A Systematic Literature Review on Supervised Machine Learning Techniques for Financial Fraud Detection

Blessing Bologi, Ridwan Kolapo, Temitope Olufunmi Atoyebi

Department of Information Technology, Faculty of Computing, Nile University of Nigeria, Abuja, Nigeria.

DOI: https://doi.org/10.51244/IJRSI.2026.1308000143

Received: 23 August 2026; Accepted: 28 August 2026; Published: 10 September 2026

ABSTRACT

Financial transaction fraud is a significant problem in the fields of digital banking, credit card transactions, online payment, and mobile financial services. This study systematically reviewed the existing literature on supervised machine learning techniques used for financial fraud detection. The review included peer-reviewed papers published between 2020 and 2026 and followed the PRISMA framework, with Parsifal used to assist the search management, screening, eligibility assessment, and data extraction. A total of 503 records were obtained from IEEE Xplore, Scopus, Web of Science, ScienceDirect, and ACM Digital Library. After removing 129 duplicates, screening 374 records, and assessing 107 full-text articles, a total of 55 studies were accepted in the final review. The findings indicated that financial fraud detection relied more on supervised learning which was the method of choice, especially in cases where labelled data of fraudulent and legitimate transactions were known. Credit/debit card fraud was the most common form of fraud, contributing to 40 studies (72.7%) of the reviewed literature. Methodologically, ensemble, boosting, and hybrid classifiers were the most common methods, occurring in 17 studies (30.9%), followed by deep/hybrid representation learning in 12 studies (21.8%) and classical supervised machine learning comparisons in 10 studies (18.2%). The review further indicated that the model performance not only depends on the algorithm choice but also on preprocessing, feature selection, class imbalance handling, and evaluation metrics. The most commonly reported metric was accuracy, which occurred in 52 studies (94.5%), whereas recall/sensitivity was present in 50 studies (90.9%), precision was in 48 studies (87.3%), F1-score was in 47 studies (85.5%), ROC-AUC/AUC was in 42 studies (76.4%), and confusion matrix was in 38 studies (69.1%). The study ends by recommending that effective supervised fraud detection is a complete methodological pipeline and not just isolated algorithm comparison.

Keywords: Financial Fraud Detection, Supervised Machine Learning, Systematic Literature Review, PRISMA, Parsifal, Class Imbalance.

INTRODUCTION

Banking and payment services have moved from branch-based and cash-centred transactions to mobile banking applications, online transfers, e-commerce platforms, digital wallets and instant-payment systems. This transition has improved convenience for customers and businesses, but it has also widened the opportunity space for fraud because transactions now occur at high speed, across several channels and with limited physical verification. Fraud in financial transactions is becoming increasingly concerning in rapidly developing and developed economies as fraudsters are continually revising their fraud methods, with financial fraud as an example.

Fraud has evolved into various schemes like stealing card details, phony account takeover, phishing scam, unauthorized transfer, ID theft and online manipulation. As stated by INTERPOL [1], networks that commit financial fraud are becoming increasingly sophisticated, which makes them tough to detect with security measures that were employed in the past. A different report from the Federal Trade Commission (FTC) [2]

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VIII August 2026

also shows that complaints regarding fraud and identity theft associated with financial fraud are still increasing.

For a number of years, fraud detection systems that were rule-based were used by financial institutions. These systems detect fraud using a specific set of instructions. For example, a payment that exceeds a certain limit or one that originates from an unusual place could be marked or blocked. The issue with this is that it will detect fraudulent behaviour by current behaviour. A fraudster can easily change their behaviour so models struggle to find new patterns. Al-Hashedi and Magalingam [3] argue that the traditional rule-based system has a limitation in its static fraud condition.

The rule-based system's inability to detect unknowns means it won't be able to tackle new frauds or complex frauds that are dynamic [3]. For this reason, the system will not be able to operate effectively against the new methods to commit fraud. As the difficulties turned to be clearer, the scholars had to make more efforts towards the investigation of machine learning for fraud detection. On the opposite side of rule-based systems, machine learning models can store transaction histories data, then find similarities between those and new ones, in order to make the latter analysis. In the context of fraud detection research, supervised learning has renewed its attention because it relies on datasets containing legitimate and fraud data that has been labelled by outside sources.

