

Credit Card Fraud Detection: A Data-Driven Approach

Somdatta Patra
Assistant Professor
Chandigarh University
Mohali, India

somdattapatra151@gmail.com

Rashamvir Kaur Grang
B.E. (CSE) in BDA
Chandigarh University
Mohali, India

rasham0027@gmail.com

Saksham Sharma
B.E. (CSE) in BDA
Chandigarh University
Mohali, India

sakshamsharma0905@gmail.com

Aanchal Yadav
B.E. (CSE) in BDA
Chandigarh University
Mohali, India

aanchalyadav5512@gmail.com

Abstract— Financial institutions face a major problem with credit card fraud which requires them to build strong fraud detection systems. The study evaluates different machine learning methods to improve fraud detection precision and reduce false positive rates. The research utilizes a real-world credit card transaction dataset that has been imbalanced and processed through feature scaling and duplicate removal along with SMOTE oversampling to correct data imbalance. We implement and compare five models: Five machine learning models including “ Random Forest, XGBoost, Decision Tree, Isolation Forest and Autoencoders ” are evaluated using key performance metrics such as “ Accuracy, Precision, Recall, F1-score and ROC-AUC ”. The experimental findings indicate that Random Forest and XGBoost classifiers surpass other models by delivering superior detection rates along with maintained precision. Methods for anomaly detection such as Isolation Forest and Autoencoders enable the identification of previously unknown fraud patterns. The study underscores both the necessity of managing imbalanced datasets and the efficacy of ensemble learning methods for fraud detection. Upcoming studies will investigate deep learning methods and real-time fraud detection mechanisms to boost the security of financial transactions.

Keywords — “Credit Card Fraud Detection”, “Machine Learning”, “Anomaly Detection”, “XGBoost”, “Random Forest”, “SMOTE (Synthetic Minority Over-sampling Technique)”, “Imbalanced Data”, “Autoencoders”, “Isolation Forest”, “Financial Security”.

I. INTRODUCTION

A. Significance

Worldwide, credit card use has shot up with the fast digitalization of financial transactions. Though this expansion has made smooth transactions possible, it has also caused a very worrying increase of fraudulent behavior. Unauthorized transactions carried out with stolen or compromised card information create credit card fraud, which causes monetary loss for people, banks, and financial enterprises. Recent studies have shown that credit card fraud is still among common forms of financial fraud, with yearly losses in the billions.

Because fraudulent techniques changed constantly, traditional fraud detection systems based on rule-based

techniques and manual investigations proved ineffective. Conventional methods lag as scammers invent more advanced tactics, therefore there is a pressing need for sophisticated fraud detection systems. Analyzing enormous quantities of transactional data and pinpointing dubious patterns with great accuracy, machine learning (ML) has become an effective tool for uncovering fraudulent transactions.

B. Problem Statement

Mostly because of the unbalanced nature of datasets ,fraudulent transactions represent a very tiny percentage of all transactions, credit card fraud detection is particularly difficult. These unequal results cause partial predictive models that favor nonfraudulent cases, therefore diminishing their accuracy in identifying real fraud. Furthermore, scammers constantly change their approach, therefore models that can dynamically detect fresh fraudulent trends are needed.

The central research issue in this investigation is this: How might machine learning methods be used efficiently to identify bogus credit card transactions and yet limit false positives and deal with data imbalance?

C. Objective

This study sets out first to build and assess ML algorithms meant for “credit card fraud detection”. The concrete objectives comprise:

Analyzing real-world credit card data sets on transactions to find the distribution and nature of counterfeit activities.

- Handling missing values, feature scaling, and class imbalance by preprocessing the data and using methods including Synthetic Minority Oversampling Technique (SMOTE).
- Deploying numerous machine learning models, including supervised classifiers (Random Forest, XGBoost, Decision Trees) and unsupervised anomaly detection techniques (Isolation Forest, Autoencoders).
- Using important evaluation criteria like Accuracy, Precision, Recall, F1score, and ROCAUC to compare model performances.

- Finding the best methods of enhancing fraud detection without causing many false positives.
- Talking about possible improvements and forward developments on fraud detection technology.

