Niravkumar Mahendrabhai Panchal, 2025, 13:1
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

A Conceptual Framework for Real-Time Fraud Detection in Digital Banking Through Prescriptive Analytics

Niravkumar Mahendrabhai Panchal
University of Ulster- London

Abstract- The rapid growth of digital banking and FinTech services has increased the risk of cybercrime and online financial fraud. Traditional fraud detection systems often struggle to manage high transaction volumes and sophisticated fraud patterns in real time. This study develops a conceptual framework for real-time fraud detection in digital banking using predictive and prescriptive analytics. The research adopts a positivist philosophy and deductive approach based on secondary data sources. The proposed framework integrates machine learning, artificial intelligence, and automated decision-support mechanisms to improve fraud detection accuracy, response speed, and cybersecurity resilience. The study highlights the importance of intelligent analytics systems in strengthening digital banking security and fraud prevention,

Keywords: Prescriptive Analytics, Digital Banking Fraud, Real-Time Fraud Detection, Predictive Analytics, Artificial Intelligence, Machine Learning, Cybersecurity.

I. INTRODUCTION

Background of the Study

The introduction of digital banking has revolutionised the global banking sector, allowing consumers to make financial transactions online, via mobile application, digital wallet, and instant payment systems. Financial technology (FinTech) has dramatically led the way in bringing digital banking services to fruition, especially for key financial centers like London. Digital banking is growing in popularity among consumers because it is convenient, fast, and easy to use - online financial transactions are now quite high in the world market (Davis et al. 2022). But this digital transformation has also put new exposure to cybercrime and online financial fraud–phishing attacks, ID theft, account takeovers, and unrecognized transactions. As cybercrime becomes more sophisticated, banks and FinTechs have to face greater threats to their security. In the modern banking landscape, advanced technologies are also being tapped to bolster fraud prevention and enhance transaction security.

Problem Statement

Current fraud prevention methods in traditional banking often center on rule-based systems and end-of-transaction analysis, but fail to effectively react to rapidly changing schemes and the 'new fraud' introduced by these methods. Suspicion of such transactions can be undetected for a long time, causing financial institutions large losses, operational problems, and reputational damage (Sokolov et al. 2023). Furthermore, the current systems for fraud detection and prevention struggle to deal with high transaction volume, complex fraud patterns, high false positive rates and real-time decision making. With digital banking transactions rapidly growing, there is an increasing demand for an intelligent and real-time fraud detection model that can incorporate predictive and prescriptive analytics to further boost the accuracy, agility and automated capabilities of fraud detection systems.

Research Aim

This research paper seeks to design and test a conceptual prescriptive analytics model that could be used to detect and trace fraudulent digital banking transactions in real time.

Research Objectives

- To explore existing fraud detection methods in digital banking.

- To learn what the role of predictive and prescriptive analytics will be in relation to fraud prevention.
- To describe and develop a conceptual solution to detect fraud in real time.
- To assess the feasibility and applicability of the framework.

Research Questions

What methods are in use today for fraud detection in digital banking?

In what ways do predictive and prescriptive analytics help in preventing fraud in digital banking?
How to create a conceptual framework that enables real-time fraud detection in digital banking transactions?

What does the efficacy and applicability of a prescriptive analytics-led fraud detection model look like for digital banking?

Significance of the Study

The app is important, mainly because it helps improve fraud prevention methods in electronic banking surroundings and utilizes predictive and prescriptive analytics. The framework proposed could enable banks and FinTech to identify fake transactions as and when they happen, minimize operational losses and improve customer confidence in electronic financial services. Regulators could also gain access to better monitoring systems, which can help them enforce compliance laws pertaining to cybersecurity and anti-fraud (Browne, 2022). On the customer side, the framework could offer better and more secure perceptions when banking online.

Practically, the study adds to the body of analytics-driven fraud detection research by incorporating concepts on real-time decision-making and prescriptive analytics to digital banking security, thereby helping facilitate the field's convergence with business practice. Academically, this is important because it brings practical ideas of real-time decision-making and prescriptive analytics into the world of digital banking security and contributes to the existing literature on analytics-driven fraud detection. The study further contributes to the emerging body of research on the application of AI and machine learning in the contexts of financial risk management and cybersecurity. Moreover, these conceptual props may build up the basis for upcoming empirical studies and advancements in technological development in the realm of intelligent fraud detection systems.

