iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

ADAPTIVE FRAUD DETECTION IN FINANCIAL ECOSYSTEMS

Firdous Sadaf Mohammad Ismail
Symbiosis Institute of Technology, Nagpur Campus,
Symbiosis International (Deemed University), Pune, India
firdoussadaf2810@gmail.com

Amit Kumar
Symbiosis Institute of Technology, Nagpur Campus,
Symbiosis International (Deemed University), Pune, India
amit.kumar@gmail.com

ABSTRACT
Fraud in the financial sector is one of the most serious problems in the digital world, which has been evolving and spreading fast. Globally, financial fraud has become a million-dollar issue with an estimated rate of the losses caused by it to the tune of 5 % of the annual revenue of the entire market. The use of rule-based systems with fixed thresholds or historical patterns for fraud detection is no longer effective since fraudsters spread out their activities to new channels, create synthetic identities and hide in large volumes of transactions. Adaptive fraud systems depend on Machine Learning, graph analytics, federated learning, and real-time feedback to be able to identify threats that are coming. This article talks about the change of the adaptive model concept, research, and the case studies of the residential financial ecosystems. Besides that, the paper touches the quite controversial issues that arise when the AI-powered fraud detection approach is used, like bias, fairness, privacy, and transparency, and gives some good practice guidelines for responsible AI. Throughout the paper, a humanized, professional tone is maintained.

Keywords:
Artificial Intelligence, Finance, ML, Graph Analytics

I. INTRODUCTION

- **The changing fraud landscape**

On the one hand, digital transformation has made financial services more accessible to the general public, but on the other hand, it has expanded the attack surface. E-commerce will contribute to almost a quarter of world retail sales by 2027. However, a survey shows that 42 % of organizations think that they have become more susceptible to online fraud because of this transition, and 66 % of consumers say that they will change their provider after a fraud incident. According to the Association of Certified Fraud Examiners (ACFE), fraud is the cause of about 5 % of an organization's annual revenue and more than US $5.6 trillion worldwide. The 2024 AFP Payments Fraud Survey revealed that in 2023, 80 % of organizations had experienced or attempted payment fraud, which is the highest rate since 2018.

Fraudsters are not holding back as they are now harnessing deep learning models, creating synthetic identities, and using social engineering. Traditional rule-based systems become quickly outdated since they are unable to adjust to the rapidly changing vectors of attacks. Machine learning models can potentially lead to better detection; however, if training is static, then it leads to the concept drift, low recall, and high false-positive rates. Adaptive ML systems, i.e., models that are continuously learning from new data, are gaining popularity as the first line of defense in modern financial ecosystems. These models are equipped with streaming analytics, iterative learning, and feedback mechanisms to adjust decision boundaries as fraud patterns evolve.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

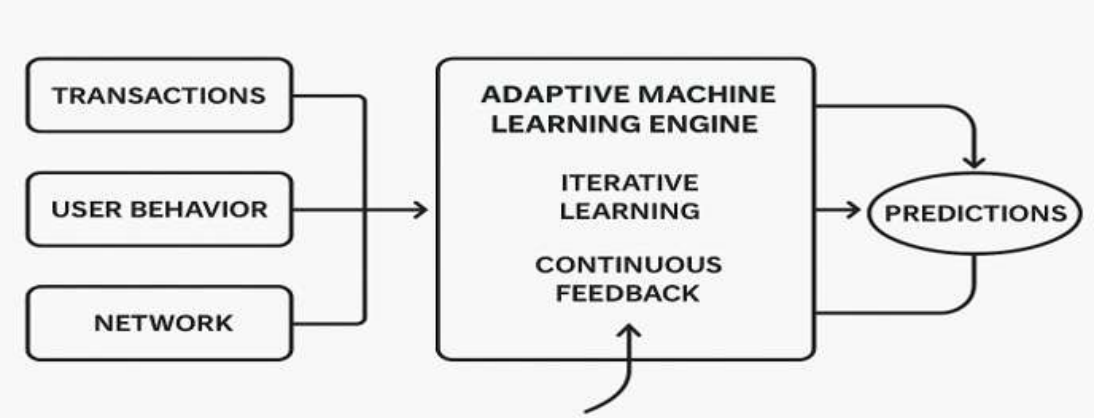

Figure 1 delineates an exemplary adaptive fraud-detection pipeline. Feature extraction is powered by transaction data, user-behavior signals, and network relationships. An adaptive Machine Learning engine employs iterative learning and perpetual feedback to create fraud predictions. Model updates through the feedback loop (e.g., analyst reviews, confirmed fraud cases, customer disputes) allow the system proficiency in detecting new fraud tactics.

