INTERNATIONAL JOURNAL OF MANAGEMENT AND ORGANIZATIONAL RESEARCH

# Predictive Analytics in Fraud Detection

**Matthew NO Sadiku [1*], David Padi [2], Janet O Sadiku [3]**
[1] Roy G. Perry College of Engineering, Prairie View A&M University, Prairie View, TX 77446, USA
[2] Alumnus Graduate School of International Business and Leadership, Midwest University, Wentzville, Missouri, USA
[3] Juliana King University, Houston, TX, USA

* Corresponding Author: **Matthew NO Sadiku**

## Article Info

**ISSN (online):** 2583-6641
**Impact Factor (RSIF):** 8.56
**Volume:** 05
**Issue:** 03
**May-June 2026**
**Received:** 25-02-2026
**Accepted:** 27-03-2026
**Published:** 29-04-2026
**Page No:** 16-23

**Abstract**
Predictive analytics is a powerful data-driven technique that leverages data, algorithms, and machine learning to identify the probability of future outcomes based on historical data. It represents a paradigm shift in the fight against fraud. It is an invaluable tool that has begun revolutionizing the world of fraud prevention. By transforming data into actionable intelligence, it empowers organizations to anticipate threats, streamline operations, and protect their assets with unprecedented precision. Predictive analytics in fraud detection have revolutionized the way financial institutions preemptively address and mitigate cyber threats, reducing the incidence of breaches and saving millions in potential losses. By examining historical data, such as transaction records, customer behavior, and external economic indicators, predictive models can identify anomalies that deviate from typical patterns. In this paper, we examine the multifaceted impact of predictive analytics on the fight against fraud or deceitful online activities.

**DOI:** https://doi.org/10.54660/IJMOR.2026.5.3.16-23

**Keywords:** Data, Data Analytics, Predictive Analytics, Artificial Intelligence, Fraud, Fraud Prevention, Fraud Detection, Predictive Fraud Analytics

## 1. Introduction

Fraud is a global problem that affects nearly every industry. It is the act of deliberately deceiving someone to gain an unfair or unlawful advantage, often for financial or personal benefit. It usually involves false representation, concealment of facts, or abuse of trust to mislead individuals, organizations, or systems. Fraud can occur in many forms, such as financial fraud, identity theft, insurance fraud, or corporate misconduct, and often results in harm to victims, whether through financial loss, reputational damage, or compromised data. Fraud can lead to significant financial losses, erode customer trust, and damage an organization's reputation. It can also result in legal repercussions, such as fines, lawsuits, and regulatory penalties. Fraud detection through predictive analytics has become a critical defense mechanism in today's digital landscape. Predictive analytics plays a transformative role in fraud detection and prevention by enabling organizations to identify, predict, and respond to fraudulent activities with greater precision and speed [1].

In an increasingly digital world, the sophistication and volume of fraudulent activities have reached unprecedented levels. Fraudsters are constantly evolving and finding new ways to get around the systems to commit fraudulent activities. Businesses today must protect against ever-growing, evolving fraud threats. They need advanced solutions to stay ahead of fraudsters. Traditional fraud detection methods, such as manual audits and investigations, have limitations in speed, accuracy, and scalability. Businesses need to rely on advanced techniques powered by predictive analytics. Predictive analytics uses historical and current data to make predictions through statistical modeling, data mining, and machine learning algorithms. It is a crucial component of predictive fraud analytics, a type of data analytics that uses current and historical data to forecast activity, behavior, and trends [2].

Fraud detection using predictive analytics is especially beneficial to businesses because it is a proactive approach that evolves with fraud tactics rather than just reacting to them. Predictive analytics fraud detection now plays a critical role in identifying and reducing these risks for companies across industries – from financial services to insurance to retail. To identify fraudulent behavior, predictive analytics combine statistical algorithms, data mining, and artificial intelligence to uncover patterns and anomalies that signal potential fraud. Companies use predictive fraud analytics to save millions of dollars, enhance security, and improve customer trust [3].

