionne (2013), risk management offers companies the opportunity to optimize their financial structure. Its ultimate goal remains to maximize a company's value by minimizing costs associated with various risks.

Financial risk management is a field that requires continuous adaptation to new economic and technological dynamics. The literature distinguishes between classical theories, which rely on probabilistic and econometric methods such as Value at Risk (VaR), structural credit models (Merton, 1974), and scoring models (Altman, 1968) and more recent approaches based on artificial intelligence and machine learning, which have significantly transformed financial risk management (Goodfellow, Bengio & Courville, 2016). Fundamentally, machine learning algorithms, such as random forests and support vector machines (SVMs), have led to major advancements in risk management processes and have demonstrated improved capabilities in detecting anomalies and financial fraud (Bolton & Hand, 2002).

Effectively managing risks means being able to anticipate them. By leveraging advanced algorithms, machine learning helps organizations identify and assess emerging risks while taking proactive measures to mitigate their impact more effectively and efficiently. Proactive fraud pattern detection relies on the analysis of transactional behaviors, which is particularly relevant for all organizations, especially small and medium-sized enterprises (SMEs). SMEs are often exposed to market fluctuations (OECD, 2020) and tend to be more vulnerable to financial risks due to their limited resources for risk management (Ngai et al., 2011).

4.3 Machine Learning

4.3.1 Definitions and Principles

Machine Learning is a branch of artificial intelligence that enables computer systems to learn from data and improve their performance without being explicitly programmed (Mitchell, 1997). According to Joshi (2020), it is an artificial intelligence approach that

allows computers to learn from data to solve complex problems without explicit programming. This approach relies on implementing algorithms and statistical models capable of analyzing large volumes of data, identifying recurring patterns, and making predictions based on observations (Dong & Quan, 2024). These algorithms can address classification, regression, and clustering problems. Three main types of learning are distinguished: supervised learning, unsupervised learning, and reinforcement learning (Jordan & Mitchell, 2015).

4.3.2 Supervised Machine Learning

Supervised learning is a method trained on a labeled dataset, meaning that the expected output is already known. The goal is to learn a function that associates inputs with the correct outputs.

A supervised learning model can be trained on a historical dataset containing transactions labeled as either fraudulent or legitimate.

Once trained, the model analyzes variables such as location, time, transaction amount, and payment frequency to recognize fraud patterns and automatically trigger alerts for new suspicious transactions.

According to Ng et al. (2021), the effectiveness of supervised learning methods in fraud detection is largely dependent on the quality and diversity of training data. However, challenges such as data scarcity, model interpretability, and regulatory constraints still hinder their full potential. Future research should focus on improving explainability and integrating hybrid learning approaches to develop more robust fraud detection frameworks.

4.3.3 Unsupervised Machine Learning

Unsupervised learning algorithms analyze data without prior labels or annotations, seeking to identify underlying structures and natural groupings within the data (Jain et al., 1999). Unlike supervised learning, which requires labeled examples to train the model, unsupervised learning processes unlabeled data. The model must discover hidden structures or patterns in the dataset without external guidance. This method is commonly used for clustering or dimensionality reduction, working autonomously to explore similarities, trends, and hidden correlations in datasets.

In financial fraud detection, anomaly detection is one of the primary applications of unsupervised learning. Using clustering algorithms such as K-means or DBSCAN, fraudulent transactions appear as outliers deviating from expected behavior (Chandola et al., 2009). Similarly, Principal Component Analysis (PCA) is a dimensionality reduction technique used to identify influential variables in detecting complex fraud cases (Aggarwal, 2015).

4.3.4 Reinforcement Learning

Reinforcement learning is an approach in which an agent learns to make optimal decisions by interacting with an environment. The intelligent agent receives rewards or

penalties based on the actions it takes, with the goal of maximizing cumulative rewards over the long term. This method, based on a trial-and-error process guided by a reward signal, is particularly useful for complex tasks.

In the context of fraud detection, reinforcement learning can continuously optimize monitoring systems. For example, a Q-Learning or Deep Reinforcement Learning (DRL) model can be trained to classify transactions as fraudulent or legitimate while minimizing false positives and false negatives (Liu et al., 2019).

5 Supervised Learning Algorithms for Fraud Detection

Due to their ability to handle complex and imbalanced data, Random Forests play a significant role in fraud detection. This type of algorithm is based on the aggregation and combination of multiple decision trees, each constructed from a random sample of the training data (Breiman, 2001). The training for each tree is done on a random subset of data, thus enhancing the robustness and accuracy of the model while reducing overfitting (Liu et al., 2008).

