SJIF Impact Factor (2026): 8.863| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 4 | April 2026 - Peer Reviewed Journal

MACHINE LEARNING IN CREDIT UNIONS: A REVIEW OF PREDICTIVE ANALYTICS FOR FRAUD DETECTION AND LOAN RISK ASSESSMENT

Evelyn Agyei [1], Eunice Abena Lettu [2]
[1]Connex Credit Union - North Haven Headquarters, Ct. Monroe Branch, USA
[2] Kwame Nkrumah University of Science and Technology, Ghana

Article DOI: https://doi.org/10.36713/epra26818
DOI No: 10.36713/epra26818

ABSTRACT
By delivering more reliable, accurate, and precise decision-making through the analysis of vast behavioral and transactional datasets, machine learning (ML) is revolutionizing credit unions and enhancing loan risk assessment and fraud detection. The current state of predictive analytics is explored in this study, with emphasis on how supervised, unsupervised, and ensemble machine learning models are changing core functions like credit scoring, fraud monitoring, and portfolio risk management. It traces the evolution from inflexible rule-based and manual processes to ML-driven frameworks that utilize anomaly detection and neural networks to capture complex, fast-evolving fraud patterns that traditional methods often fail to identify. Empirical evidence shows that ensemble and deep learning models routinely achieve ROC AUC values above 0.95, with Random Forest and Gradient Boosting reporting AUC ranges of approximately 0.91 to 0.99 and recall values up to 0.88 in highly imbalanced datasets, while XGBoost achieves F1 scores around 0.79. For loan risk assessment, models such as LightGBM and XGBoost achieve AUCs of about 0.95-0.96 and accuracy above 93 percent, outperforming traditional logistic regression models. Large training databases, standardized feature engineering, and hyperparameter tuning for reliable real-time performance are among the significant model-building strategies further highlighted in the paper. Additionally, it highlights the consequences for governance, member retention, and product customization. Future research should concentrate on continuous learning systems, data privacy, and model interpretability.

KEYWORDS: *Predictive Analytics, Machine Learning, Finance, Credit Union, Fraud*

1. INTRODUCTION TO MACHINE LEARNING IN CREDIT UNIONS

The financial services industry has witnessed a deep transformation with the integration of predictive modeling and analysis and machine learning (ML) technologies.

Global estimates suggest that organizations lose around 5% of annual revenues to fraud, corresponding to trillions of dollars, while the surge in digital transactions has made traditional manual and rule-based detection approaches increasingly inadequate [1]. Recent analyses of online payment and card fraud indicate losses in the tens of billions of dollars annually and project further growth without more advanced controls. [2]. According to the American Credit Union Organization, 79% of credit unions reported over $500, 000 in fraud losses between 2023 and 2024 [3]. Over 25% lost more than $1 million annually. Nearly 60% of financial institutions, including credit unions lost > $500, 000 in a single year. From industry survey inference, credit unions are among the most impacted segments, with loss incidence rates higher than the larger banks.

In response, ML and deep-learning-based fraud detection systems have demonstrated substantial performance gains over conventional rule-based methods, particularly in credit card and payment transaction monitoring. Ensemble and deep learning models (e.g., XGBoost, LSTM ensembles, and hybrid architectures) routinely achieve ROC-AUC values around 0.95 or higher and, in some cases, overall accuracies approaching or exceeding 99% while reducing false positives and improving recall for rare fraud events. [4]These improvements enable credit unions to leverage size, datasets, optimize decision-making procedures, reintroduce customer experiences, and mitigate risks more adequately.[5] Whereas banks and other financial institutions have adopted these technologies significantly, credit unions have peculiar opportunities and challenges when deploying such due to their member-owned structure, community-focused objective, and comparatively limited technological resources [6].

SJIF Impact Factor (2026): 8.863| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 4 | April 2026 - Peer Reviewed Journal

Table 1: Differences between Banks and Credit Unions

Dimension	Credit Unions	Banks	ML-Relevant Implications
Ownership & purpose	Member-owned, not-for-profit, cooperative; focus on member welfare and local development	Shareholder-owned, for-profit	Stronger fairness, community impact, and explainability requirements for ML decisions
Governance	Volunteer boards, less performance-linked CEO pay; more female leadership	Professional boards, high variable pay	Fewer specialized tech/ML champions on boards; more conservative risk posture
Scale & scope	Smaller, more specialized, serving defined member base; often local	Larger, diversified, wide product mix	Smaller datasets, more class imbalance, less internal model-risk expertise
Information model	Relies heavily on local “soft” information and relational lending	More standardized, “hard” data and centralized scoring	Tension between soft-information culture and data-hungry, opaque ML
Technology & productivity	Often lower labor productivity and smaller tech budgets, though efficiency can match peers when context-adjusted	Higher productivity, larger IT/analytics budgets	Fewer IT resources, more reliance on vendors, more fragility in deployment workflow

With over 5,000 credit unions and 127 million members, credit unions in the United States are the largest network of financial cooperatives in the world. In their governance, credit unions rely on volunteer directors and are significantly less incentivized by performance-based compensation relative to employees of commercial banks of similar positions [7]. In credit unions today, machine learning (ML) and predictive analysis drive operational efficiency. The industry and client demands resulted in the adoption of machine learning. Credit unions may evaluate large datasets more quickly than with traditional methods courtesy to machine learning (ML), which helps automating mundane operations, accelerate data analysis, and enable real-time decision-making [8]. The outcome of incorporating machine learning techniques in credit unions' daily operations is the main subject of this analysis, which tackles two of the most important operational issues that credit unions must deal with: Finding pertinent research from databases like Google Scholar, IEEE Xplore, ScienceDirect, and SpringerLink can aid with fraud detection and loan risk assessment. The search employed keywords such as *“machine learning in credit unions,” “fraud detection using machine learning,”* and *“predictive analytics in finance,”* combined using Boolean operators to refine results. The review focused on studies published between 2020 and 2025, from which an initial pool was machine learning techniques in credit unions’ routine operations, addressing two of the most critical operational concerns: fraud detection and loan risk assessment. It draws on relevant studies sourced scree, screened for their on relevance to fraud detection, loan machine learning and machine learning applications in financial systems. Specifically, examining how analysis and Machine leaning are used to identify anomalous transactions, reduce financial losses from fraud, assess borrower creditworthiness, and manage loan portfolios more efficiently. The review also from Scopus, screened for their relevance to fraud detection, loan, stigates implementation challenges, and ethical considerations associated with machine learning adoption in credit unions.

