SvedbergOpen
DISSEMINATION OF KNOWLEDGE

International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: https://www.svedbergopen.com/

Research Paper Open Access

Intelligent FinTech Risk Management Using Machine Learning-Based Anomaly Detection and Predictive Analytics

Anuraag Mangari Neburi[1], Naresh Bandaru[2]

[1]Vice President Richardson, TX, USA. E-mail: anuraag.mn@gmail.com
[2]Staff Data Platform Engineer Stash Financial, Inc Salem, MA. E-mail: nareshbandaru.work@gmail.com

Abstract
The rapid expansion of digital financial services has increased transaction volumes and introduced increasingly complex financial-risk patterns, creating a need for reliable computational approaches to detect fraudulent activity. Machine-learning techniques can support FinTech risk management by identifying relationships and irregularities within transaction data that may not be readily recognized through conventional monitoring methods. This study aimed to characterize fraudulent financial-payment activity across transaction categories and assess the performance of supervised and unsupervised machine-learning methods for financial-risk identification. The BankSim financial-payment transaction dataset was analyzed using descriptive statistical techniques and machine-learning methods. Transaction distributions, monetary characteristics, and category-specific fraud patterns were examined, followed by the implementation of Logistic Regression, Random Forest, and Isolation Forest. An 80:20 stratified training and testing framework was applied, and model performance was evaluated using accuracy, precision, recall, F1-score, Area Under the Receiver Operating Characteristic Curve (AUROC), and Area Under the Precision-Recall Curve (AUPRC). The analysis identified substantial differences in fraud occurrence among transaction categories and demonstrated distinct performance profiles across the evaluated approaches. The findings indicate that supervised classification and anomaly detection provide complementary perspectives for financial fraud identification. Integrating transaction-level characteristics with machine-learning analysis can support structured risk assessment, improve the identification of potentially suspicious activity, and contribute to more responsive FinTech monitoring frameworks. Future investigations should examine adaptive and advanced machine-learning approaches using broader financial transaction environments.

Keywords: Anomaly detection, Financial fraud, FinTech risk, Machine learning, Predictive analytics

1. Introduction

The rapid expansion of financial technology (FinTech) has transformed how individuals, businesses, and institutions conduct financial activities. Digital payments, electronic transactions, mobile banking, and automated financial services have increased transaction speed and accessibility while simultaneously generating large and complex streams of transactional information (Mada, 2025). These developments have also created new opportunities for fraudulent activity, making continuous financial-risk monitoring increasingly important (Pal, 2026). Traditional approaches based primarily on manual inspection and predefined rules can become difficult to maintain as transaction volumes increase and fraudulent behavior changes over time (Andronie *et al*., 2024). Data-driven approaches have consequently become important for automated financial-fraud identification, particularly through data mining and machine-learning techniques (Logapriya *et al*., 2026). Transaction aggregation has also been investigated as a mechanism for improving the representation of financial behavior for fraud analysis (Khan *et al*., 2026). These developments establish machine learning and predictive analytics as relevant tools for contemporary FinTech risk management (Ononiwu *et al*., 2023).

Financial fraud detection is a distinctive analytical challenge: fraudulent observations commonly constitute a relatively small proportion of overall transaction activity (Nawaz and Musah, 2025). Severe class imbalance can make conventional accuracy-based assessment misleading; a model may achieve high overall accuracy while failing to identify a substantial proportion of fraudulent events (Karimkhani *et al*., 2025). Fraudulent behavior may also emerge through unusual combinations of transaction amount, timing, merchant characteristics, or customer-related attributes rather than through a single abnormal variable (Mahajan, 2024). Anomaly detection addresses this challenge by identifying observations that differ substantially from expected patterns (Dixit, 2024). Comprehensive reviews have documented the application of anomaly detection, classification,

and data-mining techniques to financial fraud (Das *et al*., 2026). These approaches are particularly relevant when emerging fraudulent behaviors may not closely resemble previously observed cases.