In the context of fraud detection, where fraudulent transactions often represent a minority of the data, Random Forests prove to be particularly effective in identifying subtle and non-linear patterns that distinguish fraudulent behaviors from legitimate transactions (Phua et al., 2010). Several previous studies have highlighted the power of Random Forest algorithms in fraud detection compared to other machine learning models, such as logistic regressions or neural networks, particularly in terms of precision and recall (West et al., 2016; Abdallah et al., 2016). Moreover, they offer the advantage of effectively handling heterogeneous variables, whether qualitative or quantitative, thus capturing complex interactions between various risk factors (Bhattacharyya et al., 2011).

Another benefit of Random Forests lies in their ability to reduce errors caused by noisy data or outliers, making them ideal for financial fraud detection (Zareapoor & Leung, 2013). Furthermore, these algorithms can provide transparency regarding important variables, helping to identify the most significant features in fraud detection. This, in turn, promotes the interpretation of results and enables continuous improvement of detection systems.

5.1 Random Forests (RF)

Due to their ability to handle complex and imbalanced data, Random Forests play a significant role in fraud detection. This type of algorithm is based on the aggregation and combination of multiple decision trees, each constructed from a random sample of the training data (Breiman, 2001). The training for each tree is done on a random subset of data, thus enhancing the robustness and accuracy of the model while reducing overfitting (Liu et al., 2008).

In the context of fraud detection, where fraudulent transactions often represent a minority of the data, Random Forests prove to be particularly effective in identifying sub-

tle and non-linear patterns that distinguish fraudulent behaviors from legitimate transactions (Phua et al., 2010). Several previous studies have highlighted the power of Random Forest algorithms in fraud detection compared to other machine learning models, such as logistic regressions or neural networks, particularly in terms of precision and recall (West et al., 2016; Abdallah et al., 2016). Moreover, they offer the advantage of effectively handling heterogeneous variables, whether qualitative or quantitative, thus capturing complex interactions between various risk factors (Bhattacharyya et al., 2011).

Another benefit of Random Forests lies in their ability to reduce errors caused by noisy data or outliers, making them ideal for financial fraud detection (Zareapoor & Leung, 2013). Furthermore, these algorithms can provide transparency regarding important variables, helping to identify the most significant features in fraud detection. This, in turn, promotes the interpretation of results and enables continuous improvement of detection systems.

5.2 Support Vector Machines (SVM)

Support Vector Machines (SVM) are powerful models widely used in financial fraud detection due to their ability to efficiently classify highly noisy and imbalanced data contexts. The principle of this supervised machine learning model is based on maximizing the margin between different classes, which helps reduce the risk of misclassification and improves the model's generalization (Schölkopf & Smola, 2002).

The advantage of SVM algorithms is particularly notable in problems where distinguishing between legitimate and fraudulent transactions is complex and difficult to establish due to the presence of non-linear structures in the data (Zhang et al., 2008). Comparative studies have also demonstrated that SVMs outperform other classical approaches such as logistic regression in terms of precision and recall, especially in large-scale data contexts.

5.3 Artificial Neural Networks (ANN)

Due to their strength and ability to model complex and non-linear relationships in data (LeCun, Bengio & Hinton, 2015), artificial neural networks (ANNs) provide an advanced and effective approach for financial fraud detection. Inspired by the functioning of the human brain, these supervised learning models consist of layers of interconnected neurons that enable the automatic extraction of relevant features from raw data (Goodfellow, Bengio & Courville, 2016).

Thanks to their flexibility and processing power, ANNs are particularly suited to classification problems, especially in contexts where fraud patterns are dynamic and evolving (West & Bhattacharya, 2016). However, these models represent a promising tool for proactive fraud detection and improving financial risk management systems.

Moreover, although these algorithms offer great capacity to capture complex patterns and adapt to dynamic contexts, their effectiveness is highly dependent on the quality and volume of training data, making their application resource-intensive in terms of computational power and processing time (Luo et al., 2021).

6 Comparative Synthesis

Random forests, support vector machines (SVM), and artificial neural networks (ANN) are three major supervised machine learning models widely used in financial fraud detection. Each has its own set of strengths and limitations. Random forests, consisting of an ensemble of decision trees, are appreciated for their robustness against noise, their generalization capacity, and their interpretability, though they may be limited when faced with complex and non-linear relationships in data (Breiman, 2001).

Support vector machines (SVM) offer remarkable performance on medium-sized, balanced datasets, although they become computationally expensive when dealing with large data volumes and require precise tuning of hyperparameters to optimize their performance. As for artificial neural networks (ANN), they are characterized by their ability to automatically extract complex data representations and adapt to evolving fraud patterns. However, they require a substantial amount of data and present challenges in interpretability and computational cost (LeCun, Bengio & Hinton, 2015).

The adoption of the optimal approach largely depends on the data structure, available resources, and interpretability constraints, with each model having specific applications based on the needs of the fraud detection system. In terms of efficiency, random forests and support vector machines are often preferred and adopted for situations where the balance and interpretability of categories are significant concerns.