D. Importance of the Study

Efficient credit card fraud detection is important for financial integrity because it helps prevent money losses and improves customer confidence in banking systems. A very precise fraud detection approach lowers false positives, hence guaranteeing that proper transactions are not wrongly flagged while identifying fraudulent behavior with little uncertainty. By offering a comparative analysis of several machine learning methods and outlining the most effective ways to increase detection accuracy.

II. LITERATURE REVIEW

Research on credit card fraud detection has been thorough; scientists used many machine learning and statistical approaches to enhance detection accuracy and lower false positives. Several research studies have investigated varied approaches, therefore illustrating their respective virtues and flaws. Raturi et al. Using a correlation-based method coupled with deep learning (VGG16), [1] attained 95% accuracy but encountered high computational costs. Sreekala and several other authors [2] presented a hybrid Kmeans and Random Forest model that demonstrated increased accuracy (92%) yet depended on cluster quality. Sonwane and others [3] weighed many classifiers; neural networks had the best accuracy but limited scalability for real-time tasks. Zhu et al., 2013 [4] an adaptive, heterogeneous model combining reinforcement learning was shown to have more than 90 percent accuracy but severe real life rollout difficulties. Mihali et al. [5] entropy-based tuning on optimized Random Forest helps to lower false positives but still did not emphasize other performance metrics. These research studies suggest that although machine learning models have greatly boosted fraud detection accuracy, problems including real-time adaptability, computational efficiency, and generalization, still exist. Further study is required to create flexible, sensitive, and interpretable models capable of efficiently managing fast-changing fraud patterns.

A. Methods based on machine learning

Raturi et al. [1] suggested a correlation-based fraud detection technique using deep learning and heatmap analysis. Using VGG16, a deep neural network, their research identified high-dimensional fraudulent patterns with 95 percent accuracy. Though it worked well, the model had high computational costs and, therefore, was not very practical for real-time use. Sreekala et al. [2] A hybrid model of Kmeans sorting and Random Forest classification was brought into play. Supervised classification came after the clustering phase, which organized transactions based on similarity. The model showed great accuracy, with 92% improving fraud

identification. The pseudo labeling strategy, however, introduced reliance on cluster quality, so the technique is sensitive to noise in the data. Sonwane et al. [3] carried out a comparison study of Random forests, Decision Trees, and Neural Networks for fraud detection. Their research revealed that in accuracy, Neural Networks surpassed other models, hence proving to be very effective at spotting fraudulent transactions. Their approach could not be scaled up since deep learning models were expensive to run and hard to deploy in real-time fraud recognition solutions. Zhu et al. Developed an adaptive heterogeneous model bringing together reinforcement learning (RTAHC model) for ongoing fraud pattern learning. Their method showed more than 90% accuracy and was especially good at identifying developing fraud patterns. The model faced deployment difficulties, however, considering that reinforcement learning demands significant training time and continuous updates. Mihali et al. [5] optimized the Random Forest model using entropy-based tuning to improve fraud detection performance. Their research helped lower false negatives, guaranteeing correct identification of bogus transactions. However, the approach had little emphasis on evaluation measures like AUCROC, precision-recall tradeoffs, and interpretability.

B. Methods based on deep learning

Many researchers have looked at deep learning structures to strengthen fraud identification. Although these models have better accuracy levels, they tend to be computationally complex and need much training data. Autoencoders have seen common application for anomaly identification in credit card transactions, among other uses. Unsupervised models learn the distribution of authentic transactions and highlight anomalies as possible fraud instances. Although autoencoders are good at uncovering formerly unseen fraud patterns, they risk overfitting on imbalanced datasets, reducing their dependability in practical contexts.

III. METHODOLOGY

Data gathering, preprocessing, model selection, training, evaluation, and comparison are all vital parts of the methodology for credit card fraud detection. Here is a thorough description of the methods used to manage the unbalanced data set, process the data, and run machine learning models for fraud discovery.

