Novel Approaches in Financial Fraud Detection: Hybrid Machine Learning and Uncertainty-Based Deep Learning

Hadi Mohammadi[1], Mahdieh Rahmati[2], Tina Shahedi[3]

[1, 3] Department of Methodology and Statistics, Utrecht University, The Netherlands.

h.mohammadi@uu.nl, t.shahedi@uu.nl

[2] Department of Finance, University of Luxembourg, Luxembourg

mahdie.rahmaty@yahoo.com

Abstract. Fraud detection plays a crucial role in various industries, especially in the financial sector, where preventing fraudulent activities is essential to minimize losses and maintain consumer trust. This paper addresses key challenges in fraud detection, including data imbalance and uncertainty, which often hinder the effectiveness of detection models. To overcome these challenges, we explore traditional machine learning methods and introduce two novel approaches to enhance detection capabilities. Firstly, we propose a hybrid pipeline that integrates both supervised and unsupervised learning techniques, enabling more accurate identification of fraudulent activities. Through this hybrid model, we show improvements in performance metrics over traditional models, effectively addressing the limitations posed by data imbalance. Secondly, we develop a novel deep learning model that incorporates uncertainty into its framework. This model is specifically designed to handle the inherent uncertainties present in real-world fraud detection scenarios, allowing for more robust and reliable detection outcomes. Our empirical evaluations, using publicly available datasets, show that this new deep learning approach outperforms similar models that do not consider uncertainty. By integrating uncertainty management into the model's structure, we achieve greater accuracy and reliablity in fraud detection. These findings highlight the importance of addressing data imbalance and uncertainty in fraud detection and demonstrate the potential of hybrid and deep learning models to enhance the performance of fraud detection systems in e-commerce and other financial applications.

Keywords: Financial Fraud, Robust Fraud Detection, Hybrid Machine Learning, Deep Learning, Uncertainty Quantification.

1 Introduction

The spread of e-commerce has fundamentally altered global business dynamics, providing significant convenience to consumers and numerous opportunities for businesses. However, this shift has also led to an increase in online credit card fraud, posing

considerable challenges for financial institutions. Despite the implementation of advanced security measures like encryption and multi-factor authentication, fraudsters continue to find and exploit system vulnerabilities. This persistence in fraud activity has resulted in significant financial losses. For example, recent studies indicate that global credit card fraud losses could surpass $400 billion in the next decade, highlighting the urgency for robust fraud detection systems **(1).** The situation has been exacerbated by the COVID-19 pandemic, with the Federal Trade Commission reporting $3.3 billion in fraud-related losses in 2020, underscoring the critical need for enhanced fraud detection mechanisms. Given these trends, research in fraud detection is crucial not only for e-commerce but also for other financial sectors such as centralized banking systems, virtual currencies, and ATMs. Recent advancements in machine learning have shown promise in addressing these issues by using novel algorithms that enhance the accuracy of fraud detection. For instance, studies using advanced models like K-nearest neighbor (KNN), linear discriminant analysis, and linear regression have demonstrated improved recall in detecting fraudulent transactions, making them highly effective tools in combating fraud in real-time scenarios **(2)**.

This paper addresses these fraud detection challenges within e-commerce by proposing innovative solutions. The paper is structured as follows: Section 2 reviews existing literature, emphasizing machine learning techniques and the importance of uncertainty quantification. Section 3 outlines the main challenges in fraud detection and evaluates current approaches. Section 4 introduces a novel framework integrating data preprocessing with machine learning and deep learning models to enhance detection accuracy. Finally, Section 5 concludes the paper, summarizing findings and suggesting directions for future research.

2 Literature Review

In this section, we briefly review various machine learning methods used for fraud detection, analyzing their advantages and limitations.

