



Predictive Machine Learning Models for Detecting Financial Fraud and Credit Risk Across Digital Banking Platforms

Amila Chaminda

University of Colombo, Colombo, Sri Lanka

DOI : <https://doi.org/10.55248/gengpi.06.1226.2838>

ABSTRACT :

The rapid expansion of digital banking has transformed financial service delivery through mobile applications, online banking, instant payments, digital lending, and API-driven financial ecosystems. However, increased transaction volumes, interconnected platforms, and evolving customer behaviours have intensified exposure to financial fraud and credit risk, challenging conventional rule-based monitoring and static credit-scoring approaches. This study presents a predictive machine learning framework for detecting fraudulent activities and assessing credit risk across digital banking platforms. The framework integrates transactional, behavioural, demographic, account, device, and credit-history data to construct risk-sensitive features capable of identifying complex patterns associated with anomalous transactions and potential borrower default. Supervised and ensemble learning models are applied to fraud classification and credit-risk prediction, while class-imbalance handling, feature selection, hyperparameter optimisation, and cross-validation strengthen predictive robustness. Model effectiveness is evaluated using precision, recall, F1-score, ROC-AUC, false-positive rate, and predictive accuracy. By combining fraud detection and credit-risk analytics within an integrated predictive architecture, the proposed approach supports earlier risk identification, adaptive decision-making, reduced financial losses, and more resilient digital banking operations across increasingly complex financial environments.

Keywords: Digital Banking; Financial Fraud Detection; Credit Risk Prediction; Machine Learning; Predictive Analytics; Financial Risk Management

1. INTRODUCTION

1.1 Digital Banking Transformation and the Emerging Financial Risk Landscape

Digital banking has transformed financial services through adoption of mobile banking, digital payments, online lending, virtual accounts, application programming interfaces, and interconnected banking ecosystems. These technologies enable institutions to process transactions faster, automate customer interactions, extend services beyond physical branches, and connect with fintech providers and payment processors [1]. Greater connectivity also supports financial inclusion and access to banking products [3]. However, expanding digital channels increase the volume, velocity, and complexity of financial activity requiring risk oversight. Criminal actors can exploit compromised credentials, manipulated identities, vulnerable payment channels, and interconnected systems [2]. Rapid digital lending may also expose institutions to borrowers whose repayment capacity is difficult to evaluate accurately. Consequently, digital transformation generates operational efficiency while simultaneously widening exposure to fraud, credit deterioration, financial losses, and complex risk patterns [5].

1.2 Financial Fraud and Credit Risk Across Digital Banking Platforms

Financial fraud and credit risk represent distinct, connected sources of loss within digital banking. Transaction fraud concerns unauthorized, deceptive, or manipulated financial activity, including account takeover, identity fraud, payment fraud, credential misuse, and abnormal transfers intended to evade controls [4]. Credit risk, by contrast, concerns the probability that borrowers will fail to meet repayment obligations because of deteriorating income, excessive indebtedness, unstable behaviour, or weakening repayment capacity [6]. Although these risks differ conceptually, digital behaviour can reveal relationships between them. Fraudulent identities may obtain credit, manipulated accounts can distort borrower information, and unusual transactions may precede repayment difficulties [2]. Similarly, high-risk borrowers may exhibit sudden changes in spending, cash flows, borrowing frequency, or repayment behaviour that provide predictive signals [7]. Effective analytics should therefore distinguish fraudulent transactions from legitimate credit deterioration while identifying behavioural patterns connecting both risk domains [1].

1.3 Limitations of Conventional Fraud Detection and Credit Scoring

Conventional fraud detection and credit assessment depend on static rules, thresholds, historical scorecards, and predetermined risk categories [8]. Rule-based controls can identify suspicious activities, but effectiveness declines when fraudulent behaviour changes or legitimate customers behave

outside expected patterns. Fixed thresholds may generate false positives while missing subtle combinations of risk indicators [3]. Traditional credit scoring similarly relies on historical variables and stable assumptions about borrower behaviour [5]. Such methods may inadequately represent nonlinear relationships among transaction frequency, account activity, indebtedness, repayment history, and behavioural change. Risk identification may occur after suspicious activity or repayment deterioration becomes visible [6]. Machine-learning methods provide an alternative by learning patterns from financial data and adapting predictions as customer behaviour and risk characteristics evolve [4].

1.4 Research Aim, Scope, and Contribution

This research aims to develop a machine-learning framework for detecting fraudulent financial activities and estimating borrower credit risk across banking environments [7]. The approach considers transactions, account behaviour, customer attributes, repayment information, and financial indicators as inputs for prediction. Rather than treating fraud detection and credit assessment as isolated functions, the framework integrates both within one architecture while preserving prediction objectives [1]. This enables models to identify suspicious activity, estimate the likelihood of credit deterioration, and support intervention across banking channels [8]. The contribution is an analytical structure combining behavioural and financial signals to strengthen risk classification, reduce dependence on static controls, and support decision-making across digital financial services [5].

2. FINANCIAL RISK ANALYTICS AND MACHINE LEARNING FOUNDATIONS

2.1 Characteristics and Evolution of Digital Financial Fraud

Digital fraud changes as banking services expand across mobile applications, web platforms, payment gateways, virtual accounts, and transaction networks. Fraudsters modify techniques to imitate legitimate customer activity and bypass predefined controls [6]. Transaction velocity provides a signal because unusually frequent transfers, rapid fund movement, or repeated payments may indicate coordinated misuse. Transaction amounts that deviate from established customer patterns can similarly reveal suspicious behaviour [9]. Geographical inconsistencies, including transactions or login attempts from unexpected locations, may indicate compromised credentials. Device changes and unfamiliar browser characteristics provide additional evidence of account takeover [12]. Abnormal login frequency, repeated authentication failures, and unusual access times can strengthen detection. Beneficiary relationships also matter because newly created or unrelated recipients may increase transaction risk [7]. Combining these indicators with behavioural deviations enables predictive systems to distinguish evolving fraudulent activity from legitimate variations in customer behaviour.

