International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Adaptive Credit Card Fraud Detection Using MLOps with Real-Time Drift Detection

L. Sri Manvitha Reddy[1], Mandhadi Snehalatha[2], N. Musrat Sultana[3]

[1,2]Student, Department of Computer Science and Engineering, Mahatma Gandhi Institute of Technology, Gandipet, India.
[3]Assistant Professor, Department of Computer Science and Engineering, Mahatma Gandhi Institute of Technology, Gandipet, India.

Abstract
Credit card fraud is such a big deal these days, especially with everyone shopping online all the time. I mean, people pull out their cards for just about anything, from groceries to random stuff on apps, and that opens the door for shady things to happen without much notice. The old machine learning methods that companies relied on, they just arent cutting it anymore. Fraudsters are always changing how they operate, switching tactics before the systems can catch on. It seems like over time, those setups let more slip by, missing stuff that should be obvious. We try to fix that by blending machine learning with MLOps, you know, to monitor everything in real time sort of. First off, we train a few simple models using the data thats around, and then choose one that performs decently, I guess. Once thats done, it gets deployed to scan actual transactions as they come in, flagging anything that looks off. That part about keeping an eye constantly, it feels important because the fraud keeps evolving. Some people might think basic models are enough, but I am not totally sure, this way seems better for staying ahead.

Keywords: Credit Card Fraud Detection, MLOps, Concept Drift, Model Monitoring, Data Imbalance Handling, Classification Algorithm

1. Introduction

The expansion of payment systems and e-commerce websites has led to increased international financial transactions. Credit card fraud has become a concern for financial institutions leading to big financial losses and security risks. The volume of daily transactions exceeds manual fraud detection capability which requires development of automated fraud detection systems. Machine learning techniques have been widely adopted for fraud detection because they can learn patterns from historical transaction data. The models enable organizations to identify legitimate transactions and fraudulent activities which leads to better detection results while saving operational resources. Fraud detection systems face their main obstacle because fraudsters develop new techniques to avoid detection which makes existing training models less powerful with time.

Concept drift describes how shifts in data characteristics make static machine learning systems less effective because it creates new challenges for their performance. The inability of traditional models to adapt after training on fixed datasets results in detection failures and incorrect predictions. The implementation of Machine Learning Operations in modern fraud detection systems exists to address the operational challenges which exist in their current frameworks. MLOps enables organizations to manage

machine learning models through integration and deployment while monitoring their performance and conducting retraining processes. MLOps enables machine learning model development through automation which provides organizations with better scalability and system reliability and organizational flexibility.

The system presents a real-time credit card fraud detection system that uses Machine Learning integrated with MLOps pipelines. The system performs three essential functions by training models through transaction data which it uses to deploy the best model for predicting fraud in real time while it tracks model performance to maintain system accuracy and scalability and system reliability.

This approach enables financial institutions to quickly detect fraudulent transactions which helps them decrease financial losses while their customers gain better security through automated model retraining and monitoring and deployment workflows.

2. Literature Survey

Credit card fraud detection has been a critical area of research due to the rapid growth of digital transactions and the increasing sophistication of fraudulent activities. Over the years, researchers have explored a wide range of techniques, including statistical methods, machine learning algorithms, deep learning models, and more recently, MLOps-driven adaptive systems.

One of the fundamental challenges in credit card fraud detection is the class imbalance problem, where fraudulent transactions constitute only a small fraction of the overall dataset. Btoush *et al.* [1] conducted a comprehensive study on various resampling techniques for handling imbalanced datasets. Their work demonstrated that methods such as Synthetic Minority Oversampling Technique (SMOTE) and under sampling significantly improve classification performance by balancing the dataset. Similarly, Li [7] emphasized the importance of incorporating data balancing strategies alongside machine learning models to enhance detection accuracy and reduce bias toward majority classes. These studies highlight that preprocessing plays a crucial role in improving fraud detection systems.

In addition to preprocessing techniques, several studies have focused on evaluating and comparing different machine learning models. Zhang [6] analysed the performance of commonly used algorithms such as Decision Trees, Logistic Regression, and Support Vector Machines for fraud detection, concluding that model selection significantly impacts detection performance. Alrasheedi [4] extended this work by conducting a comparative study of multiple Machine learning models, showing that ensemble methods, such as Random Forest and Gradient Boosting, generally outperform individual classifiers due to their ability to capture complex data patterns and reduce overfitting.

