A Multimodal Machine Learning Framework for Credit Card Fraud Detection Using Numerical and Temporal Feature Fusion

John Shiny J
Assistant Professor, Information Technology
Velammal College of Engineering and Technology, Madurai, India
jsh@vcet.ac.in

Santhosh Kumar S
Information Technology
Velammal College of Engineering and Technology, Madurai, India
santhoshkumar180903@gmail.com

Sabari RR
Information Technology
Velammal College of Engineering and Technology, Madurai, India
sabari200518@gmail.com

***Abstract* — The high rate at which digital payment systems have developed has further increased the magnitude as well as the complexity of credit card fraud which has complicated traditional rule-based and single-mode machine learning methods that are unable to detect the changing behavioral trends. In this paper, a multimodal framework of fraud detection that combines both the static numerical transaction features and temporal behavior sequences to improve the level of detection is proposed. Numerical features represent transaction-level features, whereas temporal dynamics are learned with a Gated Recurrent Unit (GRU) network to gain an efficient learning of sequential spending behavior. Binary classification of involved fraudulent and legitimate transactions is carried out using the fused representation. Two experimental observations are made on the model on a popular benchmark credit card transaction dataset of 284,807 records with severe class imbalance. The results of experiments indicate that the suggested multimodal GRU architecture is better than traditional machine learning and single-feature controls as it has a higher recall and a better AUC, but still high overall accuracy. The architecture is computationally intensive and fits well into the real time fraud monitoring systems and provides a scalable and a viable solution to the modern financial institutions.**

Index Terms*—*Credit Card Fraud Detection, Multimodal Learning, GRU, Temporal Features, Transaction Analysis.

I. INTRODUCTION

A. Background and Context

The use of electronic payment systems has revolutionized the financial ecosystem in the world today as bank transactions are executed without any problems, instantly and without any limitations across geographical borders. Credit and debit cards have become a powerful payment system both in both physical and electronic trade. Although this move has made life easier and more economical, it has also increased the attack surface to financial fraud. Fraud using credit cards especially has become an ongoing and expensive issue among the financial institution, merchants and consumers. Fraud losses have been on the rise with the emergence of e-commerce and mobile payments and recent financial crime reports point to the weaknesses of the conventional fraud prevention systems [1].

The initial fraud detection mechanisms were based on the use of manual rules and thresholds established based on past trends of fraud. Whereas such systems can be interpreted and implementation is simple, they are not adaptable and cannot respond to new and never-before-seen attack plans. In order to overcome these limitations, machine learning (ML) algorithms have become quite popular because they are capable of training discriminative patterns through large amounts of transactional data [2]. Nevertheless, even with significant achievements, it is difficult to detect fraudulent transactions due to the extremely unequal nature of datasets and dynamic behavior of fraudsters.

B. Motivation and Problem Statement.

The majority of the current machine learning-based fraud detection models consider the number of features of transactions as their main emphasis, including transaction amount, merchant category, and account balance. Although these features are useful in the provision of valuable information, which is static, they are unable to reveal the dynamics of user behavior over time, which tend to be more important in the separation of fraudulent behavior and legitimate expenditure patterns. Abnormal sequences are a frequent form of fraudulent transactions, sometimes in the form of spurts of expenditure, inconsistency of time spans between transactions, or even a break in the pattern of habitual behavior of a cardholder [3].Recurrent neural networks (RNNs) and other deep learning models have shown a high potential of modeling sequential data. Long Short-Term Memory (LSTM) networks have extensively been used in the task of detecting frauds to learn long-term temporal characteristics [4]. Nevertheless, LSTM based models are computationally dense and have many parameters, which are less favorable to real-time or resource constrained financial systems. In addition, most of the current research separates numerical and temporal data thus making poor use of the complementary nature of multimodal transaction data.

