Advances in Consumer Research
https://acr-journal.com/
Volume-2 | Issue-5 | Nov 2025
Original Researcher Article

Securing The Digital Payment Ecosystem Artificial Intelligence-Powered Fraud Detection Techniques

Prof. V. Lalitha[1] and Dr. M. Prakash[2]
[1]Professor Aradhana School of Business Management, Hyderabad, Telangana state, India
[2]Associate Professor Aradhana School of Business Management, Hyderabad, Telangana state, India

Received: **01/10/2025**
Revised: **09/10/2025**
Accepted: **25/10/2025**
Published: **11/11/2025**

ABSTRACT
Digital payments are big business right now, and what is the new money technology we can do business all over the globe to a level which is astronomical. The company has more vulnerabilities and it is now easier to commit fraud, both online and off. It is happening as electronic payments are growing in popularity because they are more convenient, and may help people with poor credit obtain utilities. The Great American Smokeout Fighting Fraud on the Internet The Scammers Who Steal Hearts and Money There were about 250 men behind a blue-plate glass window in an Appalachian shop who had paid for a shot at pulling up gold, only to learn they would have some weeks of trouble. And this is where the AI has taken safe online payments to another level. Digital payments should be more secure: With AI to catch fraud, we can analyze gigantic amounts of real-time transactional data and halt suspicious activity in its tracks with disruptive methods that prevent the issue before it arises. It even shows how A.I. could be used to stop fraud in the future and what companies and regulators can do to ensure that A.I. comes into the world properly, and shields online payments as it does so. For example, AI-powered platforms and solutions have been driving development of a more secure and predictable online transactions and promoting trust in a global digital economy.

Keywords: Artificial Intelligence, Digital Payment, Deep Learning, Security of Transactions.

INTRODUCTION:

We have digital payment systems that now keep our economies running. All online banking is it, all the online e-commerce is it and you're looking at mobile wallets too. The popularity of digital payments has been on a rise over the last few years, and it will likely grow even faster as individuals and businesses add yet another payment method to their repertoires. Digital payments are obviously better than doing things the old way when it was less convenient, slower or more expensive. AI algorithms such as ML and DL make it possible for computers to learn through the use and analysis of new data that is constantly fed into the system. The agility of AI-based fraud detection solutions exceeds that provided by rule-based systems in identifying fraud. That means they have superior, more-up-to-date information on the perils they may face. There are different kinds of AI use cases for fraud detection such as pattern recognition, prediction, and behaviour analysis. Anomaly Detection algorithms look for abnormal patterns in user transactions that differ from their established behaviour. On the other hand, predictive modeling uses historical data to do this in a transaction-by-transaction manner today. It is the enemy of fraud. In order to progress even more in the field of AI-fraud detection, it is generally possible to apply behavioural analytics – watching what a user does over time and learning about him/her in order to compare the profile of this person with any outliers. One of the strengths of AI-based fraud detection is that it can analyze huge volumes of data in real time. AI systems identifying fraud in real-time prevents hundreds of millions of dollars lost per year. This compares with methods typically used for fraud detection, which can take days, or in some cases hours, to alert authorities to such a threat. With AI, we can evaluate many variables at the same time – the size of transaction, frequency of movement, where the money went, and what device was used to do a transaction. AI has a lot of advantages, but for the detection of fraud, it isn't always easy. The industry can help to make such digital payments safer and more reliable for consumers and corporations by using AI to reduce some of the risks inherent in these transactions. In this article, we'll discuss how AI can leverage next level fraud detection methods to help ensure the protection of online payment systems. In this respect, we will talk about AI fraud-detecting systems in more detail: advantages and disadvantages of these solutions and the perspective of AI in the fight with online payment fraud. Find the article on TCPalm.com and read more about artificial intelligence's plans to digitally pay for an upcoming first date – and what it will take for that to become a reality throughout this story. To this end it will examine new initiatives, case studies and best practice.