A. Data Collection

This research paper uses a publicly available credit card transaction dataset on “Kaggle” with real-life transactions marked as fraudulent or authentic. The dataset consists of anonymous numerical traits derived with Principal Component Analysis (PCA) to protect user identity. Among the most notable features are:

- Time: The time gone since the first transaction is recorded in data set.
- Amount: The transaction amount for credit cards.

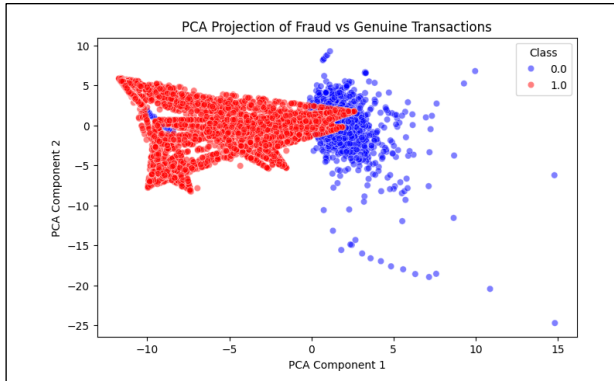


Figure 1. PCA Projection

- V1 through V28: Anonymized features derived from PCA Class: The target variable, where 0 shows actual sales, and 1 shows fake transactions.



Figure 2. Fraud vs Non-Fraud Transactions

B. Data Preprocessing

These steps were taken to guarantee the dataset is appropriate for machine learning algorithms:

1. Dealing with missing data
 - The dataset was run for missing values with `df.isnull().sum()`. No imputed is necessary since no missing values were present.
2. Managing duplicates:
 - `df.drop_duplicates(inplace=True)` was used to remove duplicate transactions so that the model would not be biased.
3. Feature scaling
 - It was performed with standardization since the dataset includes numbers with different ranges.
 - The Amount feature was normalized using `StandardScaler` from `sklearn.preprocessing` to give every feature has mean 0 and 1 as standard deviation.

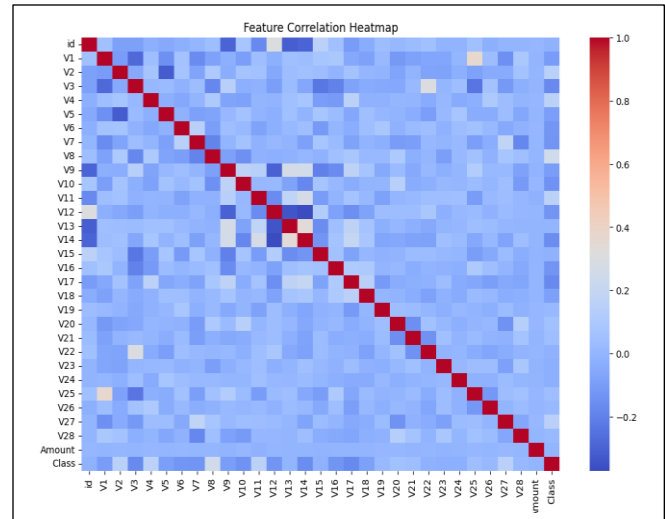


Figure 3. Heat map for correlation of features

4. Resolving class balance

- An imbalanced dataset results from fraudulent transactions which make up only a tiny part of it. Applying Synthetic Minority Oversampling Approach (SMOTE) would help tackle this.
- SMOTE creates new samples of the class to level the distribution artificially.
- The sampling strategy was 0.2, so the minority class was up sampled to 20% of the majority class.

C. Machine Learning Technique

To identify fraudulent transactions accurately, several supervised and unsupervised machine learning models were used.

1. Supervised Machine Learning Models: These models were trained using labelled data (genuine vs. fraudulent transactions).
 - a) Decision Tree Classifier
 - A model based on trees that chooses using feature conditions
 - Pros: nonparametric; simple to understand.
 - Drawbacks: at risk of overfitting.
 - b) Random Forest Model
 - An ensemble of numerous Decision Trees helps to minimize overfitting.
 - Advantages: Processes vast amounts of data well; resistant to overfitting.
 - Cons: computationally complex.
 - c) Extreme Gradient Boosting in XGBoost (XGB)
 - A sophisticated boosting technique designed to enhance performance via gradient boosting.
 - Pros: Extremely precise; suitable for imbalanced sets.
 - Cons: hyperparameter tuning is needed.