Recent advancements have introduced deep learning-based approaches to further improve fraud detection accuracy. Abdullah *et al.* [3] proposed a hybrid framework combining synthetic oversampling, autoencoders, convolutional neural networks (CNNs), and attention mechanisms. This approach effectively captures both linear and non-linear relationships in transaction data, leading to improved detection of complex fraud patterns. Hafez *et al.* [5] provided a systematic review of AI-enhanced fraud detection techniques, highlighting the growing importance of deep learning models in handling large-scale and high-dimensional datasets. These studies demonstrate that deep learning techniques offer significant improvements but often require high computational resources and large volumes of labelled data.

Apart from supervised learning, researchers have also explored unsupervised and anomaly detection approaches to detect previously unseen fraud patterns. Jiang *et al.* [11] introduced an unsupervised attentional anomaly detection network capable of identifying fraudulent transactions without relying on

labelled data. This approach is particularly useful in real-world scenarios where labelled fraud data is limited or constantly evolving. Earlier work by Niu *et al.* [14] compared supervised and unsupervised techniques, highlighting that while supervised models generally achieve higher accuracy, unsupervised methods provide better adaptability to new and unknown fraud patterns.

A major limitation of many existing fraud detection systems is their inability to handle dynamic changes in data, commonly referred to as concept drift. Fraud patterns continuously evolve as attackers adopt new strategies, leading to a mismatch between training data and real-time data. Kraus and van der Aa [9] explored machine learning-based approaches for detecting concept drift in dynamic systems, emphasizing the need for continuous monitoring. Hovakimyan and Bravo [10] conducted a systematic review of concept drift detection techniques, categorizing them into statistical, window-based, and ensemble-based methods. Furthermore, Bayram *et al.* [12] discussed performance-aware drift detection mechanisms that monitor model degradation and trigger corrective actions, such as retraining. These studies highlight that addressing concept drift is essential for maintaining long-term model performance.

With the increasing deployment of machine learning systems in real-world applications, the focus has shifted toward integrating Machine Learning Operations (MLOps) practices. Berberi *et al.* [8] provided an extensive overview of MLOps platforms and tools, emphasizing their role in automating the machine learning lifecycle, including deployment, monitoring, versioning, and retraining. MLOps ensures that models remain scalable, reliable, and continuously updated in production environments. In the context of fraud detection, Hafez *et al.* [5] highlighted the importance of combining AI techniques with operational pipelines to achieve robust and production-ready systems.

Earlier foundational studies, such as Chaudhary *et al.* [15] and Sulaiman *et al.* [13], provided comprehensive reviews of traditional fraud detection techniques, including rule-based systems and basic machine learning models. These works laid the groundwork for modern approaches but also identified limitations such as lack of adaptability and high false positive rates. Over time, research has evolved toward more intelligent and adaptive systems capable of handling real-world challenges.

Despite significant advancements in machine learning and fraud detection techniques, most existing systems still rely on static models trained on historical data. These models often fail to adapt to evolving fraud patterns, leading to performance degradation over time. Additionally, many studies focus primarily on model accuracy without addressing deployment, monitoring, and lifecycle management challenges.

Therefore, there is a clear need for an integrated approach that combines machine learning with MLOps practices to enable real-time fraud detection, continuous monitoring, and automatic model adaptation. The proposed system in this paper aims to address these gaps by incorporating streaming data processing, concept drift detection, and automated retraining within an MLOps framework.

3. Problem definition

The ongoing development of new fraudulent transaction methods creates a significant obstacle for credit card fraud detection in contemporary digital payment systems. The accuracy of traditional machine learning models decreases when new fraud patterns emerge because these models rely on historical data for their training. Static fraud detection systems become ineffective in active financial markets because they suffer from a problem called concept drift. The project will create an adaptive credit card fraud detection system which detects fraudulent transactions and uses drift detection methods to identify changes in transaction patterns and automatically trains itself with fresh data to sustain accurate fraud detection results.

4. Proposed System

The proposed system developed for detecting credit card fraud in real time uses machine learning together with MLOps methods to combat changing fraud patterns. The system operates continuously to track transactions while it automatically updates itself when its performance standards begin to decline which differs from conventional systems that maintain their initial trained state. The dataset consists of two parts which include a streaming dataset that mimics live transactions and a baseline dataset which the system uses for model development. XGBoost was selected as the machine learning model because it demonstrates better performance in detecting fraud. The final model is one of models that were tested. The trained model processes every transaction during the streaming phase to identify fraudulent activities. The system collects essential monitoring data that includes the timestamp, prediction, probability, actual label and model version together with its predictions.