Machine learning can identify relationships among multiple transaction characteristics without requiring every fraudulent pattern to be manually encoded as a rule. Supervised classifiers learn from labeled observations, whereas unsupervised methods attempt to identify unusual observations without directly depending on predefined fraud labels (Mohammed *et al*., 2026). Logistic Regression provides an interpretable baseline for binary classification, while Random Forest can model nonlinear relationships and interactions among predictors (Chen and Zhang, 2025). Isolation Forest provides an alternative unsupervised strategy for identifying observations that are distinguishable from the majority of the data (Campbell *et al*., 2024). Research has also demonstrated the value of transaction aggregation and ensemble learning in financial fraud detection (Ayarekar *et al*., 2026). Sequential transaction information has further been investigated for fraud classification, demonstrating the relevance of temporal behavioral patterns (Al Dulaimi *et al*., 2025). Ensemble-based streaming approaches have likewise been developed for scalable fraud detection.

Predictive analytics extends fraud detection from descriptive identification toward estimating whether an observed transaction is likely to belong to a risky or fraudulent class. Such analysis can help financial systems prioritize suspicious transactions for further investigation. However, evaluating predictive models solely through overall accuracy can provide an incomplete representation of performance when fraudulent events are relatively uncommon (Pundhir *et al*., 2026). Precision, recall, and F1-score provide additional information regarding the identification of fraudulent observations, whereas AUROC evaluates discriminatory performance across classification thresholds. Precision-recall analysis can be particularly informative for imbalanced classification; it emphasizes the relationship between correctly identified positive cases and false-positive predictions (Adebajo *et al*., 2026). Financial-fraud research has consequently emphasized appropriate evaluation strategies, imbalance treatment, and operational performance when comparing predictive approaches. These considerations support the use of multiple complementary performance measures when assessing FinTech risk models.

Although machine-learning research in financial-fraud detection has expanded considerably, methodological challenges remain (Prabhu *et al*., 2025). Existing investigations employ different datasets, preprocessing strategies, feature representations, algorithms, and evaluation procedures, which makes direct comparison of reported performance difficult. Class imbalance remains an important concern; conventional learning procedures can become biased toward the majority class. Recent research has also highlighted the continuing importance of appropriate sampling, evaluation strategies, and model development for highly imbalanced financial-fraud datasets. In addition, financial fraud can evolve, creating a need for methods capable of identifying both known and unusual transaction patterns. Broader discussions of artificial intelligence in financial applications emphasize the importance of reliable, interpretable, and appropriately evaluated analytical systems (Naeem *et al*., 2026). These challenges provide a rationale for comparing supervised prediction with unsupervised anomaly detection within a consistent transaction environment.

The study aimed to characterize fraudulent financial-payment activity by examining transaction distributions, monetary patterns, and variation in fraud occurrence across transaction categories, and to evaluate the effectiveness of Logistic Regression, Random Forest, and Isolation Forest for financial-risk identification by comparing accuracy, precision, recall, F1-score, AUROC, and AUPRC using the BankSim transaction dataset.

2. Materials and Methods

2.1 Study Design

This study employed a quantitative computational research design to investigate financial transaction risk through machine-learning-based fraud identification and anomaly detection. The analytical framework was structured to examine transaction characteristics, identify patterns associated with fraudulent activity, and evaluate predictive performance across different modeling approaches. The workflow consisted of data preparation, descriptive analysis, feature processing, supervised classification, unsupervised anomaly detection, and model-performance evaluation. Descriptive analyses were conducted initially to characterize transaction distributions and category-specific fraud patterns. Subsequently, machine-learning techniques were applied to the processed transaction data to distinguish legitimate and potentially fraudulent financial activities. The overall methodology was designed to provide a reproducible framework for FinTech risk assessment.

2.2 Data Source

The study used the BankSim financial-payment transaction dataset. The dataset contains 594,643 transaction records and includes information relating to transaction timing, customer characteristics, demographic coding, merchants, transaction categories, monetary amounts, and fraud status. The binary fraud variable was used to distinguish legitimate transactions from fraudulent transactions. The dataset contains 587,443 legitimate transactions and 7,200 fraudulent transactions. BankSim represents a synthetic financial-payment

environment developed for fraud-detection research and does not contain directly collected identifiable banking records. The dataset was analyzed at the transaction level to investigate financial-risk patterns and develop predictive and anomaly-detection models.