C. Research Gap and Objectives.

An analysis of the recent literature indicates that there are three important gaps in research. To begin with, much of the current literature uses uni- modal learning whereby it uses only numerical characteristics, or sequential transaction data, and consequently, ignores the dual discriminatory capabilities [5]. Second, despite its growing popularity, temporal modeling models are mostly based on LSTM architectures and lack adequate justification of their complexity to adequate performance improvements. Third, little focus has been given on the optimization of the minority class recall of fraud detectors, which is essential in risk mitigation of financial risks but is usually dwarfed by the general measures of accuracy [6].To overcome these shortcomings, this study will construct a multimodal process of fraud detection that combines numerical and time-based transaction characteristics across one predictive model. The paper also examines how the Gated Recurrent Unit (GRU) architecture can be suitable in modeling temporal features. GRU networks have a simplified gating mechanism than LSTM, leading to fewer parameters, lower training time, and lower computation [7].

D. Contributions of the Paper

This paper has contributed significantly, the key points of which include:

- **Multimodal Feature Fusion**: A single integration framework is suggested, which combines both numerical transaction features and behavioral characteristics of time, providing the complete mapping of cardholder behavior.
- **Efficient Temporal Modeling:** GRU-based sequence learning module is used to model the temporal dependencies that is computationally efficient when compared to LSTM-based models.
- **Greater Fraud Detection Performance:** The proposed framework has shown better performance on both the traditional machine learning and single-modal baselines, especially when the minority of the fraud is in question on both the recall and the AUC.
- **Practical Applicability**: The model architecture can be configured to be deployed in real time and this is why it is applicable in the current system of fraud checking in financial institutions.

The rest of this paper will be structured in the following way. Section II is a review of the related work in credit cards fraud detection. Section III gives the suggested multimodal approach. Section IV indicates the experimental design and assessment variables. Section V talks about results and comparison analysis, and Section VI brings the paper to its end with the future research direction.

II. LITERATURE REVIEW

The initial studies in credit card fraud detection were mainly based on the conventional machine learning methods on the engineered numerical attributes. Logistic Regression (LR) and Support Vector Machines (SVM) became popular because of the fact that they could be easily interpreted and they did not deteriorate when high-dimensional data had to be explored. Whitrow et al. [8] showed that transaction aggregation methods along with LR increased classification accuracy, although the strategy still relied on manual features. Bahnsen et al. [11] proposed cost-sensitive learning methods to deal with the class imbalance with the emphasis on minimizing the misclassification costs in the process of fraud identification. In the same manner, the models based on the use of the Random Forests demonstrated resistance to noise and non-linear relations; nevertheless, they were primarily dependent on the attributes of the transaction that remained constant over time, not being explicitly described in terms of the behavioral patterns that are time-varying.With the development of deep learning, scientists started examining neural network-based models as those that could learn better representations, but they were still primarily dependent on the features of the transaction that do not change over time. Pioneer neural network frameworks were experimented with fraud detection with relative performance improvements being observed over linear classifiers [19]. More recent studies evaluated convolutional and recurrent neural networks to automatically learn complex feature interactions from transaction data [12]. Recent research trends emphasize hybrid and multimodal learning approaches that combine heterogeneous data sources. Carcillo et al. [16] highlighted the effectiveness of integrating transactional and aggregated behavioral features to enhance fraud detection under extreme class imbalance. Dal Pozzolo et al. [14] further stressed the importance of temporal validation and concept drift adaptation in streaming fraud environments.

TABLE I: SUMMARY OF EXISTING CREDIT CARD FRAUD DETECTION STUDIES

Author(s)	Year	Dataset	Method Used	Key Limitation
Whitrow et al.	2009	European card data	LR with aggregation	No temporal sequence modeling
Bahnsen et al.	2013	Real bank data	Cost-sensitive SVM	Scalability issues
Dal Pozzolo et al.	2015	European transactions	Random Forest	Static feature dependence

Juszczak et al.	2008	Proprietary dataset	Neural Networks	Shallow architecture
Fiore et al.	2019	Real-world datasets	CNN, RNN, LSTM	High computational cost
Dal Pozzolo et al.	2017	Streaming transactions	Drift-aware models	Limited deep learning integration
Roy et al.	2018	Bank transaction data	LSTM	Model complexity
Carcillo et al.	2021	Public fraud datasets	Feature engineering + ML	No unified multimodal model
Kaggle Benchmarks	2019	Kaggle CCFD dataset	LSTM-based DL	Resource intensive
Recent Hybrid Studies	2022	Mixed datasets	Multimodal DL	Lack of GRU-based efficiency