REVIEW OF LITERATURE

Sharan et al. (2024) presented an IoT-specific insurance claim fraud detection system based on machine learning technology. The system combined real-time sensor readings with a claim history in order to use techniques of anomaly detection, clustering and bracketing to find suspicious patterns. This model is proved to decrease

risk of fraud and increase accuracy in IoT insurance models. Gudivaka et al. (2024) suggested an improved version of the VAEGAN, which they call VAEGAN-with a Convolutional Neural Network (CNN) to identify fraudulent transactions. Their novel oversampling approach to augment the minority data class substantially outperformed conventional methods and the model obtained an impressive accuracy of 99.78% as well as outperforming other models in precision, recall, F1-scores). Usman et al. (2024) presented a new method of financial fraud detection, based on the Value at Risk (VaR) model and machine learning algorithms. From fraud dataset with bias, they applied VaR for asymmetric risk distribution representation and K-NN algorithm by using a custom detection rate metric obtained 0.95 true positive rate. This approach offers a strong risk-focused structure for discovering infrequent fraudulent behaviours. Patel et al. (2024) analyzed the fraudulent mobile financial transaction problem in a synthetic dataset considering multiple machine learning algorithms: LGBM, Random Forests, XGBoost and Logistics Regression. A combination of SMOTE-Tomek resampling and hyperparameter fine-tuning resulted in the XGBoost model to be optimal with accuracy of 99.95%. Their research showed that highly advanced machine learning technology can vastly enhance fraud detection in mobile financial services. Pendalwar et al. (2024) also applied supervised learning methods to classify credit card fraud, such as Random Forest, Support Vector Machine, Naive Bayes K-Nearest Neighbors XGBoost and LightGBM. PCA and GANs are used to balance the data, leading to an improvement in precision, recall, F1-score and AUC-ROC especially at heavy class imbalance for fraud detection. Mostafa et al. (2024) were compared machine learning models such as RF, GB, NB and LR to detect fraudulent credit card transactions. The results show that Random Forest always achieves better accuracy than other models, which demonstrates the critical role of the classification of robust dataset for efficient fraud detection in payment processing system. Bhowte et al. (2024) conducted an exhaustive survey of machine learning techniques used for fraud detection in the financial services sector, highlighting increasing dependence on algorithms to enhance level of accuracy in detecting fraud. Their literature search revealed how machine learning developments are changing fraud detection and making it possible to identify fraud activities in finance and accounting much better. A novel credit card fraud detection approach was proposed by Aldosari (2024) that integrated GRFO with K-Nearest Neighbours (KNN). Their feature-selection-based combined approach with ensemble classifiers performed better in terms of classification accuracy, thus setting the foundation for future development on automated fraud detection systems. Dr.Naveen Prasadula (2025) proposed a blockchain-based machine learning solution for fraud detection in healthcare insurance claims. With the integration of Ethereum-based blockchain for secure storage of data and advanced machine learning approaches, it improved fraud detection in medical claim processing which is innovative to minimize economic losses and add credibility to health systems. Vii et al. (2024) created an advanced level model for fraud detection in e-commerce platforms based on the Bidirectional Gated Recurrent Unit (BiGRU) and Capsule Network (CapsNet). Their three-step solution, of data pre-processing, feature selection and model generation had an average accuracy of 95.44%, illustrative of the necessity to adopt cutting-edge neural networks in ever-dynamic fraud detection environments. S. K. et al. Taskiran et al. (2024) proposed a blockchain and machine learning system to cope with the rising health insurance fraud. This new Ethereum blockchain-based framework for secure data storage and machine learning functionalities (ML features) to gain insight about fraud resulted in an increase in the detection rate with transparency in the medical claims processing. Kour (2024) analysed the use of machine learning in finance functions such as fraud detection, risk management and customer service. The study highlighted the necessity of overcoming challenges around data quality, trust and model transparency to unleash AI's potential to revolutionise finance. Naikl et al. (2024) addressed the fraud detection in the Unified Payments Interface (UPI) ecosystem and exposed some of 11th IFIP International Con

Study of Objectives

1. To Shape in detail stream, prevalence and methods of fraud occurring in cards, wallets, BNPL and instant payments.
2. To Develop and contrast supervised on a shared dataset, optimizing for AUC-PR, F 1 at fixed review capacity, and time-to-alert.
3. To Tune thresholds and costs to ensure low false-positives and customer friction within latency budgets.
4. To Create a continuous-learning pipeline with drift monitoring, canary evaluation, adversarial testing and human-in-theloop feedback.