Structure of the Paper

This paper is written in the IMRAD style. This is the introductory section of the research, which introduces the background and objectives of the research and its significance. Research design and research process to develop the conceptual framework are described in the Methods section. The Results section relates to the findings and the next proposed results in the framework, and the Discussion interprets the results, implications, limitations and future research paths that have been followed.

II. LITERATURE REVIEW

Previous Studies on the Topic

The increasing adoption of digital banking and financial technology (FinTech) has significantly transformed financial services while simultaneously increasing exposure to cyber threats and fraudulent activities. Previous studies have highlighted that traditional fraud detection systems, which rely heavily on rule-based mechanisms and post-transaction analysis, are often inadequate for identifying sophisticated and rapidly evolving fraud patterns in real time (Sokolov et al., 2023). As digital transactions continue to grow, researchers have increasingly focused on advanced analytics, artificial intelligence (AI), and machine learning (ML) techniques to enhance fraud detection capabilities.

Davis et al. (2022) demonstrated that explainable machine learning models can improve the accuracy of risk assessment and transaction monitoring in financial services. Similarly, Shiao et al. (2022) found that machine learning algorithms can effectively identify anomalous customer behaviour and suspicious transaction patterns, reducing false positives and improving fraud detection accuracy. Malhotra and Malhotra (2023) further argued that

big data analytics and AI-driven decision-making are reshaping financial services by enabling predictive insights and faster responses to potential risks.

Theoretical Framework

This study is grounded in the Analytics Continuum Theory, which explains the progression from descriptive analytics to predictive analytics and ultimately prescriptive analytics. Predictive analytics uses historical and real-time transaction data to forecast potential fraud risks, while prescriptive analytics recommends optimal actions to prevent or mitigate those risks (Witzany & Fičura, 2023). The framework is further supported by Technology Adoption Theory, which suggests that organisations adopt innovative technologies when they provide measurable operational benefits, such as improved security, efficiency, and decision-making capabilities (Malhotra & Malhotra, 2023). Together, these theories provide a foundation for understanding how analytics-driven systems can strengthen fraud prevention in digital banking environments.

Research Gap

Although existing literature extensively discusses machine learning, predictive analytics, and AI-based fraud detection systems, limited research has explored the integration of prescriptive analytics into real-time digital banking fraud prevention frameworks. Most studies focus on predicting fraudulent activities rather than recommending automated responses to emerging threats (Davis et al., 2022; Shiao et al., 2022). Furthermore, there is insufficient conceptual research examining how predictive and prescriptive analytics can work together to support intelligent, real-time decision-making in banking systems. This gap highlights the need for a comprehensive framework that combines fraud prediction, automated response mechanisms, and continuous learning capabilities.

Conceptual Framework

The proposed conceptual framework integrates transaction monitoring, predictive analytics, machine learning algorithms, and prescriptive analytics into a unified fraud detection system. Transaction data are continuously analysed to identify anomalies and generate fraud risk scores. Based on these predictions, the prescriptive analytics component recommends appropriate actions, such as transaction approval, additional authentication, temporary account suspension, or fraud investigation alerts. This integrated approach is expected to enhance fraud detection accuracy, reduce response times, and strengthen cybersecurity resilience within digital banking environments.

III. METHODS

Research Philosophy

The research philosophy used for this study is a positivist research philosophy; that is, the research assumes that the algorithm or system of fraud detection in digital banking can be investigated directly, it accepts the results that are obtained as true facts, and it analyzes the algorithm or system of fraud detection in digital banking in a scientific way and has measurable results. The positivist approach will be suitable for research where the subject relates to technology because it focuses on the facts, statistics of the subject and model analysis (Lommers et al. 2021). A combination of transaction patterns, machine learning methods and prescriptive analytics frameworks that can measure and evaluate transaction patterns systematically is considered in this study when it comes to fraud detection. The philosophy encourages applying authoritative secondary data from academic articles, banking records and continuously updated cybersecurity reports to build a coherent and evidence-based concept to aid real-time fraud detection.

Research Approach

The study adopts a deductive method where existing theories, models and concepts related to fraud detection, predictive analytics and prescriptive analytics in digital banking are used. The deductive method will be used to analyse whether analytic technologies can enhance the real-time fraud prevention and decision-making process (Malhotra & Malhotra, 2023). Current literature and technological frameworks are discussed to delineate the gaps of the existing fraud detection systems for conceptualization of the framework. This method will be suitable because it will enable the research to validate the theoretical assumptions made about

analytics-based fraud prevention and to assess the ability of prescriptive analytics to boost banking fraud detection efficiency.