5. Design Methodology

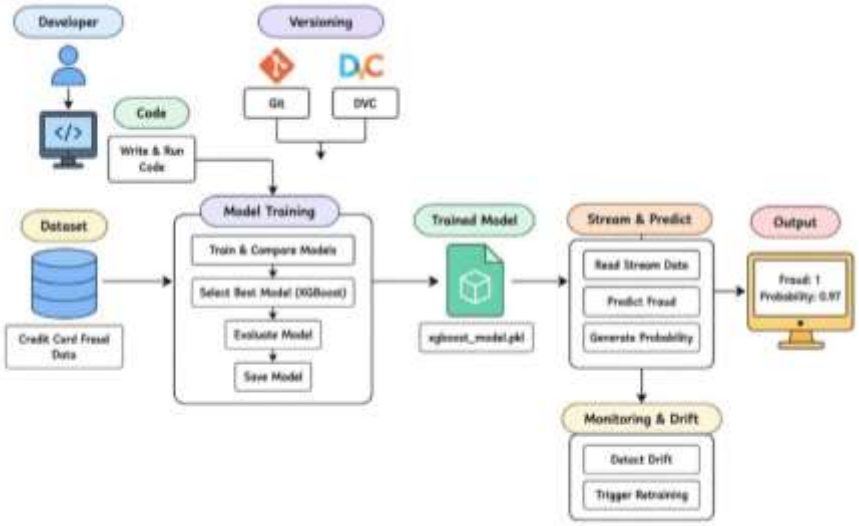

Figure 1: System Architecture of Adaptive Credit Card Fraud Detection with Real-Time Drift Detection

The Adaptive Credit Card Fraud Detection system uses machine learning and drift detection techniques to detect fraudulent transactions while its fraud detection system evolves through machine learning. The methodology consists of multiple stages including data preparation, model training, stream simulation, drift detection, automatic retraining, and version control.

The credit card transaction dataset goes through its initial stage which involves data collection and subsequent processing. The dataset is then divided into two parts: baseline data and streaming data. The baseline dataset serves as the training data for multiple machine learning models while the streaming dataset simulates actual transaction activity.

The researchers trained and assessed four machine learning models which included Logistic Regression Random Forest XGBoost and SGD Classifier using precision metrics and recall metrics and F1-score metrics and confusion matrix metrics and ROC-AUC metrics. The evaluation results show that XGBoost produces balanced classification results which led to its selection as the final fraud detection model.The streaming transactions reach the XGBoost model through the stream simulation module after the system

enters its operational phase. The system assesses every transaction to determine whether it should be marked as fraudulent or authentic.

The system achieves adaptability through drift detection which continuously compares statistical distribution patterns in incoming stream data against the baseline training data.The system detects a pattern shift when it discovers that the actual data distribution has deviated from baseline reference patterns.

The automatic retraining module initiates model retraining after it detects drift by merging updated transaction information with current dataset contents. This system enables the detection of new fraud patterns while sustaining its forecasting accuracy throughout different time periods. The entire pipeline uses Git and GitHub and DVC for management purposes which guarantees operational control of the complete data pipeline system.

5.1 Dataset Preparation

The European credit card transaction dataset is divided into two parts to simulate a real-time fraud detection environment. The baseline dataset (40%) is used for initial model training, while the streaming dataset (60%) is used to simulate incoming real-time transactions. Let the dataset be represented as:

$$D = \{(x_i, y_i)\}_{i=1}^{N}$$

where $x_i$represents transaction features and $y_i$represents the transaction label. The dataset is divided as:

$$D_{baseline} = 40\%\ of\ D$$
$$D_{stream} = 60\%\ of\ D$$

5.2 Model Training and Selection

Various different fraud detection models were tested against baseline data (Logistic Regression, Random Forest, and XGBoost) to discover which model performed best. The models were evaluated to determine: Accuracy, Precision, Recall, and F1-score. The ultimate selected model was XGBoost as it produced the best performing balanced fraud detection results.