2.3 Data Preprocessing

The raw transaction records were examined for completeness, variable structure, coding consistency, and suitability for machine-learning analysis before model development. The fraud variable was retained as the binary outcome, with legitimate and fraudulent observations represented according to their original dataset coding. The final predictive feature set comprised step, age, gender, transaction category, and transaction amount. The step and amount variables were treated as numerical predictors, while age, gender, and transaction category were converted into numerical representations through one-hot encoding. Numerical predictors were standardized when required by the modeling approach. Variables functioning primarily as identifiers were excluded from the predictive feature matrix where they did not provide meaningful generalizable information. These procedures produced a structured feature matrix suitable for subsequent statistical and machine-learning analyses.

2.4 Machine-Learning and Anomaly-Detection Models

Three complementary analytical approaches were implemented to examine financial fraud risk. Logistic Regression was used as a supervised baseline classifier to model the relationship between transaction characteristics and fraud status. Random Forest was applied as an ensemble-learning method capable of representing nonlinear relationships and interactions among transaction features. Isolation Forest was employed as an unsupervised anomaly-detection approach to identify transactions exhibiting unusual characteristics without using fraud labels during anomaly-model fitting. Class weighting was incorporated into the supervised models to address the imbalance between legitimate and fraudulent observations. The final model configurations and hyperparameters were maintained consistently throughout model development and evaluation to support reproducible comparison across the three approaches.

2.5 Model Training

The dataset was divided into training and independent testing subsets using an 80:20 stratified split with a fixed random state of 42. Stratification was used to preserve the relative representation of legitimate and fraudulent observations across the two subsets. Data-processing transformations were fitted using the training data and subsequently applied to the testing data to reduce the possibility of information leakage. Logistic Regression and Random Forest were trained using the labeled training observations, whereas Isolation Forest was fitted as an anomaly-detection model. After training, each approach generated predictions or anomaly classifications for the independent test subset. The resulting predictions were compared with the observed fraud status to provide a consistent basis for model evaluation.

2.6 Performance Evaluation and Statistical Analysis

Model performance was assessed using accuracy, precision, recall, F1-score, AUROC, and AUPRC. Accuracy represented the proportion of correctly classified observations, while precision measured the proportion of transactions predicted as fraudulent that were actually fraudulent. Recall quantified the proportion of fraudulent transactions correctly identified, and the F1-score represented the balance between precision and recall. AUROC assessed discriminatory performance across classification thresholds, whereas AUPRC provided an additional measure suited to the imbalanced fraud outcome. For Isolation Forest, anomaly scores and binary anomaly classifications were evaluated against the observed fraud-status labels to obtain the corresponding performance measures. Descriptive analyses included transaction frequencies, percentages, monetary totals, means, medians, and category-specific fraud rates.

3. Results

3.1 Transaction and Fraud Profile

The transaction-level analysis demonstrated a substantial imbalance between routine and fraudulent financial activity within the simulated payment environment. Most recorded transactions were classified as legitimate, indicating that fraudulent events represented a relatively small component of the overall transaction stream, as shown in Table 1. Despite their limited frequency, fraudulent transactions contributed disproportionately to the aggregate monetary value, with their average transaction size considerably exceeding that observed among legitimate payments. The difference between the mean and median values for fraudulent transactions also indicates a right-skewed distribution, suggesting the presence of comparatively large transactions within the fraudulent group. These findings establish a clear financial-risk pattern for subsequent machine-learning analysis.

Table 1. Distribution of Financial Transactions According to Fraud Status

Fraud status	Transactions (n)	Percentage (%)	Total transaction amount (€)	Mean amount (€)	Median amount (€)
Legitimate	587,443	98.79	18,708,432.56	31.85	26.61
Fraudulent	7,200	1.21	3,822,671.17	530.93	319.18
Total	594,643	100.00	22,531,103.73	37.89	26.90

Source: *Authors' analysis of the BankSim raw financial-payment transaction dataset (bs140513_032310.csv).*

3.2 Transaction-Category Fraud Patterns

Fraud occurrence varied markedly across the different transaction categories represented in the dataset. Several high-volume categories contained no fraudulent observations, whereas some less frequently used categories exhibited considerably greater concentrations of fraudulent activity as shown in Table 2. This contrast indicates that transaction frequency alone does not necessarily correspond to fraud exposure within the simulated payment environment. Categories associated with travel, leisure, sports and toys, and selected service activities displayed comparatively elevated fraud proportions, while transportation and food transactions showed no recorded fraudulent events. The observed heterogeneity provides useful evidence for risk-sensitive feature construction and suggests that transaction category may contain informative signals for identifying unusual financial behavior.