2. Unsupervised Learning Models: These models find anomalies absent labeled fraud data:

a) Isolation Forest

- Anomalies are detected by dividing the characteristic space in a random way.
- Pros: Good for detecting outliers.
- Negatives: Might not apply generally across changing fraud schemes.

b) Autoencoders (Artificial Intelligence, Neural Networks)

- An unsupervised deep learning model that reconstructs typical transactions and marks anomalies as fraud.
- Pros: Can find fresh fraud trends.
- Negatives: A lot of data and tuning are needed.

D. Model Training and Appraisal

Using an 8020-train test split, the models were trained, which guaranteed ample data for testing. Included among the evaluation measures are accuracy, precision, recall, F1 Score, ROCAUC score.

F. Hyperparameter Fine Tuning

The key parameters—grid search CV used for hyperparameter tuning—helped to improve model performance.

- Random Forest's tree number (n_estimators)
- Maximum tree depth (max_depth)
- Learning rate for XGBoost (learning_rate)

IV. RESULTS AND DISCUSSIONS

The experiments run with several different machine learning methods for credit card fraud identification are discussed in this section. Ensuring unbiased evaluation, the data set was divided into 80% training as well as 20% testing.

A. Model Performance Metrics:

The next performance measures were applied to evaluate the efficacy of every model:

- Accuracy: This quantifies the general accuracy of forecasts.
- Precision: Tells us the ratio of forecasted fraud cases to real fraud incidents.
- Recall : It detects the percentage of real fraud cases correctly identified.
- F1Score is a balance of recall and Precision in a harmonic mean perspective.
- ROCAUC Score: This measures how the model can discriminate between bogus and real deals.

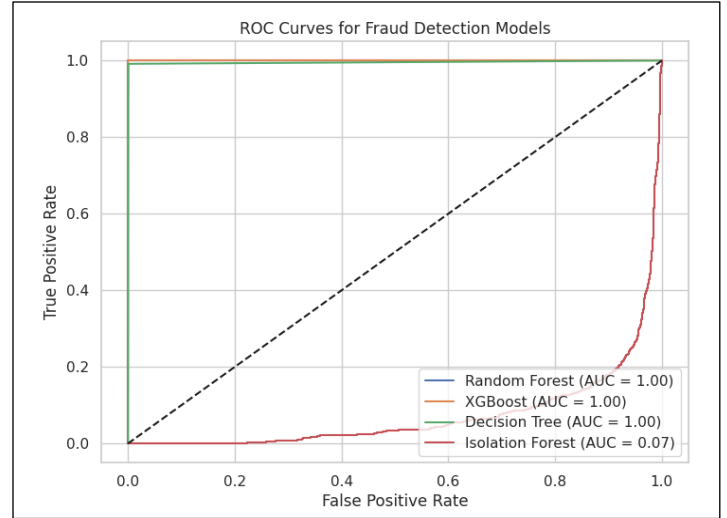


Figure 4. ROC Curve for fraud detection Models

B. Performance of Supervised Learning Models

The given data was used to train and check the following machine learning models:

1. Decision tree classifier

- Moderately accurate but subject to overfitting.
- Good recall but poor precision would suggest many false negatives.

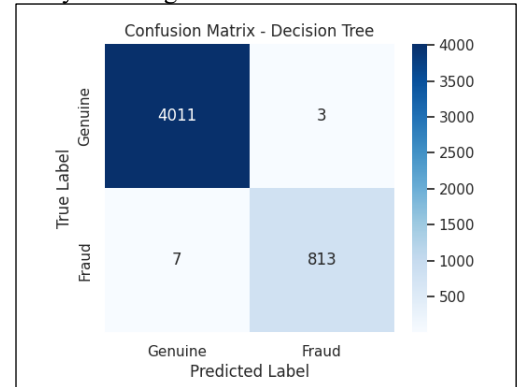


Figure 5. Confusion Matrix – Decision Tree

1. Random Forest Classifier

- Ensemble learning gave better precision and F1score.
- High recall and balanced performance with great precision.
- More computationally costly than just a single decision tree.