2.1 Machine learning methods

Credit card fraud detection research often faces challenges related to class imbalance, where legitimate transactions significantly outnumber fraudulent ones. Various methods, such as undersampling, oversampling, and Generative Adversarial Networks (GANs), have been utilized to address this imbalance, with different levels of success. Deep learning approaches like fully connected neural networks, convolutional neural networks, deep autoencoders, and Restricted Boltzmann Machines have been applied to improve fraud detection while minimizing false positives, although many models still struggle with real-world data due to differences in data distributions compared to training samples. Supervised methods like gradient boosting and random forests have shown better performance compared to unsupervised approaches in terms of AUC[1]. For

[1] **AUC** stands for **Area Under the ROC Curve**. It is a performance metric used to evaluateclassification models, particularly in situations where there is an imbalance between classes, as in fraud detection.

example (3)**,** effectively utilized a fully connected neural network to predict non-legitimate transactions, employing undersampling and oversampling techniques to manage data imbalance, achieving accuracies of 99.72% with undersampling and 99.67% with oversampling. Other techniques, such as interpolation, and alternative evaluation metrics like precision, recall, and F1 score, have also been explored by (4); they demonstrated that Support Vector Machine (SVM) performs well on highly skewed datasets, while Random Forest proves more effective when the dataset is more balanced.

The ongoing debate in fraud detection research centers on the efficacy of supervised versus unsupervised methods. For instance (5), found that gradient boosting and random forests surpassed other methods, such as restricted Boltzmann machines and GANs, achieving AUCs of 98.9% and 98.8%, respectively.

However, despite promising results, many of these models fail to generalize effectively in practical scenarios, highlighting the critical need for uncertainty quantification to improve model reliability and user trust. To better illustrate the structure of the literature, we present the codes for this table in **Table 1**.

Table 1. Literature structure codes

Category	Detail	Code
Fraud	Credit card	CC
	Automobile insurance	Auto Insurance
Uncertainty	Mont Carlo Dropout	MCD
	Multiple Criteria Decision Making	MCDM
Method	Markov Decision Process ,	MDP
	Reinforcement Learning	RL
	Latent Dirichlet Allocation	LDA
	Long Short-Term Memory	LSTM
	Intuitionistic Fuzzy Set	IFS
	Dempster-Shafer Theory	DST
	Rule-Based Component	RBC
	Scenario-Based Component	SBC
	Deep Neural Network	DNN
	Generative Adversarial Networks	Gans
	Light Gradient Boosting Machine	Lightgbm
	Recursive Feature Elimination	RFE
	Fuzzy Rough Nearest Neighbor	FRNN
	Ensemble-Based Method	EBM
	Homogeneity-Oriented Behavior Analysis	HOBA
	Back Propagation Neural Network	BPNN
	Artificial Neural Network	ANN
	Gated Recurrent Units	GRU

Table 2 provides a summary of the present study and other research, categorized based on the type of fraud, method (e.g., deep reinforcement learning (DRL), supervised learning (SL), GANs, etc), dataset and uncertainty.

Table 2. Summary of the literature on machine learning methods in fraud detection.

Study /Year		Fraud	Method	Dataset	Uncertainty
(6)	2016	×	Bayesian Approximation	two real-world datasets	MCD
(7)	2017	Banking	DRL	a real-world dataset	×
(8)	2017	CC	SL	a real-world dataset	×
(9)	2017	CC	Deep Autoencoder	a German Credit Data	×
(10)	2018	CC	MDP ,RL	a real-world dataset	×
(11)	2018	Auto Insurance	LDA	a real-world dataset	×
(12)	2018	CC	LSTM	a real-world dataset	×
(13)	2019	Banking	IFS & DST	a real-world dataset	MCDM
(14)	2019	Banking	RBC, SBC	a real-world dataset	×
(5)	2019	CC	SL	Kaggle real-world dataset	×
(15)	2019	Auto Insurance	SL	a real-world dataset	×
(3)	2019	CC	DNN	a real-world dataset	×
(16)	2019	CC	SL	a real-world dataset	×
(17)	2019	CC	GANs, DNN	Kaggle real-world dataset	×
(18)	2020	CC	LightGBM	two real-world datasets	×
(19)	2020	CC	Hybrid Learning, Deep	Kaggle real-world dataset	×
(20)	2020	CC	DNNs	a real-world dataset	×
(21)	2020	CC	SVM with RFE	three real-world datasets	×
(22)	2020	Auto Insurance	BPNN	a real-world dataset	×
(23)	2021	Auto Insurance	Rule-Based System	a real-world dataset	×
(24)	2021	CC	HOBA	a real-world dataset	×
(25)	2021	CC	SL	a real-world dataset	×
(26)	2021	CC	FRNN	two real-world datasets	×
(27)	2021	CC	A Hybrid Method	two real-world datasets	×
(28)	2021	CC	LSTM and GRU	two real-world datasets	×
(29)	2021	CC	ANN	Kaggle real-world dataset	×
(30)	2023	CC	Ensemble-based method	a real-world dataset	MCD
(31)	2023	CC	Random Forest	Kaggle real-world dataset	×
This Study	**2024**	**CC**	**Hybrid Deep Learning**	**Kaggle real-world dataset**	**MCD**

