AI-Driven Transaction Monitoring in Fintech Environments: Comparative False-Positive Reduction Across Rules-Based and Machine-Learning Detection Models

Adaora Kalu[1*], Omotayo Pedro[2], Samuel Fadero[3], Oluwatobiloba Mide-Ibrahim[4]
[1]Independent Researcher, GA, USA
[2]Citco Group Limited, Vilnius, Lithuania
[3]SanlamAllianz Life Insurance Ltd, Lagos Nigeria
[4]FinServe Pro, USA
*Corresponding Author: Adaora Kalu, adaorakalu@gmail.com

Abstract

This review evaluates the comparative effectiveness of rules-based and machine-learning approaches to transaction monitoring in fintech environments, with particular emphasis on reducing false-positive alerts without weakening financial-crime detection. The study adopts a structured review approach, synthesizing scholarly evidence on monitoring evolution, detection architectures, model performance, data quality, feature engineering, operational efficiency, explainability, governance, regulatory compliance, implementation barriers, and emerging analytical techniques. The findings show that rules-based systems remain important because they provide transparent, auditable, and regulator-aligned controls for recognized typologies, yet their reliance on static thresholds often produces excessive alerts and substantial investigative burden. Machine-learning models offer stronger contextual discrimination, behavioural pattern recognition, and adaptive risk scoring, improving alert precision when supported by representative data, robust feature construction, appropriate class-imbalance treatment, and continuous validation. However, their deployment introduces challenges related to explainability, concept drift, privacy, model risk, workforce capability, and regulatory accountability. The review further identifies hybrid architectures as a particularly effective direction because they combine deterministic safeguards with predictive analytics, dynamic prioritisation, and human oversight. It concludes that sustainable false-positive reduction depends on balancing precision with recall, false-negative risk, investigator workload, model stability, customer impact, and auditability. Fintech institutions are therefore advised to strengthen data governance, recalibrate models and thresholds continuously, maintain transparent model documentation, embed investigators within feedback loops, and adopt phased implementation strategies. Future research should prioritise graph-based analytics, federated learning, synthetic data, adaptive retraining, concept-drift management, and reproducible benchmarking across realistic transaction datasets and jurisdictions. These priorities can improve scalability, cross-institutional learning, and responsiveness while preserving proportionate controls and defensible oversight across complex digital payment ecosystems.

Keywords: Transaction monitoring; False-positive reduction; Machine learning; Rules-based detection; Financial crime; Fintech compliance.

DOI: 10.18091/ijsts.v9i3.127

1. Introduction

1.1 Evolution of Fintech Transaction Monitoring

The evolution of transaction monitoring in fintech reflects a transformation in financial surveillance from retrospective, manually intensive control toward continuous, data-driven detection. Early electronic monitoring largely translated compliance policies into deterministic scenarios: transactions were screened against predefined thresholds, customer attributes, velocity limits, geographic indicators, and known patterns of suspicious behaviour. Such systems offered consistency and auditability, but their reliance on fixed conditions made them vulnerable to changing fraud strategies and generated substantial investigative workloads when legitimate transactions satisfied rigid alert rules. The financial-fraud literature therefore increasingly treated monitoring as a data-mining problem in which classification, clustering, prediction and outlier detection could complement conventional controls (Ngai et al., 2011).

As digital banking, mobile payments and e-commerce expanded, transaction volumes and behavioural complexity exceeded manual review capacity. This accelerated adoption of automated fraud-detection systems capable of processing high-dimensional data rapidly. Research showed that traditional investigative practices were costly, time-consuming and increasingly unsuitable for large-scale digital finance, encouraging financial institutions to adopt statistical learning and computational-intelligence methods that detected subtle relationships within transaction data (West & Bhattacharya, 2016). Comparable developments in automated process-control environments also demonstrated how integrated digital platforms could centralise data capture, execute predefined logic and support real-time decisions, illustrating foundations for automated monitoring architectures (Sunday &Omoegun, 2022).

The next phase involved moving beyond static rules toward models able to learn from historical patterns. Fraud-detection research identified concept drift, class imbalance, real-time processing requirements and large data volumes as central challenges to effective automated surveillance (Abdallah et al., 2016). Payment-card research subsequently showed that disruptive technologies, including smartphones, cloud computing and contactless payments, introduced new fraud vectors faster than traditional controls could adapt, strengthening the case for machine-learning approaches capable of adaptation (Ryman-Tubb et al., 2018). Within anti-money-laundering monitoring, supervised learning demonstrated value by ranking transactions by investigation probability, converting monitoring from simple rule triggering into risk-based prioritisation (Jullum et al., 2020).

Fintech transaction monitoring consequently evolved into an increasingly hybrid environment in which rules, statistical models and machine-learning classifiers coexist. Systematic reviews indicate that support vector machines, neural networks, ensemble techniques and other learning algorithms became prominent because they identify nonlinear relationships and interactions that manually specified scenarios may miss (Ali et al., 2022). Credit-card research similarly documents a transition from conventional statistical approaches toward machine learning and deep learning, while emphasizing persistent problems associated with imbalanced datasets, feature engineering and model deployment at scale (Cherif et al., 2023). These developments shifted monitoring from identifying rule violations toward discriminating suspicious behaviour from legitimate variability with greater contextual sensitivity.

A defining contemporary development is the explicit use of machine learning to address excessive false-positive alerts. Modern architectures can position machine-learning models downstream of established scenarios to rescore, suppress, or prioritize alerts according to learned risk characteristics. Evidence from anti-money-laundering research demonstrates that hybrid designs can improve alert triage while preserving expert-defined compliance scenarios, although poorly calibrated suppression creates a corresponding risk of overlooking genuinely suspicious activity (Bakry et al., 2024). This balance is central because false-positive reduction cannot be evaluated independently of false negatives, recall, precision and regulatory accountability.

Recent work reflects greater sophistication in rare-event detection. Techniques such as adaptive synthetic oversampling, recursive feature elimination and cross-validation have been applied to credit-card fraud datasets to address severe class imbalance and improve predictive robustness (Ileberi& Sun, 2024). From an African perspective, these advances are especially relevant as fintech ecosystems expand transaction volumes across mobile and digitally mediated channels, creating pressure for monitoring systems that scale without proportionately increasing analyst workloads. Intelligent automation likewise shows how AI-enabled analytics and real-time supervisory systems can transform monitoring from reactive exception handling into predictive, continuously informed control (Omoegun et al., 2024).

1.2 False Positives in Financial Crime Detection

False positives constitute one of the most persistent weaknesses in financial-crime detection because legitimate transactions can exhibit characteristics that resemble suspicious behaviour. In fintech environments, high transaction velocity, diverse customer profiles, cross-border activity and changing payment patterns increase the probability that rigid monitoring thresholds will misclassify normal behaviour as anomalous. Excessive false alerts are operationally consequential: they consume investigative capacity, delay review of risky activity and create unnecessary friction for customers. Machine-learning research in fintech therefore treats false-positive control as a central performance objective rather than a secondary accuracy issue (Stojanović et al., 2021).

Rules-based transaction-monitoring systems are particularly exposed to this problem because scenarios are defined around fixed thresholds, combinations of red flags, or expected behavioural ranges. When legitimate customer behaviour changes, static scenarios may continue to generate alerts without corresponding increases in actual financial-crime risk. Scenario calibration is therefore essential. Quantitative threshold optimisation can reduce redundant alerts while preserving suspicious-transaction coverage, demonstrating that false-positive reduction requires systematic recalibration rather than indiscriminate relaxation of controls (Gupta et al., 2022).

Machine-learning models offer an alternative by learning multidimensional relationships within historical transaction data. Their advantage lies in assigning contextual risk rather than treating every threshold breach as equally suspicious. Tree-based models can combine expert-derived indicators with learned decision boundaries, allowing institutions to preserve interpretable control logic while reducing unnecessary alerts from legitimate transactions (Vorobyev & Krivitskaya, 2022). Such approaches are especially relevant where investigators must distinguish rare fraudulent events within overwhelmingly legitimate transaction populations.

Class imbalance further complicates performance assessment. Because fraudulent observations are scarce, a model can achieve high overall accuracy while still producing operationally unacceptable classification errors. Consequently, precision, recall, F1-score and false-positive rate are more informative than accuracy alone when evaluating detection quality. Research from South Africa similarly emphasizes dataset imbalance, feature selection, missing-data treatment and appropriate performance metrics as fundamental considerations in automated financial-fraud detection (Mongwe & Malan, 2020).

Reliable discrimination also depends on how effectively detection systems identify meaningful patterns while suppressing benign variation. Automated pattern-matching research demonstrates that detection sensitivity must be balanced against erroneous classification when systems evaluate complex observations against learned or predefined templates (Ejofodomi et al., 2014). For fintech monitoring, this principle translates into careful feature construction, threshold design, and validation against representative transaction behaviour.

Continuous monitoring further requires dependable input signals and adaptive interpretation. Sensor-based fault-detection research illustrates how real-time monitoring can distinguish abnormal states more effectively when multiple signals are evaluated contextually rather than through isolated thresholds (Sunday &Omoegun, 2022). In financial-crime environments, analogous analytical discipline is necessary: reducing false positives should preserve sensitivity to genuine threats, maintain explainability, and prevent efficiency gains from being achieved at the expense of undetected illicit activity.