The study adopts a quantitative research methodology to examine the role of predictive analytics in the detection of fraudulent transactions. The goal is to examine how predictive analytics can be used to detect, prevent, and reduce fraud by identifying unusual patterns, high-risk transactions, and suspicious behavior. It will then lead to identifying how effectively predictive analytics can identify fraudulent activities, reduce financial losses, and support faster decision-making.

## 2. Literature Review.

### 2.1. Predictive Analytics

As its name implies, predictive analytics is about predicting future trends, such as sales demand, exchange rates, and other important metrics. The technique relies on applying statistical modeling and regression analysis to historical data to determine and understand trends and to formulate future trends. Strictly speaking, predictive analytics does not predict the future but rather uses probability theories to determine what is likely to happen based on patterns and trends revealed by analyzing historical data [4]. Predictive analytics accurately anticipates customer demand, preventing overstocking and stockouts while adapting to market changes. Figure 1 illustrates predictive analytics [5], while Figure 2 shows its components [6].


**Fig 1:** Predictive analytics [5].

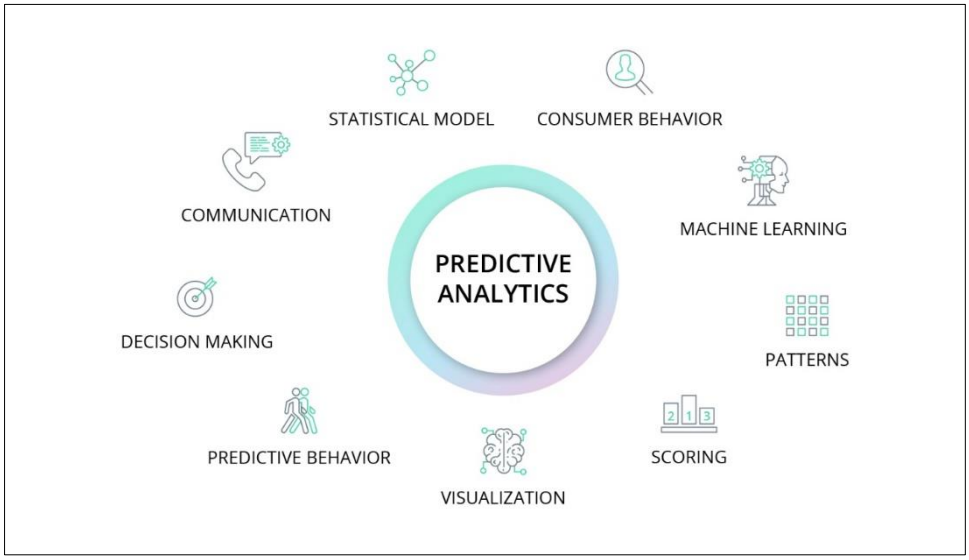


**Fig 2:** Different components of predictive analytics [6].

In general, analytics provides an efficient way to improve planning by giving you better forecasts. There are different types of data analytics.

They are briefly explained as follows [7]:

Descriptive analytics focuses on analyzing what has occurred over time within an organization. By detecting and examining

trends in historical data, this approach enables organizations to compare the same metrics across various periods. Such comparisons help in hypothesizing plausible reasons for observed changes. Descriptive analytics is often regarded as the industry standard, as it analyzes past and current data to deliver meaningful insights. These insights empower decision-makers to apply their knowledge, experience, and judgment when determining the appropriate course of action. Predictive analytics are designed to help businesses forecast future events and evaluate the potential impact of different scenarios. For instance, it can be used to anticipate supply chain bottlenecks, enabling managers to take a proactive approach rather than merely reacting to events as they arise. In supply chain management, predictive analytics identifies patterns and trends in data, enabling the anticipation of disruptions that could affect suppliers and, consequently, the production process. This type of analytics utilizes data, statistical algorithms, and machine learning techniques to estimate the likelihood of various future outcomes. Building on the results of predictive analytics, prescriptive analytics goes a step further by recommending specific actions for organizations to take to achieve their objectives. This method leverages the findings from both descriptive and predictive analytics to suggest concrete measures. Given the complexity of prescriptive analytics, powerful software is often required to rapidly process and interpret large volumes of data, ensuring that recommendations are both timely and effective. Cognitive analytics aims to replicate human thought processes and behavior to help organizations tackle complex problems. By leveraging artificial intelligence (AI), cognitive analytics systems can learn and improve over time. These systems can answer complex questions and draw contextual conclusions like human reasoning. As a result, cognitive analytics produces more meaningful insights and can scale organizational experience and knowledge, enhancing and informing decision-making.