Table 2. Transaction Volume and Fraudulent Transaction Rate by Transaction Category

Transaction category	Total transactions (n)	Fraudulent transactions (n)	Fraud rate (%)
es_transportation	505,119	0	0.00
es_food	26,254	0	0.00
es_health	16,133	1,696	10.51
es_wellnessandbeauty	15,086	718	4.76
es_fashion	6,454	116	1.80
es_barsandrestaurants	6,373	120	1.88
es_hyper	6,098	280	4.59
es_sportsandtoys	4,002	1,982	49.53
es_tech	2,370	158	6.67
es_home	1,986	302	15.21
es_hotelservices	1,744	548	31.42
es_otherservices	912	228	25.00
es_contents	885	0	0.00
es_travel	728	578	79.40
es_leisure	499	474	94.99
Total	594,643	7,200	1.21

Source: *Authors' analysis of the BankSim raw financial-payment transaction dataset (bs140513_032310.csv).*

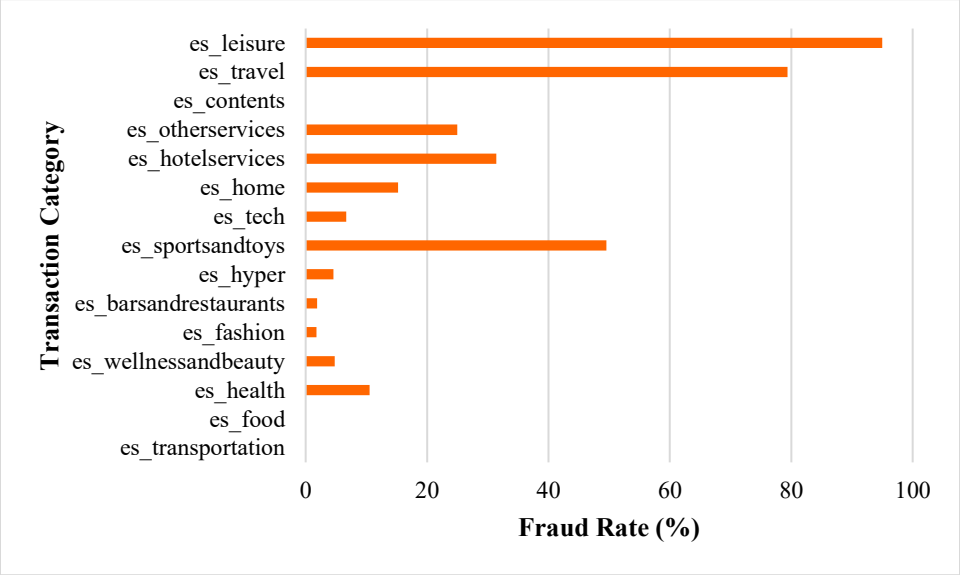

Figure 1. Fraud Rate Across Financial Transaction Categories

The substantial variation in fraudulent transaction rates across the financial payment categories. Leisure and travel transactions show the highest observed fraud proportions, followed by sports and toys and several service-related categories. Health, home, and technology transactions exhibit comparatively lower rates, whereas transportation, food, and contents show no recorded fraudulent transactions, as shown in Figure 1. This pattern indicates that fraud occurrence is not evenly distributed across transaction types. The marked differences between categories provide useful evidence for identifying transaction characteristics associated with elevated financial risk. These category-level variations can therefore support feature selection and anomaly detection within machine-learning-based FinTech risk assessment.

3.3 Machine-Learning and Anomaly-Detection Performance

The comparative modeling analysis showed meaningful differences between the supervised classification approaches and the unsupervised anomaly-detection method. Logistic Regression identified a very large proportion of fraudulent cases, reflected by its high recall, although its lower precision indicates that this sensitivity was accompanied by a greater number of false-positive classifications, as shown in Table 3. Random Forest produced a substantially more balanced relationship between precision and recall and consequently achieved the highest F1-score among the evaluated approaches. Isolation Forest provided an independent unsupervised approach and successfully identified a proportion of anomalous transactions without relying on fraud labels during model fitting. The results demonstrate complementary strengths across the evaluated methods.