Research Design

This study uses a conceptual and analytical research design to create the framework for real-time fraud detection in digital banking. The conceptual design aims to create a technical framework that brings together ideas of fraud analysis, machine learning, logical components, and automated mechanisms to support decisions. The analytical part of the design includes a discussion of the technologies and systems currently used for the detection of fraud in banks and the applications of prescriptive analytics. The suitability of the design is explained since the study takes the approach to develop a theoretical framework as opposed to experimental testing. The framework uses predictive analysis, recording unusual and out-of-the-ordinary transactions, transaction monitoring, and automated responses to effectively identify and attack fraudulent banking activity in real-time.

Data Collection

This study utilizes secondary data collection techniques with the aim of obtaining relevant data on digital banking fraud, analytics technologies and frameworks that help to prevent digital banking fraud. Secondary data is gathered from published academic journals, cybersecurity-related publications and reports from the banking industry, government reports, and online databases, including Google Scholar, Science Direct, etc. Secondary data use is beneficial for enabling the researcher to explore existing knowledge, technology and industry practices on fraud detection systems (Borkar & Jadhav, 2024). This is the method that can be used at less cost, and it is used for conceptual research to get access to a wide range of credible sources. The aggregated information is used to build and test proposed mechanisms for detecting fraud.

Data Analysis

The research adopts qualitative analytical approaches to analyze the literature and technological models associated with digital banking fraud detection. Thematic analysis is used to analyse information generated from the secondary sources, and to observe the main issues, trends, and potential applications for predictive and prescriptive analytics in fraud prevention. Analysis concentrates on transaction monitoring systems, machine learning algorithms, anomaly detection systems of anomalies, and automated decision-making processes of decisions. The performance and efficacy of traditional fraud detection systems and advanced analytics-based systems are also compared. The results of the analysis could be used to help develop the proposed conceptual framework for real-time fraud detection.

Ethical Considerations

Data privacy, customer confidentiality, and regulatory adherence, like the GDPR, are highlighted in the research (Lopez de Prado & Fabozzi, 2020). In addition, ethical implications of artificial intelligence and machine learning use in banking systems for maintaining fairness, transparency and accountability in automated decisions are also taken into account as part of the study. This is because algorithm bias and algorithmic discrimination are viewed as major issues in fraud analytics systems. In addition, secondary sources cited in the study are appropriately referenced to ensure academic propriety and avoid plagiarism.

Limitations of the Study

There are some limitations of the study that may limit the generalisation of the results. The research does not have as its aim a practical implementation or actual testing in real time of the proposed framework to detect fraud, but rather a conceptual one. Second, the study is unable to access live banking transaction information for empirical validation of the framework, due to privacy and security restrictions. Thirdly, the research is mainly based on secondary data sources like academic papers, industry reports and cybersecurity publications. Availability and quality of these information sources could affect the accuracy of the results.

IV. RESULTS

Findings from Existing Literature

Due to online banking and FinTech having grown so quickly, digital banking fraud has become much more prevalent. Cybercriminals are exploiting vulnerabilities in the digital financial system with ever more sophisticated tools like phishing, identity theft, card fraud, malware attacks and account takeover fraud (Bañado et al. 2025). It is estimated that financial institutions incur huge financial losses, incur operational changes and have suffered from reputational damage as a result of fraudulent activities. The growth of the number of real-time payment products and systems and apps for mobile banking has also brought a growth in fraud risk. Studies highlight the need for more sophisticated anti-fraud tools that can halt transactions and alert customers that might otherwise be scams, to bolster banking cybersecurity measures.

Role of Predictive Analytics in Fraud Detection

One of the significant advantages of predictive analytics in digital banking fraud detection is its ability to detect suspicious transaction patterns and to determine the risk of fraud before it causes financial losses. Historical transaction data, customer behaviour and transaction trends are analyzed using predictive systems to detect abnormal activities. The process of assigning fraud probability scores to transactions according to certain data-driven requirements is usually done using risk scoring systems, which employ machine learning models and data points. The ML classifications are very accurate as they help detect abnormal transaction behaviour using techniques like Decision trees, Support vector and neural networks (Shiao et al. 2022). Predictive analytics helps banks to track the volume of transactions efficiently and helps to spot potentially fraudulent transactions in real time.