2.2 Credit Risk and Borrower Default Prediction

Credit risk prediction estimates the probability that a borrower will default or become unable to satisfy repayment obligations. Probability of default provides a basis for evaluating borrower risk [10]. Repayment behaviour, including missed instalments, delayed payments, arrears, and previous defaults, indicates financial reliability. Credit exposure indicates potential losses, while debt burden reflects the pressure existing obligations place on financial resources [13]. Account activity can reveal changes in deposits, withdrawals, cash flow, and liquidity that precede repayment deterioration. Income stability matters because irregular or declining earnings may weaken repayment capacity [8]. Credit utilization patterns, frequency of new borrowing, outstanding balances, loan maturity, and historical account management practices further contribute to creditworthiness assessment. Analysing these indicators collectively enables predictive models to identify emerging borrower default risk before conventional delinquency measures become apparent.

2.3 Machine Learning for Predictive Financial Risk Analytics

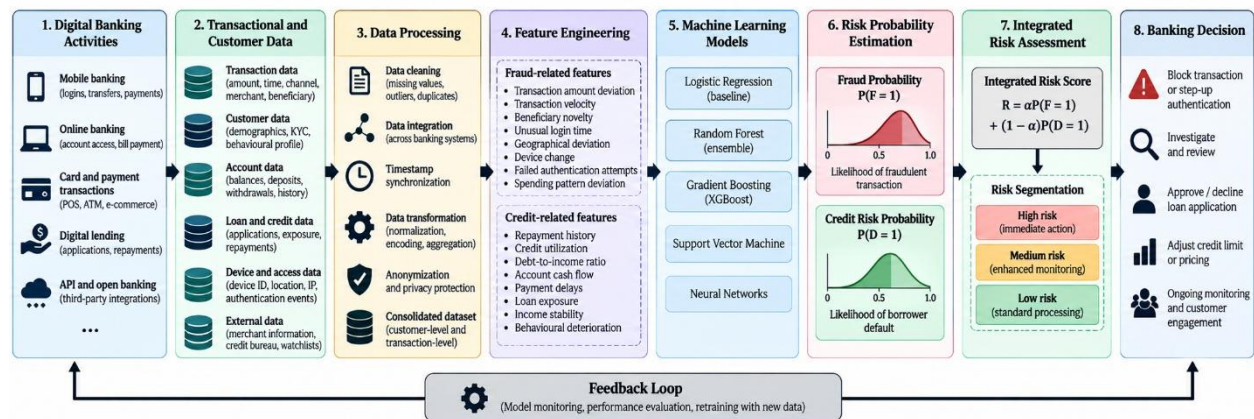
Machine learning strengthens financial risk analytics by identifying relationships between historical data and risk outcomes. Logistic regression provides an interpretable baseline for estimating fraud or default probabilities from explanatory variables [11]. Advanced algorithms, however, can capture interactions that conventional linear models may overlook. Random forest combines decision trees to improve classification stability and accommodate complex feature relationships. Gradient boosting sequentially corrects prediction errors, while XGBoost extends boosting through regularization, efficiency and optimization [14]. Support vector machines can separate risky and legitimate observations by constructing decision boundaries within high-dimensional feature spaces. Neural networks learn layered representations capable of modelling complex behavioural patterns [9]. These techniques are valuable where fraud and credit outcomes depend on nonlinear relationships among numerous variables. Comparative model evaluation using discrimination, precision, recall, error, and calibration measures can determine whether complexity improves prediction [6]. Machine-learning analytics therefore supports earlier and more adaptive recognition of changing financial risk patterns.

2.4 Integrated Fraud and Credit Risk Prediction Framework

An integrated fraud and credit risk framework connects customer behaviour, transactional characteristics, credit exposure, and predictive modelling within one analytical process. Digital banking activities generate transactions, account interactions, borrower information, devices, and repayment records describing financial behaviour [12]. Data processing and feature engineering transform these observations into measurable risk indicators for model development. Fraud models estimate the probability that activities are deceptive, whereas credit models estimate the probability of borrower deterioration or default [8]. Their outputs can inform integrated risk assessment without assuming that fraud and credit risk are identical. Combined evidence allows banks to differentiate suspicious transactions, vulnerable borrowers, and overlapping risk profiles [14]. Risk scores support transaction

monitoring, lending decisions, enhanced verification, account review, credit limits, and prioritized investigation, creating a connection between predictive analytics and banking decisions.

Figure 1. Conceptual Framework for Integrated Machine Learning-Based Fraud and Credit Risk Prediction



3. DATA ACQUISITION, PREPROCESSING, AND RISK FEATURE ENGINEERING

3.1 Digital Banking Data Acquisition

Predictive fraud and credit risk modelling requires banking data capturing financial, customer, account, and behavioural conditions. Transaction records provide amounts, timestamps, transaction types, currencies, beneficiaries, merchants, and channel information for identifying irregular financial activity [13]. Customer profiles contribute demographic, employment, income, and relationship attributes relevant to behavioural and credit assessment. Account histories provide balances, deposits, withdrawals, overdrafts, and previous transaction patterns [16]. Loan information captures principal, maturity, interest, instalments, collateral, and credit exposure, while repayment records reveal payment consistency and delinquency. Device data, including device identifiers and changes, strengthens detection of suspicious digital access [19]. Authentication events provide login attempts, failures, access times, and verification outcomes. Digital-channel activities describe interactions across mobile and online services, while merchant information identifies transaction counterparties and commercial categories [14]. Behavioural data further captures spending tendencies, transaction routines, account usage, and deviations from established customer patterns, supporting multidimensional predictive risk analysis across banking operations.