The main research questions, screened for their relevance to fraud detection, loan machine learning, questions for this review are:

1. How are machine learning and predictive analysis currently applied to fraud detection and loan assessment in credit unions?
2. What is the performance and limitation of these models present compared to traditional risk assessment methods to reduce fraud in credit unions?
3. What challenges, be it technical, organizational and ethical, affect the adoption of Machine learning in credit unions?

By answering these questions, this review’s goal is to provide a structured understanding of how machine learning, particularly predictive analysis, is modifying risk management strategies in credit unions and to identify gaps for further research.

2. PREDICTIVE ANALYTICS FOR FRAUD DETECTION

Fraud in digital banking is defined as intentional deception perpetuated through electronic financial systems with the goal of illicit financial gain or unauthorized access to resources. Fraud can also be a deviation from expected behavior that undermines the integrity of financial transactions [9]. For additional emphasis, this definition is consistent with regulatory viewpoints like those offered by the Federal Reserve System and Federal Trade Commission, which define fraud as dishonest acts that cause financial or data destruction in digital contexts. Similarly, industry frameworks from organizations like the Association of certified Fraud Examiners emphasize fraud as the misuse of systems for personal gain through deception.

As the world is gearing toward a highly advanced digital financial culture with the advent of financial inclusion and with the accelerated development of digital banking, mobile payments, and online financial services in the U.S., financial institutions particularly credit unions have become progressively targeted by advanced fraud schemes that integrate technology and social engineering strategies. Subsequently, new opportunities are created in the financial sector, making it possible for people who were previously unbanked or underbanked to access financial services, especially from credit unions [10].

Evolving Nature of Digital Fraud

Digital fraud has evolved from physical access to systems to relying on deception of authentication systems or users remotely. These schemes are committed using digital technologies where fraudsters exploit lapses in verification, authentication, or payments processes to deceive customers and financial services providers, setting up unapproved transactions or data misappropriation.

Offenders have embraced the use of technology to commit fraud. Through emails, social networking sites, false websites and data breaches, offenders are to easily and conveniently defraud victims globally. The evolution of the online environment has significantly changed the nature of fraud, from offender, victim and third-party perspectives [11].

This change has magnified the attack surface available to fraudsters. Thousands of millions of transactions are done daily with online banking portals, mobile wallets, credit cards and other digitals payment services where large-scale attacks can happen [12].

In the context of member-owned financial institutions, such as credit unions, these forms of digital fraud typically materialize through phishing, SIM-swap, and account-takeover attacks on online and mobile banking channels, as well as card-not-present payment fraud targeting members' accounts [13][14] Because member-based institutions often operate with lean IT and fraud-risk resources, yet rely on strong trust relationships with their members, they can be particularly exposed to social-engineering-driven schemes and e-channel vulnerabilities that compromise member data, disrupt service availability, and erode confidence in digital channels.[15]

Digital fraud stands out due to its dependence on rapid, high-volume, and often cross-border electronic transactions, making traditional detection strategies insufficient [16]. Fraud is also a systematic risk and is a threat to the safety and soundness of banking systems as well as its role in undermining customer confidence in digital payment infrastructures [17].

There are different digital fraud detection frameworks. First is the traditional fraud framework which has to do with manual audits, rule-based detection and compliance functions. Rapid advancements in digital innovation and globalization have significantly increased the complexity of financial networks, making them more vulnerable to fraud. Traditional fraud detection methods struggle to keep pace with evolving fraudulent strategies, contributing to an estimated global financial loss of $1 - $5 trillion [18]. Second is digital banking fraud which comprises phishing, account takeovers, and transaction laundering. This is most used in the industry due to the shift in the traditional financial system to digital systems. Last is machine learning detection. Machine learning-based technology is giving new hope. However, it is the banking or non-banking institutions that decide how they will adopt this advanced technology to have reduced human biases in loan decision making [19].

This framework consists of supervised and unsupervised learning, anomaly, and neural networks. Machine learning makes use of vast amounts of datasets and models to detect fraud in real-time. The amalgamation of machine learning (ML) and predictive analysis is fundamental to enhancing fraud detection systems as financial institutions deal with rapidly fluctuating illicit activity. The convergence of these technologies reveals how these technologies can work together to enhance the level of precision, effectiveness, and responsiveness of fraud detection systems. By using these machine learning methods and their application to identify fraudulent transactions across. Complex trends and outliers that traditional rule-based systems would overlook can be seen in a range of banking situations [20].

Supervised learning methods have become key in fraud detection due to their ability to classify transactions based on pre-labeled data [21]. Algorithms such as logistic regression, decision trees, and random forests are used extensively in financial fraud detection systems

SJIF Impact Factor (2026): 8.863| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 4 | April 2026 - Peer Reviewed Journal

[22]. Empirical comparisons on real transaction data show that ensemble methods such as Random Forest and Gradient Boosting typically achieve higher fraud-class recall, F1-score, and ROC-AUC than linear models and single trees: for example, Random Forest attains AUC values around 0.98 and recall near 0.88, outperforming logistic regression (AUC ≈ 0.97) and matching or exceeding Gradient Boosting on recall and precision in highly imbalanced datasets [23]. On benchmark credit-card data, XGBoost reaches an F1-score of about 0.79 with precision ≈ 0.84 and recall ≈ 0.74, yielding the highest PRAUC among compared models [24] while tuned Random Forest models frequently obtain accuracy above 99% and AUC ≈ 0.99 [25]. Logistic regression is highly effective in binary classification and often delivers strong precision (e.g., 0.69–0.98) but substantially lower recall on the fraud class (as low as 0.10 in some studies), limiting its ability to capture rare fraud events [26]. Decision trees offer transparency but commonly overfit; they may achieve high training accuracy yet exhibit lower test-set precision and recall than Random Forest or boosted ensembles [27] Random forests, by aggregating multiple trees, generally show the best balance, with F1-scores on the fraud class around 0.5–0.7 and AUC above 0.9 across diverse datasets [28]. These supervised methods are heavily reliant on labeled datasets, which can be challenging to obtain in large-scale financial systems [29] and may be differently constrained in credit unions based on their structure and size. Furthermore, unsupervised and semi-supervised approaches are particularly valuable in detecting unknown fraud patterns where labeled data are sparse or unavailable

Table 2: Representative statistics comparing key fraud algorithms

Model	Precision (fraud)	Recall (fraud)	F1 (fraud)	AUC
Logistic Regression	0.69 - 0.98	0.10-0.93	0.81-0.96	0.76-0.97
Decision Tree	0.61-0.81	0.61-0.79	0.61-0.78	0.74-0.79
Random Forest	0.79-0.96	0.40-0.88	0.53-0.88	0.91-0.99
Gradient/XGBoost	≈0.76–0.84	≈0.38–0.74	≈0.50–0.79	0.90-0.99

Clustering algorithms such as k-means and DBSCAN are frequently employed to identify anomalies by grouping similar transactions and flagging outliers as potential fraud [30].

