Journal of Artificial Intelligence and Semiconductor Integrated Hardware

JAISIH

Volume 1, No 1, January 2026
Available Online at: jaisih.org

Adaptive Machine Learning for Emerging Fraud Patterns in FinTech Transactions

Dr. Neha Upadhyay
Lakshmi Narain College of Technology (MCA)
LNCT Campus, Kalchuri Nagar, Raisen Road, P.O. Kolua
Bhopal, Madhya Pradesh, India
neha.upadhyay887@gmail.com

***Abstract*—Adaptive learning of new fraud behavior among financial transactions on the FinTech platform has become a research urgency due to an increasing level of digitization of the global financial ecosystem. The increased use of digital banking, mobile payments, online lending and Cryptocurrency services has not only made innovation opportunities unsurpassed, but it has exposed financial platforms to more sophisticated fraudulent activities. Machine learning has emerged as one of the enabling factors to detect frauds as its pattern recognition, anomaly identification, and predictive analytics capabilities offer the solution to complex fraud situations in real-time. Categorization and detection through traditional methods such as the logistic regression, decision trees and support system machine have been applied widely to give meaning and trustworthiness to structured information. However, the evolution of fraudulent schemes has driven the adoption of the state-of-the-art and deep-learning techniques, including recurrent neural networks, long short-term memory models, graph neural networks, and transformers that encourage flexibility and large scale. Additionally, reinforcement learning, transfer learning and hybrid ensemble model can offer dynamic solutions that can be able to detect new trends of fraud in various transaction environments. All of these adaptive machine learning approaches contribute to a higher level of protection against fraud, financial stability, and assuring the confidence of consumers, therefore, they are essential in ensuring integrity and resilience of FinTech.**

Keywords*—Adaptive Machine Learning, Fraud Detection, FinTech Transactions, Deep Learning, Reinforcement Learning, Financial Security.

I. INTRODUCTION

The rising digitalization and diversification of the transactions in the dynamic financial world of the present has presented both opportunities and challenges. These barriers have included the challenge of fraud in financial transactions that has not only posed a danger to the individual consumers and businesses, but the financial system as well [1]. Conventional methods of fraud detection have diluted with the growing number of fraud schemes and exponentially growing amounts of data. This evolving environment is the engine of the necessity to seek more efficient, intelligent and adaptive solutions to secure financial ecosystems. There is therefore a need to come up with effective mechanisms of fraud detection to ensure that financial transactions are secure and reliable to the customer and the institutions. Such systems reduce risks, unauthorized activities and trust loss in the financial services [2]. This kind of flexibility is critical to consumer trust and to integrity of financial markets in a far more connected world.

The use of technology in delivering or offering financial services, known as financial technology (FinTech) that has a loose definition has transformed the way individuals and organizations conduct their transactions and payments by offering speed, convenience and availability [3]. Present FinTech environment is characterized by mobile payments, online banking, online lending, and cryptocurrency transactions that, besides aiding to enhance efficiency, have brought new vulnerabilities [4]. Such developments have brought into existence new opportunities of more sophisticated pattern of frauds that endanger the financial stability. It becomes hard to match dynamic and evolving threats using the traditional method of fraud detection which is usually constructed on rule basis or fixed machine learning systems. In this case, adaptive machine learning has proven to be an indispensable instrument, and it can learn based on new data and correct to new methods of fraud, hence presenting a more efficient shield against financial crimes.

Adaptive machine learning has emerged as a powerful remedy to this issue. Adjustive systems that can learn on streaming information, detect new and previously unseen fraud behavior, and re-optimize their decision boundaries in seconds compared to the more traditional models. Machine Learning (ML), one of the most widespread areas of artificial intelligence, has proved to be a powerful answer to such issues due to the outstanding data processing and anomalies detection and pattern recognition capabilities [5]. Financial transaction frauds comprise a wide range of financial frauds such as credit card frauds, identity theft, among others, all of which result in massive financial losses and loss of confidence in financial institutions [6]. The flexibility of the ML-based approaches predisposes them in particular to fight these emerging threats because of the ability to constantly learn with new data and adapt to the new trends of fraud.

A. Structure of the Paper

The paper is organized as follows: Section II looks at FinTech transactions fraud and its different variations. Section III reviews machine learning in fraud detection. Section IV discusses adaptive machine learning strategies for addressing emerging patterns of fraud. Section V provides a literature review with comparative insights, and Section VI summarizes the main points and suggests avenues for further study to improve fraud detection systems.

