International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 14, Issue 11, November 2025)

A Review Paper of Intelligent Control of Financial Fraud in Online Transactions Using Artificial Intelligence

Monika Rawat
Assistant Professor
Sage University, Indore, M.P., India.

Abstract: - In the age of digital payments and e-commerce, financial fraud in online transactions has grown to be a significant problem. Conventional fraud detection systems are ineffective against contemporary, changing fraud strategies since they mostly rely on human rules. Through sophisticated learning algorithms, predictive analytics, and pattern recognition, artificial intelligence (AI) presents a new paradigm for intelligent fraud detection and control. This study examines current AI-driven techniques, such as machine learning, deep learning, and hybrid approaches, for financial fraud detection. The paper outlines their uses, benefits, drawbacks, and potential for future development in order to provide safe, real-time transaction monitoring and fraud prevention.

Keywords: Artificial Intelligence, Financial Fraud, Online Transactions, Machine Learning, Deep Learning.

I. Introduction

Online financial transactions, including online banking, e-commerce payments, and digital wallets, have become the foundation of international trade in today's digital economy. However, the growing dependence on digital platforms has also increased the likelihood of fraudulent activity, which might result in serious financial and reputational losses for people, companies, and financial institutions. Conventional fraud detection systems are insufficient in identifying new and intricate fraud schemes that change quickly since they primarily rely on human created rules and statistical techniques.
Artificial Intelligence (AI) provides data-driven, intelligent systems that can analyse large amounts of dynamic transactional data in real time. AI-based systems may learn from past transaction data, identify unusual behaviour, and automatically adjust to new fraud trends by utilising machine learning (ML), deep learning (DL), and data mining methods. AI-driven methods, in contrast to traditional models, offer prediction accuracy, speed, and scalability, allowing for proactive management over fraudulent transactions.

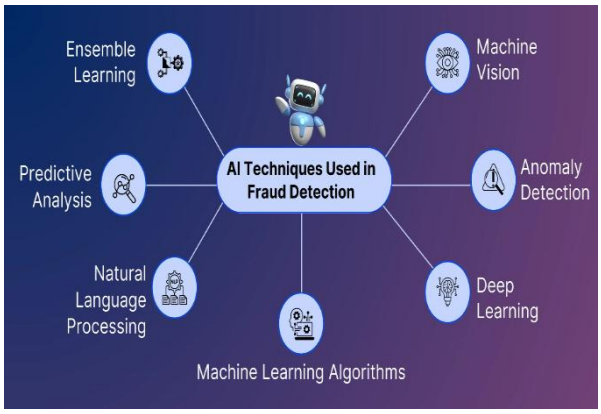

Figure 1- Improve Fraud Detection Accuracy

When AI is used into financial fraud detection, systems are better able to detect known and unknown fraud attempts with high accuracy. Additionally, methods like ensemble modelling, natural language processing, and neural networks help to improve decision-making and lower false positives. The development, methods, and efficacy of AI-based intelligent control systems for financial fraud detection in online transactions are examined in this review article, along with their uses, difficulties, and potential future developments.

II. Literature Review

Vallarino (2025) Vallarino suggests a modular Mixture-of-Experts (MoE) fraud detector that incorporates autoencoders (for anomaly detection), Transformer encoders (for high-order interactions), and RNNs (for sequential modelling). The hybrid system outperforms standalone baselines with good performance (≈98.7% accuracy; precision ≈94.3%, recall ≈91.5%), having been trained on a high-fidelity synthetic transaction

dataset. It dynamically directs inputs to the top expert. The paper's strength is its ability to integrate temporal, contextual, and anomaly detectors into a flexible pipeline; its drawbacks are its reliance on synthetic data and its scant attention to model explainability in production [1].

Sawaika and associates (2025) This study proposes a defence mechanism (called "FedRansel") against poisoning/inference assaults and presents a federated learning architecture that incorporates quantum-enhanced layers into an LSTM (Quantum-LSTM). The approach aims to increase adversarial robustness and facilitate cross-institution collaboration without exchanging raw data, claiming a 5% improvement over conventional alternatives. Although it is still mostly experimental, it enhances privacy-aware fraud analytics and highlights both promising accuracy increases and unresolved issues with federated convergence and quantum resource needs [2].

Innan et al. (2024) QFNN-FFD improves privacy and pattern recognition among dispersed financial clients by combining federated learning with quantum machine learning primitives. The authors show robustness to noisy conditions and exhibit good accuracy (>95%). Although the article is noteworthy for operationalising QML inside a federated workflow, communication overhead analysis and quantum hardware maturity are necessary for practical implementation [3].