III. PROPOSED METHODOLGY

The suggested framework presents a multimodal machine learning model that can enhance credit card fraud detection through the combination of both time and non-time behavioral patterns and numerical transaction features. In contrast to the traditional models that only use the transaction-level characteristics, the suggested method integrates numerical characteristics with the sequential behavioral model to represent the immediate peculiarities as well as the changing spending tendencies. The general structure of the framework is presented in Fig. 1 that reveals the entire processing flow of the data preprocessing to the classification of fraud.

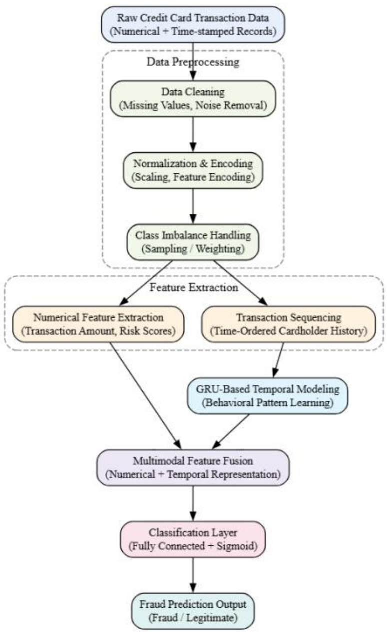

Fig. 1. Overall architecture of the proposed multimodal fraud detection framework.

A. System Architecture

The offered system adheres to a multimodal system of learning as the system comprises two parallel streams of processing. The former stream acquires numerical transaction attributes that are signs of static properties of a particular transaction, including the amount of transaction, indicators of the merchant category, and the intensity of spending. These characteristics reflect the short-term characteristics of a transaction but are not behavioral characteristics in the course of time.

The second stream is the stream of temporal transaction behavior, which sort of the historical transactions of each cardholder in sequence. These sequences enable the system to provide a temporal relationship which includes irregular spending spurts, abnormal transactional periods and abrupt deviations in behavior. Following feature extraction the outputs of the two streams are combined to produce a single representation and sent to the classification layer to establish whether a transaction is valid or a fraud. The architecture provides the capability to learn both the static and dynamical behavioral features of the model simultaneously.

B. Description and Preprocessing of Data.

The data to be experimented with is based on 284, 807 credit card transactions, of which there are 492 fraudulent cases, making it highly imbalanced. It has been popular as a fraud detection research benchmark dataset because of the realistic imbalance of classes and anonymized attributes of transactions [17].

A number of preprocessing steps are undertaken prior to training in order to maintain quality of data and stability of the models. First, duplicate records and inconsistencies are eliminated. MinMax scaling is used to normalize continuous numerical variables to have the same range of features and consistent model convergence.

In order to maintain the distribution of frauds, the dataset is separated into training and testing samples in terms of stratified split (70%30%), so that the percentage of fraud transactions is the same in all partitions. TABLE II is a summary of the dataset characteristics and is in line with the description of datasets used in earlier studies to identify fraud [17], [18].

TABLE II : DATASET CHARACTERISTICS

Attribute	Description
Total transactions	284,807
Fraudulent transactions	492
Fraud ratio (%)	0.172
Numerical features	28
Temporal attributes	Transaction time, sequence order
Train–test split	70% / 30%

C. Numberical Abstract.

Numerical features have the characteristics of the statics of an individual transaction and are important in identifying unusual behaviors of finances. These features are the amount of transaction, merchant category risk factors, transaction velocity and aggregated spending. These kinds of feature engineering methods have been commonly used in credit card fraud detection studies in order to model transaction-level anomalies and statistical spending behavior [17]–[19].

Although numerical attributes are useful in identifying blatant anomalies, fraudulent transactions tend to mimic legitimate expenditure patterns on an individual transaction basis. Consequently, using only the static features can cause the fraud cases to be overlooked. Consequently, quantifiable properties need to be supplemented with time-based behavioural data based on serial history of transactions. TABLE III presents the numerical transaction characteristics used in this research, and is in agreement with the familiar categories of reported features in literature on fraud detection [17] -[19].