II. Fraud in Fintech Transactions

Criminal or unlawful deceit with the intent to get money or other valuables is known as fraud. Systems for identifying and combating fraud are the two main tools in the toolbox The purpose of fraud detection systems is to catch criminals in the act, once they have evaded fraud protection measures and begun a fraudulent transaction [7]. Rule-induction techniques, decision trees, ANN, SVM, logistic regression and meta-heuristics such as genetic algorithms are the most popular techniques used to detect fraud in this area. Construct classifiers using these methods alone or in an ensemble setting by combining them with meta-learning approaches. Structured data, applying quantitative methodologies, has been the primary focus of data mining research on fraud detection [8]. The following are the four main areas of fraud: internal, insurance, credit, and telecommunications:

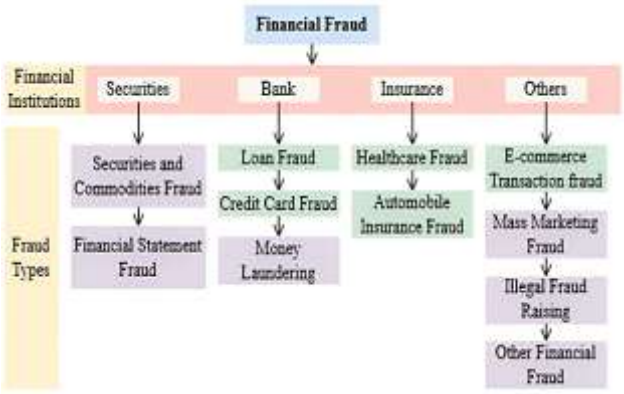

Fig. 1. Financial Fraud Classification Framework

Figure 1 shows the four primary areas of financial fraud: securities, banking, insurance, and other financial frauds. The crimes' institutional links and repercussions define these sectors. Credit card fraud, loan fraud, and money laundering are all forms of bank fraud. Securities fraud, on the other hand, comprises financial statement deceit.

A. Detection of fraudulent credit card transactions

One of the most common types of fraud is credit card fraud, which usually involves taking someone else's credit card information and using it to make an illegal purchase. Credit card fraud can be difficult to detect, although experts have suggested many solutions [9]. An early and commonly used technique for detecting suspicious transactions, rule-based detection involves establishing a set of rules (such as a minimum value for a transaction or a maximum location for a transaction, among others) and then applying them. Nevertheless, when confronted with intricate and ever-changing deception tactics, this strategy falls short. A number of popular machine learning algorithms have lately grown in prominence, including decision trees and random forest methods. By analyzing previous transaction data, these algorithms can automatically understand the characteristics of fraudulent conduct. Studies show that random forest credit card fraud detection has a decent accuracy and recall rate; nevertheless, its computational complexity may be a hindrance for real-time detection.

B. Types of Financial Fraud

This section describes the first key element of the taxonomy, which is the types of financial fraud [10]. Several types of financial fraud exist that AI-based methods aim to identify, categorized in this area of taxonomy:

1) Payment Fraud

Payment fraud encompasses schemes that utilize credit or debit cards, online payments, and QR codes, and is one of the primary categories of fraud. People use fraudulent payment methods to steal money and access personal information through credit cards, debit cards, and e-payment systems [11]. Payment fraud operates in different ways and disrupts the lives of private citizens, their work activities, and bank partners.

2) Identity Fraud

When personal information is exploited for illegal access or transactions, identity fraud occurs. People who commit identity fraud use stolen personal information to pretend to achieve financial or criminal goals [12]. When someone loses their identity through fraud, they suffer immediate damage to their money, credit history, and public standing.

3) Transaction Fraud

The application of developing an integrated system that combines both hybrid deep learning models and the Random Forest algorithm to identify financial fraud. According to the experimental analysis, the false positive rate is reduced to 15%, and the overall detection accuracy has improved to 20%.

4) Insurance and Claims Fraud

People commit insurance and claims fraud by lying to insurance companies to get money they do not qualify for. Users can commit fraudulent activities targeting multiple types of insurance, including medical coverage, auto coverage, property insurance, life insurance, and disability insurance.

C. Key Challenges in Fraud Detection

Fraud detection in FinTech transactions faces several challenges due to the dynamic, high-volume, and adversarial nature of financial ecosystems [13]. Emerging fraud patterns continuously evolve, making static detection methods less effective. Major challenges include:

- **Evolving Fraud Tactics**: Fraudsters rapidly adapt strategies to bypass existing models, leading to concept drift and reduced detection accuracy.
- **Data Imbalance**: Machine learning models and datasets are impacted by bias due to the small amount of fraudulent transactions compared to legitimate ones.
- **Real-Time Processing Requirements**: FinTech platforms demand immediate fraud detection with minimal latency, which is computationally intensive.
- **Explain ability and Transparency**: Many advanced ML models (e.g., deep learning) act as black boxes, making regulatory compliance and user trust difficult.
- **Privacy and Security Concerns**: Sharing sensitive financial data for model training can conflict with legal and ethical requirements.