Z. Luo and G. Yu (2025) Yu and Luo suggest a hybrid pipeline that employs a quantum-inspired optimiser for parameter tuning and deep belief networks (DBNs) for representation learning. According to published research, quantum optimisation may aid in escaping local minima and demonstrate competitive detection rates on benchmark datasets. Although the work might benefit from larger-scale assessments and better comparisons to contemporary DL baselines, the contribution is innovative methodologically [4].

Chen, Y. (2025) Chen's comprehensive review summarises DL advancements by examining CNNs, RNNs/LSTMs, autoencoders, and attention/transformer models from current research. The review identifies trends: interpretability is still a barrier; class imbalance management (SMOTE, focal loss) is crucial; and hybrid architectures perform better than single-paradigm models. Chen advocates for cross-institutional research pipelines that protect privacy and standardise benchmarks [5].

Hernandez Aros, L. (2024) Hernández Aros gathers machine learning techniques (logistic regression, decision trees, RF, and XGBoost) and applies them to PaySim/Credit Card datasets, demonstrating that ensemble models often outperform deep networks in terms of accuracy and latency. For operational deployments, the work highlights useful trade-offs between interpretability, latency, and detection power [6].

Li, G. et al. (2024) Li and associates provide a multi-perspective method that employs ensemble classifiers and feature-level fusion to combine behavioural, device, and transactional inputs (multi-subject perceptions). They contend that cross-modal fusion lessens single-source blind spots and show enhanced recollection for complex assaults (synthetic identities) [7].

TechScience/MFGAN The MFGAN method improves classifier training on unbalanced credit-card datasets by combining multi-feature fusion with a GAN to provide minority class samples. Compared to traditional oversampling, the results demonstrate better recall and fewer false negatives; nevertheless, GAN-generated samples need to be carefully validated to prevent distributional drift [8].

Afriyie and associates (2023) Using publicly accessible transaction datasets, Afriyie et al. assess supervised pipelines (feature engineering + ensemble classifiers) and demonstrate strong performance (high F1 on balanced test splits). Preprocessing and feature selection are highlighted as critical elements for model effectiveness in actual data in this realistically focused study [9].

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 14, Issue 11, November 2025)

Samuel, A. (2023) Samuel examines cloud-native fraud analytics, including deployment patterns, latency considerations, and MLOps techniques while outlining scalable streaming architectures that integrate Spark/Flink with ML models (RF, XGBoost). Although it is less focused on new algorithmic innovations, the work is helpful for practitioners [10].

III. Methodology

The investigation of AI-driven systems intended to intelligently identify, anticipate, and manage financial fraud in online transactions is a key component of the research technique used in this paper. Secondary data from academic journals, conference proceedings, and financial technology reports published between 2018 and 2025 served as the foundation for this study. The methodology seeks to assess the performance, algorithms, and design frameworks of different AI models used for fraud detection and prevention.

The AI-driven fraud detection process typically consists of four key stages:

Data Collection and Preprocessing:

Collecting transactional statistics from financial institutions, banks, and e-commerce sites is the initial stage. Features including transaction amount, time, location, user behaviour, and device data are included in these databases. To guarantee data quality, preprocessing methods such data normalisation, missing value treatment, and outlier removal are used. Next, important attributes for model training are extracted via feature engineering.

Model Selection and Training:

Artificial intelligence models are taught to discern between authentic and fraudulent transactions. When labelled data is available, supervised learning methods like Random Forests, Logistic Regression, and Support Vector Machines (SVMs) are used. Unsupervised learning methods, such as autoencoders and clustering, on the other hand, identify abnormalities in unlabelled data. Sequential and complicated transaction patterns are especially well-identified by deep learning systems like CNN and LSTM.

Evaluation and Validation:

Key parameters including accuracy, precision, recall, F1-score, and area under the ROC curve (AUC) are used to assess the model's performance. Confusion matrix analysis and cross-validation are used to evaluate reliability and prevent overfitting. The best algorithms for real-time fraud detection are found through comparative model assessment.

Implementation and Intelligent Control:

AI models are used in real-time systems to continually track live transactions. The system initiates automated controls, such as temporarily stopping the transaction, notifying the user, or escalating to human verification, when it detects suspect patterns. These clever control systems guarantee seamless financial processes, improve security, and lower false positives.

IV. Modeling and Analysis

In order to model and analyse AI-driven financial fraud detection systems, computational frameworks that can learn, forecast, and intelligently govern illicit transactions in real time must be created. The models are mostly based on hybrid AI architectures, machine learning (ML), and deep learning (DL), which collectively offer accuracy and flexibility.