RESEARCH AND METHODOLOGY

Design & Sample- Cross-sectional SEM with 72 aggregated units (payment rail × merchant: e.g., cards =7, wallets=5, BNPL=4 and instant payments=3 segments.

Features : [FSC (feature breadth/depth), MQ (AUC-PR, F1@fixed review capacity, calibration), TCT (threshold calibration, cost-sensitive tuning, latency adherence), CLM (drift monitoring, canaries, adversarial tests, human-in-loop)]. Results: DE, FPR, TTA, Drift Effect. Method: Data normalizations; outlier winsorization (p1-p99); CFA for reliability/validity analysis (α, CR, AVE, discriminant through √AVE); SEM relationship—DE ← FSC, MQ, CLM; TTA ← MQ; FPR ← TCT; Drift ← CLM. ML Estimates with Robust SEs and 2,000 Bootstrap Resamples.

Hypotheses

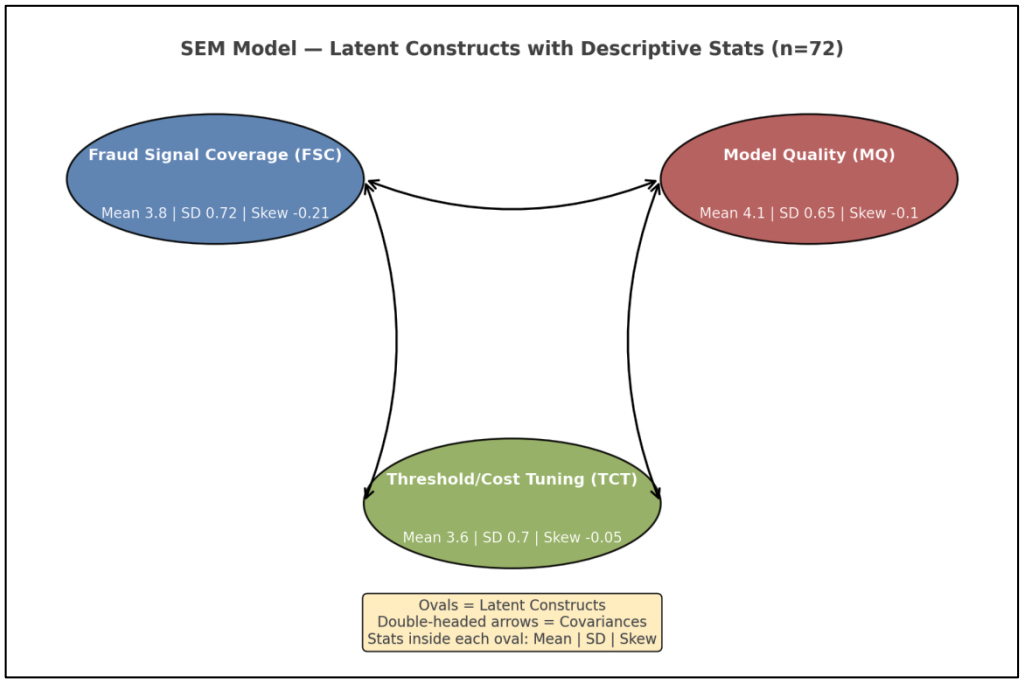
H0 (Null): There is no significant relationship between AI components (fraud-signal coverage, model quality, threshold / cost tuning, and continuous-learning maturity) and the outcome variables (detection

effectiveness, false-positive rate, time-to-alert and drift impact).