2.2 Significance of incorporating uncertainty

Incorporating uncertainty into credit card fraud detection models is crucial for enhancing reliability and effectiveness, especially when dealing with highly imbalanced datasets. Conventional models can become overconfident in predicting the dominant class, leading to false positives or missed fraudulent activities. Quantifying uncertainty

helps models express confidence levels, improving interpretability and decision-making.

Monte Carlo Dropout (MCD) is a technique used to estimate model uncertainty in deep learning, especially in neural networks. It was introduced as a way to approximate Bayesian inference for neural networks by (6), which allowed models to estimate uncertainty without significant computational overhead. Building on this foundation, (19) showed that deep learning models, such as LSTM and CNN, outperform traditional methods for fraud detection, particularly in real-time settings, using dropout as a regularization technique where a certain percentage of neurons are randomly "dropped" (set to zero) in each layer to prevent overfitting. However, they did not utilize MCD. In this technique, dropout remains activated even during inference, meaning multiple forward passes through the same input yield different outputs due to the random dropout of neurons. Recently, (30) showed that methods like MCD, ensemble techniques, and ensemble MCD significantly improved model reliability by capturing epistemic uncertainty, helping identify transactions requiring further scrutiny, thus improving efficiency and reducing costs.

There are other studies that used fuzzy approaches to deal with uncertainty in fraud detection, like(13), which showed that an MCDM approach combined with intuitionistic fuzzy sets effectively captured uncertainty in fraud detection, improving accuracy and reducing false alarms. Similarly, another study by (26) detected credit card fraud with detection rates of 84.90% and 76.30% using FRNN, although they did not explicitly quantify uncertainty.

3 Proposed methodology framework

The proposed methodology framework addresses critical fraud detection challenges through a structured approach involving data collection, preprocessing, and model development. The framework (i.e., **Fig 1**) is designed to manage issues like data imbalance using oversampling and undersampling techniques and to evaluate various classification models. A hybrid ensemble model is implemented, combining clustering and classification to improve detection accuracy. Furthermore, a deep learning model that integrates MC Dropout as an uncertainty quantification technique ensures robust and reliable predictions. By performing multiple stochastic forward passes through the model and analyzing the variance, we aim to identify instances where the model's prediction is less reliable, which is essential when dealing with highly sensitive areas like fraud detection. In this section, we implement the proposed framework on a research dataset, describe the dataset, its features, the hybrid model architecture and the uncertainty quantification appraoch.