Discussion

Financial fraud detection is a major challenge for financial institutions and businesses, requiring the adoption of supervised learning models that can efficiently identify suspicious transactions. Among the most commonly used approaches, Random Forests (RF), Support Vector Machines (SVM), and Artificial Neural Networks (ANN) stand out for their performance and distinct characteristics.

Random Forests, based on the aggregation of multiple decision trees, offer robustness in the face of data variations and provide good model generalization (Breiman, 2001). This makes them a relevant choice for fraud detection systems, due to their power to handle complex databases and interpret them effectively. They are very popular, perform well in terms of prediction, and are characterized by relatively simple hyperparameters (Hanafy & Ming, 2021). This explains why this supervised learning algorithm has better predictive performance. However, their effectiveness may decrease when fraud patterns exhibit strong non-linearity, requiring more sophisticated models (Liu et al., 2019).

Support Vector Machines (SVM) maximize the margin of separation between classes to optimize classification accuracy (Cortes & Vapnik, 1995). Their ability to solve classification problems with few examples and their robustness in handling noisy data make them an effective method for fraud detection. However, their implementation is often computationally expensive, especially when the data size increases, and selecting the appropriate kernel remains a major challenge (Bhattacharyya et al., 2011).

Artificial Neural Networks (ANN), particularly Deep Neural Networks (DNN), are capable of extracting complex representations from data and adapting to evolving fraud patterns (LeCun, Bengio & Hinton, 2015). These algorithms are particularly effective in handling large volumes of data, but they come with limitations in terms of computational cost and decision interpretability (Samek et al., 2017).

Overall, the choice of supervised learning model for fraud detection depends on a trade-off between performance, interpretability, and computational cost. Random Forests provide an efficient and easily explainable solution, SVMs excel in well-defined classification problems, while neural networks demonstrate superior potential for recognizing complex patterns, at the cost of greater technical complexity. Combining these approaches, alongside the use of class rebalancing techniques and explainability, presents a promising outlook for strengthening financial fraud detection systems.

Conclusion and Perspectives

Machine Learning techniques have revolutionized risk management across various fields, particularly in financial fraud detection. By enabling a more accurate and rapid evaluation and identification of emerging risks, as well as predictive modeling, machine learning can assist businesses in managing risks more effectively and making better-informed decisions.

This literature review highlights the essential role of supervised machine learning algorithms in financial fraud detection. The article examines various approaches used in this domain. It has been observed that models such as Random Forests, Support Vector Machines (SVM), and Artificial Neural Networks are reactive and adaptive systems, capable of analyzing transactions in real-time and identifying anomalies with high precision. These algorithms leverage historical labeled data to learn how to distinguish fraudulent transactions from legitimate activities, thereby improving the responsiveness and efficiency of detection systems.

The significance of these models lies in their ability to reduce financial losses, enhance transaction security, and automate fraud detection with increased accuracy. However, their implementation comes with its own set of risks and challenges, including bias, lack of transparency, and security issues. Furthermore, the need for quality data, model explainability, and the ever-evolving nature of fraudulent techniques requires continuous algorithm updates.

To address these challenges, multiple avenues for future research can be explored. First, improving existing models by integrating hybrid techniques that combine supervised and unsupervised learning could enhance the detection of emerging fraud. Next, leveraging new data sources, such as real-time behavioral data and information from the web and social media, could enrich predictive models. Finally, integrating these systems into broader risk management processes, in collaboration with domain experts and in compliance with financial regulations, represents a strategic lever to ensure optimal security.

In conclusion, supervised learning algorithms provide a powerful and scalable solution for detecting financial fraud, but their success relies on ongoing refinement an

seamless integration into risk management strategies. Future research should investigate new methods that combine both supervised and unsupervised learning techniques to enhance proactive fraud detection, bolster the resilience of financial systems, and contribute to a safer and more secure financial environment.

