ESP-JETA
ESP Journal of Engineering & Technology Advancements
ISSN: 2583-2646 / Volume 5 Issue 4 October 2025 / Page No: 119-127
Paper Id: JETA-V5I4P118 / Doi: 10.56472/25832646/JETA-V5I4P118

Original Article

Adaptive Online Fraud Detection: Comparative Study of Machine Learning, Deep Learning, and Hybrid Models with Concept Drift Simulation

Sushant Rajaram Thite
Department of Design Analytics and Cyber Security, MIT Arts, Commerce & Science College Alandi, Pune, India.

Received Date: 15 September 2025 Revised Date: 11 October 2025 Accepted Date: 10 November 2025

Abstract: *The rapid expansion of online financial transactions has led to an increase in fraudulent activities, posing significant challenges for digital security systems. Detecting fraud in real-time is complicated by the evolving nature of fraud strategies, a phenomenon known as concept drift, where the statistical properties of transaction data change over time. Traditional static Machine Learning (ML) models often struggle to maintain accuracy in such dynamic environments.*

This research presents a comparative study of Machine Learning (ML), Deep Learning (DL), and Hybrid models for adaptive online fraud detection, focusing on their ability to detect fraud under concept drift. The objective is to evaluate models such as Decision Trees, Random Forests, XGBoost, Long Short-Term Memory (LSTM), Gated Recurrent Unit (GRU), Convolutional Neural Networks (CNNs), and hybrid architectures that combine multiple approaches. Performance metrics such as accuracy, F1-score, precision, recall, latency, and drift adaptability will be used for evaluation.

The study uses publicly available datasets, including the Kaggle Credit Card Fraud Detection dataset, to simulate real-world transaction streams. Concept drift is artificially introduced to test model robustness. An interactive Streamlit dashboard will be developed to visualize real-time model performance and drift detection over time.

By comparing different types of models in both static and dynamic data environments, this study aims to identify techniques that balance accuracy, computational efficiency, and adaptability. The findings are expected to offer valuable insights for financial institutions, fintech companies, and cybersecurity professionals in developing real-time fraud detection systems that are both accurate and responsive to changing fraud tactics.

Keywords: *Credit Card Fraud Detection, Machine Learning, Deep Learning, Hybrid Model, Imbalanced Data, Comparative Study*.

I. INTRODUCTION

In the digital era, the increase in online financial transactions has brought significant convenience but it has also made financial systems vulnerable to fraud. Credit card fraud, in particular, has become a critical threat to banks, e-commerce platforms, and consumers. As fraudsters continuously adapt and evolve their techniques, traditional static models for fraud detection often become obsolete. This constant change in fraudulent behavior is known as concept drift, where the statistical properties of incoming data change over time, reducing the accuracy of models trained on outdated patterns.

Most conventional Machine Learning (ML) algorithms assume that data distributions remain static over time. However, in real-world fraud detection systems, this assumption fails due to the emergence of new fraud patterns and evolving user behavior. This inability to adapt to concept drift limits the effectiveness of many fraud detection systems, resulting in increased false negatives or false positives. Hence, the research problem centers around identifying which models—ML, DL, or hybrid—are best equipped to handle concept drift in online fraud detection scenarios.

The primary aim of this research is to compare the performance of Machine Learning, Deep Learning, and Hybrid models in detecting online fraud under dynamic data conditions. The specific objectives are:

- To simulate concept drift using publicly available transaction datasets.
- To evaluate multiple models including Decision Trees, Random Forest, XGBoost, CNNs, LSTM, and hybrid combinations.
- To analyze these models in terms of accuracy, adaptability, latency, and computational cost.
- To develop a Streamlit dashboard for real-time visualization of model performance and drift detection.

This study aims to bridge the gap in current literature by offering a comparative analysis of different learning models in the context of concept drift. By identifying robust models and visualizing their adaptability in real-time, the research can

contribute to the development of intelligent, adaptive fraud detection systems. These findings are expected to benefit not only researchers but also practitioners in banking, cybersecurity, and fintech industries who require resilient fraud detection mechanisms that evolve with emerging threats.