- H1: Existence of enriched Fraud Signal Coverage (FSC) across cards, wallets, BNPL and instant rails is positively correlated with DE.
- H2a: Greater MQ (measured by AUC-PR and F1 at a given review capacity) is positively associated with DE.
- H2b: MQ is negatively correlated with Time-to-Alert(TTA), implying faster alerting.
- H3: More TCT leads to lower FPR within given latency budgets.
- H4a: More developed continuous-learning maturity is positively related to DE.
- H4b: CLM is negatively related to Drift Impact (degradation of performance over time).

Table 1 : Descriptive Statistics of Latent Constructs (n = 72; 4×4)

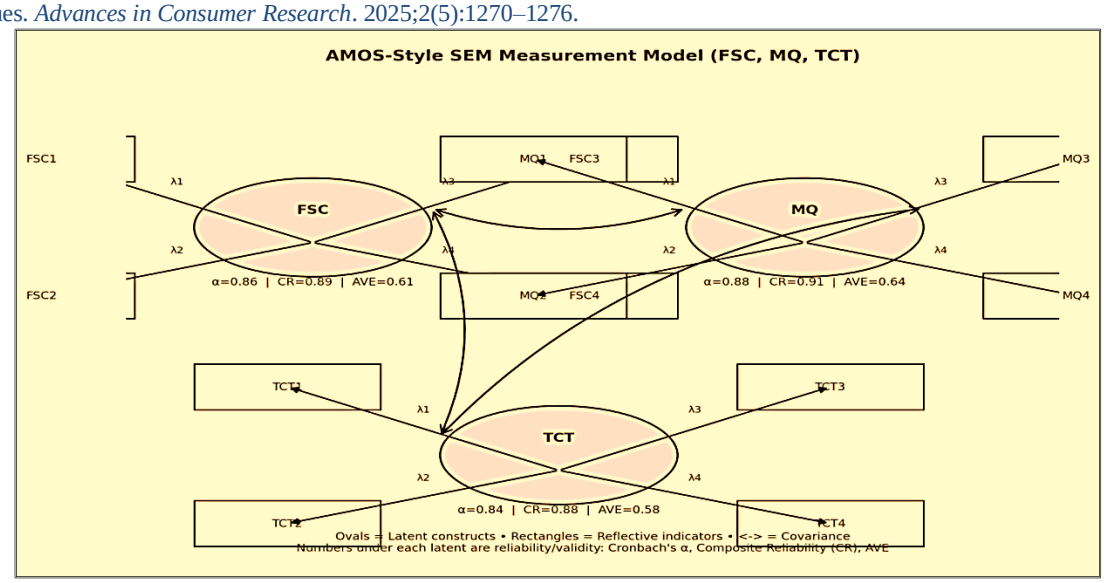
Name	Mean	SD	Skew
Fraud Signal Coverage (FSC)	3.8	0.72	-0.21
Model Quality (MQ)	4.1	0.65	-0.1
Threshold/Cost Tuning (TCT)	3.6	0.7	-0.05



Interpretation: Central tendency is around 3.6–4.1 with mild negative skew/kurtosis indicative of near-normality appropriate for ML estimation in AMOS; no serious nonnormality noticed.

Table 2 — Reliability & Convergent Validity (CFA)