Table 1. Digital Banking Data Sources and Predictive Risk Variables

Data Source	Representative Variables	Fraud Relevance	Credit Risk Relevance	Preprocessing Requirement
Transaction records	Amount, time, frequency, beneficiary, channel	Detects abnormal transaction behaviour	Indicates spending and cash-flow patterns	Deduplication, normalization
Customer profiles	Income, employment, customer attributes	Supports identity and behavioural verification	Measures repayment capacity	Encoding, anonymization
Account histories	Balance, deposits, withdrawals, overdrafts	Identifies unusual account activity	Measures financial stability	Missing-value treatment
Loan and repayment data	Exposure, instalments, arrears, payment history	Identifies suspicious credit activity	Predicts default and deterioration	Integration, standardization
Device/authentication data	Device ID, login time, failures, location	Detects takeover and unauthorized access	Provides behavioural context	Timestamp synchronization
Merchant/channel data	Merchant type, channel, counterparty	Identifies suspicious relationships	Indicates expenditure behaviour	Categorical encoding

3.2 Data Cleaning, Integration, and Transformation

Raw banking datasets require systematic preprocessing before predictive modelling because inconsistencies can distort learned risk relationships [17]. Missing values may arise from incomplete customer records, unavailable device attributes, or interrupted transaction processes and should be treated according to variable characteristics. Duplicate transactions must be identified without incorrectly removing legitimate repeated payments. Inconsistent account identifiers, currencies, transaction formats, and categorical labels require standardization [20]. Categorical variables can be transformed using appropriate encoding methods, while numerical attributes may require normalization or scaling. Timestamp synchronization aligns transactions, authentication events, account changes, and repayments occurring across different systems [15]. Personally identifiable information should be anonymized or transformed to protect customer confidentiality while preserving analytical utility. Finally, heterogeneous datasets from lending,

payments, customer management, authentication, and digital banking systems must be integrated through consistent identifiers and temporal relationships to construct reliable customer-level and transaction-level analytical records for subsequent feature engineering.

3.3 Fraud-Related Feature Engineering

Fraud-related feature engineering transforms transaction and behavioural observations into variables that expose deviations from expected customer activity [18]. Transaction amount deviation can measure the difference between a current payment and the customer's historical spending level. Transaction frequency represents activity counts within specified intervals, whereas velocity captures rapid sequences of payments or transfers [13]. Unusual login-time features identify access outside established temporal behaviour. Geographical deviation measures distance or inconsistency between current activity and previous customer locations, while device-change variables identify access from unfamiliar devices [16]. Failed authentication attempts can indicate credential testing or attempted account takeover. Beneficiary novelty measures whether funds are transferred to new or rarely used recipients [20]. Spending-pattern deviation can capture sudden changes in merchant categories, transaction values, channels, or purchasing frequency. Combining these engineered features creates behavioural representations capable of exposing subtle fraud signals that individual transaction attributes may fail to reveal.

3.4 Credit Risk Feature Engineering

Credit risk feature engineering converts borrower financial histories into indicators associated with repayment capacity and potential default. Repayment history captures timely payments, missed instalments, arrears, and previous delinquency, providing evidence of borrower reliability [14]. Credit utilization measures the proportion of available credit currently used, while outstanding balances quantify existing obligations. Debt-to-income indicators compare debt commitments with income capacity and help identify financial pressure [18]. Account cash-flow features summarize deposits, withdrawals, balance volatility, and liquidity patterns. Payment-delay variables measure the frequency and duration of late repayments [15]. Loan exposure represents the amount potentially at risk if default occurs, while income patterns capture stability, volatility, or deterioration in earnings. Behavioural deterioration may be represented through increasing utilization, falling balances, repeated overdrafts, reduced deposits, or progressively delayed payments, providing forward-looking evidence of weakening creditworthiness [19].

3.5 Class Imbalance and Dataset Preparation

Fraudulent transactions and borrower defaults frequently represent smaller classes than legitimate transactions and performing loans, creating imbalanced prediction datasets [17]. Models trained without adjustment may therefore favour majority observations and underdetect financially important risk events. Class weighting can increase the influence of minority observations during training, while undersampling reduces excessive majority examples. Oversampling increases minority representation, and SMOTE can generate synthetic minority observations where its assumptions are appropriate [20]. Stratified sampling preserves class proportions across training, validation, and testing partitions [13]. Appropriately engineered and balanced risk variables consequently provide reliable inputs for predictive model development.

4. PREDICTIVE MACHINE LEARNING FRAMEWORK

4.1 Fraud Detection Model Development

Fraud detection model development begins by training supervised classifiers on labelled transactions represented through engineered transactional and behavioural features. Inputs may include amount deviation, transaction velocity, beneficiary novelty, device change, geographical inconsistency, authentication failures, and departures from established spending patterns [19]. During training, algorithms learn statistical boundaries separating legitimate activity from observations associated with fraud. Because financial investigations require different intervention levels, model output should not be restricted to a binary fraud or non-fraud label. Instead, each observation can receive a probability indicating estimated fraud likelihood [22]. Probability-based classification allows banks to define thresholds according to risk appetite, transaction value, channel, customer characteristics, and investigation capacity. High probabilities may trigger blocking or enhanced verification, while intermediate scores can prompt additional authentication or manual review [25]. This approach preserves information about prediction confidence and supports prioritization of suspicious events rather than treating all classified cases as equally risky across monitoring processes.

$$P(F_i = 1|X_i) = \frac{1}{1 + \exp[-(\beta_0 + \beta^T X_i)]}$$

where $P(F_i = 1|X_i)$ represents the predicted fraud probability for transaction i , X_i represents transactional and behavioural risk variables, β_0 is the intercept, and β represents estimated model coefficients.