III. Machine Learning In Fraud Detection

Machine learning models, able to sift through enormous datasets and identify intricate patterns, are an essential part of real-time fraud detection systems [14]. In this field, the most common machine learning algorithms are:

- **Supervised Learning:** Using labelled datasets, many approaches can learn patterns that may indicate fraud. For example, decision trees, logistic regression, and

random forests. Several studies have shown that ensemble methods, like random forests, do quite well in detecting fraud, and this emphasizes the usefulness of supervised models.

- **Unsupervised Learning:** Clustering and anomaly detection approaches are examples of unsupervised learning models. They are great for detecting unknown sorts of fraud because they don't need labeled data. Approaches to detecting anomalies [15], including autoencoders and isolation forests, are effective in identifying a typical pattern without requiring prior knowledge of fraud cases.
- **Semi-Supervised and Self-Supervised Learning:** Semi-supervised methods have become popular considering that there is limited labeled fraud data. These approaches merge labeled and unlabeled data, and this proves the effectiveness of semi-supervised learning of minimizing false positives. A new trend in this direction is self-supervised learning, in which models create their own labels based on the data they are trained on, thereby potentially decreasing the reliance on labeled data.

A. Traditional ML Approaches

Financial technology fraud detection has made heavy use of conventional machine learning techniques such as LR, DT, RF, and SVMs [16]. These models are based on manually crafted features, historical transaction data and statistical trends to detect fraudulent activity, which can be interpreted, but can rarely respond in time to changes in fraud trends.

1) Support Vector Machine (SVM)

Support Classification and regression issues are suitable for the use of vector machines, which are supervised machine learning algorithms. The method relies on maximizing the margin between feature space classes by finding the optimum hyperplane. The optimization challenge can be mathematically addressed by using SVM to reduce the hinge loss function and punish errors. It is possible to optimize SVM's performance by adjusting its hyperparameters, which include the kernel's type (linear, polynomial, or radial basis function), regularization parameter C, and kernel coefficient gamma. SVM is highly sensitive to parameter tweaking.

2) Decision Tree

The supervised learning algorithm known as a decision tree finds use in regression and classification tasks. Its decision-making process involves recursively constructing a tree-like structure from the feature space according to predefined criteria. The goal of using entropy or Gini impurity as splitting criteria is to increase the homogeneity of the target variable in each node.

3) Logistic Regression

Logistic Regression Model Most often used for binary classification, this algorithm is a supervised learning technique. Utilizing a logistic or sigmoid form, it provides an approximation of the likelihood of a certain case concerning a specific category. To minimize the cost function, optimization procedures such as gradient descent are used. This function assesses the value of the dissimilarity between the forecasted probability and the true labels.

B. Deep Learning Approaches (RNN, LSTM, CNN, Transformers)

RNNs and LSTMs are the deep learning techniques that can be used to start modelling sequential transaction data to identify abnormal patterns over time [17].

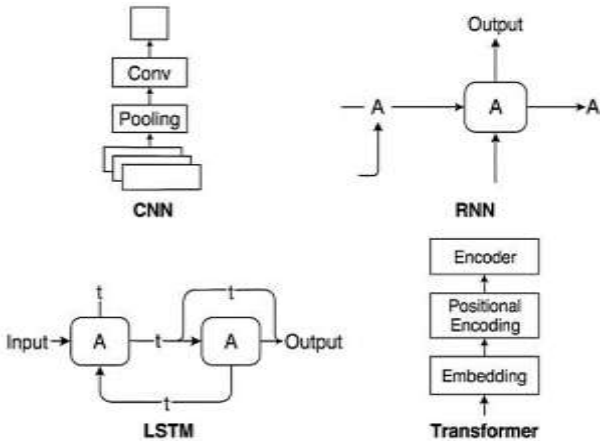

Fig. 2. Architecture Diagrams for CNN, RNN, LSTM, and Transformer

Graph Neural Networks (GNNs) can identify these complex ties in transaction networks and can identify collusive or coordinated fraud. In recent years, it recently emerged that Transformer-based models can be used with large-scale, heterogenous financial data to provide more adaptable and accurate results. The methods of Deep Learning in Figure 2:

CNNs are built to learn feature hierarchies from input images automatically and adaptively [18]. They begin with convolutional layers that extract features using kernels and then proceed to pooling layers that flatten the model's spatial dimensions. Additional methods that improve learning capacity include batch normalization, dropout, and activation functions like ReLU.