Conversely, diagnostic analytics facilitates the identification of underlying causes. It employs methods such as drill-down analysis, data discovery, data mining, and correlation assessment. This approach involves evaluating overall performance to identify the causes of errors, mistakes, and delays. Managers gain insight into disruptions, breakdowns, and delays in demand and supply processes, along with the factors contributing to them.

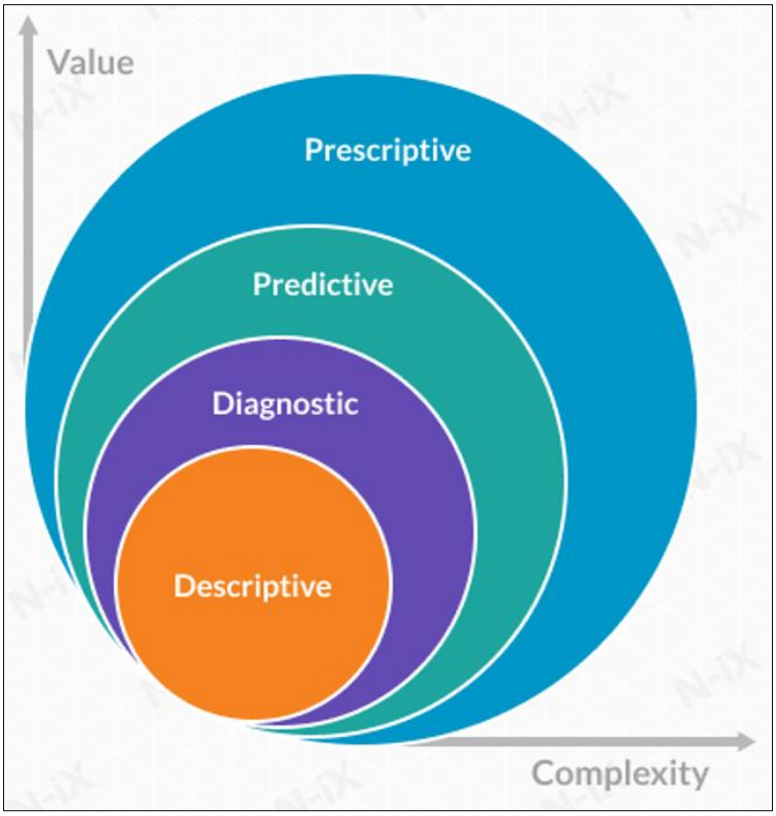


**Fig 3:** Types of data analytics [8].

Figure 3 shows these major types of data analytics [8]. Unlike diagnostic and descriptive analytics, which analyze situations after they occur, predictive analytics uses advanced data analytics techniques to forecast future outcomes. In the supply chain, the time has come to shift from mere descriptive and diagnostic analytics to predictive and prescriptive analytics. Predictive analytics is a branch of data analytics that uses historical data, along with statistical modeling, data mining, and machine learning, to predict future outcomes. Figure 4 shows how predictive analytics works [9].