The most recent examinations of supervised learning for fraud detection revealed the employment of several algorithms such as Logistic Regression, Random Forest, Decision Tree, Support Vector Machine, XGBoost, and Artificial Neural Networks [4]. Additionally, problems of feature engineering, sampling methods, class imbalance handling, and evaluation metrics were also considered by researchers who aimed at improving the performance of the fraud detection system. In fact, despite the considerable amount of attention given to fraud detection, there is a lack of consensus in the literature. In particular, examples of recent studies that assert ensemble and boosting techniques perform excellently are used, while other concerns raise questions if traditional supervised classifiers could be of the same form depending on datasets' attributes and preprocessing strategies [5].

Imbalanced classification is an essential concern in the area of financial fraud detection, where the number of fraudulent transactions (the minor class) is far lower than the genuine ones (the majority class), usually spent less than 0.5% to 1% of data. As stated by Baesens et al. [6], this difference leads the machine learning methods to prioritize the general accuracy by defaulting into predicting the majority class and hence, totally disinterested the minor class the frauds. The move to intricate, advanced fraud detection systems, indicates a watershed from traditional measures. Hybrid, deep learning, and ensemble methods while they certainly guarantee far more prevision figures of fraudulent identifiers also admit visible and operational burdens & regulatory constraints [7].

A systematic review is therefore needed to examine recent peer-reviewed studies, identify the supervised learning algorithms used, compare methodological trends, examine imbalance-handling approaches, evaluate the metrics used and clarify the remaining gaps. The review approach is appropriate because it allows evidence to be selected, screened and synthesized transparently rather than relying on isolated examples.

The aim of the study is to conduct a systematic literature review on supervised machine learning techniques for financial fraud detection.

The objectives of the Study are to:

1. Classify supervised machine learning techniques used in financial transaction fraud detection studies.

2. Compare commonly used classification algorithms in fraud detection research.

3. Evaluate the performance metrics applied in the evaluation of supervised fraud detection models.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VIII August 2026

LITERATURE REVIEW

The chapter provides an overview of both theoretical and empirical literature on the application of supervised machine learning in detecting financial transaction fraud. The broader review reveals that the supervised classification approach continues to be one of the most preferred techniques particularly in cases of the availability of labeled transaction data. Though credit card fraud is the most frequently reported form of digital fraud, the review also acknowledges online payment, mobile payment, banking transaction, and broader financial fraud studies among the contributors to the literature on the 55 peer-reviewed studies included in the study. The algorithms that were mainly identified are Logistic Regression, Decision Tree, Random Forest, Support Vector Machine, Naive Bayes, XGBoost, LightGBM, CatBoost, Artificial Neural Networks, CNN, LSTM, autoencoder-based classifiers, graph neural networks, and stacking ensembles. This finding aligns with the research of [8], [9], [10], [11], and [12].

The review provides evidence that the mere choice of algorithm does not dictate the performance of fraud detection. Preprocessing, feature selection, feature engineering, sampling, and model validation are equally as important as they shape up the information that is accessible to the classifier and the way rare fraud cases are learned. Reports including but not limited to [13], [14], [15], [16], [17], [18], [19] acknowledge that features and data representation might change substantially the outcomes entailed by the model. This suggests that the paired supervision in a fraud detection model should be seen as a full pipeline instead of merely one classifier that is picked out independently of the data-preparation process.

Class imbalance has emerged as the most enduring methodological issue reported in the literature. The transactions that are fraudulent are really scarce, so models get better in their learning of legit classes rather than the fraud class. The studies explored have employed various means such as SMOTE, ADASYN, undersampling, oversampling, SMOTE-ENN, K-SMOTEENN, hybrid sampling, generative modelling, and threshold optimization to minority class detection yet it is not clear which works best because the suitable method depends on the dataset, feature space, classifier, as well as the business cost of false positives and false negatives. The study elucidating this may be found in the works of [6], [16], [19], [21], and [22].

Additionally, the review emphasizes that the evaluation of the model must be sensitive to fraud. Sole reliance on accuracy is not enough as it may conceal poor detection of the minority class, especially when the dataset is dominated by the legitimate class. Recall, precision, F1-score, ROC-AUC, PR-AUC, confusion matrices, MCC, G-Mean, and cost-based measures are more reliable for gauging the performance of fraud detection. The risk feature is thus of significance as it brings together model outputs and the consequence they cause even such as financial loss, customer disruption, and investigation cost. The viewpoint of [23], [24] and [25] thus highlights this interpretation of evaluation in the realm of financial fraud detection.