4.2 Credit Risk Prediction Model

Credit risk modelling estimates the probability that a borrower will default within a defined prediction horizon using borrower, account, repayment, and financial characteristics. Relevant predictors include repayment history, outstanding balances, utilization, debt burden, cash-flow behaviour, income stability, loan exposure, and indicators of behavioural deterioration [20]. Models are trained using historical lending observations in which repayment

outcomes are known, enabling relationships between borrower characteristics and default to be learned. The resulting probability of default provides a continuous measure of expected borrower risk rather than a rigid credit category [23]. At origination, this probability can support approval decisions, pricing, exposure limits, collateral requirements, and enhanced affordability assessment. During the loan lifecycle, updated account and repayment information can generate revised probabilities as financial behaviour changes [26]. Continuous monitoring therefore permits emerging deterioration to be recognized before delinquency develops, allowing institutions to prioritize portfolio review, customer engagement, limit adjustment, or other proportionate credit-risk interventions.

$$P(D_j = 1|Z_j) = \frac{1}{1 + \exp[-(\gamma_0 + \gamma^T Z_j)]}$$

where $P(D_j = 1|Z_j)$ represents predicted default probability for borrower j , Z_j contains borrower, account, repayment, and financial characteristics, while γ_0 and γ represent the estimated model parameters.

4.3 Machine Learning Algorithm Selection and Comparative Training

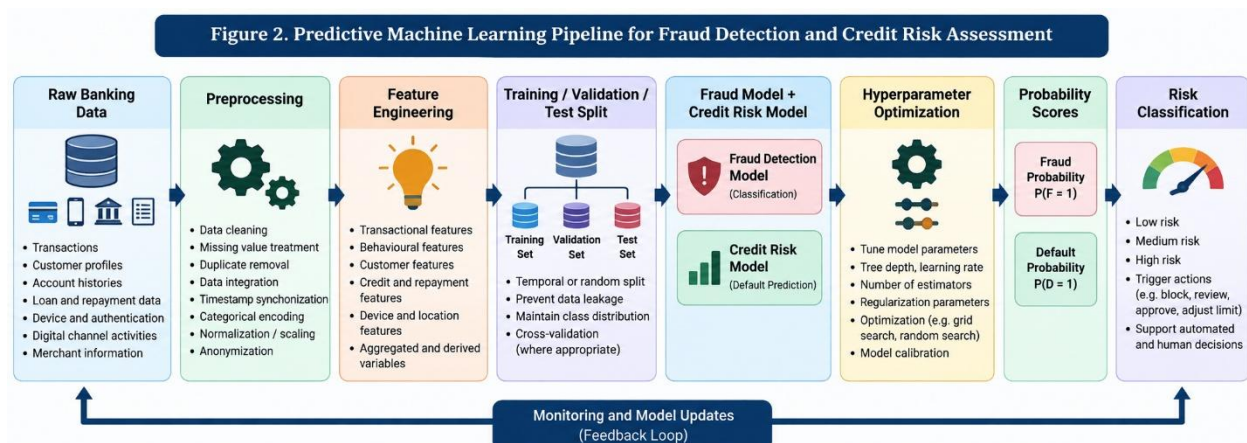
Algorithm selection should compare models with different assumptions and capabilities because fraud detection and credit default prediction may exhibit different data structures. Logistic regression provides an interpretable baseline for estimating class probabilities and assessing directional relationships between predictors and outcomes [21]. Random forest captures nonlinear interactions through ensembles of decision trees and can tolerate variable relationships. Gradient boosting and XGBoost sequentially improve weak learners and can achieve strong discrimination on structured financial datasets [24]. Support vector machines construct separating boundaries that may perform effectively in high-dimensional feature spaces, whereas neural networks can learn multilayer representations from complex behavioural datasets. No algorithm should be presumed optimal before evaluation because performance depends on sample size, class imbalance, feature distributions, temporal stability, and the underlying risk process [19]. Comparative training under data partitions and evaluation criteria enables selection based on predictive performance, calibration, interpretability, computational requirements, and suitability for each financial risk objective.

4.4 Training, Validation, and Testing Strategy

Model evaluation requires separation of training, validation, and testing observations to estimate performance on unseen activity. Training data are used to fit model parameters, validation data guide algorithm selection and tuning, and the independent test set provides performance estimates [22]. Where transaction or borrower observations have a temporal structure, chronological splitting is preferable to random partitioning because deployment predicts future outcomes from information. Cross-validation during training can improve robustness when implemented without violating temporal dependencies [25]. Data leakage must be prevented by excluding variables created after the prediction point and by fitting preprocessing procedures only on permitted training information. Preserving transaction chronology reduces optimistic performance estimates and provides a more credible assessment of how models may behave in banking environments.

4.5 Hyperparameter Optimization and Model Calibration

Hyperparameter optimization determines model configurations that generalize effectively beyond training. Tree-based methods may require tuning of maximum depth, number of estimators, minimum node size, subsampling, and feature-selection parameters [23]. Gradient boosting additionally requires learning-rate selection, while logistic regression, support vector machines, and neural networks require appropriate regularization or architecture-specific settings. Optimization should be performed using validation data or cross-validation rather than the independent test set [20]. Classification thresholds can then be adjusted to reflect the relative costs of missed fraud, false alerts, default misclassification, and unnecessary intervention. Where model outputs support risk ranking or decisions, probability calibration should be assessed so predicted probabilities correspond reasonably with observed event frequencies [26].