1.3 Artificial Intelligence in Monitoring Systems

Artificial intelligence has become a defining component of contemporary monitoring systems because it enables institutions to move beyond static thresholds toward adaptive, data-intensive surveillance. In fintech environments, AI supports the continuous evaluation of transaction streams through machine learning, anomaly detection, pattern recognition and predictive scoring. These capabilities are valuable where illicit behaviour is concealed within volumes of legitimate activity. Industry-focused AML research shows that advanced analytics can improve scalability, reveal unobserved risk patterns and support more efficient prioritisation of alerts than exclusively rules-based approaches (Oztas et al., 2024).

The operational value of AI arises from its capacity to interpret complex relationships among variables rather than assessing isolated conditions. Supervised models can learn from labelled historical cases, while unsupervised techniques identify unusual behaviour without requiring a predefined fraud class. In South African banking, AI has been examined as a means of strengthening the detection and prevention of cybercrime and financial crime through machine learning, neural networks, big-data analytics and pattern recognition, while simultaneously raising questions about regulation, accountability and responsible deployment (Chitimira& Ncube, 2021). Such considerations matter to fintech monitoring, where predictive performance must coexist with explainability and regulatory oversight.

AI-enabled monitoring is also increasingly associated with real-time and predictive decision architectures. Research on digital twins demonstrates how continuously updated virtual representations can integrate operational data, analytics and machine-learning capabilities to identify abnormal conditions earlier than conventional supervisory systems (Shittu et al., 2023). In financial transaction monitoring, an analogous architecture can combine customer profiles, transaction histories, behavioural indicators, counterparties and temporal patterns to generate dynamic risk assessments rather than relying solely on predetermined alert triggers.

The broader transition from reactive to predictive monitoring reinforces this development. Predictive systems use historical and real-time observations to identify deviations before adverse outcomes fully materialise, thereby shifting intervention from post-event response toward anticipatory risk management (Sunday et al., 2020). Applied to fintech, this logic allows AI models to evaluate behavioural changes continuously, update risk estimates and direct investigative attention toward transactions whose combined characteristics indicate elevated suspicion.

Intelligent monitoring nevertheless depends on the quality of signal interpretation. AI-integrated detection research demonstrates that machine learning can enhance pattern recognition, process complex inputs and reduce classification errors when data from multiple sources are interpreted jointly (Olorunkosebi et al., 2023). For fintech institutions, the implication is that AI should not

be treated merely as a replacement for rules. Its strategic value lies in augmenting established controls with contextual learning, adaptive prioritisation and predictive analytics, while maintaining transparent governance, model validation and human review. This combination creates the analytical basis for comparing whether machine-learning models can achieve meaningful false-positive reductions without weakening the detection of genuinely suspicious financial activity.

1.4 Review Scope, Objectives, and Significance

This review examines the evolution and comparative performance of transaction-monitoring approaches within fintech environments, with particular attention to the reduction of false-positive alerts. Its scope covers conventional rules-based systems, machine-learning models, hybrid monitoring architectures, data-quality requirements, feature engineering, explainability, governance, implementation constraints, and emerging technological directions. The analysis focuses on how these approaches identify anomalous or potentially suspicious financial activity while balancing detection sensitivity, operational efficiency, regulatory accountability, and the practical demands of high-volume digital transactions.

The principal objective is to compare rules-based and machine-learning detection models in terms of their ability to reduce unnecessary alerts without weakening the identification of genuinely suspicious activity. The review also evaluates the conditions under which machine-learning methods provide measurable advantages, including improved contextual analysis, adaptive risk scoring, and prioritisation of investigations. A further objective is to assess the continuing relevance of rules-based controls, particularly where transparency, traceability, and regulatory interpretability remain essential. Attention is also given to hybrid models that combine deterministic scenarios with predictive analytics to strengthen monitoring effectiveness.

The significance of this review lies in its emphasis on false-positive reduction as both a technical and operational challenge. Excessive alerts can increase compliance costs, burden investigators, delay case resolution, and reduce the efficiency of financial-crime programmes. At the same time, aggressive suppression can create unacceptable detection gaps. By synthesising the comparative strengths, limitations, and implementation considerations of competing monitoring approaches, this review provides a structured basis for understanding how fintech institutions can improve alert quality while preserving robust risk coverage, governance, and defensible compliance outcomes. It therefore situates model performance within an institutional context where monitoring decisions must remain transparent, auditable, and actionable.

2. Transaction Monitoring Models and Architectures

2.1 Rules-Based Detection Models and Workflows

Rules-based detection remains the institutional backbone of many transaction-monitoring programmes because it converts financial-crime typologies, regulatory expectations and internal risk appetites into explicit, auditable decision logic. A rule normally combines one or more transaction attributes with thresholds, frequencies, counterparties, geographies or customer-risk characteristics. When specified conditions are satisfied, the monitoring engine generates an alert for human review. This architecture is attractive because investigators can reconstruct why an alert fired, compliance teams can document scenario logic, and model changes can be subjected to formal governance. Early expert-system research already demonstrated how encoded knowledge could support real-time fraud alerts during consumer-credit authorisation, establishing the conceptual basis for deterministic monitoring workflows (Leonard, 1995).

In anti-money-laundering operations, rule creation typically begins with a risk assessment that identifies relevant products, customer segments, channels and suspicious behaviours. These risks are translated into scenarios such as rapid movement of funds, unusual transaction velocity, repeated amounts near reporting thresholds, abrupt behavioural change or transfers involving higher-risk jurisdictions. A rule-based approach therefore operationalises institutional knowledge in a structured form, but its effectiveness depends on whether the rule catalogue remains proportionate to evolving risk. Research on Chinese AML implementation illustrates why deterministic compliance can benefit from a risk-oriented overlay rather than mechanical adherence to uniform controls (Ai, 2012).

The workflow continues through data ingestion, standardisation, rule execution, alert generation and case allocation. Reliable data exchange is critical because rules can only evaluate information made available consistently across payment channels, customer records and transaction systems. Research on secure supervisory architectures shows the value of integrity, auditability and controlled data exchange when operational decisions depend on distributed information flows (Shittu et al., 2022). Comparable control-system research demonstrates that predefined logic can maintain stable responses when operating conditions and decision thresholds are clearly specified (Sunday et al., 2019).

Table 1. Illustrative rules-based transaction-monitoring workflow

Workflow stage	Principal activity	Typical rules-based mechanism	Operational implication
Risk identification	Define material financial-crime exposures	Typology and customer-risk mapping	Determines monitoring priorities
Scenario configuration	Translate risks into executable conditions	Thresholds, frequencies and Boolean logic	Creates deterministic alert criteria
Data ingestion	Consolidate transaction and customer attributes	Validation and standardisation rules	Supports consistent rule execution
Rule execution	Test activity against configured scenarios	If-then conditions and thresholds	Generates candidate alerts
Alert triage	Prioritise triggered cases	Severity and risk categories	Directs investigator workload
Investigation	Evaluate triggering activity contextually	Customer history and due diligence	Supports closure or escalation
Scenario tuning	Assess rule effectiveness over time	Threshold and parameter adjustment	Controls false positives and detection gaps
Governance review	Validate changes and performance	Approval, documentation and audit trails	Preserves accountability

Scenario design is followed by threshold calibration. Thresholds set too low can flood investigation queues with legitimate activity, whereas thresholds set too high can create blind spots. In engineering control environments, optimisation of operating limits similarly depends on balancing safety, reliability and efficiency under variable conditions, reinforcing the importance of calibrated rather than arbitrary trigger values (Adeniji et al., 2020). Load-distribution research further illustrates how deterministic control decisions become more effective when thresholds are contextualised against system conditions rather than applied uniformly (Sunday &Omoegun, 2019).

Once an alert is produced, it ordinarily enters a tiered investigation workflow. Analysts assess the triggering transactions alongside customer history, expected activity, counterparties, prior alerts and available due-diligence information before deciding whether to close, escalate or investigate the case further. The continued dominance of rules in AML reflects their interpretability and operational familiarity, yet empirical research shows that hand-crafted indicators can struggle to capture complex behavioural relationships and may require substantial analyst intervention (Jensen & Iosifidis, 2023). Rule-based systems therefore function most effectively when viewed as decision-support infrastructure rather than autonomous adjudicators.

Operational governance also requires version control over scenarios, documented rationales for threshold changes, back-testing against historical cases and post-implementation monitoring. These controls matter because a rule that once reflected a credible typology may become obsolete as customer behaviour, payment products or criminal tactics change. Periodic tuning should therefore examine alert volumes, conversion rates, investigation outcomes and typologies.

A persistent limitation is their sensitivity to rigid scenario definitions. Transactions satisfying a condition can be flagged even when their broader context is benign, producing substantial false-positive workloads. Research using bank data has shown that rule-driven alerting can be improved when suspicious accounts are prioritised according to broader behavioural patterns rather than evaluated only through isolated triggers (Alshantti& Rasheed, 2021). Similarly, abnormality-based financial-crime models demonstrate that incorporating behavioural comparison can reduce false positives relative to fixed-rule approaches (Rocha-Salazar et al., 2021).

Recent research has consequently explored rule generation and hybridisation rather than complete abandonment of deterministic controls. A rule-based machine-learning model can derive interpretable decision structures from transaction data while retaining measurable classification criteria, demonstrating that rules themselves can become more data-informed (Islam et al., 2024). By contrast, deep-learning fraud research from South Africa highlights the value of adaptive models for highly imbalanced and dynamic transaction environments, particularly where static patterns are insufficient (Mienye& Sun, 2023). For fintech institutions, the practical workflow is therefore increasingly layered: explicit scenarios provide transparent baseline controls, alert-management processes preserve human accountability, and analytical enhancements refine prioritisation. Rules remain valuable where governance, traceability and rapid implementation are critical, but their false-positive performance ultimately depends on disciplined scenario design, data quality, threshold calibration, periodic review and evidence-based tuning.