5.3 Real-Time Streaming Simulation

In order to simulate an actual production environment for this analysis, the streaming data will have its transactions processed serially, in the same way as if they were being evaluated by the fraud detection algorithm in real time. Thus, each transaction will be processed in the following way:

$x_t \rightarrow \mathrm{f}\,(x_t) \rightarrow \hat{y}_t$

Where:

- x_t= incoming transaction
- $f(x_t)$= prediction function of the trained model
- $\hat{y}_t$= predicted transaction label

At each event the system will store a number of key attributes about each transaction which include the following information: timestamp, prediction results, probability of fraud, actual transaction label, and model version. These attributes will allow for continued monitoring and analysis of the system's performance over time.

5.4 Drift Detection and Adaptive Learning

A key challenge in fraud detection systems is the presence of drift, where the statistical properties of data change over time. In this work, two types of drift are addressed: concept drift and feature drift.

Concept Drift Detection (Prediction Drift)

Changes to the relationship between input features and target variables are referred to as Concept Drift. Fraud Detection is an example of where concept drift occurs as the patterns used to identify fraud may change over time due to new tactics being utilised by fraudsters. To detect drift the system is constantly

monitoring how well the model's predictions are performing. Each new transaction is checked against its actual label (ie whether it was a true or false positive) and assigned a corresponding error value: 0 (for correct prediction) or 1 (for an incorrect prediction). These error values are then aggregated into an ongoing stream of values that reflect how well the model has performed over time. A significant change in the distribution of error values will indicate a potential inability of the model to correctly represent the underlying data. The system uses an adaptive rule-based statistical process (ADWIN) that employs a "sliding window" technique to maintain a recent history of observed errors. The size of the "window" containing observations is automatically calculated in order to find any changes in the mean of the error values. When the difference between the error means of the two time segments exceed a set threshold then an indication of drift will occur.

Feature Drift Detection (Data Drift)

A "distribution shift" can refer to either a shift in predictive performance (i.e., a change in how well your model predicts an outcome) or to a shift in the input data itself. This latter concept, also known as covariate shift, happens whenever the distribution of your input variables changes over time. Importantly, even as these distributions change, the relationship between your inputs and outputs may remain unchanged.

The system compares the distribution of features in your baseline dataset to a recent subset of the same features in your streaming data. Since a single metric does not suffice, it applies a statistical test on each individual feature to determine if its distribution has shifted, statistically speaking, significantly.

The Population Stability Index (PSI) is a common way to measure such differences in distributions. It measures the difference between two probability distributions by determining the proportion of observations falling into predetermined buckets in the baseline and current datasets.

The PSI value is calculated as:

$$PSI = \sum(P_i - Q_i) \cdot \ln\left(\frac{P_i}{Q_i}\right)$$

where $P_i$represents the proportion of observations in bin $i$for the baseline data, and $Q_i$represents the corresponding proportion for the current data.

Higher PSI values indicate a larger deviation between distributions, suggesting significant drift. In practice, PSI values above a certain threshold indicate that the feature has experienced substantial change.

5.5 Automated Model Retraining and Versioning

When drifts occur, the system begins a process of retraining automatically on a new data set that combines both the original set of baseline data and the portion of streaming data that was gathered prior to detecting the drift. This allows for the newly trained model to utilize both old and new patterns in training.

The new, retrained model will replace the old model and become the next version of the model. The model is kept tracked in terms of model versions to allow tracking of the evolution of the model over time as well as to allow for reproducibility of the models created. Each model version reflects the state of the data at the time of retraining and shows how the model changed due to the new way of committing fraud.

The automated retraining mechanism allows the system to produce a stable output without needing someone to do this manually, which means it can be used in real-life situations where it would need to be used.

5.6 Monitoring and Visualization

The tool collects prediction and logging results and stores them for continuous tracking of system's behavior and identification of drifts, while the collected data could be used later for visualizations and analytics.

Visualization tools offer insights on model performance tendencies and errors over time, as well as the occurrence of drift. Also, drift reports generated by the statistical monitoring tools are capable of showing the tendency in feature distributions, serving as a useful document to identify the root cause of drift and guide future optimizations.

6. Results And Discussion

6.1 Experimental Results

The algorithm was tested using a dataset for detecting the fraudulently use of a credit card. This dataset contains two type of transaction either it is legitimate or fraudulent. Due to the imbalanced dataset, different set of metric were used such as Accuracy, Precision, Recall, F1-score.