- **Adaptive fraud-detection pipeline**

Scope and contributions

The article consolidates current literature on adaptive fraud detection, reviews studies on adaptation models, and presents ethical and regulatory considerations together with the case studies of financial institutions deploying cutting-edge AI. The paper ends with recommendations for practitioners and points to future research directions.

Almarshad et al. (2025) introduced the Risk-Adaptive Bayesian Ensemble Model (RABEM) to elevate fraud detection over vast transactional data. RABEM incorporates feature engineering based on the Black–Scholes method, a hybrid variational auto-encoder (VAE), Nyström-approximation Gaussian processes, random-projection trees, and gated recurrent units integrated with Bayesian reliability fusion. The model reached an accuracy of 99.38 % with a Matthews correlation coefficient of 0.9788 and a low Brier score using the PaySim dataset with 6 million transactions and synthetic financial datasets. The authors pointed out that the conventional fraud detection has difficulties with highly imbalanced datasets; hence, the ensemble approach of RABEM and probabilistic estimates are a solution to uncertainty and changing risk levels. They also maintained that adaptive models should be designed in a way that accommodates class imbalance, captures temporal dynamics, and provides risk-adjusted predictions.

Moreover, the paper points out that Paysim and Synthetic Financial Datasets for Fraud Detection from Kaggle are very good benchmark datasets. The Paysim dataset is a simulation of mobile payment transactions, and it has more than 6 million records, whereas the Synthetic Financial Datasets have more than 100 million transactions, with a fraud rate of around 0.5 %. These datasets allow developers to test adaptive models in situations of class-imbalance and noise.

Adaptive graph neural networks and federated learning

Rahmati (2025) introduced a fraud real-time detection framework which uses adaptive Graph Neural Networks (GNNs) and Federated Learning (FL). GNNs can represent dynamically the interconnections between transactions, accounts, and entities, about which the system can later find out suspicious patterns. With Federated Learning multiple financial institutions can train a common model without the need to exchange the sensitive customer data; thus, privacy concerns and regulatory constraints are resolved. The proposed system uses Explainable AI (XAI) techniques to render the solution transparent. The results of tests with benchmark datasets and real-world transactions demonstrate the correctness of the proposed method as it allows 15-30 % improvement in detection accuracy with the reduction of false positives as compared with the conventional machine learning systems.

Adaptive machine-learning models and self-healing systems

Bello et al. (2024) have studied real-time adaptive machine-learning models as a solution to fraud prevention. They admitted that fraud schemes are raising very fast, and models that are not constantly updated are often left behind.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

Adaptive ML models use reinforcement learning, online learning, and deep learning techniques in this way they can always have the correct parameter values. Reinforcement learning is able to optimize the detection strategies by getting the feedback actions, on the other hand, online learning increments the model as new samples of data come in. Adaptive models have the capability to handle the huge amount of data in real time, find the very weak examples of the anomaly and discover the previously unknown fraud patterns. The paper calls the focus on the Explainable AI (XAI) integration to be transparent and conform with regulatory requirements.

Owen (2023) conducted a study on self-healing adaptive ML models capable of anomaly detection and error correction without human intervention. Such models are in continuous learning from new data, they are responsive to fraud tactic evolutions and their detection accuracy is constantly improving. Self-healing components can locate anomalies, execute corrective actions and upgrade performance without human interaction. The paper suggests that combining self-healing features with adaptive ML creates a strong framework that is able to keep its level of performance in the case of data quality problems and newly emerging threats.