2.2 Machine-Learning Detection Models and Techniques

Machine-learning detection has become central to contemporary fintech monitoring because it allows transaction systems to learn patterns from historical and streaming data rather than depend exclusively on predetermined rules. Supervised algorithms use labelled legitimate and fraudulent observations to estimate class membership, whereas unsupervised approaches search for unusual structures when reliable labels are scarce. In Nigerian credit-card research, hybrid anomaly detection combining genetic algorithms with multivariate Gaussian modelling demonstrated how learning systems can discriminate rare fraudulent activity within heavily imbalanced transaction data (Makolo & Adeboye, 2021).

Model selection depends on the structure of the monitoring problem. Decision trees and random forests offer interpretable partitions of transaction attributes; support vector machines construct separating boundaries in high-dimensional feature spaces; neural networks capture nonlinear interactions; and clustering or anomaly-detection models identify behaviour that departs from learned norms. A Ghanaian systematic review found supervised methods more prevalent than unsupervised techniques in financial-fraud research, while also highlighting the comparatively limited African evidence base, reinforcing the need for context-sensitive validation (Tagbo& Adekoya, 2023).

For fintech environments, the strongest architectures increasingly combine preprocessing, feature engineering, class-imbalance treatment and ensemble learning. Machine-learning integration in fraud detection and anti-money-laundering workflows can support real-time scoring, behavioural profiling and prioritisation of suspicious activity, particularly where transaction volumes exceed feasible manual review capacity (Banerjee & Roy, 2024). Yet predictive performance should be evaluated through precision, recall, F1-score and false-positive rates rather than accuracy alone, because legitimate transactions vastly outnumber confirmed financial-crime events.

Predictive monitoring also benefits from architectures capable of updating system representations as operating conditions change. AI-powered digital twins illustrate how machine-learning models can combine historical and live data to support continuous fault prediction, optimisation and interpretable monitoring, principles applicable to dynamic transaction-risk assessment (Shittu & Shittu, 2024). Similarly, condition-monitoring systems demonstrate the analytical value of extracting meaningful signals from continuous operational data, where pattern interpretation supports earlier and more precise identification of abnormal states (Omoegun et al., 2023).

Data preparation is equally consequential. Feature quality determines whether models learn genuine risk relationships or reproduce noise, bias and historical artefacts. Predictive analytics frameworks show that combining real-time data, forecasting and prescriptive analysis can improve anticipatory decision-making when information is integrated systematically across operational processes (Akin-Oluyomi& Akhigbe, 2023). In transaction monitoring, relevant features may include transaction amount, velocity, merchant category, geography, device attributes, customer history, counterparty relationships and temporal behaviour. Effective machine-learning models therefore require more than algorithmic sophistication: they depend on representative data, calibrated thresholds, robust validation, drift monitoring and human oversight. These elements determine whether improved discrimination translates into sustained false-positive reduction across rapidly evolving payment channels and customer behaviours worldwide without weakening sensitivity to genuinely suspicious financial activity.

2.3 Hybrid and Adaptive Monitoring Architectures

Hybrid and adaptive monitoring architectures represent a pragmatic response to the limitations of purely rules-based or exclusively machine-learning transaction surveillance. Rather than replacing deterministic controls, hybrid systems combine explicit compliance scenarios with statistical, anomaly-detection, network, and predictive models. This layered design allows known typologies to remain traceable while analytical components identify complex or previously unseen behavioural relationships. Research combining supervised and unsupervised learning shows that integrating outlier information with labelled fraud patterns can improve detection performance where criminal behaviour changes over time (Carcillo et al., 2021).

A central architectural principle is continuous adaptation. Conventional monitoring rules are generally calibrated periodically, whereas adaptive components can update risk assessments as transaction distributions, customer behaviours, and fraud strategies evolve. Network-based fraud detection demonstrates how transaction-specific attributes can be combined with dynamic relationships among customers and merchants, enabling suspiciousness scores to reflect both individual activity and surrounding transactional structures (Van Vlasselaer et al., 2015). Such contextualisation is particularly valuable in fintech ecosystems where payment behaviour changes rapidly across channels, devices, counterparties, and jurisdictions.

Hybridisation also addresses severe class imbalance, a persistent obstacle in financial-crime analytics. Nigerian research comparing resampling strategies shows that class weighting, undersampling, and oversampling can materially influence the ability of machine-learning models to recognise rare fraudulent observations within predominantly legitimate datasets (Udeze et al., 2022). More advanced architectures extend this logic by generating representative minority-class observations and coupling them with sequential learning. A South African study integrating generative adversarial networks with recurrent neural networks demonstrates how synthetic fraud examples can strengthen adaptive detection where authentic fraudulent cases are scarce (Mienye& Swart, 2024).

Operationally, hybrid monitoring requires an architecture capable of ingesting real-time data, applying baseline rules, generating behavioural features, producing model scores, and routing alerts according to calibrated risk. Real-time operational analytics can improve responsiveness by combining predictive modelling, behavioural clustering, and continuously updated performance information within coordinated decision processes (Akhigbe et al., 2023). In fintech monitoring, this supports dynamic alert prioritisation rather than treating every rule breach as possessing equivalent investigative significance.

Adaptability, however, must remain governed. Automated parameter adjustment or model retraining can create instability if data quality deteriorates, concept drift is misinterpreted, or model changes escape validation. Adaptive cyber-physical architectures similarly show that

intelligent systems benefit from real-time sensing and dynamic decision logic but require secure communications, explainability, interoperability, and controlled reconfiguration to remain reliable (Shittu et al., 2024). For transaction monitoring, the strongest architecture therefore combines deterministic safeguards, adaptive analytics, human review, validation controls, and feedback from investigation outcomes. This configuration can reduce unnecessary alerts while preserving auditability and responsiveness to emerging financial-crime patterns. This balance is essential for sustainable, regulatorily defensible monitoring in fintech environments.

3. Comparative False-Positive Reduction Performance

3.1 Detection Accuracy and Alert Precision

Detection accuracy and alert precision are central to evaluating transaction-monitoring systems because nominal classification accuracy can conceal serious weaknesses when suspicious transactions form only a small fraction of overall activity. In imbalanced fintech datasets, a model may classify most legitimate transactions correctly and still perform poorly on the minority class central to financial-crime detection. Precision measures the proportion of flagged transactions that are genuinely suspicious, while recall captures the proportion of actual suspicious transactions successfully identified. For operational monitoring, these metrics must be interpreted together rather than treated as interchangeable indicators of model quality (Saito &Rehmsmeier, 2015).

Comparative evaluation is important because rules-based and machine-learning models generate different error profiles. Rules-based systems provide transparent and reproducible triggers, but fixed thresholds can create large alert volumes when legitimate customer behaviour falls outside predetermined limits. Machine-learning models can improve discrimination by learning multivariate patterns from historical data, yet performance depends on training design, sampling strategy and feature representation. Comparative research using real transaction data showed that logistic regression, support vector machines and random forests produce materially different detection outcomes, demonstrating that model selection should reflect the operational consequences of classification errors rather than headline accuracy alone (Bhattacharyya et al., 2011).

Feature quality is equally decisive. Transaction amount, merchant category, purchase time, customer history, frequency, geography and aggregated behavioural variables can alter the separability of fraudulent and legitimate transactions. Feature-engineering research has shown that periodic and aggregated behavioural attributes can strengthen predictive discrimination and make fraud models more sensitive to contextual irregularities that raw transaction fields may not capture (Bahnsen et al., 2016). Consequently, gains in precision cannot be attributed solely to algorithmic sophistication; they often emerge from better representation of customer behaviour.

Realistic performance assessment must also account for concept drift and verification latency. Fraud patterns evolve, legitimate spending behaviour changes and confirmed labels may arrive only after analyst investigation. A model validated on randomly partitioned historical observations can therefore appear more accurate than it will be in production. Research using large-scale transaction streams demonstrates that class imbalance, temporal drift and delayed verification materially affect fraud-detection performance, requiring time-aware validation and operationally relevant metrics (Dal Pozzolo et al., 2018). These concerns are important when comparing adaptive models with static rule sets.

Recent Nigerian evidence further demonstrates why multiple metrics are necessary. Comparative modelling of credit-card fraud data shows that machine-learning algorithms can differ substantially in recognising the minority fraud class even when overall accuracy is high, reinforcing the need to examine precision, recall, F1-score and confusion-matrix outcomes together (Ogundunmade& Adepoju, 2024). For fintech institutions, high recall with weak precision may identify most suspicious transactions while overwhelming investigators with false alerts; conversely, very high precision achieved through aggressive thresholds may miss material suspicious activity.

Modern approaches increasingly seek to improve this trade-off through representation learning and intelligent sampling. Self-supervised learning can capture sequential customer behaviour, while sampling procedures can reduce label noise and class imbalance before classification. Evidence from real-world credit-card datasets indicates that combining intelligent sampling, behavioural representation and dynamic thresholding can improve F1 performance under practical fraud-detection constraints (Chen et al., 2024). Such results underscore that alert precision is shaped by the entire analytical pipeline rather than the classifier alone.

Operational precision also has a human dimension. South African banking research identifies specialist expertise, evolving fraud patterns and rapidly changing digital channels as important determinants of detection effectiveness, indicating that technically strong systems still require capable investigators and responsive governance (Phiri et al., 2024). Precision should therefore be evaluated statistically and by whether alerts are relevant and interpretable to support timely investigation.