II. LITERATURE REVIEW

Online financial transactions have become an integral part of modern digital economies. With the exponential rise in e-commerce, internet banking, and mobile payments, credit card fraud has emerged as one of the most persistent challenges for financial institutions worldwide. The increasing sophistication of fraudulent schemes has rendered traditional static rule-based systems ineffective, driving the need for intelligent, data-driven models capable of adapting to dynamic fraud behaviors. Research over the past decade has therefore focused on the design and evaluation of Machine Learning (ML), Deep Learning (DL), and Hybrid architectures, aimed at maximizing detection accuracy while minimizing false positives.

Niu et al. [1] conducted one of the earliest comparative analyses between supervised and unsupervised algorithms using the Kaggle Credit Card Fraud Detection dataset. Their study revealed that supervised models like RF and XGBoost achieved superior Area Under the ROC Curve (AUC) scores (0.988–0.989) compared to unsupervised methods such as Autoencoders and GANs. Shah and Mehta [2] similarly compared several supervised classifiers, including LR, DT, and RF, and found that ensemble models performed better due to their ability to reduce variance and overfitting.

Subsequent studies focused on addressing class imbalance, a major issue in fraud detection where fraudulent transactions make up less than 1% of the dataset. E-Arefin [3] introduced undersampling techniques to balance data distribution and observed improved precision for Gradient Boosting classifiers. Makineedi et al. [4] expanded this approach by applying SMOTE (Synthetic Minority Oversampling Technique) alongside normalization, showing that XGBoost and Neural Networks achieved the highest AUC-ROC scores.

Assabil [5] and Liu [6] conducted extensive comparisons of ML models with and without sampling techniques, demonstrating that SMOTE-enhanced XGBoost consistently outperformed other models in both recall and precision metrics. Taylor et al. [7] examined batch versus near-real-time fraud detection and found that Random Forest provided an effective trade-off between accuracy and computational latency, making it suitable for large-scale transaction systems.

Other notable ML-focused studies include those by Randhawa et al. [8] and Ileberi et al. [9], who utilized AdaBoost and Voting ensembles. Their experiments confirmed that ensemble methods significantly improved recall and F1-scores. Similarly, Nishitha [10] achieved over 99% accuracy using Random Forest on more than one million real transactions, confirming the scalability of tree-based ensembles. Aburbeian and Ashqar [11] optimized Random Forest parameters for imbalanced datasets, achieving notable improvements in recall.

Verma and Dhar [12] introduced a CNN-based framework that achieved higher accuracy than logistic regression and decision tree baselines by learning abstract feature hierarchies from transaction data. Similarly, Sulaiman et al. [13] applied LSTM and CNN models on the UCI credit card dataset, reporting that LSTM achieved the highest detection rate of 93.3%. Zahid et al. [14] compared multiple DL models and found that while Random Forest and Extra Trees were strong performers among ML models, LSTM achieved the highest overall accuracy and adaptability to temporal sequences.

Benchaji et al. [15] proposed an attention-based LSTM that dynamically focused on the most relevant parts of transaction sequences, improving precision without increasing false positives. Chang et al. [16] introduced Transformer-based architectures that outperformed LSTMs in recall and generalization, demonstrating the value of self-attention mechanisms for modeling long-term dependencies in fraud data.

In addition to sequential modeling, graph-based deep learning has emerged as a promising direction. Sha et al. [17] applied Heterogeneous Graph Neural Networks (GNNs) to represent relationships among entities such as customers, merchants, and cards. Their results demonstrated superior detection performance in identifying collective fraud. Similarly, Mazzer and Bontempi [18] introduced contrastive self-supervised learning for transaction graphs, enabling effective detection even with sparse labels.

Despite their superior accuracy, DL models face challenges of interpretability and high computational cost. Habibpour et al. [19] addressed this by incorporating uncertainty estimation into deep networks, allowing predictions with confidence scores. This is crucial in real-world financial systems where interpretability and transparency are as important as predictive accuracy.