Clustering algorithms have limitations like sensitivity to noise and outliers since k-means assumes compact, spherical clusters and is highly sensitive to outliers; extreme or "swinging" transaction values can distort centroids and create very small or unstable clusters. [31] Density-based methods like DBSCAN are better at isolating noise, but poor parameter choices can still misclassify many points as noise to merge distinct fraud patterns. Standard k-means are scalable, but many stronger methods, especially spectral clustering and vanilla struggle with very large financial datasets due to eigen-decomposition or neighborhood search costs. [32] Also, financial data are high-dimensional, correlated, and non-spherical; classical k-means using Euclidean distance often fail to capture elongated or rotated "strip-shaped" clusters common in correlated financial variables. [33] These techniques are highly adaptable and capable of uncovering novel fraud schemes in evolving datasets, bridges the gap between supervised and unsupervised approaches. Hybrid models combining clustering with supervised learning techniques have shown significant promise in improving detection rates by preprocessing data for enhanced anomaly identification [34]. However, a high-dimensional data and noise, which are typical features of financial information, can reduce the effectiveness of these approaches [35].

Deep Learning

By modeling intricate data patterns, advanced deep learning approaches including neural networks, long short-term memory (LSTM) the networks, and generative adversarial networks (GANs) have transformed fraud detection. Following their multilayered designs, neural networks are especially efficient at identifying non-linear relationships in data, which makes them useful for identifying complex fraud schemes [36]. Recurrent neural networks, more commonly known of the LSTM type are particularly good at analyzing sequential data, including transaction histories, which makes it possible to identify temporal trends linked to fraudulent activity [37]. Recently, GANs have attracted attention for their ability to produce artificial fraudulent instances that may be utilized to train reliable fraud detection models. Although these methods provide previously unheard-of levels of precision and adaptation, their interpretability is a problem and they often require significant computer resources. Additionally, the use of these machine learning algorithms greatly enhanced the capabilities of fraud detection systems, allowing financial institutions to effectively manage a variety of fraud scenarios. A multi-layered approach for spotting recognized and new fraud patterns is provided by combining supervised, unsupervised, and deep learning techniques. While techniques for clustering handle anomaly detection in large-scale unlabeled datasets, neural networks can be used to detect complicated fraud schemes. Despite these advances, difficulties including computational complexity, problems with data quality, and expectations for interpretability in highly regulated settings continue to be significant considerations to take into account when employing these algorithms [38]. Deep models are generally black boxes, making it hard to trace which inputs drove a credit, trading, or fraud decision. This undermines risk management and model validation as risk managers cannot easily verify whether patterns are economically plausible. Also, this affects trust and adoption as investors and managers cannot explain even when performance is high [39]

Regulatory concerns for AI and deep learning in financial institutions

Financial institutions face a dense regulatory landscape when deploying AI and deep learning for credit, fraud, and risk management. Core obligations cluster around explainability, data protection, and governance, all tightened when systems are classed as high-risk.

Legal rights, documentation, and explainability

GDPR requires "meaningful" information about the logic, significance, and consequences of automated decisions, and many scholars argue this amounts to a right to legibility or explanation, especially in credit scoring scenarios [40]. In some jurisdictions, credit customers can explicitly request reasons for decisions affecting them. This implies detailed technical documentation, logs, impact assessments, and human-oversight procedures for AI models [41].

High-risk classification and human oversight

The EU AI Act explicitly treats credit scoring and many financial risk models as high-risk AI, triggering stricter requirements on risk management, robustness, data governance, and continuous monitoring [42] High-risk systems must support effective human oversight, aligning with the "human-in-command" approach and complementing GDPR's Article 22 safeguards (right to human intervention, contestation, and to express a view) [43]

Real-Time Fraud Systems

In securing financial systems, minimizing fraud risks, and fostering customer confidence, member transactions must be monitored closely with the focus on reducing false positives and false negatives. The monitoring behavior patterns online and analyzing all transactions for signs of suspicious behavior to create precision in minimizing false alarms and flagging potential anomalies [44]. Real-time fraud and risk monitoring in finance is shifting from batch processing to streaming, event-driven architectures to meet strict sub-second or even millisecond decison-time SLAs. These systems typically ingest high-velocity transactions through distributed messaging platforms, then use stream processors to perform stateful feature engineering and online ML scoring on the go. They enrich each event with behavioral and historical context while maintaining high throughput and low latency. [45] Benchmarks show that such pipelines routinely achieve sub-second end-to-end latency at tens of thousands of transactions per second, with some architectures reporting <250 ms, sub-100 ms, or even millisecond-level detection times while preserving high fraud detection accuracy and system uptime [46] Overall, streaming-first or real-time architectures are becoming central for fraud, credit, and liquidity risk analytics because they provide earlier warning signals and materially better control than batch baselines, without sacrificing regulatory compliance or resilience [47]

3. MACHINE LEARNING IN LOAN AND CREDIT RISK

Loan risk and credit risk are closely linked but theoretically distinct components of lending decisions. Credit risk providing the statistical and behavioral foundation for prediction and management that like it is the likelihood of borrower default and the magnitude of potential loss associated with that default. The credit risk assessment (CRA) procedure includes the calculation of probability of losing money, if a borrower defaults on loan or other obligations. It quantifies probability of default (PD), loss given default (LGD), and exposure at default (EAD) in risk models [48]. In comparison, loan risk girds credit risk but also includes wider structural and portfolio factors such as concentration risk, macroeconomic stress, and temporal risk dynamics across a portfolio of loans. Credit risk is a critical problem faced by banking and financial sectors when the borrower fails to complete their commitment to pay back. The factors that could increase credit risk are non-performing assets and frauds which are improved by continuous monitoring of payments and other assessment patterns. CRA is a crucial and effective risk management tactic. It deserves financial risks and provides pertinent guidance on loan acceptance.[49]

Credit Scoring

Credit scoring, a fundamental component of the financial landscape, plays a pivotal role in assessing an individual's credit worthiness, aiding lenders in making informed decisions about extending credit. Credit scoring is a systematic process that evaluates an individual's credit risk based on various financial factors and historical behavior [50]. The primary objective is to quantify the likelihood of a borrower defaulting on credit obligations. Credit scoring relied on rule-based systems and historical data until the emergence and integration of machine learning, transforming the industry by bringing forth a new era of predictive analysis [51]. ML-based credit scoring models (tree ensembles, neural networks, SVMs, k-NN) usually deliver higher predictive accuracy than traditional logistic regression, often with sizable gains in AUC, F1, recall, or precision, especially on complex, non-linear or high-dimensional data [52] However, multiple comparative studies also show that logistic regression can match or even outperform ML models in some settings, particularly on structured, tabular banking data where relationships are closer to linear or the sample is small, reflecting its robustness and low variance. [53] This ML model could be used for credit unions since they have less datasets and are structured differently.