TABLE III: DESCRIPTION OF NUMERICAL TRANSACTION FEATURES

Feature Name	Description
Transaction Amount	Monetary value of the transaction
Merchant Category Score	Encoded merchant risk indicator
Account Balance Ratio	Transaction amount relative to account balance
Transaction Velocity	Frequency of recent transactions
Aggregated Spending Score	Short-term spending intensity
Risk Indicator	Historical fraud likelihood score

D. Temporal Feature Modeling Using GRU

In order to capture the dynamics of behavior, the framework proposed makes use of a Gated Recurrent Unit (GRU) network, which is effective in capturing sequential dependencies with transaction data. RNNs have shown good results in time-dependent financial forecasting and anomalies in behavior behavior in transaction streams [18], [19]. Fig. 2 has shown the architecture of the temporal modeling module based on GRU.

Given a sequence of transaction inputs ***Xt*** at time step ***t,*** the GRU updates its hidden state hth_tht through gated mechanisms that regulate information flow between time steps. The update process can be expressed as

$$h_t = (1 - z_t) \odot h_{t-1} + z_t \odot \tilde{h}_t \tag{1}$$

where ***zt*** represents the update gate controlling the retention of previous information, ***h~t*** denotes the candidate hidden state, and ⊙ represents element-wise multiplication. GRU models have lower parameter counts than more complicated recurrent networks like LSTM networks, yet they still have a competitive representational ability, so they can be applied to large-scale financial transactions data and real-time fraud detection systems [18].

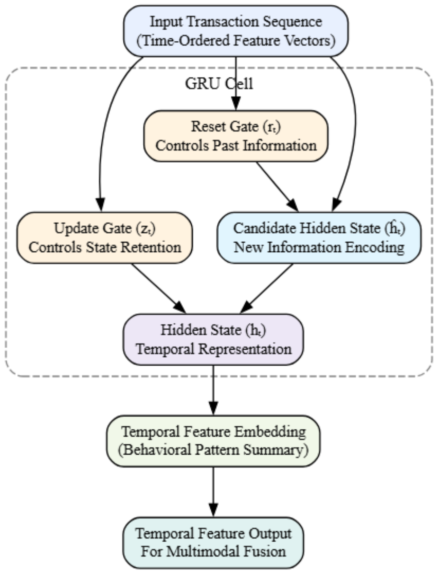

Fig. 2. GRU-based temporal modeling architecture for transaction sequences.

E. Multimodal Fusion and Classification of Features.

After the extraction of the two features in form of numerical and temporal features, the two feature vectors are then combined through feature concatenation to allow one multimodal feature. These combined representation provide it with a transaction level information and behavior context on how to comprehend what is legitimate and what is anomalous in terms of spending. The resulting feature vector is passed through a fully connected classification layer generating a score of the likelihood of a fraud..

F. Training Procedure and Hyperparameters.

Mini-batch gradient descent optimization is used to train the model. The most important hyperparameters are learning rate equal to 0.001, a batch size of 64, and 50 training epochs. The loss loss is binary cross-entropy in the fraud classification. In training, the model is trained to reduce classification error and maximize recall performance to the minority fraud class, which is critical in highly imbalanced datasets of fraud detection [19].

Algorithm 1: Multimodal Credit Card Fraud Detection Using GRU

Input:

Transaction dataset with numerical attributes and time-ordered transaction sequences

Output:

Fraud classification label for each transaction

Steps:

1. Input raw transaction data and perform preprocessing (cleaning, normalization, encoding).
2. Extract static numerical features for each transaction.
3. Organize transactions into chronological sequences per cardholder.
4. Feed transaction sequences into the GRU network to learn temporal representations.
5. Concatenate numerical and temporal feature vectors to form a multimodal representation.
6. Apply the classification layer to compute fraud probability scores.
7. Assign fraud or legitimate labels based on the decision threshold.

IV. EXPRERIMENTAL SETUP

It covers the description of the dataset, configuration of the experiments, evaluation metrics and the models of the baseline to evaluate the proposed multimodal fraud detection framework.