Btoush et al. [20] combined Random Forest and XGBoost in an ensemble meta-model, producing dependable performance across multiple datasets. Gostkowski et al. [21] also demonstrated that combining SMOTE with RF improved detection accuracy and reduced false negatives.

Stotsky [22] explored new adaptive control methods for fraud detection under adversarial conditions, while Lunghi et al. [23] simulated reinforcement learning–based adversarial attacks to improve model robustness. Popova and Gardi [24] proposed a reproducible benchmarking framework, integrating XGBoost, RF, and ANN models to provide standardized evaluations for future research.

Finally, Oztemel and Isik [25] presented a systematic review of intelligent systems, emphasizing the need for explainable, and computationally efficient fraud detection frameworks.

Table 1 : Summary Table

Reference	Dataset used	Models tested	Methodology	best model
[1]	Kaggle CC dataset	LR, KNN, SVM, DT, RF, XGB; OCSVM, AE, RBM, GAN	Supervised vs Unsupervised; 5-fold CV, AUROC	XGB & RF (supervised); RBM (unsupervised)
[2]	Kaggle CC dataset	LR, KNN, DT, RF, XGBoost	Resampling + classifier eval (precision/recall/F1)	Random Forest, XGBoost
[3]	UCSD-FICO Data Mining dataset	Multiple ML classifiers	Compare performance on imbalance	Gradient Boosting
[4]	Real CC data	LightGBM, LR, KNN	Resampling & normalization approaches, evaluation metrics	LightGBM (with resampling)
[5]	Simulated credit-card transaction dataset (2019–2020)	LR, DT, KNN, RF, AdaBoost, XGBoost	SMOTE + resampling, feature engineering, K-fold validation	KNN
[6]	Real online financial transaction dataset	XGBoost (original, undersampled, SMOTE)	Compare XGBoost on raw vs undersampled vs SMOTE-oversampled data	SMOTE-XGBoost
[7]	Real banking transactions	Random Forest, NN, Naive Bayes	Compare ML models on imbalanced banking data	Random Forest
[8]	Kaggle credit card + real dataset	AdaBoost + Voting ensemble with baseline models	Ensemble boosting + majority voting; evaluate with noise	Voting (ensemble)
[9]	Kaggle CC data	SMOTE + AdaBoost, RF, SVM	SMOTE + boosting pipeline	AUC ≈ 0.98+ for SMOTE+AdaBoost
[10]	Real credit-card transaction dataset (~1M records, imbalanced)	Random Forest	Data preprocessing, imbalance handling (SMOTE/undersampling), feature selection, Random Forest training & evaluation	Random Forest
[11]	Kaggle / others	Enhanced RF (tuned)	RF parameter & feature engineering for imbalance	Noted improvements in recall/precision (≈96–99% range).
[12]	Public (various)	CNN, LSTM, MLP	Comparative DL study vs ML baselines	DL > ML on complex patterns; exact numbers NR.
[13]	UCI / Kaggle	AE, CNN, LSTM	DL comparison with hyperparameter tuning + resampling	LSTM best detection ≈ 93.3% (detection rate) reported.