From a process-quality perspective, false positives can be treated as avoidable variation that consumes compliance resources without proportional risk value. Continuous measurement, root-cause analysis and disciplined performance improvement provide a basis for refining detection workflows (Olutimehin& Ganiu, 2022). In fintech transaction monitoring, this means comparing rules and machine-learning models through precision, recall, false-positive rate, F1-score, temporal stability and investigative yield, while ensuring that improvements in alert quality do not conceal deterioration in detecting genuinely suspicious activity.

3.2 Operational Efficiency and Investigation Burden

Operational efficiency in fintech transaction monitoring is determined not only by detection performance but also by the volume, quality, and prioritisation of alerts that investigators must process. Rules-based systems can generate review queues because each threshold breach is treated as potentially suspicious, even when contextual evidence indicates ordinary customer behaviour. The resulting workload increases case-handling time, raises compliance costs, and can divert scarce investigative capacity from genuinely high-risk activity. Workforce-oriented operations research shows that throughput depends on aligning task allocation, worker capability, workload intensity, and process bottlenecks rather than simply increasing staffing levels (Akanbi et al., 2022).

Within financial-crime operations, investigation burden is therefore a capacity-management problem as well as a detection problem. Analysts must collect customer information, reconstruct transaction histories, assess counterparties, document decisions, and determine whether escalation or suspicious activity reporting is warranted. When alert volumes exceed capacity, backlogs may develop and review quality may deteriorate. Research from South Africa notes that manual AML review can overwhelm human analysts when automated systems generate numerous false positives, reinforcing the need for technologies that improve prioritisation without weakening regulatory accountability (Chitimira et al., 2024).

Machine-learning triage offers one mechanism for reducing this burden. Graph-based alert optimisation can score alerts using behavioural and relational features, enabling institutions to suppress low-risk cases or prioritise higher-risk ones for investigation. In a real-world banking setting, this approach substantially reduced false positives while retaining a high proportion of true positives, demonstrating how analytical prioritisation can directly improve operational workload distribution (Eddin et al., 2022).

Active-learning architectures provide another pathway by directing analyst attention toward the observations that are most informative for model improvement. Rather than requiring exhaustive manual labelling, active learning selectively requests expert review, thereby reducing investigation costs while improving the detection model iteratively. This human-in-the-loop structure is particularly appropriate for AML environments where labelled suspicious cases are scarce and expert time is expensive (Labanca et al., 2022).

Workforce design remains important even when automation improves alert quality. Integrated productivity frameworks emphasise linking employee capacity, performance indicators, workload distribution, and predictive analytics so managers can identify emerging bottlenecks and rebalance resources before service quality deteriorates (Falemi et al., 2023a). Applied to fintech compliance, this means monitoring investigator caseloads, average handling times, escalation rates, alert ageing, and analyst specialisation alongside model metrics.

Scalable monitoring also requires resilience to staffing volatility. Predictive workforce planning can align labour demand with changing operational volumes, support flexible allocation, and maintain continuity during periods of rapid growth or unusual transaction activity (Falemi et al., 2023b). For fintech institutions, the most efficient operating model therefore combines higher-quality alert generation with risk-based queue management, targeted automation, specialist human judgement, and continuous capacity planning. Reducing false positives has value because it shortens unnecessary investigative work, but efficiency gains remain credible only when genuinely suspicious activity continues to receive timely, well-documented, and skilled review.

4. Data Quality and Feature Engineering

Data quality is foundational to transaction-monitoring performance because deterministic rules and machine-learning models inherit the strengths and defects of the information they process. Fintech platforms integrate payment events, customer profiles, device identifiers, merchant data, geolocation, authentication records and historical activity from heterogeneous systems. Missing fields, inconsistent formats, duplicate records, delayed updates or incorrect labels can distort risk signals and create avoidable alerts. Nigerian research on credit-card fraud demonstrates that classifier performance changes materially with data preparation and modelling choices, reinforcing the need to treat preprocessing as part of the detection architecture rather than as an administrative task (Awoyemi et al., 2017).

For rules-based systems, poor data quality can cause thresholds and scenarios to fire for reasons unrelated to genuine risk. A transaction may appear unusual because customer occupation, expected turnover, residence or account status is outdated; conversely, fragmented transaction histories can conceal patterns that would otherwise satisfy a suspicious-activity rule. Accurate identification and structured data capture are therefore essential. RFID-based information management research illustrates how automated identification, database matching and controlled data capture can reduce manual errors and improve record availability, principles transferable to monitoring infrastructures where reliable entity resolution is critical (Yusuf et al., 2023).

Machine-learning models impose additional requirements because they infer relationships directly from observed data. Feature engineering determines how raw transactions are converted into representations that reveal behavioural context. Rather than using amount or location in isolation, systems can derive transaction velocity, rolling expenditure, average deviation, time since previous payment, merchant diversity, cross-border frequency and customer-to-counterparty concentration. Transaction aggregation research shows that summarising activity over carefully selected time windows can improve fraud classification and increase robustness to population drift, although performance depends on the chosen aggregation horizon and learning method (Whitrow et al., 2009).

Temporal information is important because financial crime often emerges as a sequence rather than a single abnormal payment. Static features may overlook gradual changes in spending, repeated low-value transfers or coordinated activity distributed across time. Sequence-learning research demonstrates that modelling ordered transaction histories can identify patterns not captured by transaction-level classifiers and that manually aggregated behavioural features can still add predictive value to sequential models (Jurgovsky et al., 2018). For fintech monitoring, temporal feature construction therefore enables models to compare present activity with customer-specific baselines instead of applying population-wide thresholds indiscriminately.

Table 1. Illustrative Data-Quality and Feature-Engineering Framework for Transaction Monitoring

Data dimension	Principal quality risk	Illustrative engineered feature	Rules-based implication	Machine-learning implication
Transaction history	Missing or fragmented records	Rolling transaction velocity	Incomplete threshold evaluation	Distorted behavioural baseline
Transaction amount	Outliers and inconsistent units	Deviation from customer average	Excessive threshold alerts	Misleading anomaly scores
Time attributes	Incorrect timestamps	Inter-transaction interval	Faulty velocity rules	Weak sequential patterns
Customer profile	Stale KYC information	Profile-behaviour deviation	Misclassified expected activity	Biased risk representation
Counterparty data	Duplicate or unresolved entities	Counterparty concentration	Repeated unnecessary alerts	Fragmented relationship features
Geography	Missing location information	Cross-border frequency	Incorrect geographic triggers	Reduced contextual discrimination
Fraud labels	Delayed or inaccurate outcomes	Validated target labels	Poor scenario tuning	Biased supervised learning
Device data	Inconsistent identifiers	Device switching frequency	Missed device-related rules	Unreliable behavioural features

Feature selection is equally important. High-dimensional datasets can contain redundant, weak or correlated variables that increase computational cost and encourage overfitting. Selecting features with strong predictive content can simplify models, accelerate scoring and improve

generalisation. Research using random-forest feature ranking with support vector machines shows that reducing the input space to informative attributes can enhance credit-risk identification while maintaining computational efficiency (Rtayli&Enneya, 2020). In false-positive reduction, parsimonious features are valuable when they separate legitimate behavioural variation from characteristics associated with suspicious activity.

Class imbalance and label quality create further difficulties. Confirmed fraud or money-laundering cases constitute a minute proportion of transactions, while investigation outcomes may contain delayed, incomplete or uncertain labels. Models trained naively on such data can favour the legitimate majority and underestimate rare risks. Ghanaian mobile-money research shows that sampling strategy can influence classifier performance in highly imbalanced datasets, highlighting the importance of resampling, representative training data and evaluation through precision, recall and F1-score rather than accuracy alone (Botchey et al., 2020). Poorly designed balancing can introduce artificial patterns and must be validated against realistic transaction distributions.

Feature pipelines also require continuous governance after deployment. Fintech behaviour changes as products, payment channels, customer populations and criminal strategies evolve, meaning that previously informative variables can decay or shift in meaning. Data-driven performance frameworks emphasise integrated collection, real-time indicators, predictive analysis and continuous monitoring as mechanisms for identifying operational variation and supporting intervention (Akin-Oluyomi& Akhigbe, 2023). Transaction-monitoring programmes should therefore track missingness, schema changes, feature drift, label latency and model stability alongside alert volumes. A disciplined feature lifecycle links source validation, transformation logic, version control, monitoring and periodic recalibration, ensuring that improvements in false-positive reduction reflect better risk discrimination rather than deterioration in data completeness or detection sensitivity.

5. Explainability, Governance, and Regulatory Compliance

Explainability, governance, and regulatory compliance determine whether artificial-intelligence transaction monitoring can be trusted as an operational control rather than merely valued for predictive performance. In fintech environments, detection models influence which transactions are escalated, which customers receive scrutiny, and how investigative resources are allocated. Institutions therefore require explanations connecting model outputs to intelligible risk factors. Explainable fintech research demonstrates that transparent representations can support understanding of model-driven risk assessments without abandoning sophisticated analytical methods (Bussmann et al., 2020).

The need for interpretability becomes pronounced when monitoring decisions carry regulatory consequences. Post-hoc explanation methods can approximate why a complex model produced a

score, but approximation does not always establish that the explanation faithfully represents the model's reasoning. In high-stakes settings, inherently interpretable models may therefore be preferable where comparable predictive performance can be achieved, because decision logic remains directly inspectable and contestable (Rudin, 2019). For transaction monitoring, this distinction matters when investigators must justify why alerts were generated, suppressed, or escalated.

Explainability must operate at several levels. Compliance analysts need case-level explanations, model validators require understanding of feature effects and decision boundaries, while governance bodies require evidence concerning stability, bias, data provenance, and performance limitations. Responsible-AI scholarship treats explainability as part of a framework involving transparency, accountability, privacy, fairness, and human oversight rather than as an isolated technical feature (Barredo Arrieta et al., 2020). A model producing understandable scores but lacking disciplined governance can still create compliance risk.