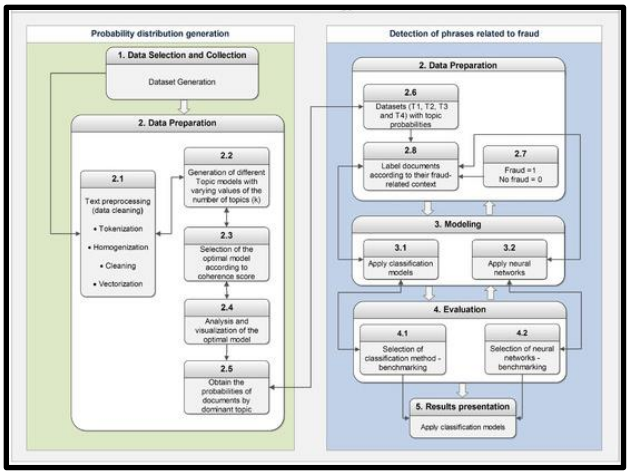

Figure_1: Predictive Fraud Analysis (Source: https://www.mdpi.com/2076-3417/12/7/3382)

Importance of Prescriptive Analytics

Prescriptive analytics is significant because it goes beyond predictive analytics; it offers actionable recommendations and automated answers to any abnormal banking actions. Predictive Analytics can provide a measure of the likelihood of the fraud occurring, and Prescriptive Analytics can provide a definition of what the best action is to take to help determine if the fraud will happen, and if it does, which steps should be taken to minimise the risk. Prescriptive systems can assist in intelligent decision-making by making recommendations based on the information available, such as the need for additional authentication, a temporary account suspension, or an alert for a fraud investigation. The capabilities for real-time intervention enhance fraud prevention processes' effectiveness and speed (Witzany & Fičura, 2023). By incorporating AI and Machine Learning, prescriptive analytics systems become more self-learning and continually optimized at detecting fraud.

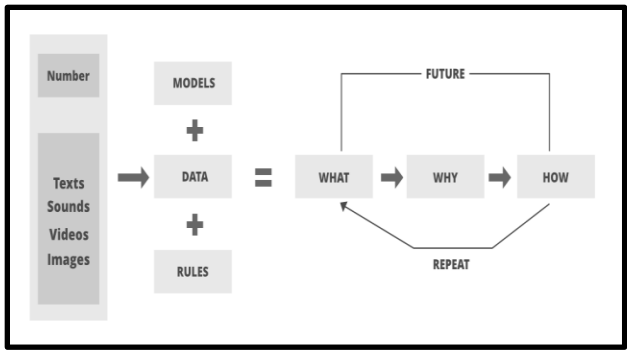

Figure_2: Prescriptive Analytics
(Source: https://www.geeksforgeeks.org/data-science/what-is-prescriptive-analytics-in-data-science/)

Proposed Framework Outcomes

The proposed fraud detection system is anticipated to enhance the effectiveness and accuracy of fraud prevention in digital banking systems. The framework can analyze the data to identify any unusual transaction patterns as they happen, using predictive analytics, machine learning and real-time monitoring capabilities. It also seeks to decrease the number of fraudulent alerts that can be responsible for preventing legitimate activities of customers from being processed, and cause a significant increase in expenses for banks. The framework implementation can help to raise response and reduce the time spent in fraud detection and decision-making processes. The improved cybersecurity being achieved and ongoing customer trust are also being anticipated as customers are increasingly likely to utilise digital banking services when they feel that their transactions and customer information are secure.

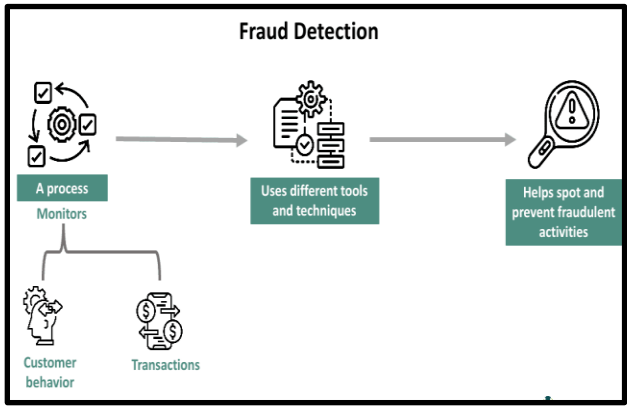

Figure_3: Fraud detection system

(Source: https://www.wallstreetmojo.com/fraud-detection/)

Expected System Workflow

The system's workflow in the proposed solution starts with a customer who initiates a digital banking transaction via a web portal or application. It instantly stores all the transaction data, customer behavioural habits, device and location information for later analysis. A machine learning algorithm and setting up the predictive analytics engine's rules for anomaly detection are used to determine the probability of fraud (Leung et al. 2021). The prescriptive analytics engine analyzes fraud risk score and determines the best possible response. The system could approve the transaction, require further authentication, temporarily block the transaction, or alert the fraud investigation team to review the transaction. This process can facilitate rapid and smart fraud prevention in real time.