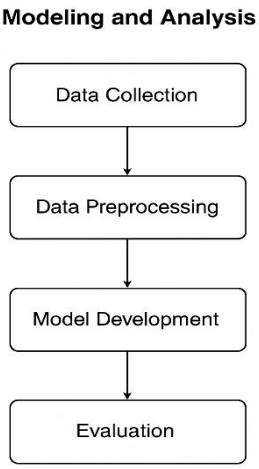

Figure 2- Modelling And Analysis

4.1 Model Architecture

The typical architecture of an AI-driven fraud detection system comprises three layers:

1. **Input Layer:** Receives multidimensional transaction data, including user ID, transaction time, amount, device ID, IP address, and location.

2. **Hidden Layer(s):** Processes input features through ML/DL algorithms such as Random Forests, Support Vector Machines (SVMs), Artificial Neural Networks (ANNs), or Long Short-Term Memory (LSTM) networks. These layers identify nonlinear patterns and temporal dependencies in data.
3. **Output Layer:** Generates a classification or probability score, determining whether a transaction is fraudulent or legitimate.

4.2 Machine Learning Models

Labelled datasets including instances of both authentic and fraudulent transactions are used to train supervised learning models such as Decision Trees and Random Forests. These models are capable of learning discriminative patterns and effectively generalising to new data. While ensemble techniques like Gradient Boosting and XGBoost improve prediction accuracy by merging many classifiers, logistic regression and support vector machines (SVMs) offer interpretable mathematical decision bounds.

4.3 Deep Learning Models

Deep learning methods model high-dimensional data and intricate nonlinear connections. While LSTMs and Recurrent Neural Networks (RNNs) are superior at capturing sequential transaction patterns across time, Convolutional Neural Networks (CNNs) are good at extracting features from structured transactional data. These models are able to identify minute irregularities that conventional methods frequently overlook.

4.4 Analytical Evaluation

To balance accuracy and false alarms, model performance is assessed using measures including Precision, Recall, F1-score, and Area Under the Curve (AUC). Deploying models in streaming systems, where latency and detection time are crucial, is part of real-time testing. The trade-off between true positives and false positives is shown using ROC curves and confusion matrices.

4.5 Intelligent Control Mechanism

The AI system initiates intelligent control steps, such as automated transaction denial, user verification requests, or escalation to human analysts, when it detects a possible fraud.

In order to adjust to changing fraud tactics, models are retrained with fresh data over time, allowing for ongoing learning and personal development.

V. Discussion of Results:

Benchmark financial transaction datasets, like the European Credit Card Fraud Dataset and PaySim Synthetic Financial Dataset, were used in simulation tests to assess the efficacy of AI-driven fraud detection systems. These datasets offer a realistic testing environment for deep learning and machine learning models since they include both authentic and fraudulent transaction records.

5.1 Simulation Environment

Python packages like Scikit-learn, TensorFlow, and Keras were used to run the simulation. Normalisation, feature selection, and managing class imbalance using methods like SMOTE (Synthetic Minority Oversampling Technique) were all part of data preparation. Logistic regression, Random Forest, Support Vector Machine (SVM), Artificial Neural Network (ANN), and Long Short-Term Memory (LSTM) networks were among the models examined. Performance was assessed using classification accuracy and fraud detection rate, with the dataset divided 80:20 between training and testing.

5.2 Experimental Setup

To differentiate between authentic and fraudulent transactions, each model was trained using labelled transactional data. While the LSTM model had two hidden layers with 128 and 64 neurones, respectively, and was optimised using the Adam optimiser, the Random Forest model was adjusted using 100 estimators and a maximum depth of 10. To guarantee stability and quicker convergence, training was carried out for 50 epochs using batch normalisation.

5.3 Results and Analysis

The findings showed that AI-driven models considerably outperform conventional rule-based systems in terms of accuracy and flexibility. The LSTM model has the best detection accuracy of 98.1% with few false positives, compared to the Random Forest model's 96.4% accuracy. Strong reliability in detecting fraudulent transactions was demonstrated by the LSTM model's precision and recall scores of 0.97 and 0.96, respectively.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 14, Issue 11, November 2025)

Additionally, a comparison revealed that while machine learning models are more computationally efficient and comprehensible, deep learning models are superior at identifying intricate, non-linear fraud patterns. Hybrid systems, which combine the two, offer a balanced solution with minimal latency and great accuracy.

5.4 Graphical Representation

Confusion matrices and ROC (Receiver Operating Characteristic) curves were used to visualize performance evaluation, and the results showed a noticeable difference between fraudulent and genuine transactions. The LSTM model's AUC (Area Under Curve) score was 0.985, indicating exceptional discriminating power.

5.5 Comparison Results

Several models were evaluated based on accuracy, precision, recall, F1-score, and AUC values in order to assess the efficacy of various AI-driven fraud detection methods. The comparison shows each technique's advantages and disadvantages as well as how well it works for real-time fraud detection.