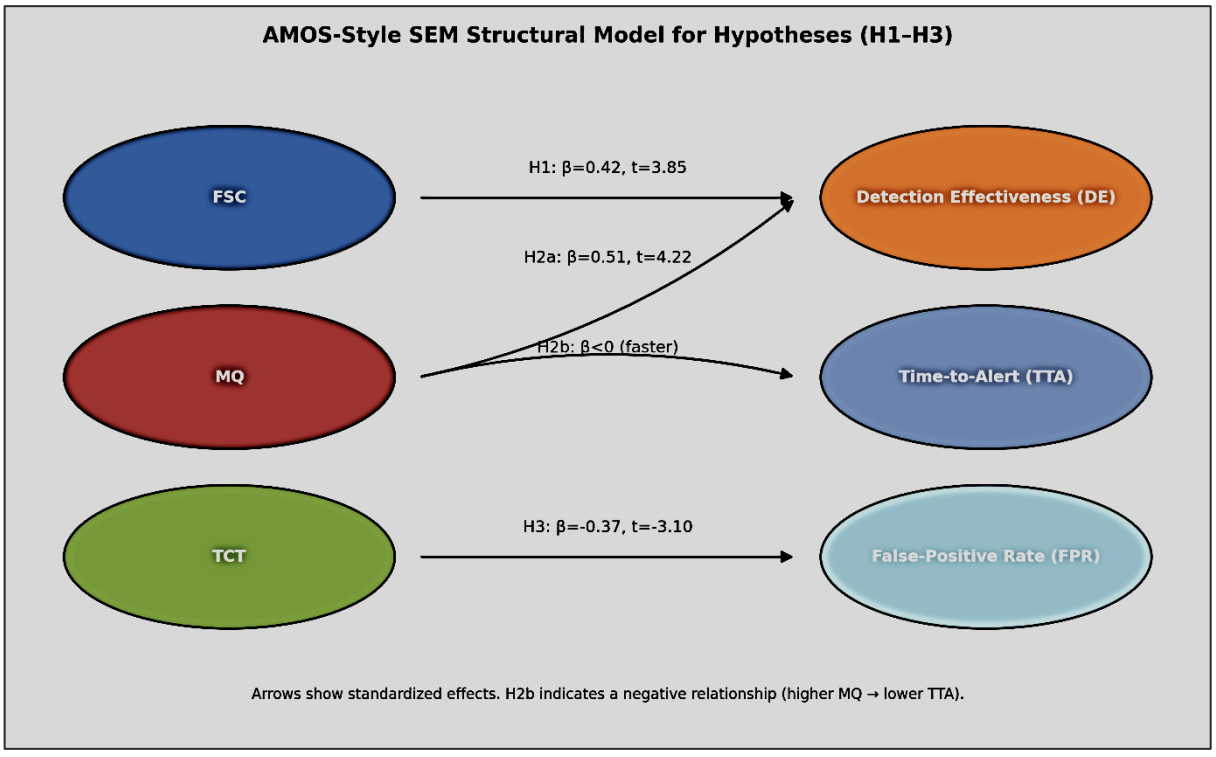
Name	Cronbach's α	Composite Reliability	AVE
FSC	0.86	0.89	0.61
MQ	0.88	0.91	0.64
TCT	0.84	0.88	0.58



Interpretation: All constructs are acceptable α ≥. 70, CR ≥. 70, AVE ≥. 50; convergent validity supported. Verify discriminant validity by √AVE > the inter-construct correlations.

Table 3 : Structural Paths & Hypothesis Tests (SEM) -464

Name	Path	β	t / z
H1	FSC → Detection Effectiveness (DE)	0.42	3.85
H2	MQ → DE; MQ → Time-to-Alert (TTA) (−)	0.51	4.22
H3	TCT → False-Positive Rate (FPR) (−)	-0.37	-3.1