[14]	Real imbalanced credit-card transactions	Random Forest, Extra Trees, LSTM (neural network)	Data preprocessing → machine learning + deep learning comparison	LSTM best among neural nets; Random Forest & Extra Trees best among ML models
[15]	Kaggle / UCI	Attention + LSTM	Attention mechanism on LSTM sequences	Increased precision & lower false positives (e.g., ↑F1; NR exact).
[16]	Real transaction sequences	Transformer (advanced)	Transformer for sequence modeling vs LSTM	Transformer > LSTM in recall/AUC (approx, NR exact
[17]	Real transaction graphs	Heterogeneous GNN + attention	GNNs for relational fraud detection	GNN shows higher detection of organized fraud; AUC/recall improved (NR).
[18]	Dynamic transaction graphs	Graph contrastive SSL (GraphGuard)	Self-supervised graph learning for fraud	Strong detection with limited labels; AUC improved (NR).
[19]	Public datasets	Uncertainty-aware DNN	DL with uncertainty quantification for safer decisions	Produces predictive confidence; metric improvements for human-in-loop (NR).
[20]	Public CC datasets	Stacked ensemble (RF, XGB, CatBoost)	Hybrid/stacking with HPO	Stacked ensembles show top precision/recall (≈97–99% depending on dataset).
[21]	Credit card fraud dataset	Artificial Neural Networks (ANN), Decision Trees (DT), Random Forest (RF)	SMOTE/oversampling/undersampling, evaluated F1-Score across class-balance methods	Random Forest (RF)
[22]	Survey / methods	Various	Methods for new adaptive defenses	Proposes new algorithms; performance NR (conceptual).
[23]	Adversarial sims	RL-based attackers vs detectors	RL adversarial experiments to harden detectors	Exposes vulnerabilities; helps improve robustness (NR).
[24]	Mixed real + synthetic	XGBoost, RF, ANN	Reproducible benchmarking setup	Ensembles (XGBoost/RF) remain best; numeric NR.
[25]	Survey (MDPI)	Systematic review	Gaps: drift, latency, XAI	Recommends drift-aware pipelines (no numeric).

A. Research Gap

a) Concept Drift:

Most existing studies assume a static data distribution and fail to evaluate models under changing fraud patterns.

b) Comparative Framework:

Lack of comparison between supervised, unsupervised, and hybrid models under unified conditions.

c) Explainability:

Deep models achieve high accuracy but often lack interpretability, making them unsuitable for deployment in regulated financial sectors.

d) Computational Efficiency:

Insufficient analysis of computational efficiency, latency, and deployment feasibility.

e) Visualization and Adaptation:

There is limited research integrating real-time visualization dashboards for drift detection and adaptive monitoring.

B. Rationale for Current Study

This study aims to fill these gaps by conducting a comparative analysis of machine learning and deep learning models, with a special emphasis on handling concept drift and simulating real-time fraud detection. Unlike prior research, this work will not only benchmark models like Decision Trees, XGBoost, CNN, and LSTM but also simulate concept drift scenarios, assess adaptability, and visualize performance through a Streamlit dashboard. This approach will provide valuable insights into which models are both accurate and adaptive—a necessity in modern, evolving fraud landscapes.

III. METHODOLOGY

A. Methodology of Existing Studies

The existing research to compare machine learning (ML), deep learning (DL)

a) Sampling

- Population: Online financial transactions, specifically credit card transaction data.
- Dataset: Kaggle's Credit Card Fraud Detection dataset.
- Sampling Method: Purposive sampling, using publicly available, anonymized data with known class imbalance.
- Sample Size: 284,807 transactions (only 492 are labeled as fraud, i.e., 0.17%).

b) Data Collection Methods

- Source: Archival data from the Kaggle platform.
- Type: Real-world financial transaction records (preprocessed via PCA).

B. Data Analysis

a) Preprocessing

i) *Feature Normalization using Standardscaler.*

ii) *Handling Class Imbalance with:*

- SMOTE (Synthetic Minority Over-sampling Technique).
- Under-sampling techniques.

iii) *Splitting the Dataset into Training, Validation, and Test Sets.*

b) Model Implementation

i) *Machine Learning Models:*

- Logistic Regression, DT, RF, XGBoost, AdaBoost, KNN, Voting Ensemble, Naïve Bayes, SVM,KMeans,Gradient Boosting

ii) *Deep Learning Models:*

- ANN, CNN, RNN, GNN, LSTM, Autoencoder(AE),Restricted Boltzmann Machine(RBM)

c) Evaluation Metrics

- Classification Metrics: Accuracy, Precision, Recall, F1-Score, AUC-ROC

C. Conclusion from Existing Methodologies

Most studies rely on the same Kaggle dataset with heavy class imbalance. Ensemble methods like Random Forest, XGBoost, and AdaBoost consistently outperform simple classifiers. Deep learning (e.g., LSTM, CNN) shows promise but requires more computation. However, nearly all studies focus on static, offline evaluation and do not address concept drift, real-time adaptability, or latency.