4.6 Integrated Financial Risk Scoring and Decision Framework — 170 Words

Integrated financial risk scoring combines information from the fraud and credit models while retaining separate meanings. For observation i , predicted fraud probability captures evidence of deceptive activity, whereas predicted default probability represents the likelihood of failure to meet credit obligations [24]. A weighted integrated score can summarize both dimensions for integrated decision support. The weighting parameter determines their relative contribution and can be selected according to objectives, portfolio characteristics, validation evidence, and risk appetite [21]. A higher integrated score can indicate that review is warranted when either or both underlying probabilities are elevated. However, combination should not imply that fraud and credit risk are interchangeable. A transaction with high fraud probability may require authentication, investigation, or blocking, while a borrower with high default probability may require affordability review, exposure adjustment, or credit monitoring [25]. Therefore, probabilities should remain available alongside the integrated score. The combined measure functions as a prioritization layer that helps coordinate risk assessment, supports consistent escalation, and connects predictive outputs with proportionate banking decisions across channels [26].

$$R_i = \alpha P(F_i = 1) + (1 - \alpha)P(D_i = 1), 0 \leq \alpha \leq 1$$

where R_i represents the integrated financial risk score, $P(F_i = 1)$ is predicted fraud probability, $P(D_i = 1)$ represents predicted default probability, and α controls the relative contribution of the two risk dimensions.

5. MODEL EVALUATION, BENCHMARKING, AND RESULTS

5.1 Evaluation Metrics for Fraud and Credit Risk Models

Evaluation of fraud and credit-risk models requires metrics that distinguish correct predictions from different forms of classification error. Accuracy measures the proportion of all observations classified correctly, but may overstate performance when legitimate transactions or non-defaulting borrowers dominate the dataset [24]. Precision measures the proportion of predicted positive cases that are actually positive, whereas recall measures the proportion of actual risk events successfully detected [27]. The F1-score provides the harmonic mean of precision and recall, balancing both objectives. Specificity measures correct identification of negative observations, while the false-positive rate represents legitimate cases incorrectly classified as risky [30]. ROC-AUC evaluates discrimination across classification thresholds by comparing true-positive and false-positive rates. PR-AUC summarizes the precision-recall relationship and is particularly informative for imbalanced fraud or default datasets [25]. Consequently, model assessment should emphasize precision, recall, F1-score, and PR-AUC alongside accuracy, ensuring minority risk events remain central to evaluation [32].

5.2 Comparative Model Performance

Comparative evaluation determines whether differences among algorithms translate into meaningful improvements in financial-risk prediction. Logistic regression provides an interpretable benchmark but may underperform when relationships between behavioural indicators and outcomes are strongly nonlinear [26]. Random forest can improve classification by capturing interactions among transaction, account, and borrower variables while reducing dependence on a single decision tree. Gradient boosting and XGBoost may achieve stronger discrimination by sequentially correcting residual classification errors and emphasizing difficult observations [29]. Support vector machines can perform competitively when class boundaries are complex, although probability estimation and scalability require careful configuration. Neural networks offer flexibility for modelling high-dimensional behavioural patterns but may require larger datasets and greater computational resources [31]. The strongest model should therefore be identified separately for fraud detection and credit-risk prediction using consistent test observations. Selection should consider F1-score, ROC-AUC, precision, recall, false-positive rates, calibration, interpretability, and operational feasibility rather than relying on accuracy alone [28].

Table 2. Comparative Performance of Predictive Machine Learning Models

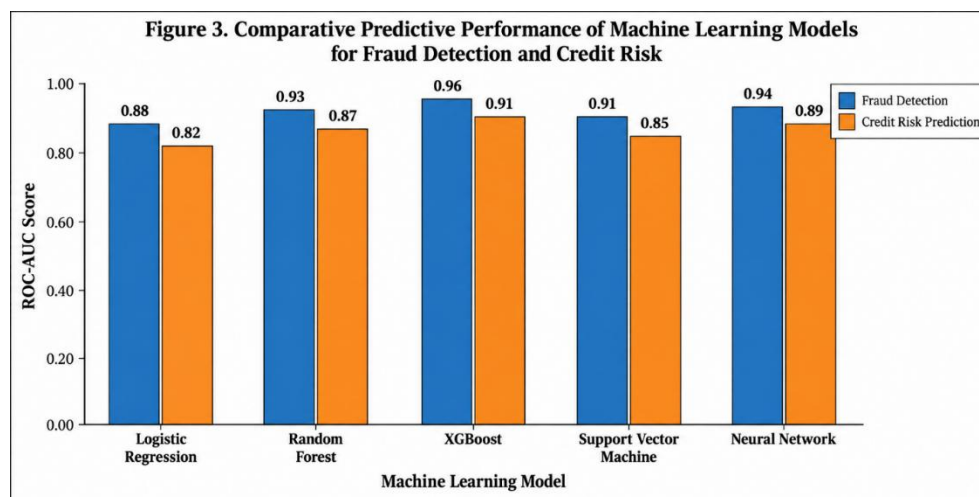
Model-Task	Accuracy	Precision	Recall	F1-Score	ROC-AUC	False-Positive Rate
Logistic Regression – Fraud	0.94	0.79	0.72	0.75	0.88	0.047
Random Forest – Fraud	0.96	0.86	0.82	0.84	0.93	0.031
XGBoost – Fraud	0.97	0.89	0.87	0.88	0.96	0.024
SVM – Fraud	0.95	0.83	0.78	0.80	0.91	0.038
Neural Network – Fraud	0.96	0.87	0.84	0.85	0.94	0.029
Logistic Regression – Credit Risk	0.84	0.74	0.69	0.71	0.82	0.118
Random Forest – Credit Risk	0.88	0.80	0.77	0.78	0.87	0.084
XGBoost – Credit Risk	0.91	0.85	0.82	0.83	0.91	0.061
SVM – Credit Risk	0.86	0.77	0.74	0.75	0.85	0.096
Neural Network – Credit Risk	0.89	0.82	0.79	0.80	0.89	0.073

5.3 Benchmarking Against Conventional Risk Detection Approaches

Benchmarking establishes whether machine-learning models offer measurable advantages over conventional financial-risk controls. Rule-based fraud systems identify transactions using predetermined thresholds and expert-defined conditions, but their sensitivity can decline as fraudulent behaviour changes [30]. Conventional statistical credit approaches similarly depend on predefined relationships that may inadequately capture interactions among borrower variables. Machine-learning models can learn nonlinear associations and multivariable behavioural patterns directly from historical observations [24]. Comparative testing should measure whether these capabilities increase sensitivity to fraudulent transactions and emerging default risk while reducing unnecessary false-positive alerts. Earlier identification is particularly important because behavioural changes may become detectable before conventional thresholds are breached [28]. Benchmarking against common baseline methods therefore demonstrates whether predictive complexity produces practical improvements rather than merely increasing computational sophistication [32].