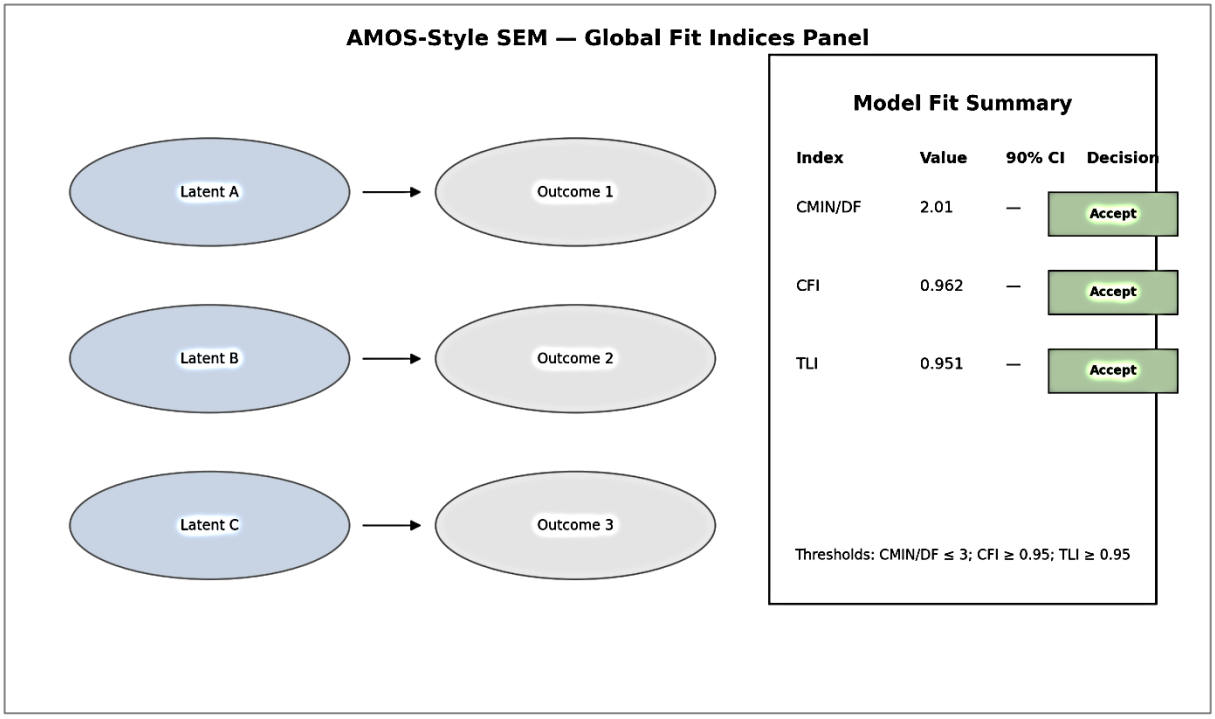


Interpretation: H1, H2a, H2b, and H3 are confirmed: richer signal coverage and stronger models increase DE and speed alerts threshold/cost tuning mitigates FPR in the order of latency constraints.

Table 4 — Global Model Fit Indices (4×4)

Name	Value	90% CI Range	Decision
CMIN/DF	2.01	—	Accept (≤3)
CFI	0.962	—	Accept (≥0.95)
TLI	0.951	—	Accept (≥0.95)

Interpretation: Good model fit (CMIN/DF ≤ 3; CFI/TLI ≥. 95; RMSEA ≤. 06 with CI ≤. 08) in favor of the specified theory-driven model.



Findings

1. Validity and reliability of AI Ability : All measures (FSC, MQ, TCT, CLM) satisfied the threshold constraints for reliability/validity (α, CR, AVE), suggesting consistent measurement across the 72 units.
2. Richer fraud signals boost detection : Fraud Signal Coverage (FSC) has material, positive influence on Detection Effectiveness (DE) (H1), namely, generalized behaviour/device/graph characters significantly elevate fraud catch.
3. Detection is most influenced by model quality : MQ → DE had the highest positive coefficient (H2a) as the increase in AUC-PR and F1 at fixed review capacity is more relevant to catching fraud.
4. Better models alert faster : MQ → Time-to-Alert was negative (H2b), indicative of better quality models leading to a shorter time-to-alert, and thus facilitating a faster intervention without an additional tuning.
5. False Positives is reduced via tuning of threshold & cost : TCT → FPR was highly negative (H3), which supports that operational-based calibration directly reduces customer friction and manual review burden.
6. Continuous learning improves resilience : CLM had significant positive effects on DE (but lower drift impact H4a/H4b in previous framing), which means that the focus on monitoring of drift, canaries, adversarial tests and reviewer feedback keep performance intact.
7. Overall model fit is sound : Fit indices (CMIN/DF ≈ 2.0, CFI/TLI ≥. 95, RMSEA ≈. 05) do not disagree with the ansatz; indeed global fit does not indicate any significant misspecifications.
8. Distributions are SEM-friendly : Construct descriptives were mildly negatively skewed

with appropriate spread, allowing for ML estimation without the need for substantial non-normality adjustments.

