Data Science Approaches to Fraud Detection in KYC and KYT

Fraud Detection in Know Your Customer (KYC)

KYC focuses on verifying customer identities and assessing risk during onboarding and beyond. Modern data-driven methods help flag potentially fraudulent users by analyzing attributes of the customer profile (demographics, account history) and relationships to other entities. Key research contributions include:

Hybrid Rule/ML Models: Kasireddy (2025) proposed a *hybrid AI architecture* for KYC fraud detection that combines rule-based decision engines with machine learning models[1]. This approach addresses the rigidity of static rules and the opacity of pure ML by balancing real-time detection with interpretability. In evaluations on synthetic KYC data, the hybrid system *significantly outperformed* both rule-only and ML-only baselines in terms of detection accuracy, efficiency, and adaptability to new fraud patterns[2]. This demonstrates the benefit of leveraging expert rules (for known fraud signals) alongside data-driven models (for adaptive pattern learning).

Fair and Explainable KYC Modeling: Agboola (2025) emphasized the importance of *fairness-aware* AI in KYC compliance[3]. Their work introduced techniques like sample re-weighting, threshold tuning, and cohort-based evaluation to ensure that fraud risk models do not unduly penalize certain demographics or customer groups. The key contribution is integrating bias mitigation into the fraud detection pipeline, so that *customer demographics* (e.g. age, region, occupation) are handled equitably while maintaining high predictive performance. This helps financial institutions meet ethical and regulatory standards (avoiding discriminatory outcomes) without sacrificing fraud detection accuracy.

Role of Demographics and Account Attributes: Recent studies highlight that *customer profile features* such as age, account tenure, and linked accounts/devices can greatly enhance KYC fraud detection. For example, Gokah *et al.* (2025) note that beyond transactions, **account-level attributes** – *account age*, history of activity, connected devices/IP addresses – and **demographic features** (customer's age, sex, income, region, etc.) "play a major role" in detecting suspicious customers[4] [5]. Incorporating these features provides context for distinguishing normal behavior from anomalies. A low-income customer with very few prior transactions, for instance, suddenly making many large international transfers would stand out against their demographic baseline and trigger an alert[6]. This evidence underlines the value of KYC data (who the user is) in complementing transaction data.

Graph-Based Identity Networks: Another frontier is using graph analytics to map relationships between customers (shared contact info, devices, addresses) and uncover fraud rings or synthetic identities. Vallarino (2025) demonstrated a Graph Neural Network approach that models customers and transactions as a network[7]. This GNN was able to **expose collusive rings and synthetic identity fraud** – e.g. groups of accounts linked through common attributes or behaviors – that traditional individual-level models often miss. It achieved higher recall than tree-based models in detecting fraud hidden in complex networks of customers[7]. The key contribution is showing that *user relationships* (network connectivity) are powerful signals: fraudsters who create many interlinked accounts or operate in rings can be identified by their network patterns.

Aged Accounts and Vulnerable Customers: Focusing on a specific KYC segment, Gokah *et al.* (2025) studied fraud in **"aged accounts"** (such as

dormant or senior citizen accounts). They applied a suite of ML techniques – supervised algorithms (Random Forests, boosting), unsupervised clustering, deep learning, even NLP – on a combination of transaction records, account metadata, and behavioral patterns[8][9]. The *AI-based system significantly outperformed* traditional rules, catching subtle fraud schemes targeting older customers (including account takeovers and elder financial abuse) with **fewer false positives and faster detection**[10]. The key contribution here is demonstrating a holistic analytics approach: by engineering features from account history, user behavior, and even external data sources, the models were able to detect anomalies (e.g. sudden reactivation of a long-dormant account) that rules had missed. This underscores how comprehensive KYC profiling (age of account, usage patterns, cross-institution data) can strengthen fraud prevention for at-risk customer groups.

Fraud Detection in Know Your Transaction (KYT)

KYT involves ongoing monitoring of customers' transaction activity to spot suspicious behavior. Data science methods in this area analyze transactional patterns – amounts, frequencies, types of payments, etc. – to distinguish fraudulent transactions from legitimate ones. Notable research contributions include:

Analyzing Spending Patterns & Balances: A 2025 *Scientific Reports* study used feature importance analysis to identify which transaction characteristics matter most in fraud detection models[11]. It found that **transaction amount** was the top indicator (fraudulent transactions tend to involve either unusually large sums or bursts of many small payments in a short time). **Transaction frequency/timing** was also critical – irregular, high-frequency transaction bursts or abnormal time intervals often signal fraud attempts[12]. Moreover, certain **transaction types** (categories of spend) carried higher risk, suggesting some payment types are more frequently associated with fraud[13]. These findings reinforce that KYT systems should monitor *spending pattern anomalies*, such as rapid balance fluctuations or off-pattern purchases, as key red flags. Combining multiple dimensions (amount, time, type, location) yielded the best results, highlighting the need for multi-feature analysis rather than any single trigger[14].

Deep Learning on Transaction Data: Jaya *et al.* (2025) introduced an innovative fraud detector based on *Deep Quantum Neural Networks (DQNN)* for online payments[15]. Their system examines each transaction's details – including the payment **type**, the transaction **quantity/amount**, and recent **balance fluctuations** – to predict fraud in real time[16]. By leveraging quantum-inspired neural networks (via the PennyLane framework), they achieved higher classification accuracy than conventional deep learning models in identifying fraudulent transactions[17]. A key contribution is the integration of an alert mechanism: when suspicious activity is flagged, the system automatically sends real-time notifications (e.g. via SMS) to account owners[18]. This study demonstrates how advanced ML (and even emerging quantum computing techniques) can boost KYT by quickly detecting anomalies in transaction streams (for example, a sudden series of out-of-character purchases) and enabling prompt intervention.