METHODOLOGY

Research Design

This chapter aims to describe the ways to carry out a thorough literature evaluation on the supervised machine learning techniques for financial transaction fraud. The literature review was conducted with the goal of finding, sorting, evaluating, and summarizing recent publications from the years 2020-2026. Evidence synthesis and literature selection are the main attention areas, rather than model development in this methodology. The review followed the PRISMA reporting structure and used Parsifal as a review management tool. PRISMA provided the structure for documenting the flow of records from identification to inclusion, while Parsifal helped with protocol development, search organization, screening decisions, and extraction planning. Together, PRISMA and Parsifal helped organise and manage the review process.

With the help of five academic databases, a total of 503 records were obtained. After manually excluding the 129 duplicate records, a total of 374 records were screened by title and abstract. Out of these, 251 records were excluded as they were not in line with the review objectives. A total of 123 reports were requested to be retrieved with 16 of them unavailable for download. Therefore, 107 full-text reports were assessed for

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VIII August 2026

eligibility. At the full-text stage, 52 reports were excluded for clearly documented reasons. The final evidence base consisted of 55 peer-reviewed studies published between 2020 and 2026.

Source and Method of Search

Boolean operators were used to create search strings in Parsifal, which were then tested on a variety of scholarly databases:

IEEE Xplore, Scopus, Web of science, ScienceDirect, ACM Digital Library.

The analysis only included English publications from 2020 to 2026.

"Machine learning" OR "supervised learning" OR "classification algorithm" AND "fraud detection" OR "fraud prediction" AND "financial transaction fraud" OR "credit card fraud" OR "online payment fraud" OR "digital banking fraud" OR "mobile payment fraud" were the main search terms used. "Credit card fraud detection" AND "machine learning" AND "supervised learning"; "financial fraud detection" AND "classification algorithms"; "online payment fraud" AND "machine learning"; and "fraud detection" AND ("Random Forest" OR "Logistic Regression" OR "Decision Tree" OR "Support Vector Machine" OR "XGBoost") were additional strings.

Inclusion and Exclusion Criteria

Before the screening process started, the inclusion and exclusion criteria were decided. This was done to prevent the review from straying into works that addressed fraud in more general legal, theoretical, or non-computational contexts and instead staying focused on supervised learning approaches for financial transaction fraud detection.

Inclusion Criteria

1. Published between 2020 to 2026
2. Peer-reviewed papers, conference papers, government publication, or systematic review.
3. Focused on Financial transaction fraud detection, including areas such as credit/debit card fraud, online payment fraud, mobile banking fraud or e-commerce transaction fraud.
4. Studies focused on supervised or classification-based fraud detection by the use, comparison, or systematic review of machine learning techniques.
5. Studies with algorithms including Logistic Regression, Decision Tree, Random Forest, SVM, Naive Bayes, XGBoost, LightGBM, CatBoost, ANN, or ensemble classifiers.
6. Only English language studies with full texts that could be accessed were selected.

Exclusion Criteria

1. Duplicates
2. Irrelevant to the search question
3. Not related to financial transaction fraud detection
4. Published outside 2020 to 2026 reviewed period
5. Any paper that lacked categorisation strategies, supervised learning methodologies, or pertinent supervised-learning review discussions.
6. Studies with ambiguous methodology, inadequate dataset descriptions, or missing performance results.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VIII August 2026