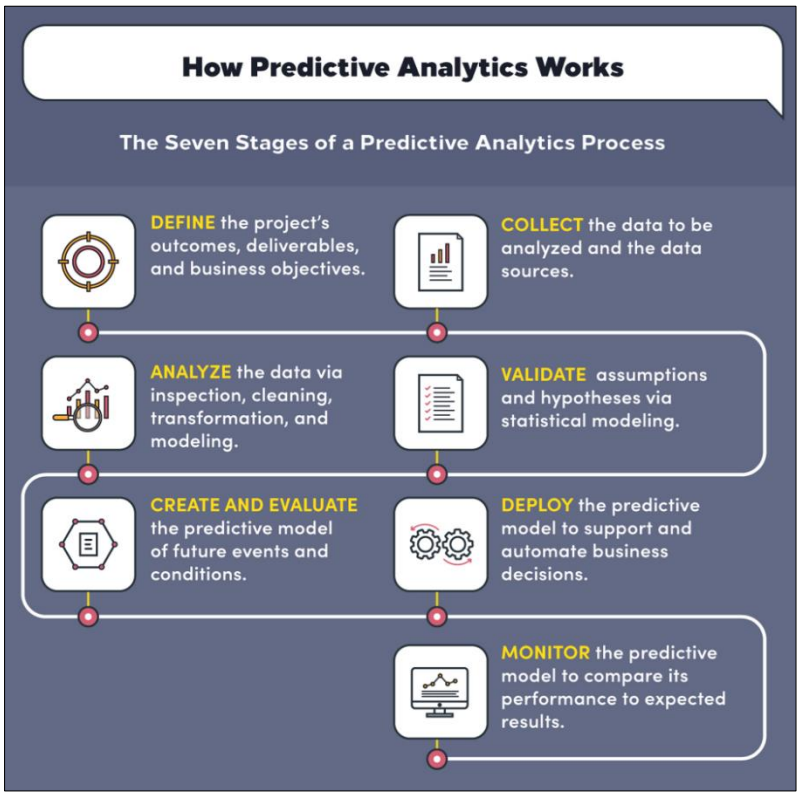


**Fig 4:** Predictive analytics process [9].

### 2.2. Predictive Analytics In Fraud Detection

Fraud is a serious issue with long-lasting consequences. Fraudsters are constantly devising new ways to deceive online businesses and exploit vulnerabilities at every turn. Businesses need to implement robust fraud prevention strategies to safeguard their assets, protect customer data, and comply with regulatory requirements. Traditional fraud detection methods, which heavily rely on manual audits and reactive investigations, are rapidly becoming obsolete. They lack the speed, accuracy, and scalability required to combat modern cyber threats. As cybercriminals leverage advanced technologies to bypass security measures, organizations are turning to predictive analytics as a proactive defense mechanism. Predictive analytics leverages historical and current data to forecast future events or outcomes. By employing advanced statistical modeling, data mining, and machine learning algorithms, this technology identifies hidden patterns within vast datasets. The goal is to predict fraudulent activity with high accuracy so organizations can take preventive or corrective measures before substantial damage occurs. The versatility of predictive analytics allows it to be tailored to the specific fraud challenges faced by various industries. From financial services to e-commerce, organizations are leveraging these advanced models to safeguard their operations and protect their customers. Advanced analytics and predictive analysis can help identify risks, improve the claim assessment methodologies, and offer targeted insurance policies. Figure 5 shows fraud detection [10], while Figure 6 shows predictive analytics for fraud detection [3].

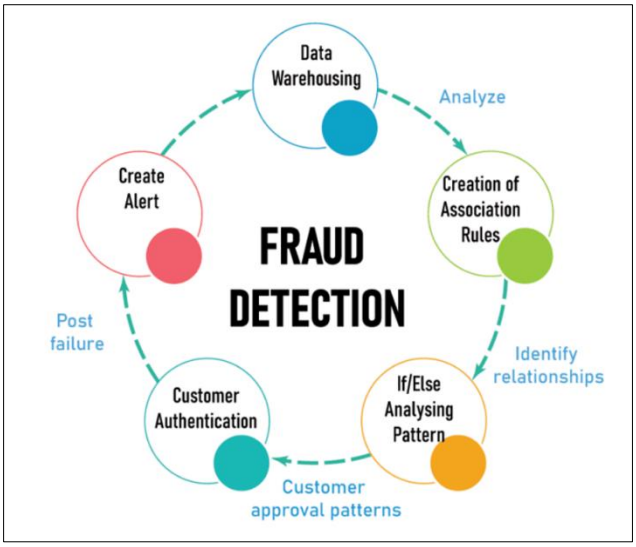


**Fig 5:** Fraud detection [10].


**Fig 6:** Using predictive analytics to detect fraud [3].

### 2.3. Application of Predictive Analytics in Fraud Detection

Predictive analytics offers a powerful defense against fraud, but it is not a "silver bullet." It enables proactive fraud detection by leveraging AI and machine learning to analyze extensive historical and real-time data analytics. Common applications of predictive analytics in fraud detection include the following [2,10-12]:

Insurance is one of the highly competitive industries with very limited predictability. It is highly risky and dependent on statistics. In the insurance sector, predictive models analyze a claimant's history, the nature of the incident, and behavioral indicators to assign a risk score to each new claim. High-scoring claims are automatically routed to specialized investigation units, streamlining the claims process for legitimate customers while rigorously scrutinizing potential fraud. Insurance companies are increasingly adopting predictive analytics to flag fraudulent claims before they are paid. For example, Allstate Insurance uses machine learning algorithms to scrutinize claims data and identify patterns indicative of fraud. Further, e*commerce fraud:* Online retailers face constant threats of fraudulent transactions, particularly from stolen credit cards and identity theft. Predictive analytics helps e-commerce platforms fight back. E-commerce predictive analytics fraud detection models can assess factors such as purchase history, device information, and geographic location to score transactions based on risk. Low-risk transactions are processed seamlessly, while high-risk ones are routed through manual checks. For example, e-commerce giants Amazon and Alibaba use predictive analytics to analyze buyer behavior in real-time. Additionally, predictive analytics uses behavioral analysis to assess the likelihood of fraud. For example, it can compare a user's current behavior with historical data, such as previous purchasing patterns or login locations, to identify discrepancies that may indicate fraud. *Fraud Data Analytics:* This practice is among the most sought-after for detecting and preventing unethical methods of acquiring sensitive data. It relies on accurate and comprehensive data sources for effective fraud detection. Such data may include transaction records, customer demographics, and behavior logs. Ensuring data quality and accuracy helps in creating predictive models that effectively identify potentially fraudulent activities. Developing robust predictive models for fraud prevention involves selecting appropriate machine learning algorithms and incorporating relevant features to detect suspicious activities effectively.

*Risk management is essential, as* Enterprise Risk Management (ERM) is the process of identifying, analyzing, and treating the enterprise's exposure as visualized by executive management. It includes reviewing various exposures, such as fraud, credit, finance, strategic, and operational matters. Despite being a significant organizational process, risk management across the globe remains a challenging business aspect to manage. Traditional risk management approaches are highly subjective and are based on individual perceptions. To survive in this new digital era, businesses should identify early indicators of potential risks and act proactively to mitigate them before they become disruptions. Implementing predictive analytics across all asset classes, the entire credit lifecycle, and credit risk models will help you maximize profits while containing credit risk within the risk portfolio. Figure 7 shows a representation of risk management [10].


**Fig 7:** A representation of risk management [10].

*Predictive risk intelligence allows p*redictive risk monitoring involves using current and historical information to identify emerging and potential risks. Using ML and AI-empowered data analytics, you can discover the hidden trends from the organizational risk data and get crucial insights about the future emergence of different types of risks. Predictive risk intelligence increases operational efficiency and resiliency and improves cost-effectiveness. *Anomaly detection* is a key feature of predictive analytics, identifying unusual behavior patterns that signal potential fraud. It includes spotting irregularities such as significant, unexpected transfers or a sudden spike in transaction volume. By recognizing these deviations, predictive analytics can prompt timely interventions, mitigating potential fraud risks.

## 3. Discussions of Benefits and Challenges

### 3.1. The Benefits

Predictive analytics methodologies offer powerful tools for detecting fraudulent activity. The integration of these advanced tools into organizations' fraud-prevention measures has led to significant improvements. It has redefined fraud prevention from a reactive analysis to a proactive approach. Other benefits of predictive analytics in fraud detection include the following [1, 11]:

*Cost savings are* a significant benefit. Fraud-related costs extend beyond direct financial losses to include legal expenses, regulatory penalties, and reputational damage. Data analytics helps organizations detect and prevent fraud early, reducing the frequency and severity of incidents. Over time, this leads to substantial cost savings by minimizing investigations, recovery efforts, and compliance-related expenses.