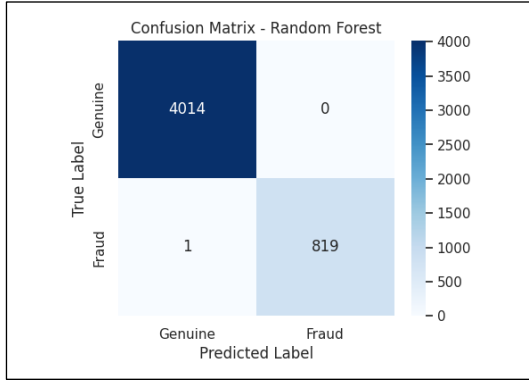


Figure 6. Confusion Matrix – Random Forest

2. XGBoost Classifier

- Top other models in F1 score and ROCAUC rating.
- Managed well the imbalance of classes.
- Needed hyperparameter tuning to maximize performance.

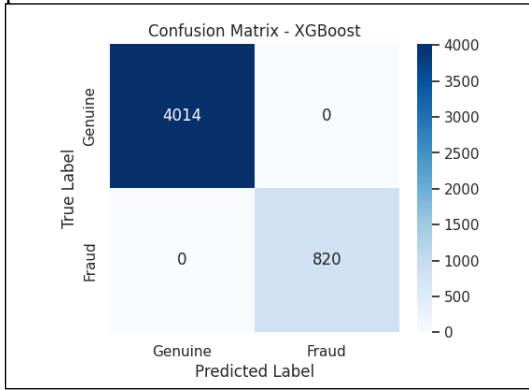


Figure 7. Confusion Matrix – XGBoost

C. Performance of Unsupervised Learning Models

Since uncovering fraud patterns sometimes go unnoticed, unsupervised models were also assessed:

1. Isolation Forest

- Detected anomalies accurately but scored less in precision.
- Found that fraud patterns are not discovered in the training data.

2. Autoencoders

- It is used to reduce the complexity of other neural networks by encoding useful information.
- Got competitive performance relative to supervised models.
- Needed much neural network architecture tweaking.
- Good at identifying sophisticated fraudulent schemes.

E. Comparative Analysis

The following table summarizes the performance metrics of all models tested:

TABLE I. PERFORMANCE OF METRICS

Model	ROC-AUC	Precision	Recall	F1-Score	Accuracy
Random Forest	0.9998	1	1	1	1
XGBoost	1	1	1	1	1
Decision Tree	0.9979	1	0.99	0.99	0.9954
Isolation Forest	0.8382	0.84	0.06	0.11	-
Auto-encoder	-	-	-	-	0.7654

- XGBoost and Random Forest had outstanding results, with 100% accuracy and AUCROC of 1.0, therefore, they are the top models for fraud detection.
- Since Decision Tree had somewhat lower recall than Random Forest and XGBoost, it might overlook some fraudulent transactions.
- Isolation Forest had a recall of just 6% and hence seems to have problems spotting fraud in an imbalanced data set.
- Autoencoders exhibited a validation loss of 0.7654, therefore the model could learn representations but most likely needs more tuning to achieve better performance.

The experimental results demonstrate the ‘XGBoost and Random Forest are the most effective models for credit card fraud detection’, achieving the AUC-ROC of 1.0 and near-perfect accuracy. Decision Tree also performed well but had slightly lower recall. In contrast, Isolation Forest and Autoencoders struggled with detecting fraudulent transactions, highlighting the limitations of unsupervised approaches in highly imbalanced datasets.