Table 1: Performance Comparison of Models

Model	ROC-AUC	Precision	Recall	F1-Score
Logistic Regression	0.96	0.08	0.92	0.14
Random Forest	0.95	0.93	0.81	0.87
XGBoost (Proposed)	0.95	0.91	0.83	0.84

The overall performances of our algorithm have been compared with previous models such as XGBoost, Logistic Regression and Random Forest and performance were evaluated.

6.2 Confusion Matrix Analysis

The confusion matrices below display how the classification performance of each model is made up of true positives, true negatives, false positives and false negatives, using Logistic Regression, a Random Forest and the XGBoost model.

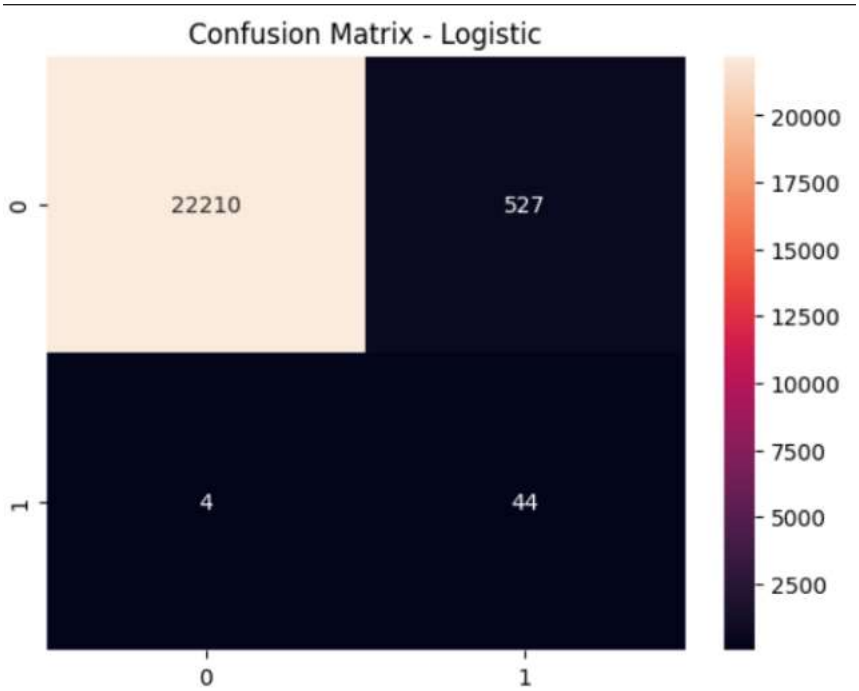

Figure 2: Confusion Matrix of Logistic Regression

Figure 2 shows that Logistic Regression correctly classifies most normal transactions but has higher false negatives, indicating missed fraud cases.

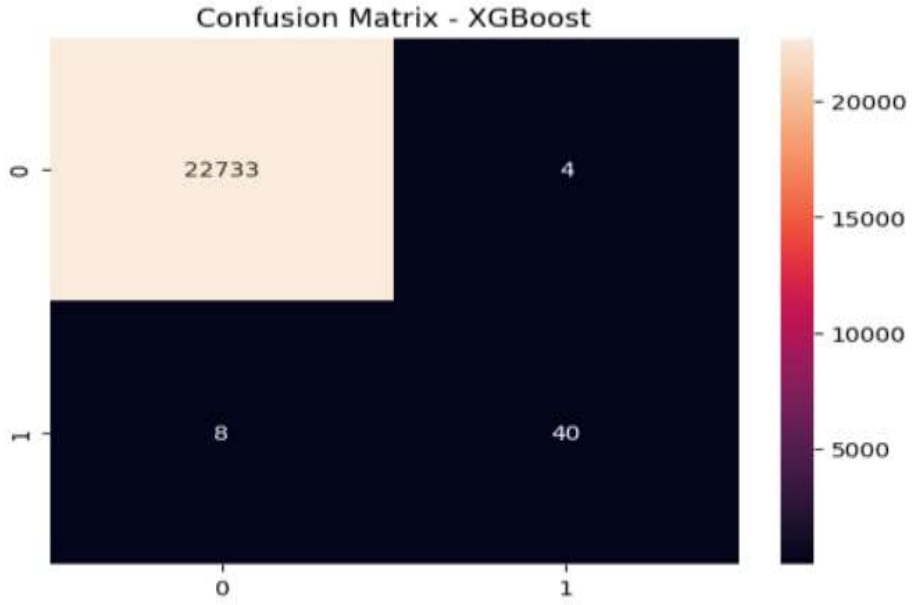

Figure 3: Confusion Matrix of Random Forest

Figure 3 shows that Random Forest improves fraud detection with fewer misclassifications, though some false negatives still remain.