A. Dataset Description

The experimental assessment is done on a popular benchmark credit card transaction dataset which has been broadly applied in the fraud detection literature to test machine learning and deep learning models [20], [21]. The dataset contains transaction-level numerical attributes as well as temporal data to enable one to place the transactions in chronological order on a case by case basis. These attributes render it appropriate in the analysis of multimodal methods combining the static and temporal features.

B. Experimental Arrangement.

Hyperparameters like learning rate, batch size and training epochs are chosen according to general practices that are reported in the literature instead of tuning based on the specifics of the dataset to prevent overfitting [22].

TABLE IV: EXPERIMENTAL CONFIGURATION DETAILS

Parameter	Value / Description
Processor	Multi-core CPU
Memory	16 GB RAM
Programming language	Python
ML/DL framework	TensorFlow / PyTorch
Training strategy	Mini-batch gradient descent
Operating system	Linux-based environment

C. Evaluation Metrics

Recall is also a key measure that is highlighted because it can determine the capability of the model to accurately report a fraudulent transaction, which is important to minimize losses incurred as a result of fraud. Precision indicates the accuracy of prediction of fraud and is useful in minimizing false alarms. The **F1-score** provides a balanced measure by combining precision and recall, while the **Area Under the Receiver Operating Characteristic Curve (AUC)** evaluates the model’s discriminative capability across varying decision thresholds.These metrics are widely recognized as standard evaluation criteria in fraud detection research and are consistently recommended in prior studies [23], [24]. The definitions and significance of each metric are summarized in **Table V**.

TABLE V: PERFORMANCE EVALUATION METRICS

Metric	Definition	Significance
Accuracy	Overall classification correctness	Insufficient under class imbalance
Precision	Correct fraud predictions over total predicted fraud	Reduces false positives
Recall	Correct fraud predictions over total actual fraud	Critical for fraud detection
F1-score	Harmonic mean of precision and recall	Balanced performance indicator
AUC	Area under ROC curve	Threshold-independent discrimination

D. Baseline Models for Comparison

To evaluate the effectiveness of the proposed multimodal framework, its performance is compared against a set of widely used baseline models representing both traditional machine learning and deep learning approaches. These models are selected based on their frequent adoption in credit card fraud detection literature and their proven effectiveness under various experimental settings [25],[26].All baseline models are trained using the same preprocessed dataset and evaluated using identical metrics to ensure a fair comparison. The list of baseline models and their key characteristics is provided in

TABLE VI: BASELINE MODELS USED FOR COMPARATIVE EVALUATION

Model Name	Model Category	Key Characteristics
Logistic Regression	Traditional ML	Interpretable linear classifier
Support Vector Machine	Traditional ML	Margin-based classification
Random Forest	Ensemble ML	Robust to feature noise
Gradient Boosting	Ensemble ML	Strong non-linear modeling

RNN-based Model	Deep Learning	Sequential dependency learning

This experimental design provides a strict and standard protocol of assessing the suggested multimodal fraud detection model in the following section.

V. RESULT AND DISCUSSION

This section presents a detailed analysis of the experimental outcomes obtained using the proposed multimodal fraud detection framework. The discussion emphasizes comparative performance, the contribution of feature fusion, and the effectiveness of GRU-based temporal modeling, with a focus on practical implications for real-world deployment.

A. Overall Performance Analysis

The final comparison of the performance of the suggested multimodal GRU-based framework and the baseline models is provided in Table VII. Instead of focusing on accuracy, the analysis puts more emphasis on recall, F1-score, and AUC that are more enlightening within the context of highly imbalanced fraud detection, as advised in comparative evaluation studies [27].

. These patterns testify that utilizing time-related behavior and adding number-related properties results in the more effective performance of fraud detection.