*Proactive detection* is the most significant advantage of predictive analytics as it shifts from a reactive to a proactive stance. Unlike traditional systems that flag transactions based on predefined thresholds, predictive models analyze thousands of variables to assign a risk score to each event in real time. It allows for immediate intervention, such as blocking a suspicious credit card transaction or flagging an insurance claim for further review before payment is issued. Furthermore, o*perational efficiency* is another significant benefit. Predictive analytics automates the labor-intensive process of manual auditing, enabling organizations to process and analyze vast amounts of data in real time. This automation not only accelerates the detection process but also significantly improves accuracy. This efficiency allows security teams to focus their resources on high-risk cases rather than wading through a sea of legitimate transactions.

Additionally, *scalability* provides a great advantage. As businesses scale, the sheer volume of data generated makes manual oversight impossible. Predictive analytics provides the scalability required to process millions of transactions per second. Predictive analytics provides the scalability necessary to handle the exponential growth in digital transactions. As businesses expand their online presence, the volume of data generated increases dramatically. Predictive models are designed to scale seamlessly, ensuring that fraud detection capabilities remain robust regardless of transaction volume.

### 3.2. Challenges

Despite its profound benefits, implementing predictive analytics for fraud detection is not without challenges. Challenges such as evolving fraud tactics, false positives, model bias issues, transparency concerns, and ethical hurdles persist. The landscape of cybercrime is highly dynamic, with fraudsters continuously evolving their tactics to bypass security measures. Consequently, predictive models must be updated constantly to remain effective. Other challenges of predictive analytics in fraud detection include the following [1, 11]:

*Data quality* is seen as a disadvantage as predictive models are only as good as the data they are trained on, and poor-quality data can lead to inaccurate predictions. In the realm of fraud prevention, several data-specific issues create persistent obstacles. Ensuring that the data is clean, relevant, and representative of the current environment is critical for the success of predictive analytics. Also, *data imbalance* is one of th*e* most significant technical challenges. In a typical financial environment, fraudulent transactions represent a tiny fraction of the total volume. This scarcity makes it difficult for machine learning models to effectively "learn" the characteristics of fraud, as they are overwhelmed by the sheer volume of legitimate data. Standard algorithms may achieve high accuracy by simply predicting that every transaction is legitimate, which is useless for fraud prevention.

*Data privacy* is of great concern. The use of personal data for predictive analytics is strictly governed by regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). These laws impose constraints on how data is collected, stored, and processed. Balancing the need for deep data analysis with the requirement for consumer privacy is a delicate act that often limits the features a model can use. A persistent challenge in fraud prevention is the "false positive"—a legitimate transaction that is incorrectly flagged as fraudulent. While missing a fraudulent transaction (False Negative) is costly, incorrectly flagging a legitimate one (False Positive) can be equally damaging. High false-positive rates not only frustrate customers but also lead to lost revenue and increased operational costs. They can overwhelm security teams, diverting their attention from genuine threats and leading to alert fatigue. Additionally, false positives can severely impact the customer experience, causing frustration when legitimate transactions are blocked or delayed. Balancing the sensitivity of predictive models to catch fraud while minimizing false alarms remains a critical ongoing challenge for data scientists and security professionals.

Other disadvantages include *concept drift.* Fraud is an adversarial game. As soon as a predictive model successfully identifies a specific fraud pattern, criminals adapt their tactics to bypass it. This phenomenon, known as concept drift, means that models trained on historical data can become obsolete very quickly. Maintaining a model's relevance requires constant retraining and the ability to detect shifts in fraud patterns in near real time. Additionally, e*xplainability* in modern deep learning models are often "black boxes," providing highly accurate predictions without a clear explanation of why a specific transaction was flagged. This lack of explainability is a major hurdle for regulatory compliance, as many jurisdictions require financial institutions to provide reasons for adverse actions (e.g., declining a transaction). The complexity of the models used in predictive analytics can make them difficult to interpret, raising concerns about transparency and accountability. Furthermore, a*lgorithmic bias* is a concern. Predictive models can inadvertently inherit or amplify biases present in the