Table 3. Performance of Machine-Learning and Anomaly-Detection Models for Fraud Risk Identification

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	AUROC (%)	AUPRC (%)
Logistic Regression	93.18	14.91	98.40	25.90	99.23	77.55
Random Forest	99.41	82.99	64.03	72.29	95.17	76.15
Isolation Forest	98.41	34.37	34.44	34.41	96.73	33.10

Source: *Authors' analysis of the BankSim raw financial-payment transaction dataset (bs140513_032310.csv). Models were evaluated using an independent 20% stratified test subset (random_state=42), with the preprocessing and model specifications described in the Methods section.*

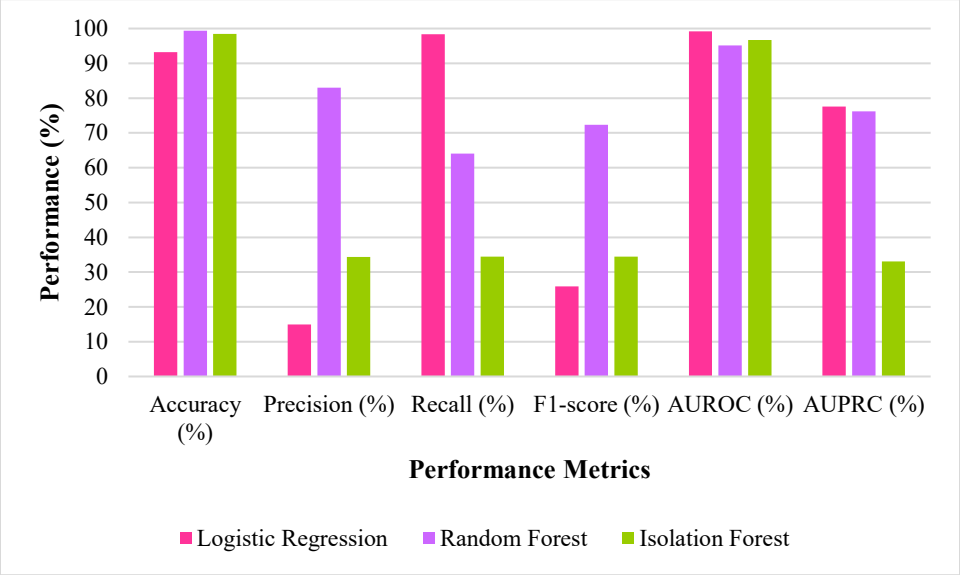

Figure 2. Comparative Performance of Machine-Learning and Anomaly-Detection Models

The predictive and anomaly-detection performance of Logistic Regression, Random Forest, and Isolation Forest across six evaluation measures. Logistic Regression demonstrates particularly high recall and AUROC, indicating strong identification of fraudulent cases and effective overall discrimination, although its precision and F1-score are comparatively lower, as shown in Figure 2. Random Forest provides a more balanced performance across precision, recall, and F1-score, while maintaining high accuracy and AUROC. Isolation Forest shows strong accuracy and AUROC but lower precision, recall, F1-score, and AUPRC than the supervised approaches. The figure illustrates meaningful differences in model behavior across complementary performance measures for financial-risk detection.

4. Discussion

The study demonstrates a substantial difference between legitimate and fraudulent financial transactions in the BankSim dataset. Of the 594,643 transactions examined, 587,443 (98.79%) were legitimate, and 7,200 (1.21%) were classified as fraudulent. Although fraudulent transactions represented a relatively small proportion of the complete transaction population, their aggregate monetary value was disproportionately high. Fraudulent transactions accounted for €3,822,671.17, with a mean transaction amount of €530.93 compared with €31.85 for legitimate transactions. This difference indicates that fraud risk cannot be evaluated solely according to transaction frequency. The considerably higher average monetary value associated with fraudulent observations highlights the importance of incorporating transaction amount and other behavioral characteristics into automated financial-risk detection. Similar concerns regarding the identification of evolving fraudulent behavior and the application of machine-learning methods to financial-risk assessment have been discussed in recent FinTech research.