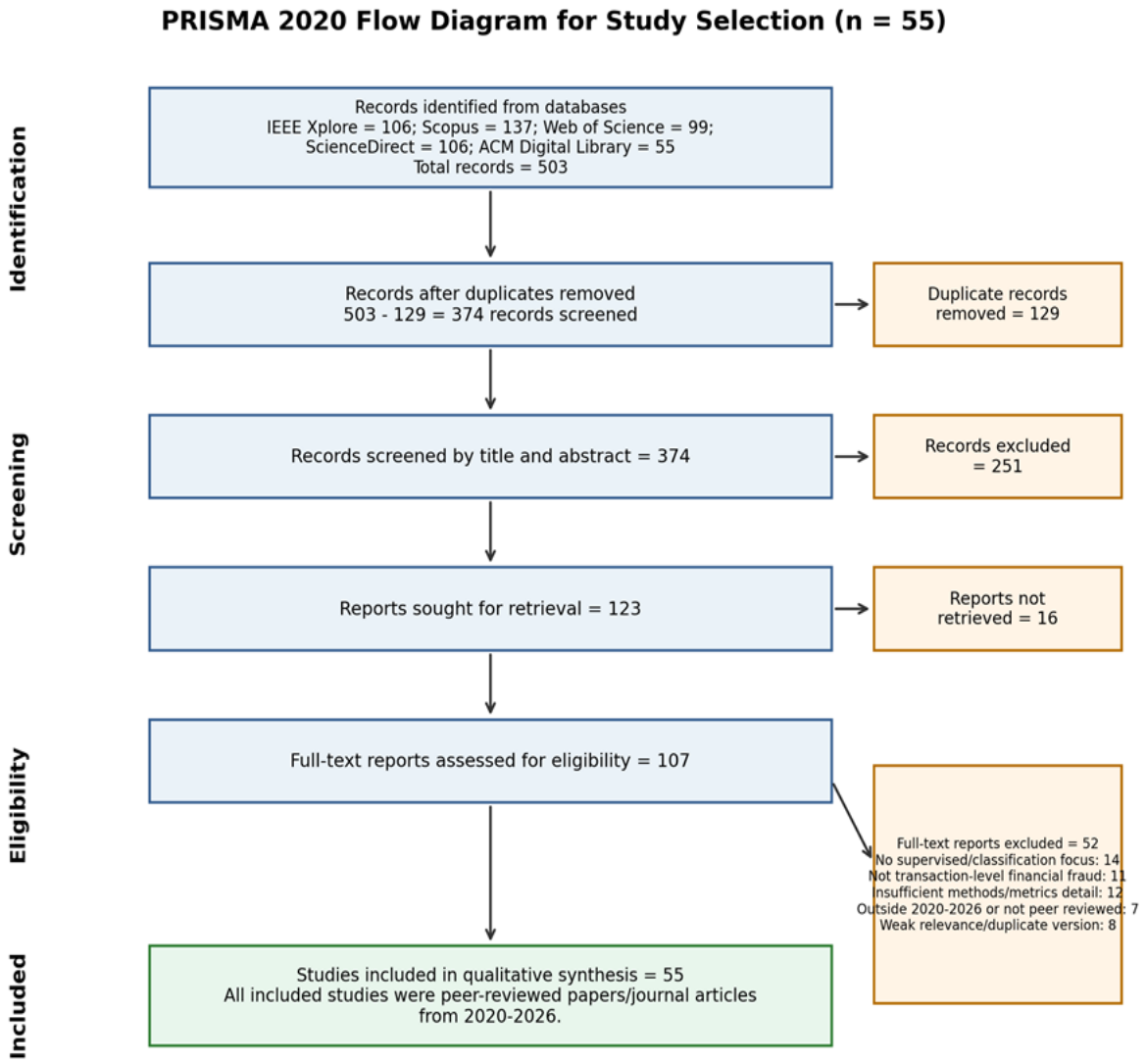

Figure 1: PRISMA flow diagram for study selection

RESULTS AND DISCUSSIONS

Descriptive Characteristics of the Included Studies

The highest number of reviewed studies were published between 2023 and 2025, accounting for 36 out of the 55 selected studies. The escalation of articles indicates a heightened focus on newer fraud detection methodologies and the essential requirement of addressing the problems brought about by the growth of digital finance platforms.

Fraud Domains Covered by the Reviewed Studies

The reviewed studies did not show a balanced examination of all financial fraud domains. Credit and debit card fraud emerged as the prominent area, constituting 40 of the 55 studies that were picked. Online and mobile payment fraud comprised five studies, banking or wider transaction fraud, four, and general financial fraud frameworks or review-based analyses were the topic of six studies. The distribution of these figures is a clear assertion that the base of the evidence is the strongest in card-related fraud, primarily due to the fact that credit card datasets are more readily available for academic research purposes and are more appropriate for supervised classification experiments. However, the fact that the studies also included online payment, mobile banking, and broader transaction fraud reiterates the increasing trend of machine learning-based fraud detection research in moving from the traditional card fraud context to digital financial systems overall.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VIII August 2026

Table 1: Distribution of Included Studies by Fraud Domain

Fraud Domain	Number of Studies	Percentage of 55 Studies
Credit/debit card fraud	40	72.70%
Online/mobile payment fraud	5	9.10%
Banking/financial transaction fraud	4	7.30%
Broad financial fraud/review	6	10.90%
Total	55	100%

Findings Based on the Research Questions

The extracted evidence shows that supervised machine learning was mainly used as a labelled classification approach. Most studies represented transactions as legitimate or fraudulent and trained models to distinguish between the two classes. This pattern appeared across classical supervised learning, ensemble models, boosting methods, deep learning models and graph-based approaches. Across the 55 studies, supervised learning was usually embedded in a wider fraud-detection pipeline involving preprocessing, feature selection or representation learning, class-imbalance handling, model training and performance evaluation.