Adaptive Voted Perceptron (VP) model

Binsawad (2025) incorporated an adaptive Voted Perceptron (VP) model in fraud detection. The model disclosed its decision boundaries by account of misclassified instances in an iterative manner. This adaptive learning method detection accuracy enhances compared to the traditional models and also solves issues like class imbalance and overfitting. The paper also compares the performance of different models such as naïve Bayes (NB), k-nearest neighbors (KNN), decision trees and rule-based methods. The results demonstrate that the recall of adaptive models and the rate of false positive is much better than those of static models. Through the VP method, the iterative changes of the weights bring the model to generalize more to intricate fraud patterns, and the paper highlights the importance of going beyond mere accuracy metrics to, for instance, recall and true positive rate.

Data sources and comparative studies

The MDPI article points out that supervised Machine Learning models such as logistic regression, SVM, KNN, naïve Bayes, and decision trees can achieve good accuracy on particular datasets but often face problems of class imbalance and concept drift. The use of ensemble methods (bagging, boosting) can lead to better results but requires careful tuning. The comparative research of Tiwari and Naik suggest that artificial neural networks and boosted models are better performers than simple classifiers. The results found here provide the impetus for using adaptive ensembles like RABEM.

Summary table: adaptive techniques

Technique	Key idea	Advantages/notes
Risk-Adaptive Bayesian Ensemble Model (RABEM)	Combines feature engineering, hybrid VAE, Gaussian processes, random-projection trees and GRU with Bayesian reliability fusion	High accuracy (99.38 %) and strong MCC; handles class imbalance; risk-adjusted predictions
Adaptive Graph Neural Networks & Federated Learning	GNNs model relationships; federated learning enables multi-institution training without sharing data	Improves detection by 15–30 %; reduces false positives; preserves privacy; integrates XAI
Adaptive Voted Perceptron (VP)	Iteratively updates decision boundaries based on misclassifications	Addresses class imbalance and overfitting; better recall and reduced false positives
Self-healing adaptive ML models	Continuously learn and autonomously correct errors	Robust to data quality issues; resilient to evolving fraud patterns; requires integration with adaptive learning
Reinforcement/online learning & adaptive ML	Models update parameters as new data arrives and optimize strategies via feedback	Real-time processing; detects novel patterns; integration with XAI improves transparency

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

CASE STUDIES

Graph-based ML at JPMorgan Chase (USA)

An AI white paper in financial ecosystems portrays the use of graph-based machine learning by JPMorgan Chase to counter the increasing cybercrime. The bank planned to lower false-positive fraud alerts and enhance real-time response rates.

Background:

The problem of cybercrime was getting worse, and high false-positive rates were the result of manual review.

Solution:

Graph-based ML models that analyze transaction networks to spot irregularities at the level of a few milliseconds were put in place by JPMorgan. The behavioral biometrics component of the system also integrated—keystroke dynamics and mouse movements—to help detect user behavior that is highly unusual.

Impact:

With this approach, false-positive alerts were reduced by 30 % and over US $150 million in attempted fraud was stopped during the first year.

Hence, Adaptive graph-based models with behavioral biometrics is an efficient way not only to bring the precision of the tasks to the limit but also to cut down the costs drastically.

Federated GNNs and explainable AI in real-time detection

The earlier discussed IJMADA framework was put through the paces using financial datasets, and the results were convincing that adaptive GNNs with federated learning led to a 15–30 % increase in fraud detection accuracy and cut down false positives. The system goes through the training cycles with different institutions, yet there is no data exchange, thus, inter-institution collaboration is made possible, at the same time, privacy is kept. To make the solution transparent to the regulator, the system implements Explainable AI. Such cross-institution models are a solution to the regulatory challenges and data silos in worldwide financial ecosystems.

Liv. Digital Bank (UAE)

Liv., a digital banking entity of the UAE, was faced with customer onboarding jam; manual KYC and approval were the processes that made account activation slow. An Agentic AI onboarding agent was deployed by the bank that extracted data from passports and IDs, carried out AML and sanctions checks, approved low-risk applicants automatically, and initiated card issuing and app activation. The main achievement was the onboarding time reduction from 48 hours to less than 10 minutes, and the account activation rate rose by 35 %. Even though the case is focused on onboarding rather than transaction fraud, it is a clear demonstration of how autonomous agents and layered AI can foster compliance and diminish fraud risk in the stage of account opening.