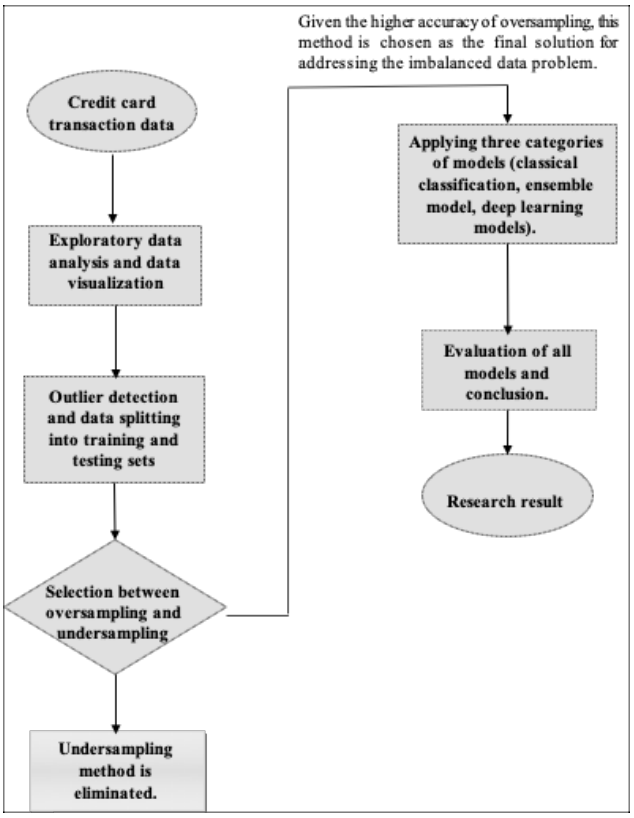

Fig. 1. Flowchart of the proposed framework.

3.1 Dataset

In this study, the Credit Card Fraud Detection dataset used consists of anonymized transaction records labeled as either legitimate or non-legitimate. It includes data for two days involving transactions made by European cardholders. Out of a total of 284,807 transactions, 492 are classified as non-legitimate. The dataset contains 30 features named *"Time", "V1", "V2", ..., "V28",* and *"Amount"*. The features, except for *"Time"* and *"Amount",* were transformed using Principal Component Analysis (PCA) to maintain data privacy. The "Time" feature represents the elapsed time in seconds from the first transaction, while "Amount" represents the value of the transaction. The target variable, *"Class",* is binary: 1 indicates non-legitimate transactions, and 0 indicates legitimate ones.

3.2 Data preprocessing

Our key steps in the preprocessing pipeline include:

- **Exploratory Data Analysis (EDA);** involves visualizing the data, detecting outliers, and using PCA to clean and format the dataset effectively for model implementation.
- **Outlier Detection;** Outliers are identified using the formula:

  $$X > Q_3 + 1.5(Q_3 - Q_1) \; or \; X < Q_1 - 1.5(Q_3 - Q_1) \qquad (1)$$

  where Q_1 and Q_3 represent the first and third quartiles of the data distribution, respectively. This method helps in identifying and removing outliers, thereby enhancing data quality.
- **PCA;** is employed to reduce the dimensionality of the dataset while preserving most of its variance. Standardizing the data before applying PCA is a critical step to avoid bias and improve the interpretability of the analysis..
- **Oversampling and Undersampling;** To balance class proportions, oversampling generates more samples for the minority class, while undersampling reduces samples from the majority class. These methods ensure that the model learns patterns from both classes effectively.

3.3 Hybrid Model

The innovative hybrid model proposed in this study uses both unsupervised and supervised learning to effectively enhance credit card fraud detection. Initially, an unsupervised K-means clustering algorithm is employed to differentiate between legitimate and non-legitimate transactions by grouping the data into homogeneous clusters. These clusters are then passed to a deep learning model for classification, allowing the supervised learning model to better exploit the underlying patterns within each cluster, thereby improving detection performance.

The first step in the hybrid approach is using K-means clustering, which aims to partition the dataset into clusters to distinguish between different transaction behaviors. By minimizing the within-cluster sum of squares (WCSS), the K-means algorithm maximizes the differences between the clusters, effectively grouping similar data points together. This unsupervised step helps segregate legitimate and fraudulent transactions based on their features, providing more refined data inputs for the deep learning model. The deep learning model employed in this study consists of multiple dense layers, including batch normalization and dropout layers to improve generalization.

3.4 Uncertainty quantification approach

We improved the reliability of our deep learning model by measuring how uncertain its predictions are. This is especially important in fraud detection, where patterns change frequently. We used a method called Monte Carlo Dropout, keeping dropout active during both training and testing. This made the model produce multiple random

predictions for the same input. By checking how much these predictions varied, we could tell how confident the model was in its decisions. We set a threshold of 0.8 for making classifications. By focusing on predictions with higher uncertainty, we identified cases where the model was less sure, allowing us to handle high-risk transactions more carefully. The model architecture can be summarized in Table 3.