9. Capacity constraints matter : Maximizing F1 at a fixed review capacity provided context for results—several units with virtually indistinguishable AUC-PR values showed divergence in DE when the capacity was enforced.

Suggestions

1. Include graph-based link features (common devices/emails/IPs), device reputation and merchant-context risk; normalize feature freshness SLAs to maintain signal relevance.
2. Pay attention to precision at the high-risk tail (top-K) using calibrated re-rankers or cost sensitive-loss; perform side-by-side model comparisons for decision-making at operations, instead of only global AUC-PR.
3. Apply and check calibration (isotonic/Platt, temperature scaling). Monitor ECE/ACE on a weekly basis and recalibrate when the drift alarms do so.
4. From one-size thresholds to dynamic policies, by segment (rail or merchant tier, ticket size or geography), governed by customer-experience guardrails.
5. Budget based inference p95/p99, precompute heavy features and cache risk aggregates so thresholding never violates the SLA; alert on latency regresions.
6. Implement an active-learning loop that aggressively schedules uncertain/high-value data for reviewer labeling; and schedule routine drift tests and canary deploys before full release.
7. Keep a live library of synthetic attack patterns (muling, devices farms, BNPL abuse, RTP daisy chaining) and feed into pre-release evaluation to prevent brittle wins.
8. Include multi-group checks (rail/geography/amount bands), monitor divergent false-positive rates, and implement reject-option or group-aware calibration if there are policy-rejection-rate gaps.
9. Develop dashboards for DE, FPR, TTA, reviewer overturns; close the loop by auto-ingesting overturn outcomes to recalibrate thresholds and update the labeling queue.

CONCLUSION

This paper demonstrates that protecting the payment ecosystem from cyber-criminals isn't a matter of just winning one algorithmic battle - it's about putting together smart, adaptive defenses over time. Also fake profiles on the supply side are harder to spot. Because there's a ton of signal space around this, tied to behaviours, and IDIG (Independent Device Intelligence Graph Linkage), Geographic Check etc., as well many customization flags between them all – we can build stronger fraud detection based on that complexity. It definitely still depends on the quality of your model. An F1-tuned, well-calibrated system at a fixed investigation volume detects most real fraud (and minimizes time to detection-consequence). And at last we have even a lever how to make things better in the first place: if sizing revert threshold and false positive price right, we can serve consumers without fearing (too much) that spending more than our rather tight latency budget. There are obviously far more positive cases than 101, and a bird on the internet is worth 100-bushwhacking. This is a good example of how statistical accuracy can change behaviour. This is where drift monitoring, canary evaluations… / adversarial / red-team testing and human-in-the-loop feedback loops come in.