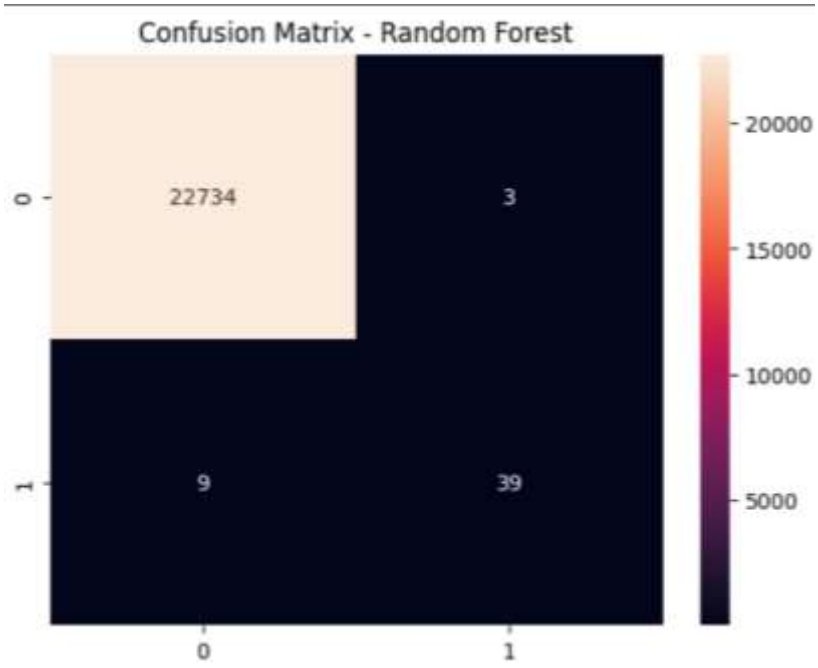

Figure 4: Confusion Matrix of XGBoost Classifier

Figure 4 shows that the XGBoost model achieves high correct classification with very few misclassifications, indicating strong fraud detection performance.

The XGBoost model shows superior performance compared to other models for every metric of evaluation. The high recall value of this model indicates its effectiveness in identifying fraud, which is essential for successfully detecting fraudulent transactions.

6.3 Drift Detection Analysis

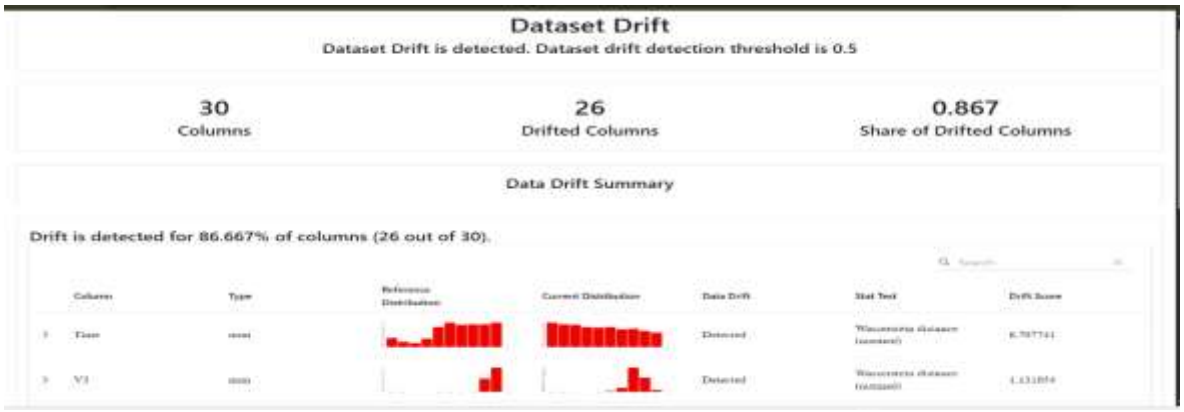

Figure 5: Report on Dataset Drift

Figure 5 shows the dataset drift analysis , there was a noticeable change in the dataset's distribution over time. From the analysis of 30 total features, 26 features have been determined to have drifted or changed over time (approximately 86.67% of total features). The threshold for drift detection was set at 0.5, the observed drift exceeded that threshold and therefore significant data drift was determined. The figure shows the distributions of each feature in reference to the distributions currently; multiple statistical measures (including distance metrics) were used to show how the reference data and the current data differ from each other. The significant differences in how feature distributions differ suggest that transaction patterns have changed and, if not addressed, could cause fraudulent detection models to experience reduced detection accuracy.