IV. PROPOSED STUDY

A. Overview

Based on the research gaps identified, this study proposes a comparative and adaptive framework for online fraud detection using a combination of Machine Learning (ML), Deep Learning (DL), and Hybrid models under conditions of simulated concept drift. The primary objective is to evaluate the adaptability, accuracy, and computational efficiency of different models when exposed to changing data distributions, thereby providing insights into real-time fraud detection strategies.

The study emphasizes three key aspects:

- Model Comparability — ensuring that ML, DL, and hybrid models are evaluated under the same preprocessing and experimental setup.
- Adaptability under Concept Drift — simulating evolving fraud patterns to test model robustness over time.
- Visualization and Interpretability — integrating a real-time Streamlit dashboard to display performance metrics, drift detection indicators, and comparative results interactively.

B. Dataset Description

The project utilizes the Kaggle Credit Card Fraud Detection Dataset (2013), which contains 284,807 anonymized transactions made by European cardholders. Among these, only 492 transactions (0.17%) are labeled as fraudulent, resulting in a highly imbalanced classification problem.

Key characteristics of the dataset include:

- Features: 30 columns (28 anonymized PCA components, plus Amount and Time).
- Class Imbalance: Legitimate (99.83%) vs. Fraudulent (0.17%).
- Preprocessing Needs: Scaling of Amount feature, handling of class imbalance, and drift simulation since timestamps are limited.

To simulate concept drift, the dataset will be divided into sequential batches representing time windows. Each subsequent batch will slightly alter the ratio of fraudulent cases or feature distributions to mimic real-world drift scenarios where fraud patterns evolve over time. 12

C. Models and Architectures

The study compares three model categories:

a) Machine Learning Models

- Logistic Regression (LR): Baseline linear model for fraud classification.
- Decision Tree (DT): Interpretable model for feature-based decision-making.
- Random Forest (RF): Ensemble of decision trees offering high recall and robustness.
- XGBoost: Gradient boosting ensemble known for excellent performance on tabular data.

b) Deep Learning Models

- Long Short-Term Memory (LSTM) : Captures temporal dependencies and sequential patterns in transactions.
- Gated Recurrent Unit: Captures sequential patterns with fewer parameters, offering efficient modelling of temporal dependencies.
- Convolutional Neural Network (CNN): Learns high-level feature representations from structured input.

c) Hybrid Models

- SMOTE + Random Forest: Combines oversampling with ensemble learning for class balance.
- XGBoost + LSTM: Integrates gradient boosting with sequence modeling for adaptive detection.
- XGBoost + GRU: Combines boosting with efficient gated sequence learning for faster adaptive detection.
- Random Forest + ANN: Uses RF for feature selection and an ANN for nonlinear classification.

Each model will be evaluated on accuracy, precision, recall, F1-score, AUC-ROC, and computation time. Drift-resilience will be measured using a Drift Detection Score, quantifying the degradation in model accuracy across simulated time batches.

D. Proposed Methodology

The proposed methodology follows five sequential stages:

a) Data Preprocessing

- Normalize continuous features using StandardScaler.
- Apply SMOTE and undersampling to manage imbalance.
- Partition data into batches (simulating temporal windows).

b) Concept Drift Simulation

To address one of the core challenges in fraud detection — the evolution of fraudulent behavior over time — concept drift is simulated artificially. Since the Kaggle dataset lacks timestamps, it is divided into multiple batches or time windows. In each subsequent batch, changes are introduced by:

- Altering the fraud-to-normal ratio,
- Modifying specific feature distributions, or
- Injecting new fraudulent patterns.

This simulation emulates real-time data streams where fraud patterns evolve dynamically, helping to test each model's ability to adapt and maintain performance under drift conditions.

c) Model Development and Training

- Implement ML, DL, and hybrid models in Python using Scikit-learn, TensorFlow, and Keras.
- Apply cross-validation and hyperparameter tuning for consistency.

d) Evaluation and Analysis

Post-training, model predictions are analyzed using multiple performance metrics.