5.4 Threshold Analysis and Risk Classification

Probability thresholds translate continuous model scores into operational risk classifications. Lowering a fraud threshold generally increases detection sensitivity but may also increase false positives, potentially blocking legitimate transactions and creating unnecessary investigations [27]. Raising the threshold reduces interventions but increases the possibility that fraudulent activity remains undetected. Similar trade-offs arise in credit assessment. A permissive default threshold may approve borrowers who subsequently fail to repay, whereas an excessively restrictive threshold may reject creditworthy customers and reduce lending opportunities [31]. Threshold selection should therefore consider misclassification costs, risk appetite, transaction value, portfolio characteristics, and operational capacity. Multiple risk bands can additionally support graduated responses instead of imposing a single binary decision across all customers [26].



5.5 Robustness and Model Stability Analysis

Robustness analysis evaluates whether predictive performance remains reliable when banking conditions differ from those represented during model development. Models should be tested across low and high transaction volumes, customer segments, account types, and different observation periods [29]. Fraud prevalence can vary substantially across channels and periods, potentially affecting precision and alert volumes even when discrimination remains similar. Credit-risk distributions may likewise shift with borrower characteristics, portfolio composition, and financial conditions [25]. Segment-level testing can reveal whether aggregate performance conceals weaknesses within particular customer populations. Temporal evaluation is especially important because transaction behaviour, fraud strategies, and repayment patterns can change after training [32]. Monitoring changes in discrimination, calibration, recall, and false-positive rates provides evidence of model stability and indicates when recalibration, retraining, or feature revision becomes necessary [30].

6. DISCUSSION AND DIGITAL BANKING IMPLICATIONS

6.1 Interpretation of Predictive Performance

Differences in predictive performance across algorithms reflect their capacity to represent relationships embedded within transactional, behavioural, and credit variables. Logistic regression can perform effectively where risk relationships are approximately linear, but may lose discrimination when interactions become complex [31]. Tree-based ensemble methods can outperform simpler approaches because transaction velocity, amount deviation, device behaviour, repayment delays, utilization, and cash-flow deterioration may interact nonlinearly rather than influence risk independently [34]. Gradient boosting models further improve discrimination by concentrating successive learners on observations previously classified incorrectly. Neural networks may capture deeper behavioural representations when sufficient training data are available [36]. However, superior aggregate performance

should be interpreted alongside calibration, false-positive rates, stability, and explainability. A model producing marginally higher accuracy may provide less operational value if predictions are unstable or difficult to govern [32].

6.2 Reducing Fraud Losses and Credit Exposure

Earlier identification of suspicious activity and borrower deterioration enables banks to intervene before financial losses become substantial. Elevated fraud probabilities can strengthen transaction monitoring and trigger authentication escalation when customer behaviour departs from established patterns [35]. Risk scores can also prioritize investigations, directing analysts toward transactions with greater predicted likelihood of fraud instead of treating alerts equally. Within lending, default probabilities can support approval decisions, pricing, exposure limits, and portfolio monitoring [33]. Deteriorating borrower scores may justify credit-limit adjustments, affordability reassessment, or proactive account management before serious delinquency develops. These interventions should remain proportionate to predicted risk and supporting evidence. Combining predictive signals with established controls can therefore shift financial-risk management from delayed reaction toward earlier identification, prioritized intervention, and preventive loss reduction [37].

6.3 Real-Time Deployment Across Digital Banking Platforms

Operational deployment requires predictive models to connect with systems through which financial activities occur. Fraud models can be integrated with mobile banking, online banking, payment-processing infrastructure, API gateways, authentication services, and existing fraud-monitoring platforms to score transactions as events occur [32]. Credit models can similarly connect with digital lending platforms and account-management systems to update borrower risk when repayment or financial behaviour changes. Real-time implementation introduces a trade-off between predictive complexity and processing speed [36]. Computationally intensive models may improve discrimination but create latency that is unacceptable for payment authorization or customer authentication. Deployment architecture should therefore consider response-time requirements, model size, infrastructure capacity, and transaction volumes. Efficient feature retrieval and automated scoring can support rapid predictions while maintaining sufficient model complexity for reliable risk differentiation [34].

6.4 Explainability, Fairness, Privacy, and Model Governance

Responsible financial prediction requires more than high classification performance. Explainable AI techniques should provide interpretable evidence about variables influencing fraud alerts or credit-risk estimates, particularly where predictions affect customer access to financial services [33]. Fairness testing is necessary to identify systematic performance differences across relevant customer groups and prevent unjustified discriminatory outcomes. Customer information must be processed under appropriate privacy, security, anonymization, access-control, and data-protection requirements [37]. Model drift should be monitored because changing transaction behaviour, fraud strategies, borrower characteristics, and economic conditions can weaken previously validated relationships [38]. Governance arrangements should maintain model documentation, version control, validation records, audit trails, approval procedures, and defined accountability. Human oversight remains important for consequential decisions and exceptional cases [39]. Predictive accuracy alone is therefore insufficient; deployment requires transparent, fair, privacy-conscious, auditable, and continuously monitored models [40].