Benefits of the Framework

The proposed framework provides various technical and business advantages for digital banking institutions. In terms of technology, the framework enables quicker detection of fraud as real-time data analysis and fraud alerts can be set to yellow/green flags for immediate identification. Adaptive learning capabilities through machine learning and artificial intelligence give the system time to learn and sensorially become more accurate in fraud detection, as new transaction patterns develop and new threats emerge. Real-time monitoring also improves the effectiveness of banking cybersecurity systems by minimizing response times and shutting off any potential financial activities when unauthorized.

From a business standpoint, the system can safeguard against fraud and cyberattacks that could lead to undesirable monetary results. Automatized fraud detection systems can reduce operation-related expenses for manual investigations and false positive alerts (de Prado, 2022). Better fraud protection can lead to greater customer satisfaction and thus improve customers' digital banking experience.

Potential Challenges Identified

The fact that it can have great benefits does not mean the proposed concept for fraud detection is easy to implement. The high cost of embedding all the advanced analytics technologies, artificial intelligence systems and real-time monitoring infrastructure into existing banking functions is one of the challenges. Some technical challenges and compatibility problems might arise due to integration with legacy banking systems. The accuracy of fraud detection models can be impaired in the event of incomplete or inaccurate transaction records in the data pipeline, known as Data Quality Issues. Fraud analytics systems also process sensitive customer data, posing privacy and data protection challenges (Ekster & Kolm, 2021). Moreover, inaccurate campaign scoring and false positive alerts can have a detrimental effect on the user experience and decrease in customer satisfaction with this automated fraud detection process.

Comparative Analysis

The proposed prescriptive analytics framework has enormous advantages over traditional fraud detection systems in terms of factors such as speed, accuracy, automation, scalability, and decision-making efficiency. Traditional systems mostly rely on rules-based approaches and post facto analyses, and tend to have high false positive rates and late fraud detections. The proposed framework, on the other hand, employs predictive and prescriptive analytics techniques to track transactions in real-time and offer automatic solutions in cases of suspicious behavior. Additionally, it is a more scalable solution as machine learning algorithms can effectively handle a large volume of transactions. Additionally, intelligent choices and support systems enhance productivity and also fortify financial institutions' cyber safety and security measures by supplying quick and accurate fraud avoidance capabilities.

V. DISCUSSION

Interpretation of Findings

The results of this study suggest that using prescriptive analytics to make informed, information and intelligence-based decisions can have a noticeable impact on the effectiveness of fraud detection in digital banking, offering an additional proactive way to manage and prevent fraud. Prescriptive analytics allows banks to anticipate and recommend real-time action for possible fraud scenarios in ways that are far more proactive than traditional methods (Chakrabarti et al. 2025). All these functions combine to enable banking systems to continuously analyze transaction patterns and accurately detect abnormal behavior. This can decrease response time, limit losses and enhance decision-making in the process of suspicious transactions.

The research also points to the fact that using predictive and prescriptive analytics is a means of bolstering bank Cybersecurity frameworks by improving fraud prevention practices. Embedded monitors and automated decision support systems enhance operational efficiencies, and the reliance on manual investigation practices is reduced. In addition, adaptive learning functions enhance fraud detection mechanisms to better adapt to new forms of fraud. Incorporating advanced analytics technologies offers a more intelligent, efficient way to bolster digital banking security and fraud prevention in today's financial world, as revealed by these findings.

Implications for Digital Banking

The digital banking ecosystem, which comprises financial institutions, customers, and regulators, has several significant implications to take into account from the proposed fraud detection framework. Financial institutions can use predictive and prescriptive analytics to enhance operational efficiency by replacing manual fraud detection efforts with automation and diminishing the manual monitoring workload. Real-time fraud detection systems also help fortify their cybersecurity defence capabilities by immediately identifying abnormal transactions and blocking unauthorised access to their client portfolios.