Governance begins with assigned ownership across the model lifecycle. Policies should specify responsibility for scenario design, training data, feature approval, validation, threshold calibration, deployment, change management, incident response, and retirement. Data-driven governance frameworks demonstrate the value of combining policy alignment, compliance monitoring, performance indicators, and continuous oversight within a control structure (Akin-Oluyomi& Akhigbe, 2022). Applied to fintech, these principles require model inventories, approval authorities, independent challenge, audit trails, and escalation procedures.

Ethical governance is equally important because regulatory compliance cannot be reduced to technical conformity. Leadership shapes whether institutions treat monitoring obligations as substantive safeguards or box-ticking exercises. African research on technological transformation and policy implementation emphasizes ethical leadership, institutional responsibility, and accountable implementation as central to converting formal policy commitments into credible practice (Enaifoghe et al., 2020). Within fintech surveillance, such governance is necessary to prevent efficiency objectives from overriding fairness, proportionality, or customer interests.

Enterprise risk management connects model risk with wider operational exposure. AI monitoring failures may arise from data drift, cyber incidents, biased features, inadequate staffing, weak validation, or inappropriate reliance on automated outputs. Integrating operational analytics with risk governance enables institutions to monitor vulnerabilities, assign accountability, and align technical controls with enterprise risk tolerances (Falemi et al., 2024). Accordingly, false-positive performance should be reviewed alongside false negatives, override rates, model drift, investigator outcomes, customer impact, and control breaches.

Security and access governance are integral because monitoring platforms process financial and identity data. Attribute-based access-control research illustrates how permissions can be linked to defined roles and attributes so information is available only to authorised actors while maintaining controlled exchange (Shittu & Nabil, 2023). Comparable fintech controls require least-privilege access, encryption, segregation of duties, logging, and traceable administrative changes.

Regulatory compliance ultimately requires lifecycle evidence rather than one-time model approval. AI auditing scholarship highlights conformity assessment and post-deployment monitoring as mechanisms for demonstrating that systems continue to satisfy applicable requirements after implementation (Mökander et al., 2022). For fintech transaction monitoring, defensible governance depends on explainable decisions, documented controls, independent validation, continuous performance surveillance, secure data handling, and meaningful human review. These safeguards make false-positive reduction credible by ensuring efficiency improvements remain auditable, proportionate, and consistent with financial-crime detection obligations.

6. Implementation Challenges in Fintech Environments

Implementing advanced transaction monitoring in fintech environments is difficult because technical sophistication must be reconciled with operational continuity, regulatory obligations, workforce capability, and heterogeneous digital infrastructures. Migration from rules-based systems to machine-learning or hybrid architectures requires redesign of data pipelines, case-management processes, model-governance routines, and investigator workflows. Technology adoption depends not only on model performance but also on whether employees possess the skills and organizational support needed to incorporate analytical tools into decisions. Readiness frameworks emphasize training, feedback, acceptance, and staged adoption as conditions for sustainable technological change (Akhigbe et al., 2024).

Legacy infrastructure is an important constraint. Established financial institutions operate core platforms built around fragmented databases, proprietary interfaces, and batch-oriented processing, whereas contemporary transaction monitoring requires real-time data access, scalable computation, and interoperable application programming interfaces. Banks may consequently face modernization costs and coordination frictions that technology-native fintech firms avoid, limiting the speed with which advanced analytics can be embedded into production systems (Stulz, 2022). Integration failures can also create incomplete customer views, delayed alerts, inconsistent feature generation, and duplicated records, weakening false-positive reduction.

Data architecture challenges are compounded by cybersecurity and privacy requirements. Artificial intelligence applications rely on granular datasets, yet expanding data access can increase exposure to unauthorized use, cyberattack, surveillance concerns, and third-party

dependency. Financial organizations adopting AI must therefore balance analytical opportunity against model risk, privacy, security, and governance obligations, particularly when capabilities are outsourced or delivered through interconnected technology ecosystems (Ashta & Herrmann, 2021). These tensions make implementation a socio-technical risk-management exercise rather than software deployment.

Human capability presents a persistent barrier. Transaction-monitoring modernization demands expertise spanning financial-crime typologies, data engineering, machine learning, model validation, compliance, and investigative practice. Distributed organizations may struggle to maintain these competencies. Capability-development research stresses systematic skills mapping, continuous learning, digital collaboration, and alignment between workforce competencies and operational objectives as mechanisms for reducing such gaps (Falemi et al., 2020). Without this foundation, advanced models may be mistrusted, misinterpreted, or overridden inconsistently by analysts.

Strategic alignment is consequential. Monitoring transformation can fail when analytics teams optimize predictive metrics while compliance leaders prioritize explainability, investigators emphasize usability, and executives focus on cost reduction. Effective implementation requires leadership structures that connect technological decisions with enterprise objectives, operational constraints, accountability, and performance measures (Akin-Oluyomi& Akhigbe, 2023). Institutions need shared criteria covering false-positive reduction, detection sensitivity, investigation throughput, customer impact, model stability, and regulatory defensibility.

Implementation conditions vary across markets. Nigerian evidence on electronic banking demonstrates that digital-finance adoption can be constrained by security concerns and infrastructural weaknesses even where access to electronic services is expanding (Aduba, 2021). These constraints matter for AI-driven monitoring because reliable detection depends on trustworthy digital records, secure channels, consistent identifiers, and sufficient computing infrastructure.

Regulation can create both discipline and uncertainty. South African research on fintech regulatory sandboxes shows that effective innovation frameworks depend on clear objectives, stakeholder cooperation, institutional capacity, and appropriate eligibility and testing arrangements (McCallum &Aziakpono, 2023). Monitoring teams must consequently interpret evolving expectations around model validation, accountability, privacy, outsourcing, and automated decision-making while meeting financial-crime obligations.

Organizational readiness determines whether implementation progresses beyond experimentation. Evidence from commercial banking indicates that management support, competitive pressure, technological compatibility, and institutional preparedness shape fintech adoption and performance outcomes (Marei et al., 2023). For transaction monitoring, successful

deployment therefore requires phased integration, reliable data foundations, multidisciplinary expertise, secure architecture, model governance, investigator engagement, and rigorous performance review. These requirements are important when machine-learning systems are introduced to reduce false positives, because operational gains are sustainable only when new models can be integrated, understood, controlled, maintained, and adapted as transaction behaviour and financial-crime risks evolve.

7. Emerging Innovations and Research Priorities

Emerging innovation in fintech transaction monitoring is moving beyond incremental classifier improvement toward architectures that are relational, privacy-preserving, adaptive, and operationally integrated. A major research priority is the representation of transactions as networks rather than isolated observations. Accounts, merchants, devices, beneficiaries, locations, and payment instruments form interconnected structures in which coordinated fraud may be visible only through relationships. Graph neural networks can exploit these dependencies while addressing severe class imbalance, offering a route toward detecting concealed transactional patterns that conventional feature vectors may overlook (Tong & Shen, 2023).

A second frontier concerns privacy-preserving collaborative learning. Financial institutions possess complementary fraud signals, yet regulatory and commercial constraints restrict raw-data sharing. Federated learning allows models to be trained across decentralized datasets while retaining transaction records locally. When combined with explainable artificial intelligence, this approach can improve cross-institutional learning while preserving transparency for investigators and governance teams (Awosika et al., 2024). Evidence from Egypt further indicates that federated fraud detection can be combined with balancing techniques to address both privacy constraints and minority-class scarcity, although communication overhead, heterogeneous data distributions, and model-security risks remain research problems (Abdul Salam et al., 2024).

Synthetic-data generation is another promising direction. Fraud examples are rare, confidential, and often poorly representative of emerging tactics. Generative adversarial networks can create plausible minority-class observations that enrich training datasets and improve sensitivity without relying exclusively on duplicated historical cases. Experimental evidence shows that GAN-based augmentation can strengthen credit-card fraud classification, although studies must examine whether synthetic records reproduce hidden biases, create unrealistic patterns, or generalize across institutions and payment channels (Fiore et al., 2019).

Adaptation to concept drift is equally critical because transaction behaviour and criminal strategies evolve continuously. Static models may deteriorate when customers adopt new channels, merchants change payment practices, or offenders modify tactics. Contextual-bandit approaches illustrate how investigation decisions can balance exploitation of known suspicious patterns with exploration of uncertain cases that improve future learning (Soemers et al., 2018).

Research should therefore prioritize drift-sensitive validation, online recalibration, feedback quality, and safe retraining triggers rather than assuming that deployment performance remains stable.

Distributed-ledger technologies may also influence monitoring architecture by strengthening transaction provenance, tamper resistance, and programmable verification. Blockchain-based peer-to-peer trading research demonstrates how decentralized records and smart contracts can support transparent exchange among participants while exposing continuing challenges involving scalability, interoperability, transaction cost, privacy, and governance (Shittu et al., 2021). In fintech environments, future work should test whether comparable architectures can enhance audit trails or cross-organizational monitoring without introducing excessive latency or new confidentiality risks.

Advanced optimization will also shape how alerts are routed and investigative resources allocated. Research on integrated path planning and slotting demonstrates the value of combining real-time information, optimization algorithms, and adaptive decision rules under changing operational conditions (Akanbi & Sunday, 2024). For transaction monitoring, analogous optimization could dynamically assign cases by risk, analyst expertise, queue age, and investigative capacity, connecting model outputs to measurable operational outcomes.