1) Recurrent Neural Networks (RNNs):

A type of network known as an RNN has connections between nodes that create a graph with time as its topology. Their sequential nature makes them ideal for jobs involving text or time series input data.

2) Long Short-Term Memory (LSTM):

LSTMs improve RNNs by the use of gating mechanisms and memory units The Forget Gate selects which pieces of data to remove. Input Gate: A decision-maker for updating values [19]. Output Gate: This gate uses the memory to generate the final output.

3) Transformers:

Transformers' self-attention system shook up deep learning. Forget about recursion; they use queries (Q), keys (K), and values (V) to calculate interdependencies between all tokens at once.

C. Ensemble and Hybrid Models

The use of multiple machine learning methods together improves fraud detection, according to recent studies. Combining deep learning with random forests yields a hybrid architecture that outperforms independent models in terms of accuracy [20]. unveiled an AI-powered cyber defense system, which improved model adaptability through the use of ML and rule-based fraud detection techniques [21]. Further, a stacked ensemble learning method can be used to lessen the

occurrence of false positives by combining various models, including RF, XGBoost, and deep neural networks (DNNs). However, real-time fraud detection systems generally struggle to implement hybrid models due to their high computational resource requirements, notwithstanding these advantages.

IV. Adaptive Machine Learning Strategies For Fraud Detection

Automated learning systems have shown to be a powerful asset in the fight against fraud. As a result of the large amounts of data transmitted, internet transactions can only have two possible results. Either of these could be real or fake. The internet firm is able to detect fraudulent actions due to the chargebacks they receive [22]. However, chargebacks are not proactive but rather reactive because they are launched after the transactions have already taken place. In order for machine learning to function, massive datasets that have been collected from various clients and businesses have to be used [23]. The complete breadth of their dataset may be controlled by even the smallest of businesses, giving them access to accurate statistics on every transaction. Companies can choose the best model for improving call volumes and accuracy with the use of the aggregated data, which gives a very accurate training dataset. The accuracy percentage is the number of fraudulent or recall transactions that the model can identify out of all the transactions.

A. Adaptive and Online Balancing Techniques

Gradual learning methods are used to create hypotheses from the training data. The learner can then use the hypothesis at any time to find and confirm the best answer to the question. To get the most accurate predictions, the PWIDB method works in a similar way by creating and testing hypotheses with each incremental window. These methods need to change so they can increase intelligence and generalize new ideas as knowledge changes throughout time [24]. They become better at learning continuously and improving their performance over time because these strategies learn incremental tasks everywhere. Data stream transmission overhead can be decreased by employing the concept of data batching. This paper's underlying premise is that, in a vast data streaming scenario, a suitable balancing technique should adapt and learn progressively to overcome the class imbalance problem, just like a communication problem that relies on a stream of information. As studies have shown, up-sampling and down-sampling are ineffective in dealing with imbalanced datasets. However, it can dynamically alter a rebalancing method with the application of incremental setting in the active learning process.

B. Transfer Learning and Domain Adaptation

Various transfer learning (TL) paradigms have been investigated, with varying assumptions on the accessibility of training data [25]. All of these systems share the need for massive amounts of tagged data from several source domains. The availability of target domain data during training is the deciding factor.

- **Domain Generalization (DG):** Training models with datasets exclusive to the source domain allows the learnt prediction function to generalize straight to the target domain, which is the ultimate goal. During training, there is a lack of data from the target domain.
- **Unsupervised Domain Adaptation (UDA):** A dataset from the target domain that is not labeled is also accessible, in addition to datasets from the source domain. Even in the absence of labeled target data, this unlabeled data aids in adjusting the prediction function for improved performance in the target domain.
- **Supervised Domain Adaptation (SDA):** The datasets from the source domain are provided along with a large unlabeled dataset and a small labeled dataset from the target domain. By combining them, the predictive function can be fine-tuned for the target domain.
- **Multi-Domain Learning (MDL):** The aim is to train a single prediction function that works well in all areas using datasets from different domains. Here, labelled data is accessible across all training domains.

C. Reinforcement Learning in Financial Fraud Detection

Table I summarizes the advantages and disadvantages of several fraud detection methods. One of the most promising methods in financial fraud detection is reinforcement learning (RL) [26]. Its strength lies in the ability to discover optimal decision policies in dynamic and constantly changing environments [27]. Contrary to the conventional methods of supervised learning, RL does not utilize labeled data only. Rather, it also acquires knowledge by engaging with the surrounding and feedback information, which makes it especially well-suited to adjusting to changing fraud patterns.