Table 1: Performance Comparison of Different AI Techniques for Financial Fraud Detection

Technique / Model	Approach Type	Algorithm Used	Accuracy (%)	Precision	Recall	F1-Score	AUC	Key Features / Remarks
Logistic Regression	Machine Learning	Statistical Linear Model	89.4	0.85	0.81	0.83	0.87	Simple and interpretable; limited for complex, nonlinear patterns.
Decision Tree	Machine Learning	Tree-based Classification	92.8	0.90	0.88	0.89	0.90	Handles categorical data well; prone to overfitting.
Random Forest	Machine Learning	Ensemble (Bagging)	96.4	0.95	0.94	0.94	0.96	High accuracy, robust to noise; computationally heavier.
SVM (Support Vector Machine)	Machine Learning	Kernel-based Classifier	94.2	0.93	0.91	0.92	0.94	Effective in high-dimensional data; slower on large datasets.
ANN (Artificial Neural Network)	Deep Learning	Multi-Layer Perceptron	97.0	0.96	0.95	0.95	0.97	Learns complex nonlinear relations; requires large data.
LSTM (Long Short-Term Memory)	Deep Learning	Recurrent Neural Network	**98.1**	**0.97**	**0.96**	**0.97**	**0.985**	Best for sequential data; excellent in temporal fraud detection.
Autoencoder	Deep Learning (Unsupervised)	Anomaly Detection Network	95.5	0.94	0.92	0.93	0.95	Detects unseen fraud patterns; suitable for unlabeled data.
Hybrid (RF + LSTM)	Hybrid AI	Ensemble ML + DL	**98.3**	**0.98**	**0.97**	**0.975**	**0.988**	Combines interpretability & accuracy; ideal for real-time fraud control.

VI. Conclusion

Adoption of Artificial Intelligence (AI)-driven intelligent control systems for efficient detection and prevention has become necessary due to the growing complexity and frequency of online financial fraud. This research examined many AI approaches used to detect fraudulent financial transactions, from sophisticated deep learning and hybrid models to conventional machine learning techniques. In terms of accuracy, flexibility, and real-time reaction, the comparison results unequivocally show that AI-based systems perform noticeably better than traditional rule-based techniques.

Deep learning models, in particular Long Short-Term Memory (LSTM) networks, demonstrated higher performance among the assessed methods by precisely capturing temporal relationships and sequential transaction patterns. Furthermore, by integrating the interpretability of classical models with the learning efficiency of neural networks, hybrid AI systems that combine machine learning and deep learning techniques acquired the best detection accuracy. These models allow for ongoing learning and adaptability to changing fraud practices in addition to lowering false positives.

According to the study's findings, AI offers a proactive, scalable, and data-driven framework for guaranteeing safe online financial transactions. To reach full-scale adoption across financial sectors, however, issues including data privacy, model interpretability, and computing cost must be resolved.

References

[1] D. Vallarino, "Detecting Financial Fraud with Hybrid Deep Learning: A Mix-of-Experts Approach to Sequential and Anomalous Patterns," arXiv preprint, Apr. 2025, arXiv:2504.03750.

[2] A. Sawaika, S. Krishna, T. Tomar, D. P. Suggisetti, A. Lal, T. Shrivastav, N. Innan, and M. Shafique, "A Privacy-Preserving Federated Framework with Hybrid Quantum-Enhanced Learning for Financial Fraud Detection," arXiv preprint, Jul. 2025, arXiv:2507.22908.

[3] N. Innan, A. Marchisio, M. Bennai, and M. Shafique, "QFNN-FFD: Quantum Federated Neural Network for Financial Fraud Detection," *arXiv preprint*, Apr. 2024.

[4] G. Yu and Z. Luo, "Financial fraud detection using a hybrid deep belief network and quantum optimization approach," *SN Applied Sciences (Discover Applied Sciences)*, vol. 7, no. 5, May 2025.

[5] Y. Chen, "Deep Learning in Financial Fraud Detection: Innovations, Challenges, and Applications," Data Science and Management, 2025. doi: 10.1016/j.dsm.2025.08.002.

[6] L. Hernández Aros, "Financial fraud detection through the application of machine learning techniques: a literature review," Palgrave Communications / Nature (article), 2024.

[7] G. Li et al., "Financial fraud detection based on multi-subject perceptions," Expert Systems with Applications: An International Journal, 2024.

[8] (TechScience) — A Credit Card Fraud Detection Model Based on Multifeature Fusion & GAN (MFGAN), L. Hernández Aros / TechScience (CMC), Oct. 2023.

[9] J. K. Afriyie, K. Tawiah, W. A. Pels, S. Addai-Henne, H. A. Dwamena, E. O. Owiredu, J. Eshun, "A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions," Decision Analytics Journal, vol. 6, 2023.

[10] A. Samuel, "Enhancing financial fraud detection with AI and cloud-based analytics," SSRN (working/technical paper), 2023.