Future research must additionally examine system-level integration rather than isolated algorithmic gains. Work on combining energy efficiency with logistics optimization emphasizes that performance improvements are strongest when interconnected processes, resource constraints, technologies, and stakeholder objectives are considered jointly (Opara et al., 2024). Fintech research should similarly compare rules-based, machine-learning, and hybrid systems using common datasets, temporal validation, investigator outcomes, explainability measures, false-positive costs, and false-negative risk. Priorities should include graph analytics, federated and privacy-enhancing learning, synthetic data, adaptive retraining, causal analysis, human-in-the-loop feedback, and reproducible benchmarking. These innovations should ultimately be evaluated not by novelty alone, but by their capacity to deliver durable false-positive reduction while preserving detection sensitivity, regulatory defensibility, operational scalability, and accountable human oversight.

Conclusion

This review examined the comparative effectiveness of rules-based and machine-learning approaches to transaction monitoring in fintech environments, with particular emphasis on false-positive reduction, operational efficiency, governance, and implementation readiness. The analysis fulfilled its objectives by tracing the evolution of monitoring architectures, evaluating the strengths and limitations of deterministic rules and data-driven models, and identifying the

conditions under which hybrid systems can deliver more precise and defensible financial-crime surveillance.

The findings show that rules-based systems remain valuable because of their transparency, auditability, and direct alignment with known typologies and regulatory expectations. However, their dependence on static thresholds and predefined scenarios can generate excessive alerts, increase investigative burden, and adapt poorly to rapidly changing transaction behaviour. Machine-learning models offer stronger contextual discrimination, behavioural pattern recognition, and adaptive risk scoring, thereby improving alert precision when supported by representative data, rigorous feature engineering, and appropriate validation. Yet their benefits are constrained by class imbalance, concept drift, data-quality weaknesses, limited explainability, and governance complexity. The review therefore finds that hybrid architectures provide the most balanced operational pathway by combining deterministic safeguards with adaptive analytics and human oversight.

The study further establishes that false-positive reduction should not be pursued as an isolated technical objective. Sustainable improvement requires simultaneous attention to recall, false-negative risk, investigator workload, model stability, regulatory defensibility, and customer impact. Accordingly, fintech institutions should strengthen data governance, adopt continuous model and threshold recalibration, maintain transparent audit trails, and integrate investigators into model feedback loops. Future research should prioritise graph-based detection, federated learning, synthetic data, concept-drift management, and comparative benchmarking using realistic temporal datasets. These priorities are important as fintech ecosystems expand across jurisdictions, payment channels, customer segments, and technologies. Ultimately, effective transaction monitoring depends not on replacing rules with artificial intelligence, but on designing accountable, adaptive, and operationally integrated systems that improve precision without compromising sensitivity to genuine financial-crime risk.

References

1. Abdallah, A., Maarof, M.A. and Zainal, A. (2016) ‘Fraud detection system: A survey’, Journal of Network and Computer Applications, 68, pp. 90–113. DOI: 10.1016/j.jnca.2016.04.007. (ScienceDirect)
2. Abdul Salam, M., Fouad, K.M., Elbably, D.L. and Elsayed, S.M. (2024) ‘Federated learning model for credit card fraud detection with data balancing techniques’, Neural Computing and Applications, 36, pp. 6231–6256. DOI: 10.1007/s00521-023-09410-2.
3. Adeniji, I.O., Shittu, H., Elumilade, R.A., Opara, I.S. and Shittu, M.A. (2020) ‘Grounding system design optimization for medium-voltage distribution networks in emerging power markets’, Iconic Research and Engineering Journals, 3(11), pp. 547–565. DOI: 10.64388/IREV3I11-1714040.

4. Aduba, J.J. (2021) 'On the determinants, gains and challenges of electronic banking adoption in Nigeria', International Journal of Social Economics, 48(7), pp. 1021–1043. DOI: 10.1108/IJSE-07-2020-0452.
5. Ai, L. (2012) '"Rule-based but risk-oriented" approach for combating money laundering in Chinese financial sectors', Journal of Money Laundering Control, 15(2), pp. 198–209. DOI: 10.1108/13685201211218225.
6. Akanbi, O. and Sunday, E.A. (2024) 'An integrated path-planning and slotting optimization model for AMR-enabled high-density warehousing', International Journal of Advanced Multidisciplinary Research and Studies, 4(6), pp. 3226–3243. DOI: 10.62225/2583049X.2024.4.6.6181.
7. Akanbi, O., Ganiu, O.S. and Sunday, E.A. (2022) 'A workforce-centric line balancing model for throughput maximization in multi-shift operations', Shodhshauryam: International Scientific Refereed Research Journal, 5(3), pp. 439–464.
8. Akhigbe, R., Falemi, A. and Akin-Oluyomi, O.T. (2023) 'A conceptual model for improving customer experience using workforce behavior and real-time operational data', International Journal of Multidisciplinary Research and Growth Evaluation, 4(6), pp. 1322–1338. DOI: 10.54660/.IJMRGE.2023.4.6.1322-1338.
9. Akhigbe, R., Falemi, A. and Akin-Oluyomi, O.T. (2024) 'An advanced framework for technology adoption that supports employee readiness in modern organizations', International Journal of Advanced Multidisciplinary Research and Studies, 4(1), pp. 1637–1659. DOI: 10.62225/2583049X.2024.4.1.5344.
10. Akin-Oluyomi, O.T. and Akhigbe, R. (2022) 'A supply chain governance model for enhancing compliance and operational quality across retail networks', International Journal of Multidisciplinary Research and Growth Evaluation, 3(6), pp. 860–878. DOI: 10.54660/.IJMRGE.2022.3.6.860-878.
11. Akin-Oluyomi, O.T. and Akhigbe, R. (2023) 'A conceptual supply chain leadership model for aligning logistics decisions with enterprise strategy', International Journal of Advanced Multidisciplinary Research and Studies, 3(1), pp. 1725–1744. DOI: 10.62225/2583049X.2023.3.1.5340.
12. Akin-Oluyomi, O.T. and Akhigbe, R. (2023) 'A proposed supply chain analytics framework for improving forecasting accuracy and reducing bottlenecks', International Journal of Advanced Multidisciplinary Research and Studies, 3(1), pp. 1686–1703. DOI: 10.62225/2583049X.2023.3.1.5338.
13. Akin-Oluyomi, O.T. and Akhigbe, R. (2023) 'An advanced framework for improving multi-site operational efficiency using data-driven performance indicators', International Journal of Advanced Multidisciplinary Research and Studies, 3(1), pp. 1763–1781. DOI: 10.62225/2583049X.2023.3.1.5343.
14. Ali, A., Abd Razak, S., Othman, S.H., Eisa, T.A.E., Al-Dhaqm, A., Nasser, M., Elhassan, T., Elshafie, H. and Saif, A. (2022) 'Financial fraud detection based on machine learning:

A systematic literature review', Applied Sciences, 12(19), 9637. DOI: 10.3390/app12199637. (MDPI)

15. Alshantti, A. and Rasheed, A. (2021) 'Self-organising map based framework for investigating accounts suspected of money laundering', Frontiers in Artificial Intelligence, 4, 761925. DOI: 10.3389/frai.2021.761925.
16. Ashta, A. and Herrmann, H. (2021) 'Artificial intelligence and fintech: An overview of opportunities and risks for banking, investments, and microfinance', Strategic Change, 30(3), pp. 211–222. DOI: 10.1002/jsc.2404.
17. Awosika, T., Shukla, R.M. and Pranggono, B. (2024) 'Transparency and privacy: The role of explainable AI and federated learning in financial fraud detection', IEEE Access, 12, pp. 64551–64560. DOI: 10.1109/ACCESS.2024.3394528.
18. Awoyemi, J.O., Adetunmbi, A.O. and Oluwadare, S.A. (2017) 'Credit card fraud detection using machine learning techniques: A comparative analysis', 2017 International Conference on Computing Networking and Informatics (ICCNI), Lagos, Nigeria, pp. 1–9. DOI: 10.1109/ICCNI.2017.8123782.
19. Bahnsen, A.C., Aouada, D., Stojanovic, A. and Ottersten, B. (2016) 'Feature engineering strategies for credit card fraud detection', Expert Systems with Applications, 51, pp. 134–142. DOI: 10.1016/j.eswa.2015.12.030.
20. Bakry, A.N., Alsharkawy, A.S., Farag, M.S. and Raslan, K.R. (2024) 'Automatic suppression of false positive alerts in anti-money laundering systems using machine learning', The Journal of Supercomputing, 80, pp. 6264–6284. DOI: 10.1007/s11227-023-05708-z. (DOI.org)
21. Banerjee, P. and Roy, R. (2024) 'Application of machine learning techniques in fintech integrations in the fields of fraud detection and AML', International Journal of Computer Trends and Technology, 72(3), pp. 46–52. DOI: 10.14445/22312803/IJCTT-V72I3P107.
22. Barredo Arrieta, A., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., García, S., Gil-López, S., Molina, D., Benjamins, R., Chatila, R. and Herrera, F. (2020) 'Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI', Information Fusion, 58, pp. 82–115. DOI: 10.1016/j.inffus.2019.12.012.
23. Bhattacharyya, S., Jha, S., Tharakunnel, K. and Westland, J.C. (2011) 'Data mining for credit card fraud: A comparative study', Decision Support Systems, 50(3), pp. 602–613. DOI: 10.1016/j.dss.2010.08.008.
24. Botchey, F.E., Qin, Z. and Hughes-Lartey, K. (2020) 'Mobile money fraud prediction—A cross-case analysis on the efficiency of support vector machines, gradient boosted decision trees, and Naïve Bayes algorithms', Information, 11(8), 383. DOI: 10.3390/info11080383.
25. Bussmann, N., Giudici, P., Marinelli, D. and Papenbrock, J. (2020) 'Explainable AI in fintech risk management', Frontiers in Artificial Intelligence, 3, Article 26. DOI: 10.3389/frai.2020.00026.