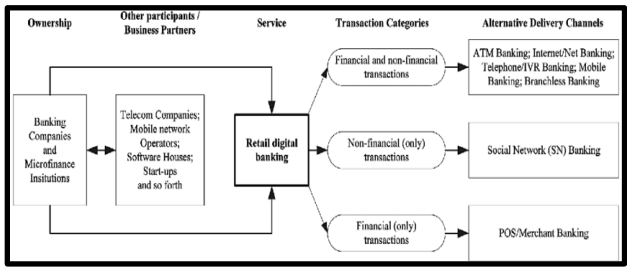

Figure_4: Digital banking ecosystem
(Source: https://www.researchgate.net/figure/Digital-banking-ecosystem_fig1_297730887)

Advanced fraud detection technologies help regulators in compliance monitoring and bolster anti-money laundering (AML) and fraud prevention policies. The banking sector could provide regulatory bodies with greater transparency of transactions, risk assessment and better protection for digital financial services.

Theoretical Implications

The research undertaken and achieved in this work builds on the current stream of work in both fraud analytics and digital banking security by combining predictive and prescriptive analytics into a real-time fraud detection system. Research advances the theory of using advanced analytics technologies to increase financial institutions' decision-making and fraud prevention capabilities. Furthermore, the findings of the study underscore the need for embracing technology according to the different technologies adopted and implemented in Financial Services (FinTech) environments. Finally, the research helps to reinforce theories of technology adoption in various technology domains in banking by illustrating the increasing significance of artificial intelligence, machine learning and automated analytics systems in financial services nowadays. Moreover, it offers a theoretical underpinning for future research into the development of intelligent fraud detection models and analytics-driven cybersecurity solutions.

Practical Implications

The suggested framework provides useful advantages for banks, FinTech service providers, and payment service providers, aiding in intelligent and automated fraud recognition processes. By leveraging real-time analytics, banks can optimize business operations, including rapid fraud detection and fast response, and make more informed decisions (Tilly et al. 2025). The framework can also be designed to gain a way to lessen the costs and effort in manual fraud tests and false positive alerts. The framework can be customized by commercial banks and payment firms for their transaction systems and cybersecurity needs. Plus, the addition of machine learning and prescriptive analytics can help in providing scalable fraud prevention measures to enhance the security for the users and preserve the customer trust in digital banking environments.

Future Research Directions

Further investigation is required to empirically test the proposed framework by using banking transaction datasets with live use to assess the relevance and reliability of the framework in actual use cases. Researchers could also focus on creating hybrid AI algorithms that integrate machine learning, deep learning, and behavioural data analysis for enhanced fraud detection. Another crucial area is the use of blockchain with a prescriptive analytics environment to further increase the transparency and security of transactions. Further research may also address cross-border fraud detection issues, ethical issues regarding the use of AI in decision-making, and issues of scale and the ability of real-time fraud prevention systems to function effectively in a digital banking setting on a global scale.

REFERENCES

1. Bañados, D., Japke, M., Canessa, E., & Atkinson, J. (2025). Combining Prediction Models and Multiagent Systems for Automated Financial Trading. Journal of Financial Data Science, 7(1). https://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=26403943&AN=183116702&h=IBm16W868uDOYhFkZswZiKMpBsuZ%2FXGVqtaWUeY%2FJVZWUmJZ%2F5PZAWmR8zjGAksn10uX4rR9nHI726b8%2Fc9UdA%3D%3D&crl=c
2. Borkar, S., & Jadhav, A. (2024). Reinforcement Learning Techniques for Stock Trading: A Survey of Current Research. Journal of Financial Data

Science, 6(3). https://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=26403943&AN=179072220&h=D%2FyH5tXkm6e4mcXFNgKf1RBNZRspVEIhsUTUooSTJI4hcWbAApfR2zOht%2FO1tEEM5n1vhjjDq%2BA7pzLQVBUHmw%3D%3D&crl=c