UBS Client Advisory (Europe)

The same white paper argues that UBS has taken a Generative AI system onboard to create personalized portfolio review reports. Previously Relationship managers spent time and effort on preparing reports; however, the AI solution did the job of generating tailored summaries and incorporated human-in-the-loop validation for compliance. The time spent on preparation was reduced from 3 hours to 15 minutes, and the follow-up meetings were increased by 22 %. Although these are not directly fraud cases, the examples serve to show productivity enhancements, and the human oversight mechanisms needed for responsible AI implementation.

EMERGING USE CASES AND INDUSTRY STATISTICS

An industry blog in 2025 points out that the credit card fraud losses are expected to hit US $43 billion by 2026 and that the spending on fraud prevention solutions may reach US $32.2 billion by 2029. Some of the frequently occurring use cases are the following: e-commerce transaction fraud, money laundering for the purpose of the fraud, manipulating insurance claims, cheating in loan applications, and Buy-Now-Pay-Later (BNPL) fraud. PayPal points out that the Machine Learning models have the ability to scrutinize gigantic volumes of transaction data in a matter of milliseconds, take customer behavior into account in real-time, and adjust themselves to the ever-changing fraud patterns. The company suggests that the most reliable approach for fraud prevention is the use of a combination of supervised, unsupervised, and reinforcement learning techniques in order to strike a balance between precision and recall.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

ETHICAL AI IN ADAPTIVE FRAUD DETECTION

Bias and fairness

The use of AI in fraud detection has contributed significantly in terms of speed and accuracy but on the other hand, bias and fairness issues have come up. Busari (2025) notes that AI systems based on training from the past tend to extend biases existing in society and institutions. Biases may come from unbalanced datasets, assumptions made by the model or its deployment environment. In the context of finance, the over-scrutiny of underprivileged communities may be the end result of that.

Fairness metrics are represented by the concepts of statistical parity, equalized odds, and calibration. Statistical parity ensures that groups are treated equally, equalized odds requires that the false-positive and false-negative rates are equal, and calibration ensures that the scores mean the same for different groups. These metrics often contradict one another, which makes it difficult to come up with a universally fair model. The paper states that ethical AI have to be able to strike a balance between fraud-detection performance and attributes like fairness and transparency.

Ethical risks and societal implications

Among the ethical risks are the following: discrimination, lack of transparency, accountability traceability issues, and the trust of consumers getting lower. Unintended discrimination happens when models use certain groups as unfair targets while opaque models make it hard to explain the decisions. Accountability gaps occur when the responsibilities are shared between developers, vendors, and financial entities without being clearly defined.

Responsible AI guidelines

The most effective measures from the Gleecus whitepaper point to setting up governance and oversight of AI as the main activities, which should include cross-functional ethics committees, AI risk officers and accountability matrices. Companies that employ Explainable AI (XAI) methods (e.g., SHAP, LIME) should make it clear how decisions are taken and give the customers the right to challenge the AI results. Adopting privacy-first principles such as pseudonymization, anonymization, and federated learning can significantly help in safeguarding sensitive information. Bias impact assessments and counter-factual testing should be done before and after deployment to spot and fix unfair results.

Among the security measures are the deployment of AI-specific threat models to counter data poisoning and adversarial attacks, encryption of model weights and data, and penetration testing of AI endpoints. Human oversight in situations with high risk—like loan approvals or fraud blocking—can guarantee that the critical decisions are in the hands of humans. According to the whitepaper, AI is becoming a fundamental capability and those institutions that show ethical AI behavior will be winners in the competitive market.

Regulatory and privacy considerations

The 2025 review on AI in fraud prevention highlights that AI is capable of diminishing false positives while also freeing up compliance staff from routine tasks like KYC and AML. These systems improve detection as they are always learning from fresh data and are able to do risk assessments in real-time. Yet, a set of ethical challenges remain: algorithmic bias, data privacy, and transparency require that they are continuously addressed. Adversarial attacks can alter input data with the aim of fooling AI models. The review stresses the need for explainability, ethical AI principles, and cybersecurity to counter the threats. Privacy-friendly methods such as homomorphic encryption and differential privacy are becoming more popular. Federated learning allows the institutions to share the gained knowledge while the raw data stays with each party. Regulators all over the world are setting up AI governance frameworks—like the EU AI Act and the US National Institute of Standards and Technology (NIST) AI Risk Management Framework—and being compliant will be a differentiator.