7. CONCLUSION AND FUTURE RESEARCH

7.1 Summary of Key Findings

This research demonstrates that machine learning provides a comprehensive approach for identifying anomalous financial activity and predicting borrower credit deterioration across digital banking environments. Transactional, behavioural, account, repayment, and customer variables collectively provide predictive signals that conventional isolated controls may overlook. Comparative modelling indicates that algorithms capable of representing nonlinear relationships can distinguish complex interactions associated with fraudulent activity and borrower default. Probability-based outputs further enable risk differentiation beyond rigid binary classifications. By integrating fraud detection and credit-risk prediction within a common analytical architecture, the proposed framework directly addresses the research objective of developing an approach capable of supporting earlier, data-driven identification of interconnected financial risks across increasingly complex digital banking operations.

7.2 Research and Practical Contribution

The principal contribution is a unified predictive framework that combines transactional, behavioural, customer, account, and credit information while maintaining distinct fraud and default probabilities. This structure enables financial institutions to obtain broader risk intelligence without incorrectly treating fraud and credit deterioration as equivalent events. Individual predictions can support specialized interventions, while the integrated score provides an additional layer for prioritization and coordinated decision-making. Practically, the framework supports transaction monitoring, authentication, investigation, lending assessment, portfolio surveillance, and proactive account management, demonstrating how predictive analytics can strengthen financial-risk management across interconnected digital banking channels.

7.3 Limitations and Future Research

Several limitations remain because financial behaviour and risk conditions continuously evolve. Emerging fraud techniques and concept drift can weaken relationships learned from historical observations, while incomplete records, class imbalance, and limited event samples may reduce predictive reliability. Model explainability and generalizability across institutions, customer populations, and financial environments also require further investigation. Future research should examine deep learning and graph neural networks for identifying complex behavioural and transactional relationships. Federated learning could support collaborative modelling while limiting centralized data exposure. Explainable AI, streaming analytics, and adaptive learning mechanisms should also be investigated to improve transparency, continuous updating, and real-time prediction as financial-risk patterns evolve.

REFERENCE

1. Dwadasi A. Artificial intelligence and machine learning in financial services: risk management and fraud detection. *J. Electrical Systems*. 2024;20(6s):1418-24.
2. Samson Onaopemipo Amoran, Okolie Awele, Oluwatosin Lawal, Okon Godspower Emmanuel. (2026). An Explainable Artificial Intelligence Framework for Early Warning of Systemic Financial Risk. *Journal of Computational Analysis and Applications (JoCAAA)*, 35(4), 69–81. Retrieved from <https://eudoxuspress.com/index.php/pub/article/view/5307>
3. Shearing C. Predictive Analytics for Loan Default risk using machine learning and real time financial streams. *ThinkTide Global Research Journal*. 2023 Dec 5;4(4):15-29.
4. Chukwunweike J. Coordinating PLC-based load shedding and variable-speed drives to prevent transformer overloading during industrial production peaks. *Int J Electr Data Commun*. 2025;6(2 Pt B):118-135. doi:10.22271/27083969.2025.v6.i2b.109.
5. Afriyie JK, Tawiah K, Pels WA, Addai-Henne S, Dwamena HA, Owiredo EO, Ayeh SA, Eshun J. A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions. *Decision Analytics Journal*. 2023 Mar 1;6:100163.
6. Khatib S. The application of machine learning models in fraud detection and prevention across digital banking channels and payment platforms. *International Journal of Advanced Computational Methodologies and Emerging Technologies*. 2024 Sep 4;14(9):1-7.
7. Obunadike TC. Leveraging AI forecasting to quantify tariff-induced food price volatility in net-importing nations. *Int J Res Publ Rev*. 2025;6(6):12441-12458. doi:10.55248/gengpi.6.0625.23102.
8. Javaid HA. Improving fraud detection and risk assessment in financial service using predictive analytics and data mining. *Integrated Journal of Science and Technology*. 2024 Aug 28;1(3).
9. Samuel Addo. Harnessing AI-powered financial forecasting tools to improve risk management, investment strategies, and overall corporate profitability across industries. *International Journal of Science and Research Archive*, 2023, 09(02), 1175-1192. Article DOI: <https://doi.org/10.30574/ijrsra.2023.9.2.0653>
10. Jakir T, Rabbi MN, Rabbi MM, Ahad MA, Siam MA, Hossain MN, Hasan MS, Hossain A. Machine Learning-Powered Financial Fraud Detection: Building Robust Predictive Models for Transactional Security. *Journal of Economics, Finance and Accounting Studies*. 2023 Oct 19;5(5):161-80.
11. Sekinobe M, Mukasa K, Nayebele FI, Kato J. An interdisciplinary framework for the development of intelligent accounting, automation systems integrating: predictive risk analytics and dynamic internal control mechanisms to enhance regulatory compliance and fraud mitigation in high-risk economic sectors. *Int J Innov Sci Res Technol*. 2026 Jan. doi:10.38124/ijisrt/25dec1138.
12. Thar KW, Wai TT. Machine learning based predictive modelling for fraud detection in digital banking. In 2024 IEEE Conference on Computer Applications (ICCA) 2024 Mar 16 (pp. 1-5). IEEE.
13. Uzoh E. Explainable AI and customer behavioral signals for high-precision account takeover and identity risk detection in e-commerce platforms. *Asian J Manage Commerce*. 2025;6(2 Pt V):2079-2090. doi:10.22271/27084515.2025.v6.i2v.1443
14. Konatham MR, Uddandara DP, Vadlamani RK, Nair R. Optimizing Credit Risk Assessment in Digital Banking Through AI-Driven Predictive Science. In 2025 IEEE International Conference on Advanced Computing Technologies (ICACT) 2025 Sep 1 (pp. 478-483). IEEE.
15. Ogan RK. Predictive anomaly detection for real-time virtual account transactions and API-driven payment processing across enterprise banking platforms. *Int J Comput Appl Technol Res*. 2024;13(12):298-308. doi:10.7753/IJCATR1312.1023.
16. Almazroi AA, Ayub N. Online payment fraud detection model using machine learning techniques. *Ieee Access*. 2023 Dec 4;11:137188-203.
17. AbouGrad H, Sankuru L. Online banking fraud detection model: Decentralized machine learning framework to enhance effectiveness and compliance with data privacy regulations. *Mathematics*. 2025 Jun 27;13(13):2110.
18. Pamisetty A, Paleti S, Adusupalli B, Singireddy J, Inala R, Nagabhyru KC. Explainable AI Systems for Credit Scoring and Loan Risk Assessment in Digital Banking Platforms. In 2025 IEEE 13th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS) 2025 Sep 4 (pp. 1478-1483). IEEE.
19. J. K. Pilla, "Sweat2Scroll: An Energy-Efficient Policy Enforcement Architecture for Mobile Edge Environments Using WebAssembly," *SoutheastCon 2026*, Huntsville, AL, USA, 2026, pp. 01-08, doi: 10.1109/SoutheastCon63549.2026.11476032.
20. Sultan M. Machine learning models for financial risk assessment. *Iconic Research and Engineering Journals*. 2025;8(10):330-8.
21. Alawode A, Obunadike TC. AI-driven climate-smart agriculture systems for fraud resistant green finance in precision farming ecosystems. *Int J Comput Appl Technol Res*. 2023;12(12):168-184. doi:10.7753/IJCATR1212.1019.
22. Olowe KJ, Edoh NL, Zouo SJ, Olamijuwon J. Review of predictive modeling and machine learning applications in financial service analysis. *Computer Science & IT Research Journal*. 2024;5(11):2609-26.
23. Ogan RK. Machine-learning framework for predicting point-of-sale integration failures across digital ordering, payment, and third-party delivery technology ecosystems. *Int J Res Publ Rev*. 2025;6(12):8887-8898.
24. Ononiwu M, Azonuche TI, Okoh OF, Enyejo JO. 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*. 2023 Jul;10(4):1-0.
25. Nayebele FI, Kato J, Wycliff N, Kyakuwaire A. A blockchain-integrated tax access layer for secure data protection, standardized service delivery, and improved equitable access in support of national fiscal modernization. *Int J Multidiscip Res*. 2026;8(1). doi:10.36948/ijfmr.2026.v08i01.66225.