26. Carcillo, F., Le Borgne, Y.-A., Caelen, O., Kessaci, Y., Oblé, F. and Bontempi, G. (2021) 'Combining unsupervised and supervised learning in credit card fraud detection', Information Sciences, 557, pp. 317–331. DOI: 10.1016/j.ins.2019.05.042.
27. Chen, C.-T., Lee, C., Huang, S.-H. and Peng, W.-C. (2024) 'Credit card fraud detection via intelligent sampling and self-supervised learning', ACM Transactions on Intelligent Systems and Technology, 15(2), Article 35, pp. 1–29. DOI: 10.1145/3641283.
28. Cherif, A., Badhib, A., Ammar, H., Alshehri, S., Kalkatawi, M. and Imine, A. (2023) 'Credit card fraud detection in the era of disruptive technologies: A systematic review', Journal of King Saud University – Computer and Information Sciences, 35(1), pp. 145–174. DOI: 10.1016/j.jksuci.2022.11.008. (ScienceDirect)
29. Chitimira, H. and Ncube, P. (2021) 'The regulation and use of artificial intelligence and 5G technology to combat cybercrime and financial crime in South African banks', Potchefstroom Electronic Law Journal, 24, pp. 1–35. DOI: 10.17159/1727-3781/2021/v24i0a10742.
30. Chitimira, H., Torerai, E. and Jana, V.L.M. (2024) 'Leveraging artificial intelligence to combat money laundering and related crimes in the South African banking sector', Potchefstroom Electronic Law Journal, 27(1), pp. 1–33. DOI: 10.17159/1727-3781/2024/v27i0a18024.
31. Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C. and Bontempi, G. (2018) 'Credit card fraud detection: A realistic modeling and a novel learning strategy', IEEE Transactions on Neural Networks and Learning Systems, 29(8), pp. 3784–3797. DOI: 10.1109/TNNLS.2017.2736643.
32. Eddin, A.N., Bono, J., Aparício, D., Polido, D., Ascensão, J.T., Bizarro, P. and Ribeiro, P. (2022) 'Anti-money laundering alert optimization using machine learning with graphs', AAAI Workshop on AI in Financial Services: Adaptiveness, Resilience and Governance. DOI: 10.48550/arXiv.2112.07508.
33. Ejofodomi, O.A., Gideon, E.N., Oladipo, G.O. and Oshomah, E.R. (2014) 'Automated detection of architectural detection in mammograms using template matching', International Journal of Biomedical Science and Engineering, 2(1), pp. 1–6. DOI: 10.11648/j.ijbse.20140201.11. (Science Publishing Group)
34. Enaifoghe, A., Dlamini, N.P. and Agwuna, L.U. (2020) 'African economic integration development in technological transformation: Accessing the importance of ethical leadership for policy implementation in SADC', Journal of Economics and Behavioral Studies, 12(6), pp. 11–20. DOI: 10.22610/jebs.v12i6(J).3102.
35. Falemi, A., Akhigbe, R. and Akin-Oluyomi, O.T. (2020) 'A conceptual supply chain talent development model for capability building across distributed operations', International Journal of Multidisciplinary Research and Growth Evaluation, 1(5), pp. 439–456. DOI: 10.54660/.IJMRGE.2020.1.5.439-456.
36. Falemi, A., Akhigbe, R. and Akin-Oluyomi, O.T. (2023a) 'A proposed framework for integrating employee retention systems with operational productivity metrics',

International Journal of Advanced Multidisciplinary Research and Studies, 3(1), pp. 1704–1724. DOI: 10.62225/2583049X.2023.3.1.5339.

37. Falemi, A., Akhigbe, R. and Akin-Oluyomi, O.T. (2023b) 'A supply chain workforce optimization framework for addressing staffing volatility during rapid expansion cycles', International Journal of Advanced Multidisciplinary Research and Studies, 3(1), pp. 1745–1762. DOI: 10.62225/2583049X.2023.3.1.5342.
38. Falemi, A., Akhigbe, R. and Akin-Oluyomi, O.T. (2024) 'A conceptual enterprise risk management model that integrates HR strategy with operational analytics', International Journal of Multidisciplinary Research and Growth Evaluation, 5(6), pp. 1730–1753. DOI: 10.54660/.IJMRGE.2024.5.6.1730-1753.
39. Fiore, U., De Santis, A., Perla, F., Zanetti, P. and Palmieri, F. (2019) 'Using generative adversarial networks for improving classification effectiveness in credit card fraud detection', Information Sciences, 479, pp. 448–455. DOI: 10.1016/j.ins.2017.12.030.
40. Gupta, A., Dwivedi, D.N. and Jain, A. (2022) 'Threshold fine-tuning of money laundering scenarios through multi-dimensional optimization techniques', Journal of Money Laundering Control, 25(1), pp. 72–78. DOI: 10.1108/JMLC-12-2020-0138. (ScienceDirect)
41. Ileberi, E. and Sun, Y. (2024) 'Advancing model performance with ADASYN and recurrent feature elimination and cross-validation in machine learning-assisted credit card fraud detection: A comparative analysis', IEEE Access, 12, pp. 133315–133327. DOI: 10.1109/ACCESS.2024.3457922. (Directory of Open Access Journals)
42. Islam, S., Haque, M.M. and Karim, A.N.M.R. (2024) 'A rule-based machine learning model for financial fraud detection', International Journal of Electrical and Computer Engineering, 14(1), pp. 759–771. DOI: 10.11591/ijece.v14i1.pp759-771.
43. Jensen, R.I.T. and Iosifidis, A. (2023) 'Fighting money laundering with statistics and machine learning', IEEE Access, 11, pp. 8889–8903. DOI: 10.1109/ACCESS.2023.3239549.
44. Jullum, M., Løland, A., Huseby, R.B., Ånonsen, G. and Lorentzen, J. (2020) 'Detecting money laundering transactions with machine learning', Journal of Money Laundering Control, 23(1), pp. 173–186. DOI: 10.1108/JMLC-07-2019-0055. (ScienceDirect)
45. Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P.-E., He-Guelton, L. and Caelen, O. (2018) 'Sequence classification for credit-card fraud detection', Expert Systems with Applications, 100, pp. 234–245. DOI: 10.1016/j.eswa.2018.01.037.
46. Labanca, D., Primerano, L., Markland-Montgomery, M., Polino, M., Carminati, M. and Zanero, S. (2022) 'Amaretto: An active learning framework for money laundering detection', IEEE Access, 10, pp. 41720–41739. DOI: 10.1109/ACCESS.2022.3167699.
47. Leonard, K.J. (1995) 'The development of a rule based expert system model for fraud alert in consumer credit', European Journal of Operational Research, 80(2), pp. 350–356. DOI: 10.1016/0377-2217(93)E0249-W.

48. Makolo, A. and Adeboye, T. (2021) 'Credit card fraud detection system using machine learning', International Journal of Information Technology and Computer Science, 13(4), pp. 24–37. DOI: 10.5815/ijitcs.2021.04.03.
49. Marei, A., Mustafa, J.A., Othman, M., Daoud, L., Lutfi, A. and Al-Amarneh, A. (2023) 'The moderation of organizational readiness on the relationship between TOE factors and fintech adoption and financial performance', Journal of Law and Sustainable Development, 11(3), e730. DOI: 10.55908/sdgs.v11i3.730.
50. McCallum, W. and Aziakpono, M.J. (2023) 'Regulatory sandbox for FinTech regulation: Do the conditions for effective adoption exist in South Africa?', Development Southern Africa, 40(5), pp. 1100–1116. DOI: 10.1080/0376835X.2023.2182759.
51. Mienye, I.D. and Sun, Y. (2023) 'A deep learning ensemble with data resampling for credit card fraud detection', IEEE Access, 11, pp. 30628–30638. DOI: 10.1109/ACCESS.2023.3262020.
52. Mienye, I.D. and Swart, T.G. (2024) 'A hybrid deep learning approach with generative adversarial network for credit card fraud detection', Technologies, 12(10), 186. DOI: 10.3390/technologies12100186.
53. Mökander, J., Axente, M., Casolari, F. and Floridi, L. (2022) 'Conformity assessments and post-market monitoring: A guide to the role of auditing in the proposed European AI regulation', Minds and Machines, 32(2), pp. 241–268. DOI: 10.1007/s11023-021-09577-4.
54. Mongwe, W.T. and Malan, K.M. (2020) 'A survey of automated financial statement fraud detection with relevance to the South African context', South African Computer Journal, 32(1), pp. 74–112. DOI: 10.18489/sacj.v32i1.777. (South African Computer Journal)
55. Ngai, E.W.T., Hu, Y., Wong, Y.H., Chen, Y. and Sun, X. (2011) 'The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature', Decision Support Systems, 50(3), pp. 559–569. DOI: 10.1016/j.dss.2010.08.006. (fs-ise.github.io)
56. Ogundunmade, T.P. and Adepoju, A.A. (2024) 'Modelling credit card fraud data using machine learning algorithms', International Journal on Computational Engineering, 1(2), pp. 43–49. DOI: 10.62527/comien.1.2.10.
57. Olorunkosebi, M.T., Ayinde, M.K., Mensah, G.K. and Penddah, A.L. (2023) 'Integrating artificial intelligence and advanced biosensors for rapid and sensitive detection of antimicrobial-resistant foodborne pathogens', Journal of Advances in Microbiology Research, 4(2), pp. 175–182. DOI: 10.22271/micro.2023.v4.i2b.293.
58. Olutimehin, A.O. and Ganiu, O.S. (2022) 'Integrating Lean Six Sigma with reliability-centered maintenance: A unified framework for manufacturing excellence', International Journal of Multidisciplinary Research and Growth Evaluation, 3(6), pp. 983–996. DOI: 10.54660/.IJMRGE.2022.3.6.983-996.