3. Browne, S. (2022). Gains and Losses Revisited: Skill Detection and Similarity Assessment. Journal of Financial Data Science, 4(4). https://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=26403943&AN=169649437&h=cT1Wgt8AFk689EibH720XO1Je9nLrA097pNZ5iY344MsLLW6RZ3HNyfrt86J0ms%2F%2Ft4o0dG%2Fi0AvjeymiE8OgQ%3D%3D&crl=c
4. Chakrabarti, M., Fabozzi, F. J., Narain, A., & Sood, A. (2025). Ethical AI in Asset Management: Frameworks for Transparency, Compliance, and Trust. Journal of Financial Data Science, 7(1). https://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=26403943&AN=183116697&h=PUH%2F27yFf0Bskd0ff%2FjL8fz0h2cOl30x%2BKNxW0DoQFt69Pp4%2BN8L5H451ST11dIh9598K9CCdsesOOsvEFzgow%3D%3D&crl=c
5. Davis, R., Lo, A. W., Mishra, S., Nourian, A., Singh, M., Wu, N., & Zhang, R. (2022). Explainable machine learning models of consumer credit risk. Available at SSRN, 4006840. https://www.garp.org/hubfs/Whitepapers/a2r5d000003s85tAAA_RiskIntell.WP.MLModels.Feb24.22.pdf
6. de Prado, M. L. (2022). Machine learning for econometricians: The readme manual. The Journal of Financial Data Science, 4(3), 10-30.https://openurl.ebsco.com/fulltext/gcd:169649296?sid=ebsco:plink:crawler-gcd&id=ebsco:gcd:169649296&crl=f&jrnl=26403943
7. Ekster, G., & Kolm, P. N. (2021). Alternative data in investment management: Usage, challenges, and valuation. The Journal of Financial Data Science, 3(4), 10-32.https://smallake.kr/wp-content/uploads/2021/01/SSRN-id3715828.pdf
8. Leung, E., Lohre, H., Mischlich, D., Shea, Y., & Stroh, M. (2021). The promises and pitfalls of machine learning for predicting stock returns. Available at SSRN 3546725.https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=3546725
9. Lommers, K., Harzli, O. E., & Kim, J. (2021). Confronting machine learning with financial research. arXiv preprint arXiv:2103.00366. https://arxiv.org/pdf/2103.00366
10. Lopez de Prado, M., & Fabozzi, F. J. (2020). Crowdsourced investment research through tournaments. Journal of Financial Data Science, 2(1). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3459806
11. Malhotra, R., & Malhotra, D. K. (2023). The Impact of Technology, Big Data, and Analytics: The Evolving Data-Driven Model of Innovation in the Finance Industry. Journal of Financial Data Science, 5(3). https://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=26403943&AN=169990127&h=ruyH7wlDW7HLEY25KKM3AmfwqKW6he%2Biv12bJZpIY%2Bz5WR0l2kzytO8A0Lukt6mh6x2SuYCd5kj8ds%2Boj8qa5Q%3D%3D&crl=c
12. Shiao, H. T., Pagliaro, C., & Mehta, D. (2022). Using Machine Learning to Model Advised-Investor Behavior. Journal of Financial Data Science, 4(4). https://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=26403943&AN=169649436&h=ua6PQv4L%2BF7PoFI6sIhW8rssIWpw%2BZf96QGxxUJ7JhJ1623xiViTp8C4d7%2FbBzAGr8ycXuZCK08AfdYgdz2%2Ffg%3D%3D&crl=c
13. Sokolov, A., Kim, J., Parker, B., Fattori, B., & Seco, L. (2023). RIFT: Pretraining and Applications for Representations of Interrelated Financial Time Series. Journal of Financial Data Science, 5(4). https://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=26403943&AN=173644433&h=%2FJgNxNgNMn%2BSlbjcgT55J4lWht8TUsRYiuvYGXOm6JtpN0xLDuW4JBTDmvCXHMyeSP4%2Blmw85151k526TKxdaw%3D%3D&crl=c
14. Tilly, S., Amri, I., Le Guenedal, T., Sakout, S., & Sekine, T. (2025). Leveraging AI Tools for Novelty Detection in News Narratives. Journal of Financial Data Science, 7(3).

https://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=26403943&AN=187367258&h=GuwTrxLGGWb448wXpVn8uuYd18DaB9RcG6qbyu7paRWTUTV9VCDXLW7MBoWhRdrL8msutYni0GrlybT4rks85g%3D%3D&crl=c

15. Witzany, J., & Fičura, M. (2023). Machine learning applications for the valuation of options on non-liquid option markets. Faculty of Finance and Accounting, University of Economics. https://quantitative.cz/wp-content/uploads/2023/05/machine_learning_applications_for_the_valuation_of_options_on_non-liquid_option_markets.pdf