The result for RQ1 is that supervised fraud detection is not reported in the literature as a single modelling step. It is better understood as a pipeline in which the dataset, features, class distribution and evaluation metrics influence the reported performance of the classifier.

The reviewed studies used a wide range of supervised and classification-based methods. These were grouped into six methodological categories: ensemble/boosting/hybrid classifiers, deep/hybrid representation learning, classical supervised machine learning comparison, class imbalance and feature engineering, graph/network/relational learning, and systematic review/framework papers.

The largest methodological group was ensemble, boosting and hybrid classifiers. This indicates that recent fraud-detection research increasingly favours methods that can handle nonlinear transaction behaviour and imbalanced data. The second-largest community consisted of deep and hybrid representation learning, whereas the classical supervised machine learning remained a significant part as a baseline and comparison category.

The outcome for RQ3 is that there isn't a single algorithmic family that is the sole master of the entire evidence base. Traditional algorithms continue to be practical, however, the recent trend in investigations is the transition towards ensembles, boosting, hybrid learning, representation learning, and graph-based techniques.

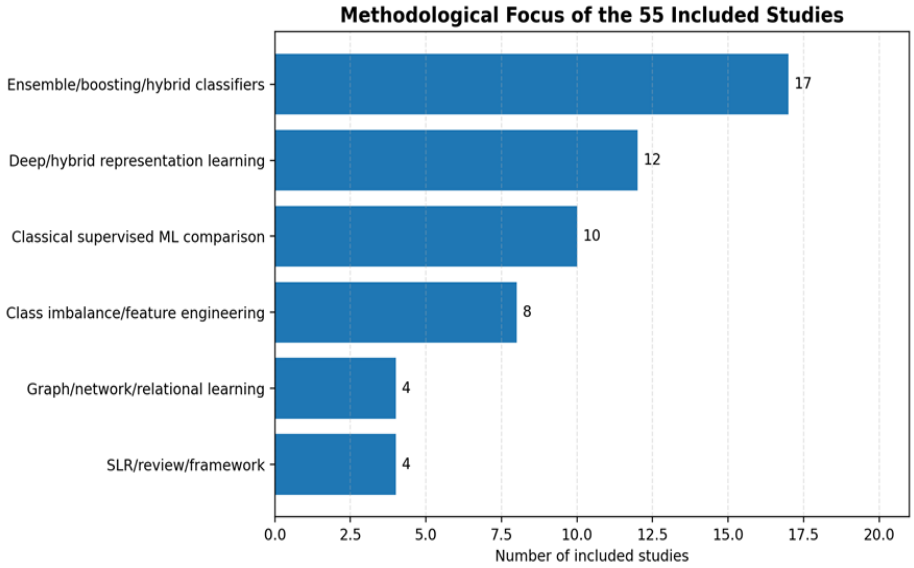

Figure 2: Methodological Focus of the 55 Included Studies

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VIII August 2026

Preprocessing, Feature Selection and Class-Imbalance Handling

The analyzed research articles reveal that the repeating methodological elements were preprocessing, feature selection and class-imbalance handling. These techniques were revisited more than once since transaction-fraud datasets are predominantly imbalanced and often high-dimensional, anonymised or redundant factors.

Supervised fraud detection studies have been found to increasingly view data preparation as a component of model design. The technical steps of sampling, feature selection, feature extraction, and threshold tuning that they not minor; they had direct effects on the ability of the models to detect minor fraud cases.

Evaluation Metrics

The final research question examined the evaluation metrics reported across the 55 included studies. Accuracy was the most commonly reported metric, but recall, precision, F1-score, ROC-AUC and confusion matrix were also frequently reported.

The result shows that evaluation practice is improving but remains uneven. Accuracy is still highly visible, while fraud-sensitive metrics such as recall, precision and F1-score are also widely reported. More specialized metrics such as PR-AUC, MCC, G-Mean and cost-based measures appeared less frequently, even though they are useful for rare-event fraud detection. This pattern is consistent with the concerns raised in recent fraud-detection studies that model evaluation should go beyond headline accuracy.