Graph-Based Transaction Networks: Islam *et al.* (2025) developed *LayerWeighted-GCN (LWG)*, a graph neural network tailored for financial transaction networks[19]. This model represents transactions as a graph (linking senders, receivers, merchants, etc.) and introduces an adaptive layer-weighting mechanism that lets the GCN focus on different pattern scales. The key innovation is capturing **intricate transaction patterns** – both local and global structures in the flow of money – that traditional models struggle with[20]. They also created a synthetic benchmark dataset (SIFT) to evaluate varied fraud scenarios. In experiments, LWG-GCN achieved higher detection **accuracy** than baseline ML and even outperformed other GNN models, while also **reducing false positive**

rates[21]. This work's contribution lies in improving KYT by using relational learning: for instance, it can identify complex fraud typologies (like circular fund flows or multiple small transfers that aggregate to large amounts) through the graph of transactions. By dynamically re-weighting network layers, the model adapts to both immediate anomalies and broader transaction network structures, making it a robust tool for catching sophisticated fraud schemes in payment networks.

Graph Databases & Feature Extraction: Patil *et al.* (2024) likewise harnessed graph techniques for KYT, integrating a Neo4j graph database with machine learning[22]. Their approach first models the financial data as a graph of entities (customers, accounts, merchants) and relationships (transactions, payments), then extracts **graph-based features** that capture relationships and behaviors (e.g. the connectivity of a customer to merchants, transaction cycles). By feeding these features into standard ML algorithms, they achieved effective fraud detection across multiple transaction types (credit card, debit card, online banking)[22]. The paper's key contribution is demonstrating near *real-time anomaly detection* by querying the graph for patterns – for example, detecting if one customer account is making payments to many different merchants in a short span, or if multiple accounts funnel funds to the same recipient (potential indicators of fraud rings). The results showed improved accuracy and lower false alarm rates, validating that graph-enriched features (like network centrality or link analysis) provide valuable signals for transaction monitoring systems.

Holistic AML Pipelines: Many recent studies bridge KYC and KYT under the umbrella of anti-money laundering. For instance, an *AML compliance* pipeline described by Zhang *et al.* (2025) integrates heterogeneous data sources – transactions, KYC profiles, and external watchlists – and applies a combination of supervised classifiers, anomaly detectors, and even NLP for unstructured data[23]. Such systems use **transaction monitoring** models in tandem with KYC risk scores, adjusting thresholds dynamically and employing *graph analytics* to capture cross-entity laundering patterns[24]. The overarching finding is that AI-driven approaches can drastically reduce false positives (which in older rule-based systems often exceeded 95%[25]) while detecting complex, cross-customer schemes that were previously overlooked. This highlights how combining *Know-Your-Customer data (who is transacting)* with *Know-Your-Transaction analytics (how and when they transact)* yields a more powerful fraud detection strategy. The research consensus is that robust fraud prevention requires both dimensions: continuous KYC profiling to understand the user, and continuous KYT surveillance to catch anomalous transactions in context.

References

Each cited study above comes from peer-reviewed journals or conference proceedings in machine learning, data mining, or financial fraud detection. These works collectively advance the state of fraud detection by employing data science techniques – from ensemble learning and deep neural networks to graph analysis – tailored to the KYC/KYT domains. By leveraging rich customer data (age, relationships, etc.) and transaction patterns (amounts, frequencies, networks), they demonstrate significant improvements in identifying fraudulent behavior while minimizing false alarms[10][21]. The provided citations link to the full articles for further details on methodology and results.

---

[1] [2] tijer.org

https://tijer.org/tijer/papers/TIJER2505242.pdf

[3] [23] [24] [25] arxiv.org

https://www.arxiv.org/pdf/2512.06240

[4] [5] [6] [8] [9] [10] (PDF) AI-driven detection of fraudulent activities in aged accounts within the U.S. financial system

https://www.researchgate.net/publication/398827120_AI-driven_detection_of_fraudulent_activities_in_aged_accounts_within_the_US_financial_system

[7] (PDF) Graph AI for Fraud Detection: Improving Risk Management and Compliance in Digital Finance

https://www.researchgate.net/publication/390424252_Graph_AI_for_Fraud_Detection_Improving_Risk_Management_and_Compliance_in_Digital_Finance

[11] [12] [13] [14] The analysis of fraud detection in financial market under machine learning | Scientific Reports

https://www.nature.com/articles/s41598-025-15783-2?error=cookies_not_supported&code=b455d4d2-f197-46d1-9676-93920a5e7ae1

[15] [16] [17] [18] Online Payment Fraud Detection Using Deep Quantum Neural Network | Atlantis Press

https://www.atlantis-press.com/proceedings/iccsce-25/126017438

[19] [20] [21] Detecting Fraudulent Transactions for Different Patterns in Financial Networks Using Layer Weigthed GCN | Human-Centric Intelligent Systems

https://link.springer.com/article/10.1007/s44230-025-00097-3

[22] Enhancing fraud detection in banking by integration of graph databases with machine learning - PMC

https://pmc.ncbi.nlm.nih.gov/articles/PMC11016795/