Table 3. The hybrid model architecture.

function define Model Architecture
Input layer: 30 units
Hidden layers:
Layer 1: 385 units
Layer 2: 128 units
Layer 3: 128 units
Layer 4: 64 units
Batch Normalization: After Layer 3 and Layer 5
Dropout Layers (rate = 0.3): After Layer 3 and Layer 5
Further Layers:
Layer 5: 128 units
Layer 6: 64 units
Layer 7: 32 units
Output layer: 1 unit with *Sigmoid* activation
Activation function: *ReLU* for all layers
Compile model: *Adam* optimizer with learning *rate = 0.001*
end function
function Predict with Uncertainty (*model, X_test, n_passes*)
Input: Model, test data, number of forward passes (*n_passes*)
Initialize *fwd_passes* as empty list
for each pass from 1 to *n_passes* **do**
Perform prediction with dropout enabled (*model(X_test, training=True)*)
Append prediction to *fwd_passes*
end for
Convert *fwd_passes* to *NumPy* array
Calculate mean predictions and variance across *fwd_passes*
Return: mean predictions, variance
end function
Usage for Predictions
Call *predict_with_uncertainty()* with trained model and test data
Apply *threshold (0.8)* to mean predictions for binary classification
Evaluate Model
Calculate Confusion Matrix and Classification Report
Calculate average uncertainty from variance values

4 Model Evaluation

The Evaluation metrics for both supervised and unsupervised models are essential for evaluating model performance. In unsupervised evaluation, methods like the Elbow and Silhouette coefficient measure cluster cohesion and separation, aiding in the determination of optimal clustering. In supervised evaluation, metrics such as accuracy, recall, precision, and F1 score, derived from the confusion matrix, provide a understanding of the model's classification performance. In this section, we outline the analytical tools used. The results are evaluated using predefined metrics to assess the effectiveness of the proposed model.

4.1 Classification models

To evaluate the proposed framework, we first applied five standard classification models to the dataset and measured their accuracy using various metrics. We also compared the effectiveness of oversampling and undersampling techniques. Confusion matrices were generated for each model to compute additional metrics, as summarized in **Table 4.**

Table 4. Confusion matrix in this research.

Valid transaction **correctly** predicted as **valid** (TN)	**Valid** transaction predicted as **non-legitimate** (FN)
Non-legitimate transaction predicted as **valid** (FP)	**Non-legitimate** transaction **correctly** predicted as **non-legitimate** (TP)

The confusion matrices for each classification algorithm are as follows:

Table 5. Confusion Matrices for Different Classification Algorithms

Algorithm	TN	FN	TP	FP
Decision Tree (DT)	1992	0	7	1
K-Nearest Neighbors (KNN)	1992	0	0	8
Logistic Regression (LR)	1991	1	8	0
Support Vector Machine (SVM)	1992	0	0	8
Random Forest (RF)	1992	0	6	2

Given the high cost associated with failing to detect fraudulent transactions, the recall metric was prioritized.

4.2 Using the oversampling method

To mitigate the data imbalance, we applied oversampling to increase the representation of the minority class. The confusion matrices for each classification algorithm oversampling are as follows:

Table 6. Confusion Matrices for Different Classification Algorithms with Oversampling.

Algorithm	TN	FN	TP	FP
Decision Tree (DT)	1576	0	28336	0
K-Nearest Neighbors (KNN)	14865	39	15008	0
Logistic Regression (LR)	14480	424	14512	496
Support Vector Machine (SVM)	10901	4003	6299	8709
Random Forest (RF)	14486	418	14517	491

The overall recall improved with the oversampling method, highlighting its importance in fraud detection.

4.3 Using the undersampling method

For In the undersampling approach, we reduced the majority class sample size. The confusion matrices after undersampling:

Table 7. Confusion Matrices for Different Classification Algorithms with Undersampling.

Algorithm	TN	FN	TP	FP
Decision Tree (DT)	9790	151	10000	0
K-Nearest Neighbors (KNN)	9922	19	10000	0
Logistic Regression (LR)	9667	274	9733	267
Support Vector Machine (SVM)	7264	2677	4261	5739
Random Forest (RF)	9925	16	9852	148

Based on the experimental results, the oversampling method consistently outperformed the undersampling method across all metrics. As such, oversampling was selected for further analysis with the innovative model.

4.4 Hybrid Model implimentation

Clustering was used to identify similar patterns in the data rather than directly separating transactions. We evaluated the optimal number of clusters (2, 3, and 5) using inertia reduction, as depicted in **Figure 2**. Three clusters were chosen to avoid overfitting.