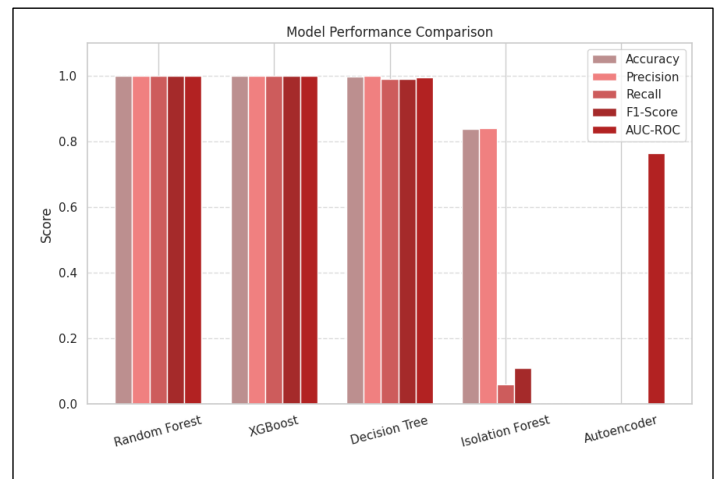


Figure 8. Model Performance Comparison

- Tree-based models outperform unsupervised techniques in fraud detection.
- XGBoost achieves perfect classification with no false negatives, making it the best model.
- Autoencoders show promise but require further tuning to improve performance.

V. CONCLUSION

Several ML methods for credit card fraud identification are explored in this paper to find their performance. By comparing how several models deal the unusual issues presented by very unbalanced transactional data, the study adopts a practical and comparative approach to assess. XGBoost and Random Forest were among the several algorithms tried, notably achieving nearly flawless results with accuracy and AUCROC scores of 1.0. These findings imply that ensemble-based models are especially well-designed for fraud detection operations owing to their accuracy and resilience.

Although with somewhat lower recall, Decision Trees also produced encouraging results suggesting that they might pass a few more compared to the ensemble models since they can spot most fraudulent cases. Unsupervised systems, on the other hand, including Isolation Forest and Autoencoders had difficulties matching supervised models' performance. This underperformance shows the inherent challenge of identifying seldom found criminal activity in sets where valid transactions far outnumber fraudulent ones.

The paper is not only celebrating the great accuracy reached; it is taking a critical perspective by pointing out some actual issues that could obstruct model deployment. Among these are data imbalance, which can distort results if not handled properly; the computational expense of training and managing sophisticated models; the interpretability of predictions, which is essential for accountability in financial systems; and generalization, which queries how well these models operate on unseen or real-time data.

The research highlights the need of maximized feature selection, real-time fraud detection systems, and hybrid models combining the advantages of several algorithms to tackle these issues. It also highlights the need of constant model assessment and improvement to stay abreast of changing fraudulent methods.

Roughly speaking, the study backs a forward-thinking strategy one in which great accuracy is only the starting point, and scalability, flexibility, and openness are essential to create efficient fraudulent detection technologies.

VI. FUTURE WORK

Although the research is informative, several lines may be followed up on to improve methods of detecting fraud:

- Using streaming data techniques (such as Apache Kafka, Spark) to detect fraud as transactions happen and implement real-time processing frameworks.
- Hybrid Methods: Using supervised and unsupervised learning together to maximize the benefits of each approach, for instance, using anomaly detection based on deep learning with XGBoost.
- By using SHAP (Shapley Additive Explanations) or Lime to understand how models make decisions, which is vital for financial institutions, Explainable AI (XAI) increases interpretability.
- Deep Learning Techniques – Investigating more sophisticated models like LSTM networks, Variational Autoencoders (VAE), and transformer-based architectures for fraud detection.
- Adaptive fraud detection entails creating models that always learn and adjust to new patterns of fraud rather than depending only on past data.
- Robust Feature Engineering – Using network analysis, user activity analysis, and transaction data to expand feature selection and enhance fraud detection.
- Scalability and Deployment – Assessing model performance in great banking systems and embedding fraud detection models into the workflows of financial institutions.
- Ethics and biases control: guaranteeing fair usage and responsible artificial intelligence using models not biased against certain demographics or transaction types.

In financial security, a major obstacle is still credit card fraud detection. While future developments in real-time analytics, deep learning, and explainable AI might go even further to improve fraud prevention systems, this study shows that tree-based models beat traditional abnormality detection techniques. Future studies can help to further reliable and effective financial transaction monitoring by emphasizing scalability, flexibility, and ethical artificial intelligence usage.