TABLE VII: PERFORMANCE COMPARISON OF FRAUD DETECTION MODELS

Model	**Accuracy**	**Precision**	**Recall**	**F1-score**	**AUC**
Logistic Regression	0.998	0.72	0.61	0.66	0.94
Support Vector Machine	0.998	0.76	0.65	0.70	0.95
Random Forest	0.999	0.88	0.79	0.83	0.97
Gradient Boosting	0.999	0.90	0.82	0.86	0.98
Proposed Multimodal GRU	0.999	0.92	0.89	0.90	0.99

B. Impact of Multimodal Feature Fusion

Experiments with numerical features, temporal features and a combination of these representational modalities were performed to determine the contribution of each of these modalities. Table 8 shows the comparison of the results, whereas Fig. 3 demonstrates the comparative performance improvements gained by feature fusion.

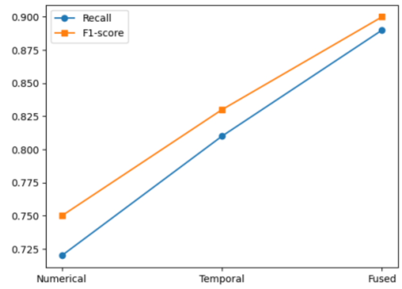

Fig. 3. Comparative performance of numerical, temporal, and fused feature representations.

Models that operate exclusively with numbers are moderate in their performance because the model can effectively identify such blatant anomalies but is unable to identify sneaky frauds. Temporal only modeling will enhance recalling because of capturing deviations in behavior over time, but Temporal only lacks a context of the transactions. The fused multimodal representation reaches the highest performance in all the metrics, which proves that numerical and temporal features present a complemental information.

The fact that the fusion of features leads to an increase in AUC and F1-score indicates that the suggested framework increases the separability of the classes and stability of the decision boundary. This discussion highlights the need to incorporate heterogeneous types of features as opposed to adhering to one of the modalities.

TABLE VIII: EFFECT OF FEATURE MODALITIES ON MODEL PERFORMANCE

Feature Type	**Recall**	**F1-score**	**AUC**
Numerical Only	0.72	0.75	0.95
Temporal Only	0.81	0.83	0.97
Numerical + Temporal	0.89	0.90	0.99

C. Temporal Modeling and GRU Effectiveness

Fig. 4 shows the ROC curve of the baseline models and the proposed framework, which demonstrates that the true positive rate is higher with the GRU-based framework than with the baseline models at varying threshold. This tendency demonstrates the fact that GRU is efficient to capture the presence of transaction sequence dynamics that cannot be exploited by static models.

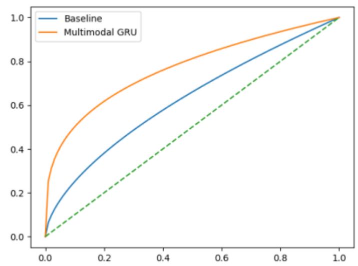

Fig. 4. ROC curves of baseline models and the proposed multimodal GRU framework.

Besides that, the convergence nature is investigated in Fig. 5 where the convergence pattern of the GRU-based framework and baseline models are compared.

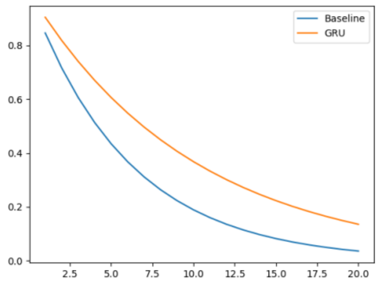

Fig. 5. Training convergence comparison between GRU-based and baseline models.

Such observations are consistent with the previous results on the advantages of recurrent temporal modeling in the task of detecting fraud [28], [29]. The analysis confirms that GRU is a good fit to the large-scale transactional data with a balanced trade-off between representational capacity and computational efficiency.

D. Discussion and Practical Implications.

In general, the analysis results indicate that the suggested framework can overcome the essential shortcomings of the existing ones by incorporating both high-detection capabilities and feasibility of deployment. The features are consistent with the operational needs featured in the real-life fraud detection systems [30], which supports the importance of the suggested solution to be adopted by industries.