References

1. ACFE (2022). Report to the Nations: 2022 Global Study on Occupational Fraud and Abuse. Association of Certified Fraud Examiners.
2. Abdallah, A., Maarof, M. A., & Zainal, A. (2016). Fraud detection system: A survey. *Journal of Network and Computer Applications*, 68, 90-113.
3. Aggarwal, C. C. (2015). *Outlier Analysis* (2nd Ed.). Springer.
4. Altman, E. I. (1968). Financial ratios, discriminant analysis and the prediction of corporate bankruptcy. *The Journal of Finance*, 23(4), 589-609.
5. Baesens, B., Van Vlasselaer, V., & Verbeke, W. (2015). *Fraud Analytics Using Descriptive, Predictive, and Social Network Techniques: A Guide to Data Science for Fraud Detection*. Wiley.
6. Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. *Decision Support Systems*, 50(3), 602-613.
7. Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. *Statistical Science*, 17(3), 235-255.
8. Breiman, L. (2001). Random forests. *Machine Learning*, 45(1), 5-32.
9. Carcillo, F., Le Borgne, Y. A., Caelen, O., Bontempi, G., & Sebban, M. (2019). Combining unsupervised and supervised learning in credit card fraud detection. *Information Sciences*, 479, 448- 460.
10. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys*, 41(3), 1-58.
11. Chong, A. Y. L., Liu, M. J., Luo, J., & Ooi, K. B. (2017). Predicting online fraud victimization: A two-stage model using neural networks. *Industrial Management & Data Systems*, 117(7), 1326-1342.
12. Cortes, C., & Vapnik, V. (1995). Support-vector networks. *Machine Learning*, 20(3), 273-297.
13. Dionne, G. (2013). Risk management: History, definition, and critique. *Risk Management and Insurance Review*, 16(2), 147-166.
14. Doherty, N. A. (2000). *Integrated Risk Management: Techniques and Strategies for Managing Corporate Risk*. McGraw-Hill.
15. Dong, X., & Quan, J. (2024). Advances in machine learning: Trends and applications. *Artificial Intelligence Review*, 57(1), 1-28.
16. Embrechts, P., Puccetti, G., Rüschendorf, L., Wang, R., & Beleraj, A. (2013). Model uncertainty and VaR aggregation. *Journal of Banking & Finance*, 37(8), 2750-2764.
17. Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press.
18. Hull, J. C. (2018). *Risk Management and Financial Institutions* (5th ed.). Wiley.
19. Iglewicz, B., & Hoaglin, D. C. (1993). *How to Detect and Handle Outliers*. ASQC Quality Press.
20. Jain, A. K., Murty, M. N., & Flynn, P. J. (1999). Data clustering: A review. *ACM Computing Surveys*, 31(3), 264-323.
21. Jordan, M. I., & Mitchell, T. M. (2015). Machine learning: Trends, perspectives, and prospects. *Science*, 349(6245), 255-260.
22. Joshi, N. (2020). *Machine Learning and Artificial Intelligence: A Guide for Beginners*. TechPress.
23. Kaelbling, L. P., Littman, M. L., & Moore, A. W. (1996). Reinforcement learning: A survey. *Journal of Artificial Intelligence Research*, 4, 237-285.
24. Kotsiantis, S. B., Zaharakis, I., & Pintelas, P. (2007). Supervised machine learning: A review of classification techniques. *Artificial Intelligence Review*, 26(3), 159-190.

25. Kou, Y., Lu, C. T., Sirwongwattana, S., & Huang, Y. P. (2004). Survey of fraud detection techniques. *Proceedings of the 2004 IEEE International Conference on Networking, Sensing and Control* (Vol. 2, pp. 749-754). IEEE.
26. LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, 521(7553), 436-444.
27. Liu, Y., Li, X., Kwok, J. T., & Zhou, Z. H. (2019). Learning deep forest with multi-layer feature extraction. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 41(7), 1609-1622.
28. Liu, Y., Nath, B., & Kotagiri, R. (2008). Anomaly detection via combining one-class SVMs and PCA. *Australasian Joint Conference on Artificial Intelligence*, 160-170.
29. Luo, X., Liu, Y., Li, X., & Rong, X. (2021). Machine learning for fraud detection: A survey. *ACM Computing Surveys*, 54(2), 1-36.
30. Merton, R. C. (1974). On the pricing of corporate debt: The risk structure of interest rates. *The Journal of Finance*, 29(2), 449-470.
31. Mitchell, T. M. (1997). *Machine Learning*. McGraw-Hill.
32. Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems*, 50(3), 559-569.
33. OECD (2020). *Financing SMEs and Entrepreneurs 2020: An OECD Scoreboard*. OECD Publishing.
34. Perols, J. L. (2011). Financial statement fraud detection: An analysis of statistical and machine learning algorithms. *Auditing: A Journal of Practice & Theory*, 30(2), 19-50.
35. Samek, W., Wiegand, T., & Müller, K. R. (2017). Explainable artificial intelligence: Understanding, visualizing and interpreting deep learning models. *ITG-Fachbericht-Künstliche Intelligenz*, 47(2), 35- 50.
36. Schölkopf, B., & Smola, A. J. (2002). *Learning with Kernels: Support Vector Machines, Regularization, Optimization, and Beyond*. MIT Press.
37. Shabbir, J., & Gardezi, S. J. S. (2020). Artificial intelligence and its role in near future. *arXiv preprint arXiv:2004.01396*.
38. West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. *Computers & Security*, 57, 47-66.
39. Zareapoor, M., & Leung, H. (2013). Credit card fraud detection using transaction behavior. *International Journal of Information and Communication Technology Research*, 5(4), 617-624.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