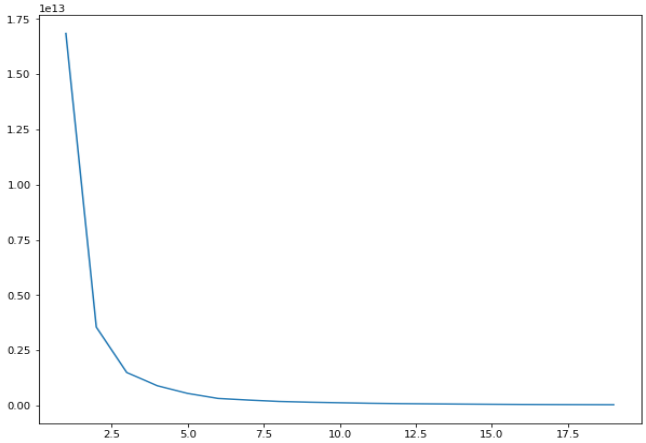

Figure 2. Evaluating the number of clusters in the k-means method.

The final number of clusters was confirmed to be 3 based on evaluation metrics. Classification algorithms were then applied to each cluster, and their average metrics were computed. Confusion matrices for the hybrid model, in comparison with the basic deep learning model is as follows:

Table 8. Confusion Matrices for Different Classification Algorithms with hybrid DL.

Algorithm	TN	FN	TP	FP
Hybrid DL	5485	11	4504	0
Basic DL	4871	23	5106	0
Random Forest with oversampling	14486	418	14517	491

To comprehensively evaluate the performance of the models, we considered several evaluation metrics, including precision, recall, F1-score, and accuracy. The comparison aims to identify strengths and weaknesses in fraud detection and classification across different models. Additionally, we examined computational efficiency and the trade-offs between model complexity and interpretability to provide a balanced analysis of each model's practical applicability. The results.in comparison with the basic and hybrid deep learning model and Random Forest (the best traditional model), are summarized in **Table 9**.

Table 9. Comparison of the best model outputs.

Metric	Hybrid DL	Basic DL	Random Forest
Precision	0.9980	0.9953	0.9637
Recall	1.0	1.0	0.9720
F1-Score	0.9990	0.9976	0.9696
Accuracy	0.9989	0.9977	0.9696

5 Discussion and Conclusion

This study investigated the application of advanced machine learning techniques to enhance credit card fraud detection using a comprehensive dataset of 284,807 transactions, including 492 fraudulent cases. We addressed the main challenge of data imbalance using oversampling and undersampling techniques, concluding that oversampling provided superior performance. Undersampling was found to be less effective due to the reduction in sample diversity. During preprocessing, various visualization techniques were employed to gain insights into the dataset, guiding algorithm selection and design. The comparative analysis of several well-known classification models highlighted the strengths and weaknesses of different approaches.

The study used clustering to identify transaction patterns, applying classification algorithms to each cluster. and then applied classification algorithms to each group. This customized approach for the dataset showed that combining these methods is effective. we explored the use of deep learning models with Monte Carlo Dropout to quantify uncertainty. The hybrid DL achieved high performance. Similarly, the basic DL also achieved high performance. The F1-scores of the hybrid DL and Basic DL, showing their imbalanced performance. This imbalance made these models less effective for minimizing false alarms, despite being able to identify most fraudulent transactions effectively.

One notable aspect of the hybrid DL was its ability to quantify uncertainty through Monte Carlo Dropout, which provided valuable insights for manual review. This approach allows for prioritizing manual review on transactions that the model is uncertain about, thereby enhancing the reliability of fraud detection. By emphasizing transactions with high uncertainty, financial institutions can allocate resources more effectively to investigate potentially risky cases, thereby reducing the chances of overlooking true fraud instances.

Future Research Recommendations:

- Test the combined model on different credit card fraud datasets to validate its generalizability.
- Apply the model to other domains, such as insurance fraud detection, to evaluate its broader applicability.
- Explore additional machine learning and deep learning algorithms to enhance model performance.
- Investigate various methods of uncertainty quantification to improve prediction reliability.
- Introduce noise into datasets to evaluate the robustness of the models under real-world conditions.