SJIF Impact Factor (2026): 8.863| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 4 | April 2026 - Peer Reviewed Journal

ML models

Recent research shows the broad adoption of diverse ML models in loan risk assessment like gradient boosted trees including XGBoost and LightGBM, random forests and support vector machines and neural networks. These models consistently outperform statistical models by capturing non-linear patterns, interactions, and heterogeneous borrower traits. With high-dimensional financials datasets like public credit risk datasets, they provide vigorous performance and offer high predictive power. [54] These algorithms can learn from historical data, automatically adapt to new patterns, and make data-driving decisions. As these models are highly dependent on data, a critical element in loan risk modeling is feature selection or engineering. Recent empirical work strongly supports the claim that tree-based ensemble ML models (especially gradient boosting, XGBoost, LightGBM, random forests) outperform traditional statistical models such as logistic regression in credit/loan risk prediction.

Table 3: Representative cross-study comparison

Study / Context	Models Compared	Best-Performing Models & Key Metrics	citation
Credit default, real-world dataset	LR, DT, RF, GB, SVM, XGBoost, LightGBM	LightGBM AUC 0.96, Acc 93.1%; XGBoost AUC 0.95 vs LR AUC 0.85	[55]
Loan defaults (business process mgmt)	GB, XGBoost, RF, LightGBM	GB Acc 0.8887, F1 0.8084, Recall 0.8021; XGBoost AUC 0.9714; stated as outperforming traditional statistical models	[56]
U.S. mortgage defaults, Freddie Mac	GBM, XGBoost, LightGBM vs LR	XGBoost/LightGBM ≈98% Acc, higher AUC/F1; LR poorest at identifying bad loans	[77]
Mortgage defaults, Freddie Mac	XGBoost vs LR, NN, RF, GB, DT	XGBoost Acc 98% test, >90% on all other metrics; superior to LR and others	[78]
Bank client credit / FICO benchmark	LR, SVM, RF, GB, DNN, XGBoost	DNN and XGBoost achieve highest AUC/accuracy; ML-based scores would have reduced expected credit losses vs FICO	[79]
Credit card default (UCI)	LDA, LR vs SVM, RF, XGBoost, DNN	Modern ML (RF/XGBoost/DNN) beat LR/LDA on F1, G-mean, AUC	[80][81]

4. FEATURE ENGINEERING

Feature Selection (FS) or engineering is a pivotal technique in machine learning (ML) that improves predictive performance, model interpretability, and computational efficiency by reducing data dimensionality and isolating the most informative variables. [57] In a credit union context, these features can include member-level financial indicators such as payment history, credit utilization, loan amounts, savings and share account behavior, and income stability. They can be further enriched with behavioral attributes and carefully governed alternative data which complement traditional variables and enhance the model's ability to discriminate between low-and high-risk members while supporting fair and transparent credit decisions.

Machine learning model development for fraud detection and credit risk prediction in credit unions depends on vast datasets. Fraud detection systems require scalability and high-volume data processing in real-time since financial systems generate millions of transactions each day. Improvements made in credit risk and fraud detection modeling have transformed from the classical use of statistics to advanced machine learning and deep learning [58].

Handling Data Challenges (Imbalance and Scale)

Imbalanced data is a major challenge in machine learning and the usage of machine learning models. This occurs when the class distribution within a dataset is uneven, resulting in what is referred to as imbalance [59]. Imbalanced datasets present four key challenges:

SJIF Impact Factor (2026): 8.863| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 4 | April 2026 - Peer Reviewed Journal

bias, overlap, feature vector size, and dataset size [60]. Imbalance is prevalent in domains such as credit fraud detection [61]. In fraud detection, the machine learning model tends to exhibit bias towards the predominant class, causing a decrease in True Positives (TP) and an increase in False Positives (FP), allowing fraudulent activities to go undetected. Thus, addressing imbalanced data is imperative for building reliable and effective ML systems. Cost-sensitive learning and ensemble techniques are two key algorithm-level strategies for handling the extreme class imbalance typical of fraud detection. Cost-sensitive learning modifies the loss function or decision rule so that misclassifying a fraud (false negative) incurs a much higher penalty than misclassifying a legitimate transaction (false positive). By encoding asymmetric misclassification costs in a cost matrix or cost-aware loss, the model is pushed to prioritize detecting rare fraudulent cases, aligning predictions with actual financial risk rather than raw accuracy [62] Imbalance can be corrected by simply duplicating existing instances or creating new, synthetic ones through methodologies like SMOTE (Synthetic Minority Oversampling Technique). SMOTE and its derivatives, such as Borderline-SMOTE and ADASYN, synthesize new samples by interpolating between minority class instances that connect through line segments to their nearest neighbors with the same class [63].

Hyperparameter Optimization

Another important factor for success with machine learning models is hyperparameter tuning. Hyperparameters optimization is a technique that is used to select the best hyperparameters that yield the highest performance [64]. Hyperparameters are generally the most fundamental configurations that regulate the behavior of a machine learning model. Examples include learning rate, depth of decision trees, number of estimators, and many more. Optimizing these hyperparameter values could highly influence both model accuracy and efficiency. Advanced hyperparameter optimization techniques, especially Bayesian Optimization, Genetic Algorithms, and grid search methods, have over the past couple of years begun to make the process easier by automating and streamlining it [65]

Evaluation Metrics (Fraud vs Credit Risk)

When handling imbalanced datasets in machine learning, choosing the appropriate evaluation metrics is crucial for precisely assessing model performance. Accuracy is a fundamental assessment criterion utilized in machine learning and data mining. However, accuracy can result in misaddressing if used with an unbalanced dataset. A model may still achieve high overall accuracy even if its classification performance for minority categories is poor if it performs well in the majority categories. Evaluation of metrics like accuracy and precision may not adequately capture model performance in imbalanced datasets. Hence, metrics such as PR-AUC (area under the precision-recall (PR) curve) and ROC-AUC (area under the receiver operating characteristic (ROC) curve), and the F1-score have been proposed and shown to be effective in classifying tasks with imbalanced data [66]. AUC and G-mean are commonly used because they remain robust and mildly influenced by class distribution imbalances and threshold selection. AUC is based on the entire ROC curve, while G-mean incorporates different parts of the confusion matrix, ensuring a more balanced model performance evaluation. This makes them suitable for dealing with situations where there are large differences in the number of positive and negative class samples [67]. In highly imbalanced fraud datasets, evaluation metrics must emphasize correct detection of rare fraudulent cases rather than overall accuracy. ROC-AUC summarizes performance in terms of true positive rate vs. false positive rate and is mathematically invariant to the class ratio when the score distributions are fixed, which can make it appear strong even when precision on the minority (fraud) class is poor [68]. By contrast, PR-AUC summarizes precision vs. recall, so it directly reflects “of all transactions flagged as fraud, how many were actually fraud?” across thresholds, and its baseline value drops as fraud becomes rarer. This makes PR-AUC much more sensitive to changes in false positives and better aligned with business impact in rare-event problems such as card or Medicare fraud, where a model can have high ROC-AUC yet still generate many false alarms or very low precision [69]. Consequently, fraud-detection studies increasingly report PR-AUC (alongside ROC-AUC) as the primary metric for comparing models under extreme class imbalance [70].