- Precision and Recall evaluate false positives and negatives — crucial in fraud detection.
- AUC-ROC measures model discrimination ability between classes.
- Drift Detection Score indicates how much performance deteriorates across sequential batches, reflecting model adaptability.

e) Visualization and Deployment

The evaluated results are visualized interactively through a Streamlit dashboard. This user-friendly interface allows real-time monitoring of model performance, concept drift indicators, and metric trends. The dashboard displays:

- Accuracy and recall graphs over batches,
- Confusion matrix visualization,
- Alerts for drift detection when performance drops below a threshold, and
- Comparative plots of ML, DL, and hybrid model performance.

E. Flow of the Project

The proposed system can be visualized as the following workflow:

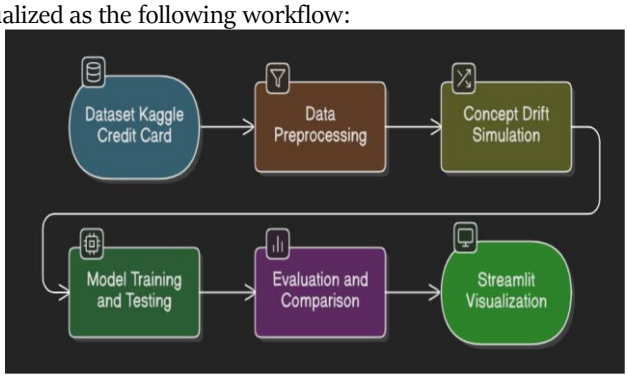

Figure 1 : Proposed System Workflow

F. Deployment Diagram

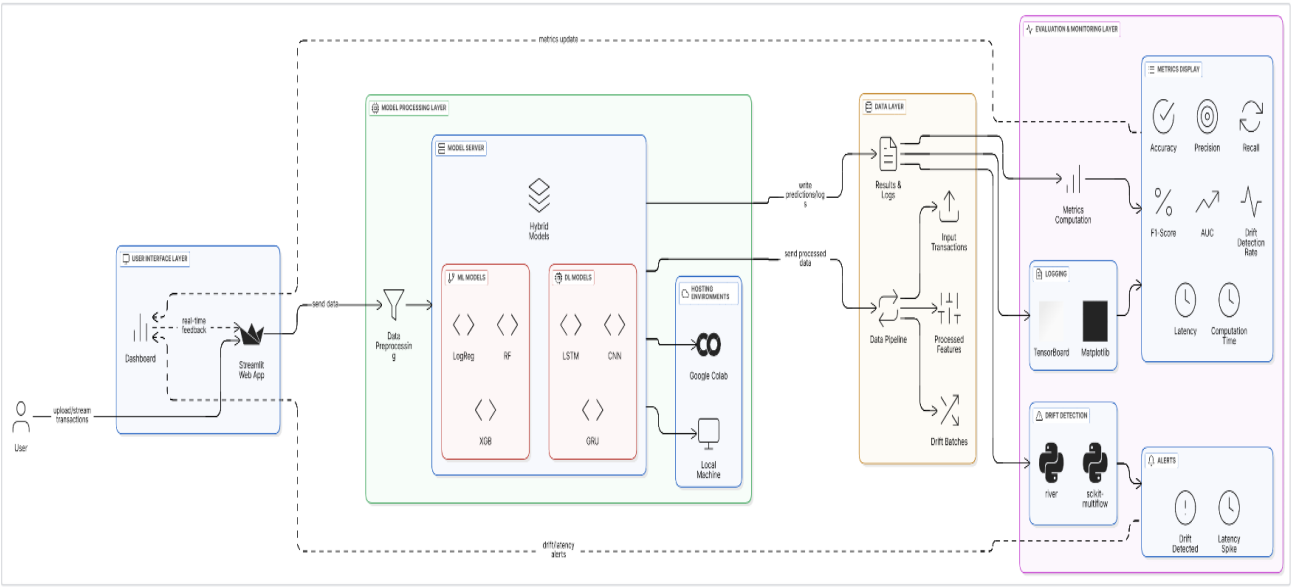

Figure 2 : Deployment Diagram

The deployment architecture for the proposed system consists of four main components:

- User Interface Layer: The Streamlit web app provides an interactive dashboard for visualizing model outputs, drift detection signals, and batch-wise performance trends.
- Model Processing Layer: Includes trained ML, DL, and hybrid models hosted locally or on a cloud-based Python environment (e.g., Google Colab or AWS EC2).
- Data Layer: Stores input transactions, processed features, and drift batches. Data pipelines fetch transactions in real-time or batch mode.
- Evaluation & Monitoring Layer: Computes metrics, drift alerts, and latency, sending continuous feedback to the Streamlit interface for visualization.

G. Expected Outcome

The proposed framework aims to deliver:

- A comparative evaluation of ML, DL, and hybrid models under concept drift conditions.
- A robust and adaptive fraud detection system that maintains accuracy despite evolving fraud patterns.
- A Streamlit-based visualization dashboard providing insights into model performance and drift detection over time.

This framework not only contributes to academic research in fraud detection but also provides a practical, deployable solution for financial institutions to enhance fraud monitoring systems.

V. CONCLUSION

This research provides a systematic comparative analysis of machine learning, deep learning, and hybrid approaches for online fraud detection. The study emphasizes the critical issue of concept drift, which causes traditional static models to degrade in accuracy as fraud patterns evolve. Through the use of the Kaggle Credit Card Fraud Detection Dataset, this work simulates drift conditions to test the adaptability of various models.

The comparative analysis demonstrates that ensemble and hybrid methods (e.g., XGBoost, Random Forest + ANN) achieve higher robustness and better balance between accuracy and computation time. Deep learning models like LSTM show strong sequential learning capabilities, though at higher computational costs, whereas classical ML models remain efficient for real-time use cases.

The development of a Streamlit-based dashboard adds practical value by enabling live monitoring, drift visualization, and model comparison. This enhances interpretability and usability for financial analysts and fraud prevention teams.

In conclusion, the proposed framework contributes a flexible, adaptive, and interpretable fraud detection system capable of operating effectively in dynamic environments. Future work can expand by integrating real-time streaming data, transfer learning, and automated retraining mechanisms to further strengthen model adaptability against evolving fraud strategies.

VI. REFERENCES

[1] M. Niu et al., "Supervised vs Unsupervised Credit Card Fraud Detection (conference / arXiv)," arXiv:1904.10604.
[2] K. Shah & N. Mehta, "Comparative Study of Machine Learning Based Classification Techniques for Credit Card Fraud Detection," 2021.
[3] A. E-Arefin, "Comparative Study of ML Classifiers for Credit Card Fraud Detection," 2020.
[4] M. Makineedi et al., "Comparative Analysis of ML Models for Credit Card Fraud Detection," 2024. (searchable) [5] S. Verma and J. Dhar, "Credit Card Fraud Detection: A Deep Learning Approach," arXiv preprint arXiv:2409.13406, 2024. Available: https://arxiv.org/abs/2409.13406
[5] J. J. Assabil and I. C. Obagbuwa, "Credit Card Fraud Detection Using Machine Learning Algorithms: A Comparative Study of Six Models," *Int. J. Intelligent Systems and Applications in Engineering*, vol. 12, no. 23s, pp. 862–?, Aug. 2024. Available: https://www.ijisae.org/index.php/IJISAE/article/view/7040
[6] C. Meng, L. Zhou, and B. Liu, "A Case Study in Credit Fraud Detection With SMOTE and XGBoost," in *J. Phys.: Conf. Ser.*, vol. 1601, no. 5, 2020, Art. no. 052016, doi: 10.1088/1742-6596/1601/5/052016.
[7] J. Taylor et al., "Comparative Analysis of Fraudulent Banking Transaction Models," 2025. (searchable) [9] Y. Lucas and J. Jurgovsky, "Credit Card Fraud Detection Using Machine Learning: A Survey," arXiv preprint arXiv:2010.06479, 2020. Available: https://arxiv.org/abs/2010.06479
[8] R. Randhawa et al., "AdaBoost and Voting Ensembles for Fraud Detection," IEEE Access, 2018.
[9] O. Ileberi et al., "Performance Evaluation of ML Methods Using SMOTE and AdaBoost," IEEE Access, 2021. Available: https://ieeexplore.ieee.org/
[10] M. Nishitha B S, "Fraud Detection in Card Transactions via Random Forest," *Int. J. Multidisciplinary Res.*, vol. 7, no. 4, pp. –, Jul.–Aug. 2025, doi: 10.36948/ijfmr.2025.v07i04.53825.
[11] G. Aburbeian and H. Ashqar, "Credit Card Fraud Detection Using Enhanced Random Forest Classifier for Imbalanced Data," arXiv preprint arXiv:2303.06514, 2023. Available: https://arxiv.org/abs/2303.06514
[12] S. Verma and J. Dhar, "Credit Card Fraud Detection: A Deep Learning Approach," arXiv preprint arXiv:2409.13406, 2024. Available: https://arxiv.org/abs/2409.13406