Marked differences were observed in fraudulent transaction rates across the 15 transaction categories. Leisure transactions recorded the highest fraud rate at 94.99%, followed by travel at 79.40% and sports and toys at 49.53%. In contrast, transportation, food, and contents recorded no fraudulent observations. Other categories, including hotel services, other services, home, health, and technology, demonstrated intermediate levels of fraudulent activity. These findings indicate that fraud occurrence was not uniformly distributed across the financial transaction environment (Shehadeh, 2025). Instead, particular transaction categories demonstrated substantially greater concentrations of fraudulent activity. Such heterogeneity is relevant to FinTech risk management; category-level information can contribute to the identification of transaction patterns that warrant enhanced monitoring. Upadhyay (2026) similarly emphasizes the importance of adaptive machine-learning approaches for recognizing emerging fraud patterns in FinTech transactions. The findings therefore support the value of category-sensitive analytical approaches rather than treating all financial transactions as having equivalent risk characteristics.

The model evaluation demonstrated meaningful differences among Logistic Regression, Random Forest, and Isolation Forest. Logistic Regression achieved the highest recall (98.40%) and AUROC (99.23%), indicating strong identification of fraudulent observations and strong discriminatory ability. However, its precision was comparatively low at 14.91%, resulting in an F1-score of 25.90%. This indicates that the model identified a large proportion of fraudulent transactions but also generated a considerable number of false-positive classifications. Random Forest produced a more balanced pattern, with 82.99% precision, 64.03% recall, and a

72.29% F1-score, while maintaining 99.41% accuracy. Isolation Forest achieved 98.41% accuracy and 96.73% AUROC, but its precision, recall, and F1-score were lower than those of Random Forest. These findings are consistent with the broader use of supervised and unsupervised machine learning for identifying both established and unusual financial-risk patterns. Recent FinTech research has similarly explored machine-learning and hybrid approaches for adaptive risk management.

The results also demonstrate why class imbalance must be considered when evaluating financial-fraud models. Only 1.21% of the transactions were fraudulent, meaning that legitimate transactions substantially outnumbered fraudulent observations. Under these circumstances, accuracy alone may provide an incomplete representation of practical detection capability. For example, Random Forest and Isolation Forest achieved accuracies above 98%, but their recall and precision values differed considerably (Zangana and Mohammed, 2025). Logistic Regression illustrates the opposite issue: its very high recall indicates strong detection of fraudulent observations, but its lower precision indicates that many transactions classified as fraudulent were not actually fraudulent. Therefore, financial-risk models should be evaluated using several complementary measures rather than relying on a single metric. Shukla (2024) emphasizes machine learning as an important approach for financial-risk assessment and fraud detection, while adaptive approaches are increasingly relevant where fraud patterns change over time.

The findings have practical implications for intelligent FinTech risk-management systems. The category-level differences observed in Table 2 suggest that transaction characteristics can provide useful signals for prioritizing potentially risky activity. At the same time, the model results indicate that different algorithms provide different operational characteristics. A model emphasizing recall may be useful when minimizing missed fraudulent transactions is the principal concern, whereas stronger precision may be desirable when investigation resources are limited and excessive alerts could increase operational workload. Consequently, model selection should be connected to the intended risk-management application rather than based exclusively on overall accuracy. Recent work has proposed adaptive and hybrid machine-learning architectures for FinTech cybersecurity and risk management, reflecting the increasing need for systems capable of responding to changing threat environments. The findings support this broader direction by demonstrating the value of combining predictive classification and anomaly-detection perspectives.

The study provides a computational framework for examining financial fraud through both supervised classification and unsupervised anomaly detection. Its comparison of Logistic Regression, Random Forest, and Isolation Forest demonstrates that no single performance measure fully describes model behavior in an imbalanced fraud-detection environment. Future research could extend the framework by incorporating temporal transaction sequences, customer behavioral histories, graph-based relationships, adaptive learning, and deep-learning architectures. Graph neural networks and reinforcement-learning approaches have recently been investigated for adaptive cybersecurity risk management in FinTech environments (Radha *et al*., 2025). Similarly, machine-learning frameworks for mobile-payment security have explored combinations of behavioral analytics, anomaly detection, Random Forest, and Isolation Forest to address evolving threats. Further investigations could therefore evaluate adaptive models on larger real-world datasets and examine their stability under changing fraud patterns. Such developments may strengthen the practical applicability of machine-learning-based financial-risk management.