Deployment and Regulatory Considerations

When deploying machine learning models in credit unions, efficiency in operation should be balanced with governance and compliance. To provide both real-time streaming and batch processing while guaranteeing scalability and low latency, models must be coupled with core banking systems via API-based serving. For credit unions, smaller scale, member focus, and tighter compliance budgets make operational tuning of fraud systems at least as important as model choice. For credit unions, smaller scale, member focus, and tighter compliance budgets make operational tuning of fraud systems at least as important as model choice. Operationally, credit-union fraud systems must handle concept drift, thresholds, and false-positive workload together: member and fraudster behavior change over time, so drift-aware strategies such as sliding-window/ensemble learning, separate treatment of rapid investigator feedback versus delayed cardholder disputes, and adaptive models (including reinforcement learning or parallel incremental ensembles) are needed to maintain accuracy in streaming credit-card data. [71]

Thresholds should be calibrated using cost-sensitive criteria to balance fraud losses against member friction and limited fraud-team capacity, often via multiple cut-offs (e.g., auto-block vs. send-to-review) rather than a single global score [72]. Properly tuned, these adaptive and cost-aware approaches can both improve detection (18–38% gain in some banking datasets) and keep false-positive alert volumes within small-team workloads, substantially boosting alert precision.

Reliability and auditability depend on appropriate model versioning, monitoring, and rollback procedures. Regulatory and ethical requirements are also crucial: models must adhere to legislative frameworks like the ECOA, GLBA, GDPR, and CCPA, provide clarity through tools like SHAP or LIME, and reduce bias to guarantee equitable treatment of members. Regulators and supervisors require institutions to justify individual decisions (e.g., why a loan was denied), document model logic for audits, and monitor discrimination and bias, which rules out purely opaque "black-box" systems. Explainable AI (XAI) tools address this by making model outputs interpretable without discarding accuracy. SHAP provides global and local feature attributions that show which variables (such as income, transaction amount, or payment history) drive overall risk patterns and specific decisions, supporting policy design, fairness analysis, and regulatory reporting [73]. LIME enables institutions to explain to a consumer or examiner which features most impacted a certain decision in credit scoring or fraud detection by building straightforward local surrogate models around a single prediction [74]. By demonstrating key characteristics (such as payment history, debt ratios, and transaction frequency) while retaining high predictive performance, case studies in credit risk and fraud highlight how SHAP and LIME improve trust and compliance. This helps ensure ML improves efficiency and decision quality while maintaining equity, credibility, or public trust. [75] This guarantees that the use of ML improves the application of Machine Learning (ML) in credit unions presents important opportunities and challenges across member service, risk management, and operational efficiency.

5. IMPLICATIONS OF APPLICATIONS OF ML MODELS IN CREDIT UNIONS

Through ML models, enhanced risk management and personalized services are basically transforming credit unions' engagement with its members, directly impacting retention and product adoption. The use of ML models predicts a higher level of accuracy of loan repayment and default than traditional methods. This gives an accurate assessment of potential borrowers leading to an informed lending decision and management of members' portfolios. These models also tend to lead to hyper-personalized services by analyzing big datasets such as transaction histories, account activity, and preferences. ML can therefore create particularized member profiles. Algorithms can forecast needs like home purchase, retirement as well as deliver aimed messaging and recommendations at the right time that can lead to higher product offer response rates.

The use of personal and financial data in ML models makes it necessary to enforce strict data privacy, regulatory compliance, and ethical standards to maintain member trust. In deploying ML models, bias must be mitigated [76]. Discrimination in lending and credit rating can be maintained by machine learning algorithms that are trained on historical data and replicate societal biases. Certain populations might be negatively impacted by this. ML models must therefore be prepared using a variety of datasets and frequent bias audits. ML systems must use security features like encryption and anonymization, conform with laws like the CCPA and GDPR, and only gather information that is strictly necessary to protect privacy.

6. FUTURE DIRECTIONS

For more predictive capabilities, future research must concentrate on developing more intricate, reliable, and comprehensible models employing fresh datasets and resources. Emerging fields in financial machine learning research, such as federated learning, privacy-preserving machine learning, and graph-based fraud detection, can be factored in as well in future work. Future research may concentrate on improving precision even more, possibly using even more sophisticated ensemble techniques, or strive for implementation in real time in high-throughput financial systems. Extending similar techniques to fraud detection systems outside of this dataset for cross-domain verification could be another intriguing strategy. Additionally, expanding research into graph-based models, dynamic transaction network analysis, and fairness-aware anomaly detection can further improve the detection of complex fraud patterns and ensure equitable model performance across diverse populations.

Transformation in the data infrastructure is required to efficiently and effectively manage rapidly evolving threats like fraud and navigate dynamic credit market conditions. Real-time analytics platforms can be used to detect fraud, assess credit risk, and manage market risk with minimal latency. Real-time AI can cut processing time and adapt sharply to new patterns and evolving threats, while also supporting scalable, privacy-aware, and network-driven analytical frameworks for modern financial systems.

Conclusion

Machine learning and predictive analytics are transforming fraud detection and loan risk assessment in credit unions by generating real-time anomaly detection, adaptive responses to sophisticated threats, and data-based decisions. With techniques like ensemble models, neural networks, and graph-based learning. Credit unions can work on large-scale transactional, behavioral, and loan data to identify fraud, predict defaults, and manage portfolios with greater accuracy than traditional procedures. Nevertheless, there are new challenges with these advanced models such as class imbalance, limited resources, data sparsity and regulatory constraints which make it necessary to have careful model designs, hyperparameter optimization and a look out for fairness, explainability and privacy. Future endeavors aim at real-time analytics, federated and privacy-preserving learning, and adaptive prevention frameworks. With all factors taken into account, the adoption of machine learning and predictive analytics into credit unions offers substantial potential to enhance consumer experiences, risk management, and efficiency in operations in a secure, controlled, and scalable way.