59. Omoegun, G.O., Sunday, E.A., Essien, M.A. and Oluokun, O.A. (2023) 'Vibration-based condition monitoring of rotating machinery using LabVIEW', International Journal of Scientific Research in Civil Engineering, 7(6), pp. 82–108. DOI: 10.32628/IJSRCE237529.
60. Omoegun, G.O., Sunday, E.A., Essien, M.A. and Oluokun, O.A. (2024) 'Implementing smart automation solutions in medium-scale industries using SCADA systems', International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 10(5), pp. 1207–1231. DOI: 10.32628/CSEIT241061242. (DOI.org)
61. Opara, I.S., Elumilade, R.A., Liadi, K.O., Shittu, H. and Adeniji, I.O. (2024) 'A theoretical review of synergizing energy efficiency with transportation logistics optimization: Towards a sustainable U.S. infrastructure', International Journal of Advanced Multidisciplinary Research and Studies, 4(6), pp. 2968–2975. DOI: 10.62225/2583049X.2024.4.6.5738.
62. Oztas, B., Cetinkaya, D., Adedoyin, F., Budka, M., Aksu, G. and Dogan, H. (2024) 'Transaction monitoring in anti-money laundering: A qualitative analysis and points of view from industry', Future Generation Computer Systems, 159, pp. 161–171. DOI: 10.1016/j.future.2024.05.027.
63. Phiri, J., Lavhengwa, T. and Segooa, M.A. (2024) 'Online banking fraud detection: A comparative study of cases from South Africa and Spain', South African Journal of Information Management, 26(1), a1763. DOI: 10.4102/sajim.v26i1.1763.
64. Rocha-Salazar, J.-d.-J., Segovia-Vargas, M.-J. and Camacho-Miñano, M.-d.-M. (2021) 'Money laundering and terrorism financing detection using neural networks and an abnormality indicator', Expert Systems with Applications, 169, 114470. DOI: 10.1016/j.eswa.2020.114470.
65. Rtayli, N. and Enneya, N. (2020) 'Selection features and support vector machine for credit card risk identification', Procedia Manufacturing, 46, pp. 941–948. DOI: 10.1016/j.promfg.2020.05.012.
66. Rudin, C. (2019) 'Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead', Nature Machine Intelligence, 1(5), pp. 206–215. DOI: 10.1038/s42256-019-0048-x.
67. Ryman-Tubb, N.F., Krause, P. and Garn, W. (2018) 'How artificial intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark', Engineering Applications of Artificial Intelligence, 76, pp. 130–157. DOI: 10.1016/j.engappai.2018.07.008. (ScienceDirect)
68. Saito, T. and Rehmsmeier, M. (2015) 'The precision-recall plot is more informative than the ROC plot when evaluating binary classifiers on imbalanced datasets', PLOS ONE, 10(3), e0118432. DOI: 10.1371/journal.pone.0118432.
69. Shittu, H. and Nabil, M. (2023) 'Smart supply chain management with attribute-based encryption access control', 2023 IEEE 13th Annual Computing and Communication

Workshop and Conference (CCWC), pp. 198–204. DOI: 10.1109/CCWC57344.2023.10099268.

70. Shittu, H.A. and Shittu, M.A. (2024) 'AI-powered digital twins for predictive maintenance and operational optimization of renewable energy systems', International Journal of Science, Architecture, Technology and Environment, 1(7), pp. 151–163. DOI: 10.63680/ijsate0324085.011.
71. Shittu, H.A., Shittu, M.A. and Olagunju, F. (2024) 'Cyber physical resilience in digital substations: IoT enabled adaptive protection for secure DER integration', International Journal of Science, Architecture, Technology and Environment, 1(3), pp. 81–99. DOI: 10.63680/ijsate032532.08.
72. Shittu, H.A., Shittu, M.A., Adeleke, O.J. and Adedokun, O.J. (2021) 'Blockchain based energy trading models for peer-to-peer renewable microgrids', International Journal of Research in Electrical and Electronics Engineering, 4(3), pp. 1–19. DOI: 10.34218/IJREEE_04_03_001.
73. Shittu, M.A., Adeniji, I.O., Shittu, H. and Opara, I.S. (2022) 'Blockchain-assisted secure data exchange architectures for SCADA-controlled power systems', Iconic Research and Engineering Journals, 6(3), pp. 359–380. DOI: 10.64388/IREV6I3-1714041.
74. Shittu, M.A., Shittu, H.A., Adeleke, O.J. and Adedokun, O.J. (2023) 'Digital twin modeling for real time monitoring and fault detection in smart substations', International Journal of Industrial Engineering Research and Development, 14(2), pp. 25–44. DOI: 10.34218/IJIERD_14_02_003.
75. Soemers, D.J.N.J., Brys, T., Driessens, K., Winands, M.H.M. and Nowé, A. (2018) 'Adapting to concept drift in credit card transaction data streams using contextual bandits and decision trees', Proceedings of the AAAI Conference on Artificial Intelligence, 32(1), pp. 7831–7836. DOI: 10.1609/aaai.v32i1.11411.
76. Stojanović, B., Božić, J., Hofer-Schmitz, K., Nahrgang, K., Weber, A., Badii, A., Sundaram, M., Jordan, E. and Runevic, J. (2021) 'Follow the trail: Machine learning for fraud detection in fintech applications', Sensors, 21(5), 1594. DOI: 10.3390/s21051594. (MDPI)
77. Stulz, R.M. (2022) 'FinTech, BigTech, and the future of banks', Journal of Applied Corporate Finance, 34(1), pp. 106–117. DOI: 10.1111/jacf.12492.
78. Sunday, E.A. and Omoegun, G.O. (2019) 'Optimizing electrical load distribution for hybrid solar installations in developing economies', International Journal of Scientific Research in Mechanical and Materials Engineering, 3(6), pp. 27–47.
79. Sunday, E.A. and Omoegun, G.O. (2022) 'Automation of process control systems using Siemens TIA Portal: A case study approach', International Journal of Scientific Research in Mechanical and Materials Engineering, 6(5), pp. 30–55. No verifiable article-specific DOI identified. (ResearchGate)

80. Sunday, E.A. and Omoegun, G.O. (2022) 'Smart fault detection in HVAC systems using sensor-based monitoring', International Journal of Scientific Research in Science, Engineering and Technology, 7(4), pp. 380–403. (ResearchGate)
81. Sunday, E.A., Omoegun, G.O., Essien, M.A. and Oluokun, O.A. (2019) 'Thermodynamic efficiency and control strategies in residential air conditioning systems', International Journal of Scientific Research in Civil Engineering, 3(3), pp. 52–76. DOI: 10.32628/IJSRCE19339.
82. Sunday, E.A., Omoegun, G.O., Essien, M.A. and Oluokun, O.A. (2020) 'Transitioning from reactive to predictive maintenance in mechanical systems', International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 6(6), pp. 425–447.
83. Tagbo, S.K. and Adekoya, A.F. (2023) 'A systematic literature review of machine learning techniques in financial fraud prevention and detection', International Journal of Society Systems Science, 14(4), pp. 303–348. DOI: 10.1504/IJSSS.2023.135915.
84. Tong, G. and Shen, J. (2023) 'Financial transaction fraud detector based on imbalance learning and graph neural network', Applied Soft Computing, 149, 110984. DOI: 10.1016/j.asoc.2023.110984.
85. Udeze, C.L., Eteng, I.E. and Ibor, A.E. (2022) 'Application of machine learning and resampling techniques to credit card fraud detection', Journal of the Nigerian Society of Physical Sciences, 4(3), 769. DOI: 10.46481/jnsps.2022.769.
86. Van Vlasselaer, V., Bravo, C., Caelen, O., Eliassi-Rad, T., Akoglu, L., Snoeck, M. and Baesens, B. (2015) 'APATE: A novel approach for automated credit card transaction fraud detection using network-based extensions', Decision Support Systems, 75, pp. 38–48. DOI: 10.1016/j.dss.2015.04.013.
87. Vorobyev, I.A. and Krivitskaya, A.D. (2022) 'Reducing false positives in bank anti-fraud systems based on rule induction in distributed tree-based models', Computers & Security, 120, 102786. DOI: 10.1016/j.cose.2022.102786. (ScienceDirect)
88. West, J. and Bhattacharya, M. (2016) 'Intelligent financial fraud detection: A comprehensive review', Computers & Security, 57, pp. 47–66. DOI: 10.1016/j.cose.2015.09.005. (ScienceDirect)
89. Whitrow, C., Hand, D.J., Juszczak, P., Weston, D. and Adams, N.M. (2009) 'Transaction aggregation as a strategy for credit card fraud detection', Data Mining and Knowledge Discovery, 18(1), pp. 30–55. DOI: 10.1007/s10618-008-0116-z.
90. Yusuf, M., Akintunde, A., Habeeb, S. and Quadri, A. (2023) 'Radio Frequency Identification (RFID) based library management system', International Journal of Technology and Systems, 8(2), pp. 21–35. DOI: 10.47604/ijts.2041.