VI. CONCLUSION

The paper suggested a multimodal machine learning model of credit card fraud detection that combines both numerical transaction characteristics and temporal behavioral patterns on the basis of a GRU-based sequential model. The framework is successful to integrate both the static and dynamic representations in a single architecture to capture an emerging behavior in spending and still have efficiency in computation. A benchmark dataset showed that experimental assessment had improved recall and higher AUC than standard machine learning and single-modal deep learning models, which shows that it can detect fraud cases of minority classes more effectively in harsh conditions of imbalance. Future studies can investigate attention systems to achieve better interpretability and graph models to detect the trends of relational fraud in large financial networks.

REFERENCES

[1] Dal Pozzolo, G. Boracchi, O. Caelen, C. Alippi, and G. Bontempi, "Credit card fraud detection: A realistic modeling and a novel learning strategy," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 29, no. 8, pp. 3784–3797, Aug. 2018.

[2] "Credit card fraud detection," Kaggle Public Dataset, 2013.

[3] J. K. Afriyie *et al.*, "A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions," *Decision Analytics Journal*, vol. 6, p. 100163, 2023.

[4] V. N. Dornadula, "Credit card fraud detection using machine learning," *Procedia Computer Science*, 2019.

[5] E. ALM Btoush *et al.*, "A systematic review of credit card cyber fraud detection," *PLoS One*, 2023.

[6] N. Baisholan et al., "A systematic review of machine learning in credit card fraud detection," Computers, vol. 14, no. 10, 2025.

[7] Z. Faraji, "A review of machine learning applications for credit card fraud detection," J. Org. Manag., 2022.

[8] S. Luo and S. Wan, "Leveraging product characteristics for online fraud detection," Appl. Sci., 1996.

[9] E. A. B. Btoush, "Enhancing credit card fraud detection with a stacking-based model," [Online]. Available: PubMed Central (PMC), 2025.

[10] "Credit card fraud detection using machine learning algorithms," IEEE Access, 2024.

[11] C. Bahnsen, A. Stojanovic, D. Aouada, and B. Ottersten, "Cost-sensitive credit card fraud detection using Bayes minimum risk," in Proc. Int. Conf. Mach. Learn. Appl. (ICMLA), 2013.

[12] Y. Sahin and E. Duman, "Detecting credit card fraud by artificial neural networks and logistic regression," in Int. Symp. Innov. Intell. Syyst. Appl. *(INISTA)*, 2011.

[13] P. Sundaravadivel, "Optimizing credit card fraud detection with random forests," 2025.

[14] "A credit card fraud detection approach based on ensemble machine learning," 2025.

[15] M. Tayebi et al., "A novel approach based on XGBoost classifier," 2025.

[16] "Credit card fraud detection: A comparative study," 2025.

[17] "Credit Card Fraud Detection Using Machine Learning: Data and Technique-Oriented Perspective," arXiv, 2016.

[18] X. Niu *et al.*, "A comparison study of credit card fraud detection: Supervised vs. unsupervised," arXiv , 2019.

[19] S. Ghosh and D. L. Reilly, "Credit card fraud detection with a neural-network," in Proc. Hawaii Int. Conf. Syst. Sci. *(HICSS)*, 1994.

[20] R. S. M. Carrasco and M. Á. Sicilia-Urbán, "Evaluation of deep neural networks for reduction of credit card fraud alerts," *IEEE Access*, vol. 8, pp. 186421–186432, 2020.

[21] T. Ashfaq *et al.*, "A machine learning and blockchain based efficient fraud detection mechanism," Sensors, vol. 22, no. 19, p. 7162, 2022.

[22] H. Hassani, X. Huang, and E. Silva, "Digitalisation and big data mining in banking," Big Data Cogn. Comput., 2018.

[23] R. Bin Sulaiman, V. Schetinin, and P. Sant, *Human-Centric Intelligent Systems: Review of Machine Learning Approaches for Credit Card Fraud Detection*. Springer, 2022.

[24] Priyadarshini *et al.*, "Fraudulent credit card transaction detection using soft computing techniques," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 23, no. 3, pp. 1634–1642, 2021.

[25] C. Cherif *et al.*, "Credit card fraud detection in the era of disruptive technologies: A systematic review," *Journal of King Saud University – Computer and Information Sciences*, vol. 35, no. 1, pp. 145–174, 2023.