REFERENCES

1. *Chen, Y., Zhao, C., Xu, Y., Nie, C., & Zhang, Y. (2025). Year-over-year developments in financial fraud detection via deep learning: A systematic literature review. arXiv preprint arXiv:2502.00201.*
2. *hmadi, S. (2024). Open AI and its Impact on Fraud Detection in Financial Industry. Journal of Knowledge Learning and Science Technology, ISSN: 2959-6386 (online). https://doi.org/10.60087/jklst.vol2.n3.p281.*
3. *https://www.americascreditunions.org/blogs/americas-credit-unions/credit-unions-battle-frauds-viral-spread-collaborative-defense*
4. *Al-Maari, A., Abdulnabi, M., Nathan, Y., Ali, A., Ali, U., & Khan, M. (2025). Optimized Credit Card Fraud Detection Leveraging Ensemble Machine Learning Methods. Engineering, Technology & Applied Science Research. https://doi.org/10.48084/etasr.10287.*
5. *Olowe, K. J., Edoh, N. L., Zouo, S. J. C., & Olamijuwon, J. (2024). Review of predictive modeling and machine learning applications in financial service analysis. Computer Science & IT Research Journal, 5(11), 2609-2626.*
6. *Migdalski, M. (2024). Credit Union Models in Poland and USA in Comparative Perspective. PRAWO i WIĘŹ, (4).*
7. *van Rijn, J. (2022). The cooperative identity at US credit unions. Journal of Co-Operative Organization and Management, 10(1), 100152.*
8. *Famoti, O., Omowole, B. M., Okiomah, E., Muyiwa-Ajayi, T. P., Ezechi, O. N., Ewim, C. P. M., & Omokhoa, H. E. (2024). Enhancing customer satisfaction in financial services through advanced BI techniques. International Journal of Multidisciplinary Research and Growth Evaluation, 5(06), 1558-1566.*
9. *George, M. Z. H., Alam, M. K., & Hasan, M. T. (2025). Machine learning for fraud detection in digital banking: a systematic literature review REVIEW. arXiv preprint arXiv:2510.05167.*
10. *Girish, K. K., & Bhowmik, B. (2023, December). Historical analysis of financial fraud and its future. In International Conference on Applied Soft Computing and Communication Networks (pp. 51-64). Singapore: Springer Nature Singapore.*
11. *Cross, C. (2022). Meeting the challenges of fraud in a digital world. In The handbook of security (pp. 217-238). Cham: Springer International Publishing.*
12. *Faisal, M. A., & Ahmed, T. (2025, May). Design and implementation of a secure mobile financial payment system. In 2025 IEEE 15th Symposium on Computer Applications & Industrial Electronics (ISCAIE) (pp. 18-23). IEEE.*
13. *H, K., M, N., & Kumar, Y. (2025). Emerging Trends in Digital Banking Fraud: A Case Analysis. International Journal of Research Publication and Reviews. https://doi.org/10.55248/gengpi.6.0325.1281.*
14. *Gavrilko, T., & Poliukhovych, S. (2025). RISKS OF FINANCIAL FRAUD IN THE DIGITAL ENVIRONMENT: METHODS OF COUNTERACTION. Business Navigator. https://doi.org/10.32782/business-navigator.80-50*
15. *ang, H., & S, S. (2021). A Survey on Digital Fraud Risk Control Management by Automatic Case Management System. March 2021. https://doi.org/10.36548/jeea.2021.1.001.*
16. *Thar, K. W., & Wai, T. T. (2024). Machine learning based predictive modelling for fraud detection in digital banking. 2024 IEEE Conference on Computer Applications (ICCA).*
17. *Nair, S. S., Lakshmikanthan, G., Belagalla, N., Belagalla, S., Ahmad, S. K., & Farooqi, S. A. (2025). Leveraging AI and Machine Learning for Enhanced Fraud Detection in Digital Banking System: A Comparative Study. 2025 First International Conference on Advances in Computer Science, Electrical, Electronics, and Communication Technologies (CE2CT)*
18. *Sarna, N. J., Rithen, F. A., Jui, U. S., Belal, S., Amin, A., Oishee, T. K., & Islam, A. M. (2025). AI Driven Fraud Detection Models in Financial Networks: A Review. Ieee Access.*
19. *Kumar, A., Sharma, S., & Mahdavi, M. (2021). Machine learning (Ml) technologies for digital credit scoring in rural finance: a literature review. Risks, 9(11), 192.*
20. *Owen, O., & Morgan, L. (2025). Integrating Machine Learning and Data Analytics for Enhanced Fraud Detection Systems. Available at SSRN 5406842.*
21. *Liu, C. (2025). Retail Fraud Transaction Detection Based on Machine Learning Algorithms. Applied and Computational Engineering. https://doi.org/10.54254/2755-2721/2025.28886.*
22. *Xu, T. (2024). Fraud Detection in Credit Risk Assessment Using Supervised Learning Algorithms. Computer Life. https://doi.org/10.54097/qw9j1892.*
23. *Shahidullah, M., Esa, H., Rob, M., Kamal, M., Rashid, M., Bhuiyan, M., Alam, M., & Shahi, D. (2024). Intelligent Fraud Detection: Applying Advanced Analytics and Cybersecurity Insights in U.S. Finance. Journal of Posthumanism. https://doi.org/10.63332/joph.v4i3.3593.*
24. *Shah, D., & Sharma, L. (2025). Benchmarking Machine Learning Techniques for Credit Card Fraud Detection. Indian Journal Of Science And Technology. https://doi.org/10.17485/ijst/v18i21.903.*
25. *Sopiyan, M., Fauziah, F., & Wijaya, Y. (2022). Fraud Detection Using Random Forest Classifier, Logistic Regression, and Gradient Boosting Classifier Algorithms on Credit Cards. JUITA: Jurnal Informatika. https://doi.org/10.30595/juita.v10i1.12050.*
26. *Wang, C., Nie, C., & Liu, Y. (2025). Evaluating Supervised Learning Models for Fraud Detection: A Comparative Study of Classical and Deep Architectures on Imbalanced Transaction Data. ArXiv, abs/2505.22521. https://doi.org/10.48550/arxiv.2505.22521.*
27. *Lee, C., Fu, M., Wang, C., & Azis, M. (2025). Evaluating Machine Learning Algorithms for Financial Fraud Detection: Insights from Indonesia. Mathematics. https://doi.org/10.3390/math13040600.*