TABLE I. Summarizing different fraud detection approaches, highlighting their strengths and weaknesses

Approach	Description	Strengths	Weaknesses
Rule-Based	Identifies potentially fraudulent financial activities using established criteria.	Effective against recognized fraud patterns; easy to implement and understand.	Requires regular manual updates, has low flexibility, and produces a significant number of false positives.
Supervised Learning	Trains models to categorize transactions using labelled data.	Robust machine learning algorithms, excellent accuracy for previously identified fraud patterns.	Concept drift is a problem, because it fails to detect new forms of fraud because it mandates massive labelled datasets.
Unsupervised Learning	Uses clustering or anomaly detection to find outliers in unlabeled data.	Adapts to new risks, finds new fraud patterns, and works with unlabeled data.	High false positives, difficult interpretation, needs additional validation.
Reinforcement Learning (RL)	Agent acquires the most effective policies for detecting fraud through the use of reward-based learning.	Optimised strategies are adjusted in real-time in response to changing fraud patterns; labelled data is unnecessary.	Computationally intensive, sensitive to reward design, requires long training time.

Rank-based learning outperforms supervised learning when it comes to fraud detection since it provides more flexible options. Traditional models exhibit idea drift tendencies due to the constant evolution of fraudsters' strategies. Without the characteristics of tagged data, RL agents can detect new fraud tendencies in real-time communications thanks to their constantly changing policies

[28]. Financial firms that need fraud prevention predictive systems might greatly benefit from relational learning due to its adaptable nature. Reward delays: RL agents are able to handle reward delays, allowing them to create comprehensive fraud detection systems that go beyond just responding quickly.

V. Literature Review

In this literature Overview, several machine learning models have been identified with a particular focus on supervised model, unsupervised model, ensemble model, and deep learning model to detect FinTech fraud. It has been found that there have been radical developments and yet, the unresolved problems of data imbalance and interpretability and future tendencies of adaptive, hybrid and context-specific resolutions.

Joy Nnenna Okolo et al. (2025) ML techniques' function in improving fraud detection capabilities, informed by data-driven knowledge for efficient and dynamic fraud prevention. The authors of the research classify ML methods according to their strengths in detecting fraudulent trends: supervised, unsupervised, and reinforcement learning. While supervised models rely on labeled data for classification, unsupervised algorithms excel in finding outliers in unlabeled data. Reinforcement learning, on the other hand, is constantly training detection strategies with the use of real-time feedback [29].

Odufisan et al. (2025) the opportunities of AI and ML to promote the increased fraud detection and prevention in Nigeria. They be able to study numerous AI methodologies, such as supervised, unsupervised, and DL. Discuss their application in network analysis, risk scoring, behavioural analysis and anomaly detection. Organizations that are able to react to new fraud schemes can do so through the strength of a constant learning process that AI can provide. The article hints the benefits of AI-powered fraud-detection, including high level of efficiency, improved accuracy and avoidance of risks. That aside, such problems as technical disadvantages and legal considerations are confessed. Last but not the least, explore the bright future of AI and ML to transform the situation with financial crime prevention in Nigeria [30].

Palivela et al. (2024) a sequential model framework that utilizes neural networks to enhance the classification of transactions as either fraudulent or not. Gradient Boost, Random Forest, Logistic Regression, Voting Classifiers, and hyperparameter optimization to avoid overfitting are some of the ensembles learning methods that have been proposed. Some methods, such as the Synthetic Minority Over-sampling Technique (SMOTE) and under-sampling, employing particular machine learning (ML) algorithms, can be employed to address the issue of inconsistency in the credit card dataset. A supervised learning technique was used to generate a model that significantly outperformed the baseline strategy, using the attributes as input. Using metrics like recall, accuracy, precision, and F1-score, the model was tested on a massive dataset of anonymized credit card transactions [31].

Shetty et al. (2023) these problems with up-to-date machine learning algorithms. Decision trees are known to be employed to detect fraud in real time by giving insight into data. Also, the detection of complex patterns of fraud is performed with the help of DL methods and ANN, and the likelihood of a fraud is modelled with the help of logistic regression. The precision of these techniques, among them, decision trees, logistic regression, ANN are all assessed with an accuracy of 99.8, 99.9 and 99.94 respectively. Contributing to machine learning-based fraud detection, these findings can be useful for businesses in selecting effective anti-fraud solutions and for understanding the adaptability of algorithms in practical financial contexts [32].