The findings highlight the need for a drift detection mechanism to be built into the system proposed here. By detecting large-scale drifts in a timely manner, this mechanism will ensure that the system retrains its detection model as needed in order to maintain accurate detection rates and avoid degradation of model performance. The findings indicate that real-time fraud detection systems must adapt continuously to the ever-changing data environments in which they are deployed, in order to remain effective.

6.4 Discussion

This study shows how well the presented system detects fraudulent transactions. The efficiency of XGBoost's use of complex patterns and handling of imbalanced data has produced superior results compared to other techniques - like Logistic Regression, which utilizes linear relationship assumptions, and Random Forest, which suffers from overfitting in some applications. XGBoost has also developed an appropriate mix of accuracy vs. bias versus variance.

The advancement of drift detection is a significant improvement to the system because drift detection resolves one of the primary problems that real-world fraud-detection systems face. Drift analysis continually adapts the model as new patterns emerge, ensuring relevance and correctness over time.

There are limitations, however, primarily due to the retraining aspect of the system causing processing overhead in real-time. Additionally, choosing appropriate drift thresholds may also require additional tuning.

Overall, this study provides an effective, adaptive, and scalable methodology for credit-card fraud detection that can be implemented successfully within dynamic systems.

7. Conclusion

This paper presented an adaptive credit card fraud detection system using the XGBoost algorithm integra-

ted with drift detection mechanisms. The proposed model effectively identifies fraudulent transactions by leveraging the strong predictive capabilities of gradient boosting techniques while addressing the challenges posed by highly imbalanced data.

The experimental results demonstrated that the XGBoost model outperforms traditional machine learning approaches such as Logistic Regression and Random Forest in terms of accuracy, precision, recall, and F1-score. In particular, the model achieved higher recall, which is crucial for minimizing undetected fraudulent transactions.

Furthermore, the incorporation of drift detection enabled the system to monitor changes in data distribution over time. The dataset drift analysis revealed that a significant proportion of features exhibited distributional changes, highlighting the dynamic nature of financial transaction data. By detecting both prediction and feature drift, the system can trigger timely model retraining, thereby maintaining consistent performance in real-world scenarios.

Overall, the proposed approach provides a robust, scalable, and adaptive solution for fraud detection in dynamic environments. Future work can focus on implementing real-time drift adaptation, exploring deep learning techniques, and optimizing computational efficiency for large-scale deployment.

8. Future Scope

The system that was developed for this research represents a promising platform for real-world fraud detection; nevertheless, additional opportunities exist to enhance and extend its potential. One future direction for implementation of the system to improve fraud detection capabilities is to deploy the system in a fully real-time environment, utilizing streaming technologies to analyze transactions as they occur. By utilising real-time capabilities, financial institutions will be able to prevent fraudulent transactions from occurring, instead of detecting fraudulent transactions after they occur.

The other area where potential for enhancement exists is with the concept drift handling mechanism. As the system automates the replacement of obsolete models, future development can focus on the implementation of more sophisticated drift detection techniques and adaptive learning techniques, such as incremental or online learning models. This will enable the system to continue to learn from data and improve operational efficiencies and response rates without requiring complete retraining.

The incorporation of Explainable Artificial Intelligence (EAI) can also significantly improve the usability and trustworthiness of the system. By providing a clear rationale for why a transaction is classified as fraudulent, the system can provide significant assistance to analysts in making decisions based on the data, thus increasing the overall transparency of the system. Future exploration of deep learning techniques, such as autoencoders or recurrent neural networks, could also enhance the ability of the system to identify complex and new patterns of fraud.