28. *Xu, T. (2024). Fraud Detection in Credit Risk Assessment Using Supervised Learning Algorithms. Computer Life. https://doi.org/10.54097/qw9j1892.*
29. *Nabrawi, E., & Alanazi, A. (2023). Fraud Detection in Healthcare Insurance Claims Using Machine Learning. Risks. https://doi.org/10.3390/risks11090160.*
30. *Aiken, E., Bellue, S., Karlan, D., Udry, C., & Blumenstock, J. E. (2022). Machine learning and phone data can improve targeting of humanitarian aid. Nature, 603(7903), 864-870.*
31. *Herman, E., Zsidó, K., & Fenyves, V. (2022). Cluster Analysis with K-Mean versus K-Medoid in Financial Performance Evaluation. Applied Sciences. https://doi.org/10.3390/app12167985.*
32. *Chen, Y., Zhou, L., Pei, S., Yu, Z., Chen, Y., Liu, X., Du, J., & Xiong, N. (2021). KNN-BLOCK DBSCAN: Fast Clustering for Large-Scale Data. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 51, 3939-3953. https://doi.org/10.1109/tsmc.2019.2956527.*
33. *Chen, Y., Zhou, L., Pei, S., Yu, Z., Chen, Y., Liu, X., Du, J., & Xiong, N. (2021). KNN-BLOCK DBSCAN: Fast Clustering for Large-Scale Data. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 51, 3939-3953. https://doi.org/10.1109/tsmc.2019.2956527.*
34. *Rahman, M., & Kumar, V. (2020, November). Machine learning based customer churn prediction in banking. In 2020 4th international conference on electronics, communication and aerospace technology (ICECA) (pp. 1196-1201). IEEE.*
35. *Sureja, N., Mehta, K., Shah, V., & Patel, G. (2023). Machine learning in wearable healthcare devices. In Machine learning for advanced functional materials (pp. 281-303). Singapore: Springer Nature Singapore.*
36. *Zhuo, Z., & Zhang, S. (2019, February). Research on the application of big data management in enterprise management decision-making and execution literature review. In Proceedings of the 2019 11th International Conference on Machine Learning and Computing (pp. 268-273).*
37. *Sen, J., Sen, R., & Dutta, A. (2021). Machine learning in finance-emerging trends and challenges. arXiv preprint arXiv:2110.11999.*
38. *Jabin, J. A., Khondoker, M. T. H., Sobuz, M. H. R., & Aditto, F. S. (2024). High-temperature effect on the mechanical behavior of recycled fiber-reinforced concrete containing volcanic pumice powder: An experimental assessment combined with machine learning (ML)-based prediction. Construction and Building Materials, 418, 135362.*
39. *Lo, A., & Singh, M. (2023). Deep-learning models for forecasting financial risk premia and their interpretations. Quantitative Finance, 23, 917 - 929. https://doi.org/10.1080/14697688.2023.2203844.*
40. *Malgieri, G., & Comandé, G. (2017). Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation. International Data Privacy Law, 7, 243-265. https://doi.org/10.1093/idpl/ipx019.*
41. *Lazcoz, G., & Hert, P. (2023). Humans in the GDPR and AIA governance of automated and algorithmic systems. Essential pre-requisites against abdicating responsibilities. Comput. Law Secur. Rev., 50, 105833. https://doi.org/10.1016/j.clsr.2023.105833.*
42. *Anang, A., Ajewumi, O., Sonubi, T., Nwafor, K., Arogundade, J., & Akinbi, I. (2024). Explainable AI in financial technologies: Balancing innovation with regulatory compliance. International Journal of Science and Research Archive. https://doi.org/10.30574/ijsra.2024.13.1.1870.*
43. *Juliussen, B. (2025). The Right to an Explanation Under the GDPR and the AI Act. , 184-197. https://doi.org/10.1007/978-981-96-2071-5_14.*
44. *Stumbauer, S. (2025). Transaction Monitoring – Finding the Needle in the Haystack, but Are We Looking at the Right Haystack? The Next Wave of Global Anti-Money Laundering Enforcement: From Strict Compliance to Intelligent Risk Management that Creates Value, 127-144.*
45. *Liu, C., Tang, H., Yang, Z., Zhou, K., & Cha, S. (2025). Big Data-Driven Fraud Detection Using Machine Learning and Real-Time Stream Processing. ArXiv, abs/2506.02008. https://doi.org/10.48550/arxiv.2506.02008.*
46. *Islam, M., Ahmad, M., Zerine, I., Biswas, Y., & Islam, M. (2025). Real-Time Data Stream Analytics and Artificial Intelligence for Enhanced Fraud Detection and Transaction Monitoring in Banking Security. American Journal of Innovation in Science and Engineering. https://doi.org/10.54536/ajise.v4i3.5630.*
47. *Kumar, S. (2025). Real-Time Data Streaming: Transforming FinTech Through Modern Data Architectures. European Journal of Computer Science and Information Technology. https://doi.org/10.37745/ejcsit.2013/vol13n184964.*
48. *Ayari, H., Guetari, P. R., & Kraïem, P. N. (2025). Machine learning powered financial credit scoring: a systematic literature review. Artificial Intelligence Review, 59(1), 13.*
49. *Amarnadh, V., & Moparthi, N. R. (2023). Comprehensive review of different artificial intelligence-based methods for credit risk assessment in data science. Intelligent Decision Technologies, 17(4), 1265-1282.*
50. *Ashofteh, A., & Bravo, J. M. (2021). A conservative approach for online credit scoring. Expert Systems with Applications, 176, 114835.*
51. *Addy, W. A., Ajayi-Nifise, A. O., Bello, B. G., Tula, S. T., Odeyemi, O., & Falaiye, T. (2024). AI in credit scoring: A comprehensive review of models and predictive analytics. Global Journal of Engineering and Technology Advances, 18(2), 118-129.*
52. *[52] Ghoujdam, M., Chaabita, R., Elkhalfi, O., Zehraoui, K., Elalaoui, H., & Idamia, S. (2024). Consumer credit risk analysis through artificial intelligence: a comparative study between the classical approach of logistic regression and advanced machine learning techniques. Cogent Economics & Finance, 12. https://doi.org/10.1080/23322039.2024.2414926.*