These recommendations aim to extend the applicability and robustness of the proposed model, ensuring its effectiveness in diverse scenarios. The findings of this study

underscore the importance of addressing data imbalance and incorporating uncertainty measures to enhance the reliability of fraud detection systems in financial applications.

6 Disclosure of Interests.

The authors have no competing interests to declare that are relevant to the content of this article

References

1. Feng X, Kim SK. Novel Machine Learning Based Credit Card Fraud Detection Systems. Mathematics. 2024;12(12):1869.
2. Chung J, Lee K. Credit card fraud detection: an improved strategy for high recall using KNN, LDA, and linear regression. Sensors. 2023;23(18):7788.
3. Shenvi P, Samant N, Kumar S, Kulkarni V. Credit card fraud detection using deep learning. In: 2019 IEEE 5th International Conference for Convergence in Technology (I2CT) [Internet]. IEEE; 2019 [cited 2024 Oct 21]. p. 1–5. Available from: https://ieeexplore.ieee.org/abstract/document/9033906/
4. Banerjee R, Bourla G, Chen S, Kashyap M, Purohit S. Comparative analysis of machine learning algorithms through credit card fraud detection. In: 2018 IEEE MIT Undergraduate Research Technology Conference (URTC) [Internet]. IEEE; 2018 [cited 2024 Oct 24]. p. 1–4. Available from: https://ieeexplore.ieee.org/abstract/document/9244782/
5. Niu X, Wang L, Yang X. A Comparison Study of Credit Card Fraud Detection: Supervised versus Unsupervised [Internet]. arXiv; 2019 [cited 2024 Oct 21]. Available from: http://arxiv.org/abs/1904.10604
6. Gal Y, Ghahramani Z. Dropout as a Bayesian Approximation: Representing Model Uncertainty in Deep Learning [Internet]. arXiv; 2016 [cited 2024 Oct 23]. Available from: http://arxiv.org/abs/1506.02142
7. El Bouchti A, Chakroun A, Abbar H, Okar C. Fraud detection in banking using deep reinforcement learning. In: 2017 Seventh International Conference on Innovative Computing Technology (INTECH) [Internet]. IEEE; 2017 [cited 2024 Oct 21]. p. 58–63. Available from: https://ieeexplore.ieee.org/abstract/document/8102446/
8. Dal Pozzolo A, Boracchi G, Caelen O, Alippi C, Bontempi G. Credit card fraud detection: a realistic modeling and a novel learning strategy. IEEE transactions on neural networks and learning systems. 2017;29(8):3784–97.
9. Kazemi Z, Zarrabi H. Using deep networks for fraud detection in the credit card transactions. In: 2017 IEEE 4th International conference on knowledge-based engineering and innovation (KBEI) [Internet]. IEEE; 2017 [cited 2024 Oct 21]. p. 0630–3. Available from: https://ieeexplore.ieee.org/abstract/document/8324876/
10. Mead A, Lewris T, Prasanth S, Adams S, Alonzi P, Beling P. Detecting fraud in adversarial environments: A reinforcement learning approach. In: 2018 Systems and Information Engineering Design Symposium (SIEDS) [Internet]. IEEE; 2018 [cited 2024 Oct 21]. p. 118–22. Available from: https://ieeexplore.ieee.org/abstract/document/8374720/