Table 2: Evaluation Metrics Reported Across Included Studies

Evaluation metric	Number of studies reporting metric	Percentage of 55 studies
Accuracy	52	94.50%
Recall/Sensitivity	50	90.90%
Precision	48	87.30%
F1-score	47	85.50%
ROC-AUC/AUC	42	76.40%
Confusion matrix	38	69.10%
PR-AUC/MCC/G-Mean/cost-based metrics	18	32.70%

Note: Counts are multiple-response because a single study may report more than one metric.

Thematic Synthesis of the Findings

The thematic synthesis of the 55 included studies produced six major findings. First, supervised classification remains central because many fraud detection studies use labelled transaction outcomes. Second, ensemble, boosting and hybrid methods are strongly represented in recent studies. Third, class imbalance remains one of the most persistent methodological concerns. Fourthly, the selection of features, the development of features, and the learning of representations are crucial in dictating the quality of inputs to models. Fifthly, the practice of evaluation is dynamically shifting from a mere reporting of accuracy towards metrics like recall, precision, F1-score, ROC-AUC, confusion matrices, and cost-aware interpretation. Sixthly, the deployment of sophisticated models brings about practical issues like the need for explainability, the problem of scalability, privacy, deployment, and concept drift.

The synthesis's main output is that supervised financial fraud detection is best viewed as a comprehensive evidence pipeline instead of an isolated algorithm conflict. The studies examined indicate not only that algorithm selection is essential but also that it must be together with data quality, feature representation, imbalance handling, validation design, and evaluation metrics to be meaningful. Therefore, compared with a direct model ranking, the theme-based presentation of results is more appropriate.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VIII August 2026

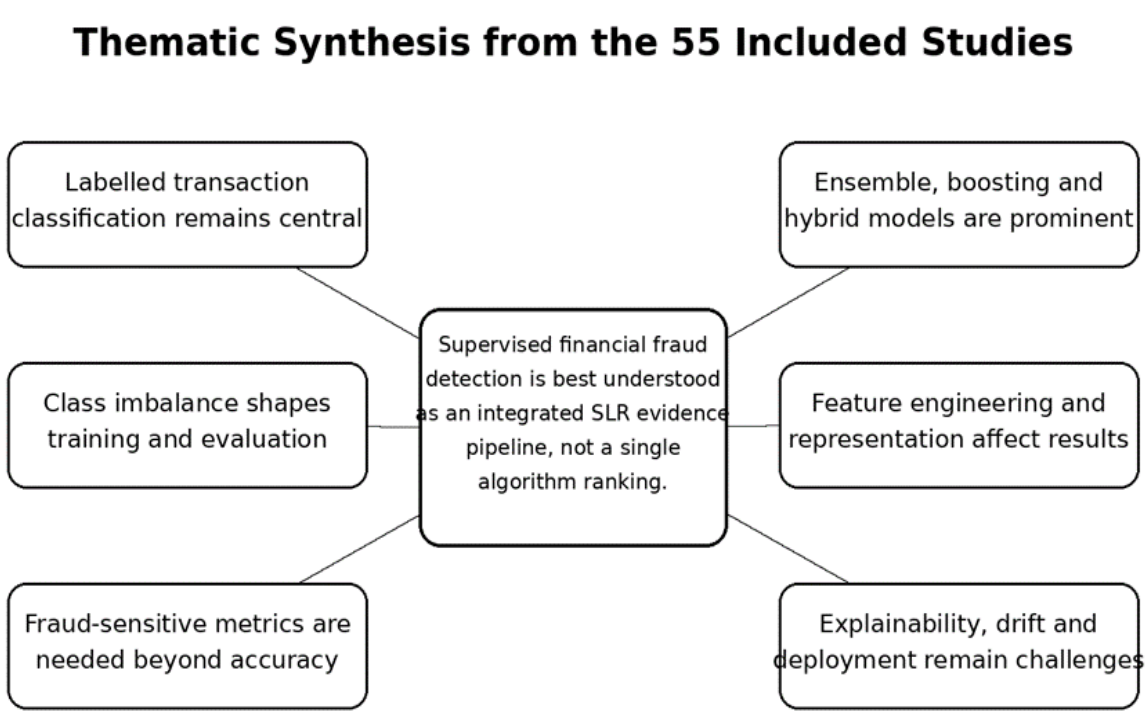

Figure 3: Thematic synthesis of findings from the 55 included studies.