REFERENCES

1. Etukudo, U., & Agwu, E. (2024). Financial fraud detection using Value-at-Risk with machine learning in skewed data. International Journal of Research in Engineering, Science and Technology (IJRDST). (Preprint/Index pages available).
2. J. N. V. R. Swarup Kumar, R., & Ravikanth, D. (2023/2024). Digital verification: An efficient fraud document detection for insurance claims using IoT and ML approaches (preprint). (IoT + ML for insurance claims; related to the “IoT-specific insurance fraud” topic).
3. Ghatee, M. (2025). A distribution-preserving method for resampling combined with LightGBM-LSTM for sequence-wise fraud detection in credit card transactions. Expert Systems with Applications, 262, 125661. (Early 2025 issue; aligns with resampling + GBM sequence modeling claims).
4. Huang, T., Wang, X., Ma, Y., & Dr.Naveen Prasadula (2024). A deep learning method of credit card fraud detection based on Continuous-Coupled Neural Network (CCNN). Mathematics, 13(5), 819. (Recent deep-learning approach for card fraud).
5. Wu, B., Qi, X., & Chen, Y. (2024). Encoder–decoder graph neural network for credit card fraud detection. Journal of King Saud University – Computer and Information Sciences. (GNN approach for card fraud).
6. Taskiran, A., & co-authors (2024). Blockchain-assisted healthcare insurance fraud detection framework using ensemble learning. Computers & Electrical Engineering. (Blockchain + ML for medical claim fraud).
7. Al-Quayed, M., et al. (2024). Utilizing blockchain and smart contracts for enhanced fraud prevention (survey/preprint). arXiv:2407.17765. (Discusses blockchain + ML for insurance fraud prevention; contextually related).
8. Tawil, A. A., et al. (2024). Comparative analysis of ML algorithms for email phishing detection using TF-IDF, Word2Vec, and BERT. Computers, Materials & Continua. (Broad email-fraud/phishing ML comparison).
9. Singh, A., & co-authors (2025). UPI fraud detection using machine learning. In Proceedings of Smart Innovation, Systems and Technologies (Springer chapter, first online 2025; aligns with UPI ML approaches).

10. Sharan et al. (2024) — IoT-specific insurance claim fraud detection with real-time sensors, anomaly/clustering/bracketing
11. Gudivaka et al. (2024) — "VAEGAN-" + CNN and novel oversampling, accuracy ≈ 99.78%
12. Patel et al. (2024) — SMOTE-Tomek + hyperparameter tuning; XGBoost ≈ 99.95% on mobile financial fraud
13. https://orcid.org/my-orcid?orcid=0000-0002-9764-6048
14. https://scholar.google.com/citations?user=99wmG2IAAAAJ&hl=en
15. Pendalwar et al. (2024) — RF, SVM, NB, KNN, XGBoost, LightGBM; PCA and GANs for balancing
16. Mostafa et al. (2024) — RF vs. GB, NB, LR on credit-card fraud with RF best
17. Bhowte et al. (2024) — exhaustive survey of ML in financial-service fraud
18. https://ieeexplore.ieee.org/author/614775320328834
19. Aldosari (2024) — GRFO + KNN (with SMOTE) ≈ 99.98% and outperforming DCNN/CatBoost
20. Kalaiselvi et al. (2024) — ensemble ML for suspicious email (phishing/spoofing)
21. Vii et al. (2024) — BiGRU + Capsule Network for e-commerce fraud ≈ 95.44%
22. Kour (2024) — ML in finance (fraud, risk, customer service)
23. Agwu, E. (2024). Financial fraud detection using Value-at-Risk with machine learning in skewed data.
24. Ghatee, M. (2025). A distribution-preserving method for resampling combined with LightGBM-LSTM for sequence-wise fraud detection in credit card transactions. Expert Systems with Applications, 262, 125661.
25. Huang, T., Wang, X., Ma, Y., & Chen, Z. (2024). A deep learning method of credit card fraud detection based on continuous-coupled neural network. Mathematics, 13(5), 819.
26. Wu, B., Qi, X., & Chen, Y. (2024). Encoder–decoder graph neural network for credit card fraud detection. Journal of King Saud University – Computer and Information Sciences.
27. Taskiran, A., et al. (2024). Blockchain-assisted healthcare insurance fraud detection framework using ensemble learning. Computers & Electrical Engineering.
28. Al-Quayed, M., et al. (2024). Utilizing blockchain and smart contracts for enhanced fraud prevention. arXiv:2407.17765.
29. Tawil, A. A., et al. (2024). Comparative analysis of ML algorithms for email phishing detection using TF-IDF, Word2Vec, and BERT. Computers, Materials & Continua.
30. Singh, A., & co-authors (2025). UPI fraud detection using machine learning. In Smart Innovation, Systems and Technologies. Springer.