11. Wang Y, Xu W. Leveraging deep learning with LDA-based text analytics to detect automobile insurance fraud. Decision Support Systems. 2018;105:87–95.
12. Jurgovsky J, Granitzer M, Ziegler K, Calabretto S, Portier PE, He-Guelton L, et al. Sequence classification for credit-card fraud detection. Expert systems with applications. 2018;100:234–45.
13. Eshghi A, Kargari M. Introducing a new method for the fusion of fraud evidence in banking transactions with regards to uncertainty. Expert Systems with Applications. 2019;121:382–92.
14. Eshghi A, KARGARI M. A new framework for combining supervised and semi-supervised methods in fraud detection. 2019 [cited 2024 Oct 21]; Available from: https://www.sid.ir/paper/784191/fa
15. Itri B, Mohamed Y, Mohammed Q, Omar B. Performance comparative study of machine learning algorithms for automobile insurance fraud detection. In: 2019 Third International Conference on Intelligent Computing in Data Sciences (ICDS) [Internet]. IEEE; 2019 [cited 2024 Oct 21]. p. 1–4. Available from: https://ieeexplore.ieee.org/abstract/document/8942277/
16. Thennakoon A, Bhagyani C, Premadasa S, Mihiranga S, Kuruwitaarachchi N. Real-time credit card fraud detection using machine learning. In: 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence) [Internet]. IEEE; 2019 [cited 2024 Oct 21]. p. 488–93. Available from: https://ieeexplore.ieee.org/abstract/document/8776942/
17. Fiore U, De Santis A, Perla F, Zanetti P, Palmieri F. Using generative adversarial networks for improving classification effectiveness in credit card fraud detection. Information Sciences. 2019;479:448–55.
18. Taha AA, Malebary SJ. An intelligent approach to credit card fraud detection using an optimized light gradient boosting machine. IEEE access. 2020;8:25579–87.
19. Nguyen TT, Tahir H, Abdelrazek M, Babar A. Deep Learning Methods for Credit Card Fraud Detection [Internet]. arXiv; 2020 [cited 2024 Oct 21]. Available from: http://arxiv.org/abs/2012.03754
20. Carrasco RSM, Sicilia-Urban MA. Evaluation of deep neural networks for reduction of credit card fraud alerts. IEEE Access. 2020;8:186421–32.
21. Rtayli N, Enneya N. Enhanced credit card fraud detection based on SVM-recursive feature elimination and hyper-parameters optimization. Journal of Information Security and Applications. 2020;55:102596.
22. Yan C, Li M, Liu W, Qi M. Improved adaptive genetic algorithm for the vehicle Insurance Fraud Identification Model based on a BP Neural Network. Theoretical Computer Science. 2020;817:12–23.
23. Baumann M. Improving a rule-based fraud detection system with classification based on association rule mining. 2021 [cited 2024 Oct 21]; Available from: https://dl.gi.de/items/a1d76fd7-fece-4b65-93bc-192bf80b04ad
24. Zhang X, Han Y, Xu W, Wang Q. HOBA: A novel feature engineering methodology for credit card fraud detection with a deep learning architecture. Information Sciences. 2021;557:302–16.

25. Carcillo F, Le Borgne YA, Caelen O, Kessaci Y, Oblé F, Bontempi G. Combining unsupervised and supervised learning in credit card fraud detection. Information sciences. 2021;557:317–31.
26. Hussein AS, Khairy RS, Najeeb SMM, Alrikabi HTS. Credit Card Fraud Detection Using Fuzzy Rough Nearest Neighbor and Sequential Minimal Optimization with Logistic Regression. International journal of interactive mobile technologies [Internet]. 2021 [cited 2024 Oct 21];15(5). Available from: https://lib.uowasit.edu.iq/books/25bde32a8e71b8d3f0912c6d6edaaffdf436.pdf
27. Li Z, Huang M, Liu G, Jiang C. A hybrid method with dynamic weighted entropy for handling the problem of class imbalance with overlap in credit card fraud detection. Expert Systems with Applications. 2021;175:114750.
28. Forough J, Momtazi S. Ensemble of deep sequential models for credit card fraud detection. Applied Soft Computing. 2021;99:106883.
29. Asha RB, KR SK. Credit card fraud detection using artificial neural network. Global Transitions Proceedings. 2021;2(1):35–41.
30. Habibpour M, Gharoun H, Mehdipour M, Tajally A, Asgharnezhad H, Shamsi A, et al. Uncertainty-aware credit card fraud detection using deep learning. Engineering Applications of Artificial Intelligence. 2023;123:106248.
31. Aburbeian AM, Ashqar HI. Credit Card Fraud Detection Using Enhanced Random Forest Classifier for Imbalanced Data. In: Daimi K, Al Sadoon A, editors. Proceedings of the 2023 International Conference on Advances in Computing Research (ACR'23) [Internet]. Cham: Springer Nature Switzerland; 2023 [cited 2024 Oct 24]. p. 605–16. (Lecture Notes in Networks and Systems; vol. 700). Available from: https://link.springer.com/10.1007/978-3-031-33743-7_48