Alarfaj et al. (2022) The main goal is to detect these frauds, and they include such problems as the accessibility of the public data, its large class imbalance, the alteration of nature of the fraud, and the large rate of false alarm. The machine learning approach to credit card identification has been covered in the literature in a number of ways. They are XG Boost, DT, RF, SVM, as well as LR, among others. Even with cutting-edge deep learning algorithms, reducing fraud losses remains a challenge owing to low accuracy. Using the most current developments in deep learning algorithms to achieve this goal has been the main emphasis. Prior to applying a machine learning algorithm to the dataset, fraud detection accuracy was enhanced to a certain degree [33].

Stojanović et al. (2021) ML techniques are used to find strange things in Fintech apps. In order to foresee potential frauds, they create models that target questionable behavior in financial datasets. They are in a prime position to weigh in on this critical subject and offer advice on anomaly detection techniques. Several synthetic and real-world datasets that contained fake information were used for the experiments. The outcomes validate that ML techniques do, to varied degrees, aid in fraud detection. various approaches' efficacy in terms of detection rate [34].

Table II provides a brief overview of current research on the topic of adaptive ML in financial technology fraud detection. The studies examined various methodologies, identified important discoveries, discussed current obstacles, and suggested future possibilities for enhancing the effectiveness of detection.

TABLE II. Summary of a Study on Adaptive Machine Learning for Emerging Fraud Patterns in FinTech Transactions

Author	Study On	Approach	Key Findings	Challenges	Future Directions
Joy Nnenna Okolo et al., (2025)	Improving fraud detection skills with the use of ML	Reinforcement Learning: Supervised and Unsupervised	Categorized ML methods for fraud detection; highlighted adaptability of RL in real-time fraud scenarios	Dependence on labeled data (SL), difficulty in interpretation (UL), computational demands (RL)	Improve hybrid adaptive models and expand use of reinforcement learning for real-time fraud prevention
Odufisan et al., (2025)	Fraud detection in Nigeria using AI and ML	Supervised, Unsupervised, Deep Learning	AI improves anomaly detection, behavioral analysis, and proactive risk mitigation	Problems with technology, worries about regulations, and moral dilemmas	Strengthen AI integration with regulatory frameworks; explore context-specific ML deployment
Palivela et al., (2024)	Sequential model framework for	Ensemble Learning (Gradient Boost, RF,	Ensemble models improved classification; data imbalance	Dataset inconsistency; overfitting risk	Optimize ensemble models with robust data balancing and hyperparameter tuning

	fraud classification	LR, Voting), SMOTE	handled via under-sampling and SMOTE		
Shetty et al., (2023)	Advanced ML techniques in real-time fraud detection	Decision Trees, ANN, Logistic Regression	Achieved high accuracy (DT: 99.8%, LR: 99.9%, ANN: 99.94%)	Model adaptability in real contexts; reliance on structured data	Expand ANN and hybrid methods for unstructured data fraud detection
Alarfaj et al., (2022)	Credit card fraud detection	Traditional ML (SVM, RF, LR, XGBoost), Deep Learning	Highlighted ML algorithms but stressed need for DL to reduce losses	High imbalance in datasets; false alarms; low accuracy in traditional models	Use cutting-edge deep learning to build scalable and adaptable fraud detection systems.
Stojanović et al., (2021)	ML-based anomaly detection in FinTech	Anomaly Detection (various ML models)	ML improves anomaly detection in financial datasets; varying success across methods	Dataset diversity; effectiveness varies by technique	Develop more robust anomaly detection with cross-dataset generalization

VI. Conclusion and Future Work

Fraud detection in FinTech transactions is an increasingly complex challenge as digital ecosystems expand and fraudulent strategies continuously evolve. This review reflects the historical shift of classical machine learning model, including logistic regression, decision trees, SVMs, and other, towards modern deep learning models, including RNNs, LSTMs, GNNs, and Transformers. Older methods are understandable and efficient, but are usually not scalable to changing fraud strategies, whereas deep learning approaches are more accurate and scalable, but at a cost of large computing resources and transparency. Further resiliency is offered by adaptive strategies, such as reinforcement learning, domain adaptation, and online balancing methods, that allow models to adapt to new fraud trends as they appear in real-time. Hybrid frameworks also increase the performance, by integrating the benefits of different models. However, these advances do not resolve challenges such as imbalance in the classes, high computation and interpretation cost and dependence on high quality labeled data still constrain their effective application at large scale. A remedy to the above-mentioned disadvantages remains a vital issue in the development of robust, reliable, and future resistant fraud detection models.

Future directions would include development of light weight yet accurate adaptive models which offers a trade-off between efficiency and interpretability. More focus on privacy-protecting mechanisms, synthetic data synthesis, and explainable AI can provide more reliable, fair and scalable fraud finding in dynamic FinTech environments.