training data. For example, if certain demographics have historically been flagged more often due to systemic factors, the model may continue to disproportionately target those groups, leading to discriminatory fraud detection. Ensuring fairness and mitigating bias is a critical ethical and legal requirement that adds another layer of complexity to model development. Collaboration is becoming essential as fraud is not confined to one organization or sector, which is why. Sharing anonymized threat intelligence across industries allows businesses to benefit from collective knowledge and spot fraud patterns faster. Working together, businesses, regulators, and law enforcement can stop fraud by sharing information and increasing detection efforts. Sharing data helps businesses work together, but they need to keep it private and secure. They must follow rules and protect customers' sensitive information. Finally, s*kill gaps* pose some issues. Many organizations lack the in-house expertise to properly implement predictive analytics.

Data analytics consulting companies provide access to skilled data scientists and analysts who can fill this gap and guide organizations through the process of developing custom fraud prevention models.

## 4. Results

The findings of the study suggest that predictive analytics has emerged as a critical tool in the fight against financial fraud. Its advanced capabilities allow organizations to detect fraudulent activity more efficiently and accurately than traditional methods. It significantly enhances fraud detection accuracy by enabling the identification of unusual transaction patterns and high-risk behaviors that often signify fraudulent activity [13, 14]. This approach improves the reliability of fraud detection systems and supports earlier identification of suspicious transactions.

Furthermore, predictive analytics facilitates early detection and helps reduce financial losses. Early intervention prevents fraudulent transactions from escalating, resulting in significant cost savings and reduced financial risk for organizations [14]. In addition, predictive analytics supports a balanced detection system by minimizing missed fraud cases while reducing false positives. This ensures that legitimate transactions are not incorrectly flagged, thereby improving overall fraud management efficiency [15].

Through predictive analytics, organizations gain deeper insights into fraud behavior and its associated risk factors, enabling the development of targeted, proactive fraud prevention strategies. The results also indicate improvements in operational efficiency and scalability, as predictive systems can adapt to evolving threats while reducing operational costs [15].

Finally, machine learning models, which underpin predictive analytics, consistently outperform traditional fraud detection methods. Their effectiveness enables rapid response to fraud attempts, contributing to early detection, reduced financial losses, and improved operational efficiency [13, 14].

## 5. Future of Predictive Analytics in Fraud Detection

Predictive analytics involves gathering and analyzing large datasets to create models that forecast future behaviors or events. As technology continues to advance, predictive analytics will remain the cornerstone of a secure digital landscape, enabling businesses to innovate and grow without compromising their customers' safety or the integrity of their operations.

As technology advances, so do the methods used by fraudsters. Fraud tactics continue to evolve, making it critical for organizations to adopt advanced technologies that stay ahead of emerging threats. Artificial intelligence is reshaping fraud detection by introducing powerful methods such as transformer-based models, explainable AI, and federated learning. The integration of artificial intelligence and machine learning will continue to enhance the capabilities of predictive analytics. Figure 8 shows the future trends in predictive analytics for fraud prevention [16].


**Fig 8:** Future trends in predictive analytics for fraud prevention [13].

## 6. Conclusion

Costing billions of dollars a year and eroding public confidence in financial institutions, financial fraud poses a threat to both individuals and organizations. The more sophisticated the approaches that fraudsters use, the more difficult it is for standard detection tools to keep up. In a world where fraud is constantly evolving, data analytics and predictive models have become essential for proactive fraud detection. Predictive analytics has fundamentally transformed the paradigm of fraud detection, offering a powerful, proactive defense against increasingly sophisticated cyber threats. By leveraging historical data to anticipate and identify fraudulent activities, financial institutions can enhance their ability to detect and prevent fraud. By harnessing the capabilities of data mining, machine learning, and advanced statistical modeling, organizations across industries can identify hidden risks, automate complex analyses, and protect their assets with unprecedented

accuracy. Predictive analytics in fraud detection have revolutionized the way financial institutions preemptively address and mitigate cyber threats, reducing the incidence of breaches and saving millions in potential losses. Although predictive modeling implies a focus on forecasting the future, it can also predict outcomes, for example, the probability that a transaction is fraudulent. More information on the use of predictive analytics in fraud detection and prevention is available from the books in [17-21] and the following related journals:

- Journal of Financial Crime
- Journal of Risk and Financial Management

**References**


1. TrustCloud. Uncovering fraud with data analytics: 4 Cutting-edge techniques to detect anomalies. Available from: https://community.trustcloud.ai/docs/grc-launchpad/grc-101/compliance/uncovering-fraud-with-data-analytics-a-modern-approach/
2. Financial Crime Academy. Predictive analytics in fraud detection: Challenges and evolution in the face of sophisticated cyber threats. 2026 Mar. Available from: https://financialcrimeacademy.org/predictive-analytics-in-fraud-detection/
3. Albert C. How companies use predictive analytics to detect fraud. VivaTech. 2025 Jun. Available from: https://vivatech.com/news/how-companies-use-predictive-analytics-to-detect-fraud/
4. River Logic. Supply chain predictive analytics: What is it and who's doing it?. Available from: https://riverlogic.com/?blog=supply-chain-predictive-analytics-what-is-it-and-whos-doing-it
5. Babin N. AI and predictive analytics: Revolutionizing demand forecasting in supply chain management. LinkedIn. Available from: https://www.linkedin.com/pulse/ai-predictive-analytics-revolutionizing-demand-supply-nicolas-babin-xrj2e/
6. Inkl. From insight to innovation: Why data analysis will define industry leaders in 2025. Available from: https://www.inkl.com/news/from-insight-to-innovation-why-data-analysis-will-define-industry-leaders-in-2025
7. An overview of supply chain analytics. 2023 Feb. Unknown source.
8. Tymchuk I. Big data and predictive analytics in supply chain: Success stories and tips. N-iX. 2020 Nov. Available from: https://www.n-ix.com/big-data-predictive-analytics-supply-chain-case-study/
9. Maryville University. Predictive analytics in insurance: Types, tools, and the future. 2020 Oct. Available from: https://online.maryville.edu/blog/predictive-analytics-in-insurance/
10. Roy K. Data science for risk management. DatatoBiz. Available from: https://www.datatobiz.com/blog/data-science-for-risk-management/
11. Manus.im. Available from: https://manus.im
12. Fraud.com. The role of predictive analytics in fraud prevention. Available from: https://www.fraud.com/post/predictive-analytics-in-fraud-prevention
13. Vapnik VN. The Nature of Statistical Learning Theory. New York, NY: Springer; 1995.
14. Breiman L. Random forests. Machine Learning. 2001;45(1):5–32.
15. Fawcett T, Provost F. Adaptive fraud detection. Data Mining and Knowledge Discovery. 1997;1(3):291–316.
16. Saini N. The role of predictive analytics in fraud prevention. HashStudioz. 2025 Jan. Available from: https://www.hashstudioz.com/blog/the-role-of-predictive-analytics-in-fraud-prevention/
17. Bari A, Chaouchi M, Jung T. Predictive Analytics For Dummies. 2nd ed. For Dummies; 2016.
18. Baesens B, Vlasselaer VV, Verbeke W. Fraud Analytics Using Descriptive, Predictive, and Social Network Techniques: A Guide to Data Science for Fraud Detection. Wiley; 2015.
19. Innoware PJP. Unveiling Deception: Leveraging AI and Predictive Analytics for Fraud Detection in Finance. Kindle Edition; 2024.
20. Innoware PJP. Harnessing AI and Predictive Analytics for Healthcare Fraud Detection. Independently Published; 2024.
21. Spann DD. Fraud Analytics: Strategies and Methods for Detection and Prevention. Wiley; 2013.


**How to Cite This Article**

Sadiku MNO, Padi D, Sadiku JO. Predictive analytics in fraud detection. Int J Manag Organ Res. 2026 May–Jun;5(3):16–23. doi:10.54660/IJMOR.2026.5.3.16-23

**Creative Commons (CC) License**