CONCLUSION

This study was a systematic assessment of 55 peer-reviewed studies which employed the supervised machine learning techniques for the financial fraud detection within the time frame of 2020 to 2026. In the process of the review, it was seen that because of the characteristic of many fraud problems to be represented as labelled classification tasks, supervised learning is still the dominant technique in transaction fraud detection. However, the research also proved that the choices of algorithm is only a part of the issue in regard to the performance of supervised fraud detection.

In summary, the effective application of supervised fraud detection is dependent on the adoption of the complete methodological pipeline from the reliable labelled data, preprocessing, feature selection or representation learning, class-imbalance handling, supervised model training, fraud-sensitive evaluation to the continuous monitoring. Classical supervised models as an interpretable baseline continue to be useful whereas the ensemble, boosting, deep and graph-based models are the tools for the advanced transaction patterns that they give. The additional benefits from more complex models are off-set by the new concerns that come with the issues of explainability, computation, scalability and deployment.

The review additionally mentions that accuracy does not suffice as the only criterion of the fraud detection model's performance. Given that fraud datasets are largely imbalanced, the suitable metrics for the evaluation should be recall, precision, F1-score, ROC-AUC, PR-AUC, confusion matrix and cost-aware measures. The metrics outlined give more head-up to the model capability in case of fraud situations that are rare in character without too many false alerts.

Broadly speaking, the study has made its contribution to the field of supervised financial fraud detection by restructuring available evidence, mapping methodological patterns, marking observed gaps as well as offering a structured optimal framework for future studies. The result of this study implies that the future of supervised fraud detection would be realised not through the selection of the most complex model but through the design of transparent, balanced, risk-aware and adaptable systems which would enable reliable fraud decision making in a volatile financial environment.

REFERENCES

1. International Criminal Police Organization. (2026, March 16). INTERPOL report warns of increasingly sophisticated global financial fraud threat. INTERPOL. https://www.interpol.int/en/News-and-Events/News/2026/INTERPOL-report-warns-of-increasingly-sophisticated-global-financial-fraud-threat
2. Federal Trade Commission. (2025). Consumer Sentinel Network data book 2024. Author. https://www.ftc.gov/system/files/ftc_gov/pdf/csn-annual-data-book-2024.pdf
3. Al-Hashedi, K. G., & Magalingam, P. (2021). Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019. Computer Science Review, 40, 100402. https://doi.org/10.1016/j.cosrev.2021.100402
4. Afriyie, J. K., Tawiah, K., Pels, W. A., Addai-Henne, S., Dwamena, H. A., Owiredu, E. O., Ayeh, S. A., & Eshun, J. (2023). A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions. Decision Analytics Journal, 6, 100163. https://doi.org/10.1016/j.dajour.2023.100163
5. Hafez, I. Y., Hafez, A. Y., Saleh, A., Abd El-Mageed, A. A., & Abohany, A. A. (2025). A systematic review of AI-enhanced techniques in credit card fraud detection. Journal of Big Data, 12, 6. https://doi.org/10.1186/s40537-024-01048-8
6. Baesens, B., Höppner, S., & Verdonck, T. (2021). Data engineering for fraud detection. Decision Support Systems, 150, 113492. https://doi.org/10.1016/j.dss.2021.113492
7. Chen, Y., Zhao, C., Xu, Y., Nie, C., & Zhang, Y. (2025). Deep learning in financial fraud detection: Innovations, challenges, and applications. Data Science and Management. Advance online publication. https://doi.org/10.1016/j.dsm.2025.08.002
8. Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., Elhassan, T., Elshafie, H., & Almogren, A. (2022). Financial fraud detection based on machine learning: A systematic literature review. Applied Sciences, 12(19), 9637. https://doi.org/10.3390/app12199637
9. Cherif, A., Badhib, A., Ammar, H., Alshehri, S., Kalkatawi, M., & 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), 145–174. https://doi.org/10.1016/j.jksuci.2022.11.008
10. Aros, L. H., Bustamante Molano, L. X., Gutierrez-Portela, F., Moreno Hernandez, J. J., & Rodriguez Barrero, M. S. (2024). Financial fraud detection through the application of machine learning techniques: A literature review. Humanities and Social Sciences Communications, 11, 1130. https://doi.org/10.1057/s41599-024-03606-0
11. Thivaios, S., Kostopoulos, G., Stefani, A., & Kotsiantis, S. (2026). A survey of machine learning and deep learning for financial fraud detection: Architectures, data modalities, and real-world deployment challenges. Algorithms, 19(5), 354. https://doi.org/10.3390/a19050354
12. Ileberi, E., Sun, Y., & Wang, Z. (2022). A machine learning based credit card fraud detection using the GA algorithm for feature selection. Journal of Big Data, 9, 24. https://doi.org/10.1186/s40537-022-00573-8
13. Ghosh Dastidar, K., Jurgovsky, J., Siblini, W., & Granitzer, M. (2022). NAG: Neural feature aggregation framework for credit card fraud detection. Knowledge and Information Systems, 64, 831–858. https://doi.org/10.1007/s10115-022-01653-0
14. Du, H., Lv, L., Guo, A., & Wang, H. (2023). AutoEncoder and LightGBM for credit card fraud detection problems. Symmetry, 15(4), 870. https://doi.org/10.3390/sym15040870
15. Van Belle, R., Baesens, B., & De Weerdt, J. (2023). CATCHM: A novel network-based credit card fraud detection method using node representation learning. Decision Support Systems, 164, 113866. https://doi.org/10.1016/j.dss.2022.113866
16. Salekshahrezaee, Z., Leevy, J. L., & Khoshgoftaar, T. M. (2023). The effect of feature extraction and data sampling on credit card fraud detection. Journal of Big Data, 10, 6. https://doi.org/10.1186/s40537-023-00684-w
17. Siam, A. M., Bhowmik, P., & Uddin, M. P. (2025). Hybrid feature selection framework for enhanced credit card fraud detection using machine learning models. PLOS ONE, 20(7), e0326975. https://doi.org/10.1371/journal.pone.0326975