CONCLUSION

Adaptive fraud detection is a radical change in the paradigm of how financial ecosystems fight fraud. Even though traditional rule-based systems are still somewhat helpful, they are not able to keep up with the fraudsters that use advanced technologies and constantly change their tactics. Adaptive models such as risk-adaptive Bayesian ensembles, graph neural networks with federated learning, self-healing ML models, and adaptive perceptrons continuously ingest streaming data, recognize concept drift, and provide strong, real-time protection. To back up these claims, the paper cites empirical studies that show adaptive approaches increase accuracy and reduce false-positive

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

rates; e.g., adaptive GNNs contributed to detection improvement by 15–30 % and JPMorgan's graph-based models cut false positives by 30 %.

The installation of adaptive AI does not mean the abolition of ethical oversight. The issues of bias, fairness, transparency, and privacy are still there. To combat these issues, companies should establish governance frameworks, apply explainable AI methods, use privacy-first designs, mitigate bias, strengthen security, and employ human-in-the-loop controls. Studies indicate that ethical AI can even become a brand differentiator thus leading to higher customer trust and easier regulatory compliance.

The next step in research would be to think about how generative AI, agentic AI, and digital twins could be integrated in fraud detection. Generative AI might generate synthetic fraud scenarios when testing the robustness of the model whereas agentic AI could be automating multi-step investigations and compliance workflows. On the other hand, collaboration between institutions via federated learning and secure data-sharing platforms would be the way to go. Last but not least, regulators, technologists, and ethicists should partner with one another to make sure that adaptive fraud-detection systems not only keep the financial ecosystems safe but also are in line with the principles of fairness, transparency, and human dignity.

REFERENCES

1) Almarshad, F.A., Zakariah, M., Gashgari, G.A. Vaiyapuri, T. (2025). RABEM: risk-adaptive Bayesian ensemble model for fraud detection. Scientific Reports, 15 (Article 36796). doi:10.1038/s41598-025-20651-0.
2) Rahmati, M. (2025). Real-Time Financial Fraud Detection Using Adaptive Graph Neural Networks and Federated Learning. International Journal of Management and Data Analytics, 5(1), 98-110.
3) B. B. Chaudhari, S. Kabade and A. Sharma, "Leveraging AI to Strengthen Cloud Security for Financial Institutions with Blockchain-Based Secure E-Banking Payment System," 2025 International Conference on Networks and Cryptology (NETCRYPT), New Delhi, India, 2025, pp. 1490-1496, doi: 10.1109/NETCRYPT65877.2025.11102639.
4) Owen, A. (2023). Adaptive Machine Learning Models for Fraud Detection in Financial Systems: A Self-Healing Approach. ResearchGate preprint.
5) Binsawad, M. (2025). Enhanced Financial Fraud Detection Using an Adaptive Voted Perceptron Model with Optimized Learning and Error Reduction. Electronics, 14(9), 1875.
6) "Optimization Algorithms for Pension Asset Allocation Under Market Volatility", TIJER - TIJER - INTERNATIONAL RESEARCH JOURNAL (www.TIJER.org), ISSN:2349-9249, Vol.11, Issue 9, page no.a813-a819, September-2024, Available :https://tijer.org/TIJER/papers/TIJER2409089.pdf
7) Association of Financial Professionals (2024). Payments Fraud and Control Survey. As cited in SmartDev blog.
8) PayPal Editorial Staff (2024). Harnessing machine learning fraud detection technologies. PayPal Business Resource Center.
9) Busari, M. (2025). Bias, Fairness, and Ethics in AI-Based Financial Fraud Detection. ResearchGate preprint.
10) Adejumo, A.A. & Ogburie, C. (2025). The Role of AI in Preventing Financial Fraud and Enhancing Compliance. GSC Advanced Research and Reviews, 22(03), 269–282.
11) Gleecus TechLabs Inc. (2025). The Role of Artificial Intelligence in Modern Financial Ecosystems – Whitepaper.
JPMorgan Chase, UBS, Liv. Digital Bank and responsible AI best practices case studies are included.