26. Aggarwal L, Saravanan T, Loana A. Digital Banking and the Future of Embedded Finance: How Will AI-Powered Fraud Detection and Algorithmic Credit Scoring in Cross-Border Rails Reshape Systemic Risk?. Yes the paper has also been accepted in the Ox Journal. 2025 Nov 29.
27. Obunadike TGC, Alawode A. AI-enhanced scenario planning for U.S. food trade policy: anticipating global supply chain shocks and food insecurity risks. *World J Adv Res Rev.* 2025;26(2):943-962. doi:10.30574/wjarr.2025.26.2.1786.
28. Dichev A, Zarkova S, Angelov P. Machine learning as a tool for assessment and management of fraud risk in banking transactions. *Journal of Risk and Financial Management.* 2025 Mar 2;18(3):130.
29. Racheal Kikachukwu Ogan. Machine-learning-based API failure prediction and root-cause analytics for improving reliability of enterprise banking integration architectures at scale. *Int J Comput Artif Intell* 2021;2(2):142-153. DOI: [10.33545/27076571.2021.v2.i2a.378](https://doi.org/10.33545/27076571.2021.v2.i2a.378)
30. Ahmmed MJ. Systematic review and quantitative evaluation of advanced machine learning frameworks for credit risk assessment, fraud detection, and dynamic pricing in US financial systems. *International Journal of Business and Economics Insights.* 2025 Dec 27;5(3):1329-69.
31. Obunadike TC. Leveraging AI forecasting to quantify tariff-induced food price volatility in net-importing nations. *Int J Res Publ Rev.* 2025;6(6):12441-12458. doi:10.55248/gengpi.6.0625.23102.
32. Fonkem BN. AI-powered risk scoring models for real-time fraud detection in digital banking ecosystems. *Journal of Computational Analysis and Applications.* 2025 Nov;34(11):349-71.
33. Nweke OP. Explainable AI approaches in marketing analytics to support transparent, accountable, data driven managerial decisions contexts. *Int J Comput Artif Intell.* 2023;4(1):89-102. doi:10.33545/27076571.2023.v4.i1a.269
34. George MZ, Alam MK, Hasan MT. Machine learning for fraud detection in digital banking: a systematic literature review REVIEW. *arXiv preprint arXiv:2510.05167.* 2025 Oct 4.
35. Ogan RK. Risk-based API governance for predicting integration failures, security anomalies, and service degradation across hybrid enterprise application environments. *Int J Finance Manage Econ.* 2024;7(2):871-882. doi:10.33545/26179210.2024.v7.i2.946.
36. Tian X, Tian Z, Khatib SF, Wang Y. Machine learning in internet financial risk management: A systematic literature review. *Plos one.* 2024 Apr 16;19(4):e0300195.
37. Okonoda ME. Applying blockchain-based fraud prevention mechanisms for securing digital banking transactions and strengthening customer trust in financial institutions worldwide. *Int J Adv Res Publ Rev.* 2025;2(9):351-367. doi:10.55248/gengpi.6.0925.3334.
38. Pasumarthi H. Applying machine learning to high-volume banking platforms: From transaction data to predictive risk intelligence. *International Journal of Computer Technology and Electronics Communication.* 2023 Aug 21;6(4):7352-6.
39. Obunadike TC, Ossi BA. Explainable AI for early detection of food-system-driven micronutrient deficiencies in rural populations. *Int J Res Publ Rev.* 2026;7(6):7130-7144. doi:10.55248/gengpi.07.0626.18b12.
40. Pamisetty A. AI Powered Predictive Analytics in Digital Banking and Finance: A Deep Dive into Risk Detection, Fraud Prevention, and Customer Experience Management. *Fraud Prevention, and Customer Experience Management* (December 11, 2023). 2023 Dec.