9. References

1. E. Btoush, T. Kobbaey, H. Tamimi, and X. Zhou, “Machine Learning-Based Cyber Fraud Detection: A Comparative Study of Resampling Methods for Imbalanced Credit Card Data,” Appl. Sci., vol. 16, no. 2,Art.no.850,Jan.2026.DOI:10.3390/app16020850. Available: https://www.mdpi.com/2076-3417/16/2/850
2. S. Pasi, Dr. S. Degadwala, and M. Joshi, “Symptom-Based Classification of Common Syndromes Using Machine Learning: A Review,” Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol., vol. 12, no. 1,

pp. 1–6,Jan.–Feb.2026,doi:10.32628/CSEIT26121. Available: https://ijsrcseit.com/index.php/home/article/view/CSEIT25111239

3. P. Abdullah, M. Majid, M. A. Khan, R. Ali, and S. Das, "A hybrid deep learning framework using synthetic oversampling, autoencoder, convolutional neural networks, and an attention mechanism for credit card fraud detection," J. Big Data, vol. 12, Art. no. 6, 2025. DOI: 10.1186/s40537-025-01331-2. Available: https://link.springer.com/article/10.1186/s40537-022-00573-8
4. Alrasheedi, M.A."Enhancing Fraud Detection in Credit Card Transactions: A Comparative Study of Machine Learning Models." Comput Econ (2025). Available: https://doi.org/10.1007/s10614-025-11071-3
5. I. Y. Hafez, A. Y. Hafez, A. Saleh, A. A. Abd El-Mageed, and A. A. Abohany, "A systematic review of AI-enhanced techniques in credit card fraud detection," J. Big Data, vol. 12, Art. no. 6, Jan. 2025. DOI: 10.1186/s40537-024-01048-8. Available: https://link.springer.com/article/10.1186/s40537-024-01048-8
6. L. Zhang, "Credit card fraud detection based on machine learning algorithms," Appl. Comput. Eng., vol. 197, pp. 104–111, Oct. 2025, DOI: 10.54254/2755-2721/2025.AST27335. Available: https://ace.ewapub.com/article/view/27335
7. Li,Y. (2025). Research on Enhancing Credit Card Fraud Detection Based on a Comparative Study of Machine Learning Models and Imbalanced Data Strategies. Advances in Economics, Management and Political Sciences,170,129-136. Available: https://aemps.ewapub.com/article/view/23976
8. Berberi, L., Kozlov, V., Nguyen, G., Sáinz-Pardo Díaz, J., Calatrava, A., Moltó, G., Tran, V., and López García, Á., "Machine learning operations landscape: platforms and tools," Artificial Intelligence Rev., vol. 58, no. 6, Art. no. 167, June 2025, doi: 10.1007/s10462-025-11164-3. Available: https://link.springer.com/article/10.1007/s10462-025-11164-3
9. Kraus, A., van der Aa, H. Machine learning-based detection of concept drift in business processes. Process Sci 2, 5 (2025). Available: https://doi.org/10.1007/s44311-025-00012-w
10. G. Hovakimyan and J. M. Bravo, "Evolving strategies in machine learning: A systematic review of concept drift detection," Information, vol. 15, no. 12, art. no. 786, 2024, doi: 10.3390/info15120786. Available: https://www.mdpi.com/2078-2489/15/12/786
11. S. Jiang, R. Dong, J. Wang, and M. Xia, "Credit card fraud detection based on unsupervised attentional anomaly detection network," Systems, vol. 11, no. 6, p. 305, Jun. 2023, doi: 10.3390/systems11060305. Available: https://www.mdpi.com/2079-8954/11/6/305
12. F. Bayram, B. S. Ahmed, and A. Kassler, "From concept drift to model degradation: An overview on performance-aware drift detectors," arXiv:2203.11070, Mar. 2022. Available: https://arxiv.org/abs/2203.11070
13. Bin Sulaiman, R., Schetinin, V. & Sant, P. Review of Machine Learning Approach on Credit Card Fraud Detection. Hum-Cent Intell Syst 2, 55–68 (2022). Available: https://doi.org/10.1007/s44230-022-00004-0
14. X. Niu, L. Wang, and X. Yang, "A comparison study of credit card fraud detection: Supervised versus unsupervised," arXiv:1904.10604, Apr. 2019. Available: https://arxiv.org/abs/1904.10604
15. K. Chaudhary, J. Yadav, and B. Mallick, "A review of fraud detection techniques: Credit card," Int. J. Comput. Appl., vol. 45, no. 1, pp. 39–44, May 2