18. Gupta, R. K., Hassan, A., Majhi, S. K., Parveen, N., Zamani, A. T., Anitha, R., Ojha, B., Singh, A. K., & Muduli, D. (2025). Enhanced framework for credit card fraud detection using robust feature selection and a stacking ensemble model approach. Results in Engineering, 26, 105084.
19. https://doi.org/10.1016/j.rineng.2025.105084
20. George, R., & Roy, B. (2022). Handling class imbalance in fraud detection using machine learning techniques. In A. Kumar, S. Senatore, & V. K. Gunjan (Eds.), ICDSMLA 2020: Lecture Notes in Electrical Engineering (Vol. 783, pp. 803–813). Springer. https://doi.org/10.1007/978-981-16-3690-574
21. Ileberi, E., & Sun, Y. (2024). Advancing model performance with ADASYN and recurrent feature elimination and cross-validation in ML-assisted credit card fraud detection: A comparative analysis. IEEE Access, 12, 133315-133327. https://doi.org/10.1109/ACCESS.2024.3457922
22. Albalawi, T., & Dardouri, S. (2025). Enhancing credit card fraud detection using traditional and deep learning models with class imbalance mitigation. Frontiers in Artificial Intelligence, 8, 1643292. https://doi.org/10.3389/frai.2025.1643292
23. Damanik, I. S., & Liu, Y. (2025). Advanced fraud detection: Leveraging K-SMOTEENN and stacking ensembles to tackle data imbalance and extract insights. IEEE Access, 13, 10356-10370. https://doi.org/10.1109/ACCESS.2025.3528079
24. Vanini, P., Rossi, S., Zvizdic, E., & Domenig, T. (2023). Online payment fraud: From anomaly detection to risk management. Financial Innovation, 9, 66. https://doi.org/10.1186/s40854-023-00470-w
25. Baisholan, N., Dietz, J. E., Gnatyuk, S., Turdalyuly, M., Matson, E. T., & Baisholanova, K. (2025). FraudX AI: An interpretable machine learning framework for credit card fraud detection on imbalanced datasets. Computers, 14(4), 120. https://doi.org/10.3390/computers14040120
26. Awad, S. S., Hamza, A. A., Sobh, M. A., & Bahaa-Eldin, A. M. (2026). Applying explainable artificial intelligence to interpret supervised ensemble learning models for robust credit card fraud detection. Scientific Reports, 16, 15220. https://doi.org/10.1038/s41598-026-49939-5