References

[1] E. Pan, "Machine Learning in Financial Transaction Fraud Detection and Prevention," *Trans. Econ. Bus. Manag. Res.*, vol. 5, pp. 243–249, 2024, doi: 10.62051/16r3aa10.

[2] M. Binsawad, "Enhanced Financial Fraud Detection Using an Adaptive Voted Perceptron Model with Optimized Learning and Error Reduction," *Electron.*, vol. 14, no. 9, 2025, doi: 10.3390/electronics14091875.

[3] H. Kali, "Optimizing Credit Card Fraud Transactions identification and classification in banking industry Using Machine Learning Algorithms," *Int. J. Recent Technol. Sci. Manag.*, vol. 9, no. 11, pp. 85–96, 2024.

[4] G. Kou and Y. Lu, "FinTech: a literature review of emerging financial technologies and applications," *Financ. Innov.*, vol. 11, no. 1, pp. 1–34, 2025, doi: 10.1186/s40854-024-00668-6.

[5] O. A. Bello, A. Folorunso, O. E. Ejiofor, F. Z. Budale, K. Adebayo, and O. A. Babatunde, "Machine Learning Approaches for Enhancing Fraud Prevention in Financial Transactions," *Int. J. Manag. Technol.*, vol. 10, no. 1, pp. 85–108, 2023.

[6] H. Kali and G. Modalavalasa, "Artificial Intelligence (AI)-Driven Business Intelligence for Enhancing Retail Performance with Customer Insights," *Asian J. Comput. Sci. Eng.*, vol. 9, no. 4, pp. 1–9, 2024, doi: 10.22377/ajcse.v10i2.210.

[7] S. J. Wawge, "A Survey on the Identification of Credit Card Fraud Using Machine Learning with Precision, Performance, and Challenges," *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 4, pp. 3345–3352, May 2025, doi: 10.38124/ijisrt/25apr1813.

[8] S. K. Aljunaid, S. J. Almheiri, H. Dawood, and M. A. Khan, "Secure and Transparent Banking: Explainable AI-Driven Federated Learning Model for Financial Fraud Detection," *J. Risk Financ. Manag.*, vol. 18, no. 4, 2025, doi: 10.3390/jrfm18040179.

[9] C. Cheng, "Research on Fraudulent Transaction Detection," *Appl. Comput. Eng.*, vol. 158, no. 1, pp. 35–40, 2025, doi: 10.54254/2755-2721/2025.tj23322.

[10] N. J. Sarna *et al.*, "AI Driven Fraud Detection Models in Financial Networks: A Review," *IEEE Access*, vol. 13, no. August, pp. 141204–141233, 2025, doi: 10.1109/ACCESS.2025.3596060.

[11] M. Farouk *et al.*, "Fraud_Detection_ML: Machine Learning Based on Online Payment Fraud Detection," *J. Comput. Commun.*, vol. 3, no. 1, pp. 116–131, Feb. 2024, doi: 10.21608/jocc.2024.339929.

[12] H. P. Kapadia and K. C. Chittoor, "AI Chatbots for Financial Customer Service: Challenges & Solutions," *J. Adv. Futur. Res.*, vol. 2, no. 2, p. 7, 2024.

[13] G. K. Kulatilleke, "Challenges and Complexities in Machine Learning based Credit Card Fraud Detection," pp. 1–17, 2022.

[14] S. Owoade, A. Uzoka, J. Akerele, and P. U. Ojukwu, "Automating fraud prevention in credit and debit transactions through intelligent queue systems and regression testing," *Int. J. Front. Eng. Technol. Res.*, vol. 7, no. 2, pp. 044–056, Nov. 2024, doi: 10.53294/ijfetr.2024.7.2.0048.

[15] S. Gajula, "A Review of Anomaly Identification in Finance Frauds using Machine Learning System," *Int. J. Curr. Eng. Technol.*, vol. 13, no. 06, Jun. 2023, doi: 10.14741/ijcet/v.13.6.9.

[16] V. R. Modhugu and S. Ponnusamy, "Comparative Analysis of Machine Learning Algorithms for Liver Disease Prediction: SVM, Logistic Regression, and Decision Tree," *Asian J. Res. Comput. Sci.*, vol. 17, no. 6, pp. 188–201, 2024, doi: 10.9734/ajrcos/2024/v17i6467.

[17] P. D. Mashru, "Comparative Analysis of CNN, RNN, LSTM, and Transformer Architectures in Deep Learning," *Educ. Adm. Theory Pract.*, vol. 29, no. 4, pp. 5439–5443, 2023, doi: 10.53555/kuey.v29i4.10364.

[18] S. Mathur and S. Gupta, "Classification and Detection of Automated Facial Mask to COVID-19 based on Deep CNN Model," in *2023 IEEE 7th Conference on Information and Communication Technology, CICT 2023*, 2023. doi: 10.1109/CICT59886.2023.10455699.