A key limitation of the study is that the analysis was conducted using the synthetic BankSim financial-payment environment rather than directly observed banking transactions. Consequently, the observed fraud patterns and model performance should be interpreted within the characteristics of the dataset and should not be assumed to represent all real-world financial systems. Future studies using validated real-world transaction data could provide additional evidence regarding the generalizability and operational performance of the evaluated approaches.

5. Conclusion

This study investigated financial transaction risk using machine-learning-based fraud classification and anomaly detection within the BankSim financial-payment environment. The findings demonstrated clear differences between legitimate and fraudulent transaction patterns and showed that fraudulent activity was not distributed uniformly across transaction categories. These observations highlight the importance of examining transaction characteristics and behavioral patterns when developing automated approaches for financial-risk identification. The comparative evaluation demonstrated that Logistic Regression, Random Forest, and Isolation Forest exhibited different performance characteristics. Logistic Regression showed strong capability for identifying fraudulent observations, while Random Forest provided a more balanced classification profile. Isolation Forest offered an alternative unsupervised approach for identifying unusual transaction behavior. The results demonstrate that financial-fraud detection should consider multiple complementary performance measures rather than relying on a single indicator of model effectiveness. The findings support the use of machine learning and anomaly detection as complementary analytical approaches within FinTech risk-management systems. Category-specific transaction patterns can assist in identifying

potentially higher-risk activities, while different modeling approaches can provide complementary information for fraud monitoring and investigation. Future studies should examine these approaches using larger real-world financial datasets and incorporate temporal transaction behavior, customer-level histories, adaptive learning, graph-based relationships, and advanced machine-learning architectures. Such developments could improve the ability of FinTech systems to identify evolving and previously unseen fraudulent patterns.

References

1. Adebajo, O. O., Babatunde, S. A., Oni, A. A., Abiola, J. O., & Adebajo, O. A. (2026). Anomaly Detection Frameworks for Cybersecurity in Nigerian Fintech Startups Using Unsupervised Machine Learning Techniques.
2. Al Dulaimi, H. A., Furaijl, H. B., Baddour, L. S., Ramada, A. A., Srayyih, F. H., Jasim, S. R., ... & Ibrahem, D. K. (2025, July). AI-driven behavioral anomaly and fraud detection models for real-time high-frequency financial transactions in FinTech systems. In the *2025 3rd International Conference on Cyber Resilience (ICCR)* (pp. 1-7). IEEE.
3. Andronie, M., Blažek, R., Iatagan, M., Skypalova, R., Uţă, C., Dijmărescu, A., ... & Dijmărescu, I. (2024). Generative artificial intelligence algorithms in Internet of Things blockchain-based fintech management. *Oeconomia Copernicana*, *15*(4), 1349-1381.
4. Ayarekar, S., Nangare, V., & Pawar, P. (2026). Sustainable FinTech Risk Management Using Reinforcement Learning and Predictive Analytics. *International Journal of Computer Information Systems and Industrial Management Applications*, *18*(3s), 680-694.
5. Campbell, D., Ansari, A., & Singh, V. V. (2024). Machine Learning in Fintech. *The Adoption of Fintech: Using Technology for Better Security, Speed, and Customer Experience in Finance*, 206.
6. Chen, J., & Zhang, Y. (2025). AI-Driven Financial Risk Management and Decision Support Systems: A Comprehensive Framework for Real-Time Anomaly Detection and Predictive Analytics. *Spectrum of Research*, *5*(1).
7. Das, S. R., Afroz, S., Rashid, H. U., & Chowdhury, M. A. A. (2026). Deep Learning-Driven Financial Fraud Detection: An Enterprise Risk Analytics Framework for Real-Time Anomaly Detection and Regulatory Compliance. *The USA Journals TAJET*, *8*(06), 38-63.
8. Dixit, S. (2024). Advanced generative AI models for fraud detection and prevention in FinTech: Leveraging deep learning and adversarial networks for real-time anomaly detection in financial transactions.
9. Karimkhani, M., Aluvihara, S., Karimkhani, M., & Alqasi, N. J. K. (2025). The Machine Learning (ML) Revolution in Financial Risk Management from Traditional Methods to a Predictive Paradigm: A Review. In *Proceedings of the Second National Conference on A World Without Oil; Iranian E-Commerce Scientific Association: Tehran, Iran*.
10. Khan, S. U., Zafar, U., Imran, S., & Ali, M. (2026). Artificial Intelligence–Driven Fraud Detection in FinTech: Strengthening Cybersecurity Against Digital Financial Scams. *Journal of Business Insight and Innovation*, *5*(6), 72-82.
11. Logapriya, T., Thangamayan, S., Niranjana, K., Girija, S., Premalatha, R., & Thilakanandan, C. (2026, May). Predictive Analytics in Fintech: AI-Driven Risk Assessment Models. In *2026 2nd International Conference on Sustainable Computing and Integrated Communication in Changing Landscape of AI (ICSCAI)* (pp. 553-559). IEEE.
12. Mada, L. (2025). AI and ML in FinTech and Payments Processing: Exploring Models, Use Cases, and Success Stories. *Journal Of Engineering And Computer Sciences*, *4*(10), 1-9.
13. Mahajan, N. (2024). AI-enabled risk detection and compliance governance in fintech portfolio operations. *Cuestiones de Fisioterapia*, *53*(03), 5366-5381.
14. Mohammed, H. S., Sallow, Z. B., & Zangana, H. M. (2026). AI-Driven Fraud Detection in Digital Banking: A Hybrid Approach using Deep Learning and Anomaly Detection. *Sistemasi: Jurnal Sistem Informasi*, *15*(1), 209-219.
15. Naeem, W., Butt, M. A., & Javeid, U. (2026). Machine Learning-Based Fraud Detection Systems and Their Effectiveness in Reducing Cybersecurity Risks in Digital Banking. *Social Science Review Archives*, *4*(2), 2553-2573.
16. Nawaz, Y., & Musah, M. (2025). Enhancing Fintech Security and Efficiency: A Unified Framework for Real-Time Fraud Detection Using Deep Neural Networks.
17. Ononiwu, M., Azonuche, T. I., Okoh, O. F., & Enyejo, J. O. (2023). Machine learning approaches for fraud detection and risk assessment in mobile banking applications and fintech solutions. *International Journal of Scientific Research in Science, Engineering and Technology*, *10*(4), 1-10.
18. Pal, T. (2026). The Role of AI-Based Decision Support in Financial Risk Management and Anomaly Detection. *American Journal of Data Science and Analytics*, *7*(06), 327-359.