53. *Li, Y., & Chen, W. (2020). A Comparative Performance Assessment of Ensemble Learning for Credit Scoring. Mathematics. https://doi.org/10.3390/math8101756.*
54. *Nguyen, Q., Nguyen, L., Hosen, M., Rasel, M., Shorna, J., Mia, M., & Khan, S. (2025). Enhancing Credit Risk Management with Machine Learning: A Comparative Study of Predictive Models for Credit Default Prediction. The American Journal of Applied Sciences. https://doi.org/10.37547/tajas/volume07issue01-04.*
55. *Zhang, X., Zhang, T., Hou, L., Liu, X., Guo, Z., Tian, Y., & Liu, Y. (2025). Data-Driven Loan Default Prediction: A Machine Learning Approach for Enhancing Business Process Management. Syst., 13, 581. https://doi.org/10.3390/systems13070581.*
56. *Vakrani, D. S., Padhye, P. S., Gupta, S. K., Roy, J. K., Nerlekar, V. S., & Parashar, N. (2025). Evaluating AI-driven credit scoring models versus traditional statistical techniques. Discover Artificial Intelligence.*
57. *Atef, M., Gabr, M. I., Seoud, W., & Ouf, S. (2025). Feature Selection and Classification in Machine Learning: Methods and Models for Peer-to-Peer Lending. MSA-Management Sciences Journal, 4(4), 96-113.*
58. *Cao, L., Yang, Q., & Yu, P. S. (2021). Data science and AI in FinTech: An overview. International Journal of Data Science and Analytics, 12(2), 81-99.*
59. *Haykin, S. (1994). Neural networks: a comprehensive foundation. Prentice hall PTR.*
60. *Sowjanya, A. M., & Mrudula, O. (2023). Effective treatment of imbalanced datasets in health care using modified SMOTE coupled with stacked deep learning algorithms. Applied Nanoscience, 13(3), 1829-1840.*
61. *Alamri, M., & Ykhlef, M. (2024). Hybrid undersampling and oversampling for handling imbalanced credit card data. IEEE Access, 12, 14050-14060.*
62. *Priatna, W., Purnomo, H., Iriani, A., Sembiring, I., & Wellem, T. (2024). Optimizing Multilayer Perceptron with Cost-Sensitive Learning for Addressing Class Imbalance in Credit Card Fraud Detection. Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi). https://doi.org/10.29207/resti.v8i4.5917.*
63. *Elreedy, D., Atiya, A. F., & Kamalov, F. (2024). A theoretical distribution analysis of synthetic minority oversampling technique (SMOTE) for imbalanced learning. Machine Learning, 113(7), 4903-4923.*
64. *Wasswa, H., Lynar, T., & Abbass, H. (2023, September). Enhancing IoT-botnet detection using variational auto-encoder and cost-sensitive learning: A deep learning approach for imbalanced datasets. In 2023 IEEE Region 10 Symposium (TENSYMP) (pp. 1-6). IEEE.*
65. *S. Riyanto, I. S. Sitanggang, T. Djatna, and T. D. Atikah, "Comparative analysis using various performance metrics in imbalanced data for multi-class text classification," Int. J. Adv. Comput. Sci. Appl., vol. 14, no. 6, pp. 1–9, 2023.*
66. *Tayebi, M., & El Kafhali, S. (2024). Performance analysis of metaheuristics based hyperparameters optimization for fraud transactions detection. Evolutionary intelligence, 17(2), 921-939.*
67. *Abdelghafour, E. B., Mohamed, C., Noura, A., & Abdelhamid, B. (2024). Enhancing Credit Card Fraud Detection Using a Stacking Model Approach and Hyperparameter Optimization. International Journal of Advanced Computer Science & Applications, 15(10).*
68. *Saito, T., & Rehmsmeier, M. (2015). The Precision-Recall Plot Is More Informative than the ROC Plot When Evaluating Binary Classifiers on Imbalanced Datasets. PLoS ONE, 10. https://doi.org/10.1371/journal.pone.0118432.*
69. *Hancock, J., Khoshgoftaar, T., & Johnson, J. (2023). Evaluating classifier performance with highly imbalanced Big Data. Journal of Big Data, 10, 1-31. https://doi.org/10.1186/s40537-023-00724-5.*
70. *Leevy, J., Khoshgoftaar, T., & Hancock, J. (2022). Evaluating Performance Metrics for Credit Card Fraud Classification. 2022 IEEE 34th International Conference on Tools with Artificial Intelligence (ICTAI), 1336-1341. https://doi.org/10.1109/ictai56018.2022.00202.*
71. *Somasundaram, A., & Reddy, S. (2018). Parallel and incremental credit card fraud detection model to handle concept drift and data imbalance. Neural Computing and Applications, 31, 3-14. https://doi.org/10.1007/s00521-018-3633-8.*
72. *Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C., & Bontempi, G. (2018). Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy. IEEE Transactions on Neural Networks and Learning Systems, 29, 3784-3797. https://doi.org/10.1109/tnnls.2017.2736643.*
73. *Chavakula, S., Albert, C., Ebenezer, E., Bhagat, M., & Mahamuni, C. (2025). Explainable AI (XAI) Using SHAP and LIME for Financial Fraud Detection and Credit Scoring. 2025 International Conference on Advanced Computing Technologies (ICoACT), 1-8. https://doi.org/10.1109/icoact63339.2025.11005238.*
74. *Misheva, B., Osterrieder, J., Hirsa, A., Kulkarni, O., & Lin, S. (2021). Explainable AI in Credit Risk Management. ArXiv, abs/2103.00949. https://doi.org/10.2139/ssrn.3795322.*
75. *Bücker, M., Szepannek, G., Gosiewska, A., & Biecek, P. (2020). Transparency, auditability, and explainability of machine learning models in credit scoring. Journal of the Operational Research Society, 73, 70-90. https://doi.org/10.1080/01605682.2021.1922098.*
76. *Raziyeva, S., & Meraliyev, M. (2025). Bias and Fairness in Automated Loan Approvals: A Systematic Review of Machine Learning Approaches. Journal of Emerging Technologies and Computing. https://doi.org/10.47344/jbzmnx25.*
77. *Nguyen, C. (2025). Advanced loan default prediction models using Machine Learning boosting algorithms. Journal of High School Science. https://doi.org/10.64336/001c.144823.*
78. *Nguyen, C., & Dean, V. (2025). Identifying Optimal Innovative Machine Learning Models for Predicting U.S. Mortgage Loan Defaults: A Comparative Analysis. International Journal of Innovative Technology and Exploring Engineering. https://doi.org/10.35940/ijitee.i1127.14100925.*
79. *Munkhdalai, L., Munkhdalai, T., Namsrai, O., Lee, J., & Ryu, K. (2019). An Empirical Comparison of Machine-Learning Methods on Bank Client Credit Assessments. Sustainability. https://doi.org/10.3390/su11030699.*

80. *Bhandary, R., & Ghosh, B. (2025). Credit Card Default Prediction: An Empirical Analysis on Predictive Performance Using Statistical and Machine Learning Methods. Journal of Risk and Financial Management. https://doi.org/10.3390/jrfm18010023.*
81. *Chang, A., Yang, L., Tsaih, R., & Lin, S. (2022). Machine learning and artificial neural networks to construct P2P lending credit-scoring model: A case using Lending Club data. Quantitative Finance and Economics. https://doi.org/10.3934/qfe.2022013.*