[19] S. Almotairi, D. D. Rao, O. Alharbi, Z. Alzaid, Y. M. Hausawi, and J. Almutairi, "Efficient Intrusion Detection using OptCNN-LSTM Model based on hybrid Correlation-based Feature Selection in IoMT," *Fusion Pract. Appl.*, vol. 16, no. 1, pp. 171–194, 2024, doi: 10.54216/FPA.160112.

[20] K. B. Thakkar and H. P. Kapadia, "The Roadmap to Digital Transformation in Banking: Advancing Credit Card Fraud Detection with Hybrid Deep Learning Model," in *2025 2nd International Conference on Trends in Engineering Systems and Technologies (ICTEST)*, 2025, pp. 1–6. doi: 10.1109/ICTEST64710.2025.11042822.

[21] R. R. Devarakonda, "Machine Learning Approach for Fraud Detection in a Financial Services Application," *SSRN Electron. J.*, vol. 14, no. 1, pp. 1–13, 2025, doi: 10.2139/ssrn.5234670.

[22] M. Dayalan and R. Publications, "Adaptive Fraud Detection Through Machine Learning," *SSRN Electron. J.*, vol. 4, pp. 328–

331, 2017.

[23] S. Gajula, "Cloud Transformation in Financial Services: A Strategic Framework for Hybrid Adoption and Business Continuity," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 11, no. 2, pp. 1244–1254, Mar. 2025, doi: 10.32628/CSEIT25112464.

[24] R. A. Mohammed, K.-W. Wong, M. F. Shiratuddin, and X. Wang, "Improving fraud prediction with incremental data balancing technique for massive data streams," 2019.

[25] R. R. Pereira, J. Bono, H. Ferreira, P. Ribeiro, C. Soares, and P. Bizarro, "Evaluating Transfer Learning Methods on Real-World Data Streams: A Case Study in Financial Fraud Detection," vol. 2, no. Ml, pp. 1–16, 2025.

[26] V. Verma, "Deep Learning-Based Fraud Detection in Financial Transactions : A Case Study Using Real-Time Data Streams," vol. 3, no. 4, pp. 149–157, 2023, doi: 10.56472/25832646/JETA-V3I8P117.

[27] T. Fayemi, "Real-time fraud detection with reinforcement learning: An adaptive approach," *Int. J. Sci. Res. Arch.*, vol. 6, no. 2, pp. 126–136, Aug. 2022, doi: 10.30574/ijsra.2022.6.2.0068.

[28] J. Mishra, B. B. Biswal, and N. Padhy, "Machine Learning for Fraud Detection in Banking Cyber security Performance Evaluation of Classifiers and Their Real-Time Scalability," in *2025 International Conference on Emerging Systems and Intelligent Computing (ESIC)*, IEEE, Feb. 2025, pp. 431–436. doi: 10.1109/ESIC64052.2025.10962752.

[29] J. N. Okolo, S. A. Adeniji, O. Onwuegbuchi, and S. Sanni, "Analyzing the use of machine learning techniques in detecting fraudulent activities," *World J. Adv. Res. Rev.*, vol. 26, no. 1, pp. 1198–1209, Apr. 2025, doi: 10.30574/wjarr.2025.26.1.1097.

[30] O. I. Odufisan, O. V. Abhulimen, and E. O. Ogunti, "Harnessing artificial intelligence and machine learning for fraud detection and prevention in Nigeria," *J. Econ. Criminol.*, vol. 7, no. January, p. 100127, 2025, doi: 10.1016/j.jeconc.2025.100127.

[31] H. Palivela *et al.*, "Optimization of Deep Learning-Based Model for Identification of Credit Card Frauds," *IEEE Access*, vol. 12, no. August, pp. 125629–125642, 2024, doi: 10.1109/ACCESS.2024.3440637.

[32] V. R. Shetty, P. R., and R. L. Malghan, "Safeguarding against Cyber Threats: Machine Learning-Based Approaches for Real-Time Fraud Detection and Prevention," in *RAiSE-2023*, Dec. 2023, p. 111. doi: 10.3390/engproc2023059111.

[33] F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan, and M. Ahmed, "Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms," *IEEE Access*, vol. 10, pp. 39700–39715, 2022, doi: 10.1109/ACCESS.2022.3166891.

[34] B. Stojanović *et al.*, "Follow the Trail: Machine Learning for Fraud Detection in Fintech Applications," *Sensors*, vol. 21, no. 5, p. 1594, Feb. 2021, doi: 10.3390/s21051594.