19. Prabhu, S., Jothikantham, P. V., Mary, R. A., & Thirunavukkarasu, M. (2025). AI in Finance: Predictive Analytics for Fraud Detection and Risk Management. In *Advanced AI and Data Science Applications* (pp. 234-247). Auerbach Publications.
20. Pundhir, S. K. S., Mittal, R., Anand, I., Muneeb, S. M., & Singh, K. (2026). AI and Machine Learning-Based Predictive Models for Risk Assessment and Fraud Detection in the Finance Sector. In *Harnessing AI and Predictive Analytics for Decision-Making and Competitive Advantage* (pp. 1-30). IGI Global Scientific Publishing.
21. Radha, M., Vasa, Y., Kumbham, A. R., Vallurupalli, P., & Kumar, S. A. (2025, July). A Hybrid Graph Neural Network-Based Reinforcement Learning Approach for Adaptive Cybersecurity Risk Management in FinTech. In *2025 International Conference on Computing Technologies & Data Communication (ICCTDC)* (pp. 1-6). IEEE.
22. Shehadeh, M. (2025). Exploring cutting-edge algorithms in FinTech: Leveraging machine learning and artificial intelligence for achieving sustainability.
23. Shukla, S. S. (2024). Machine Learning for Financial Risk Assessment and Fraud Detection. *Journal of Emerging Intelligence and Engineering Technologies*, *1*(01), 27-36.
24. Upadhyay, N. (2026). Adaptive Machine Learning for Emerging Fraud Patterns in FinTech Transactions. *Journal of Artificial Intelligence and Semiconductor Integrated Hardware*, *1*(1), 7-13.
25. Zangana, H. M., & Mohammed, H. S. (2025). Cybersecurity in FinTech: A Machine Learning-Based Framework for Threat Detection in Mobile Payments. *Intelligent Methods In Engineering Sciences*, *4*(3), 66-73.