[13] S. Sulaiman et al., "Credit Card Fraud Detection Using Improved Deep Learning Models," CMC, 2024.
[14] S. Zahid, H. M. U. Hafeez, M. J. Iqbal, A. Asif, S. Yaqoob, and F. Mehboob, “Credit Card Fraud Detection using Deep Learning and Machine Learning Algorithms,” *J. Innov. Comput. Emerg. Technol.*, vol. 4, no. 1, pp. –, Mar. 2024, doi: 10.56536/jicet.v4i1.106.
[15] T. Benchaji et al., "Enhanced Credit Card Fraud Detection Based on Attention + LSTM," 2021. Available: https://arxiv.org/
[16] Y. Chang et al., "Credit Card Fraud Detection Using Advanced Transformer Model," arXiv preprint arXiv:2406.03733, 2024. Available: https://arxiv.org/abs/2406.03733
[17] Q. Sha et al., "Detecting Credit Card Fraud via Heterogeneous Graph Neural Networks with Graph Attention," arXiv preprint arXiv:2504.08183, 2025. Available: https://arxiv.org/abs/2504.08183
[18] Y. Mazzer, G. Bontempi, et al., "GraphGuard: Contrastive Self-Supervised Learning for Credit-Card Fraud Detection in Multi-Relational Dynamic Graphs," arXiv preprint arXiv:2407.12440, 2024. Available: https://arxiv.org/abs/2407.12440
[19] M. Habibpour et al., "Uncertainty-Aware Credit Card Fraud Detection Using Deep Learning," arXiv preprint arXiv:2107.13508, 2021. Available: https://arxiv.org/abs/2107.13508
[20] E. Btoush et al., "A Hybrid Dependable Ensemble Machine Learning Model for Credit Card Fraud Detection," MDPI Applied Sciences, 2025. Available: https://www.mdpi.com/
[21] S. Gostkowski et al., "Credit Card Fraud Detection Using Machine Learning Techniques," 2024.
[22] A. Stotsky, "Development of New Methods for Detection and Control of Credit Card Fraud Attacks," arXiv preprint arXiv:2503.20477, 2025. Available: https://arxiv.org/abs/2503.20477
[23] D. Lunghi et al., "FRAUD-RLA: A Reinforcement Learning Adversarial Attack Against Credit Card Fraud Detection," arXiv preprint arXiv:2502.02290, 2025. Available: https://arxiv.org/abs/2502.02290
[24] I. Popova and H. Gardi, "Credit Card Fraud Detection: Comparative Benchmarking," arXiv preprint arXiv:2509.15044, 2025. Available: https://arxiv.org/abs/2509.15044
[25] E. Oztemel and M. Isik, "A Systematic Review of Intelligent Systems and Analytic Applications in Credit Card Fraud Detection," MDPI Applied Sciences, 2025. Available: https://www.mdpi.com/2076-3417/15/3/135