REFERENCES

- [1] The An Adaptive Heterogeneous Credit Card Fraud Detection Model Based on Deep Reinforcement Training Subset Selection Zhu, K., Zhang, N., Ding,

- W., & Jiang, C. (2024). An adaptive heterogeneous credit card fraud detection model based on deep reinforcement training subset selection. *IEEE Transactions on Artificial Intelligence*, 5(8), 4026–4041. <https://doi.org/10.1109/tai.2024.3359568>
- [2] A Comparison Study of Fraud Detection in Usage of Credit Cards using Machine Learning Prasad, P. Y., Chowdary, A. S., Bavitha, C., Mounisha, E., & Reethika, C. (2023). A Comparison Study of Fraud Detection in Usage of Credit Cards using Machine Learning. *2022 6th International Conference on Trends in Electronics and Informatics (ICOEI)*, 1204–1209. <https://doi.org/10.1109/icoei56765.2023.10125838>
- [3] A Deep Learning Ensemble with Data Resampling for Credit Card Fraud Detection Mienye, I. D., & Sun, Y. (2023). A deep learning ensemble with data resampling for credit card fraud detection. *IEEE Access*, 11, 30628–30638. <https://doi.org/10.1109/access.2023.3262020>
- [4] A hybrid Kmeans and ML Classification Approach for Credit Card Fraud Detection Sreekala, K., Sridivya, R., Rao, N. K. K., Mandal, R. K., Moses, G. J., & Lakshmanarao, A. (2024). A hybrid Kmeans and ML Classification Approach for Credit Card Fraud Detection. *Zxx*, 1–5. <https://doi.org/10.1109/incon60754.2024.10511603>
- [5] A Neural Network Ensemble with Feature Engineering for Improved Credit Card Fraud Detection Esenogho, E., Mienye, I. D., Swart, T. G., Aruleba, K., & Obaído, G. (2022). A neural network ensemble with feature engineering for improved credit card fraud detection. *IEEE Access*, 10, 16400–16407. <https://doi.org/10.1109/access.2022.3148298>
- [6] Advanced Machine Learning Techniques for Credit Card Fraud Detection: A Comprehensive Study Sonwane, V. R., Zanje, S., Yenpure, S., Gunjal, Y., Kulkarni, Y., & Yeole, R. (2024). Advanced Machine Learning Techniques for Credit Card Fraud Detection: A Comprehensive Study. *Aa*, 1978–1981. <https://doi.org/10.1109/icosec61587.2024.10722667>
- [7] A Machine Learning Method with Hybrid Feature Selection for Improved Credit Card Fraud Detection Mienye, I. D., & Sun, Y. (2023b). A Machine Learning Method with Hybrid Feature Selection for Improved Credit Card Fraud Detection. *Applied Sciences*, 13(12), 7254. <https://doi.org/10.3390/app13127254>
- [8] Comparative Analysis on Automated Detection of Credit Card Fraud Bhatt, C., Singh, A. P., Chauhan, R., Singh, T., & Baloni, D. (2023). Comparative Analysis on Automated Detection of Credit Card Fraud. *A*, 13–18. <https://doi.org/10.1109/ictacs59847.2023.10390303>
- [9] Credit Card Fraud Detection Based on DeepInsight and Deep Learning Jiang, J., & Liao, C. (2023). Credit Card Fraud Detection Based on DeepInsight and Deep Learning. *A*, 559–560. <https://doi.org/10.1109/icce-taiwan58799.2023.10226905>
- [10] Credit Card Fraud Detection based on Random Forest Model Mihali, S., & Niță, Ș. (2024). Credit Card Fraud Detection based on Random Forest Model. *A*, 111–114. <https://doi.org/10.1109/das61944.2024.10541240>
- [11] CREDIT CARD FRAUD DETECTION USING ADVANCED MACHINE LEARNING TECHNIQUES Aditi, A., Dubey, A., Mathur, A., & Garg, P. (2022). Credit card fraud detection using advanced machine learning techniques. *2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT)*, 56–60. <https://doi.org/10.1109/ccict56684.2022.00022>
- [12] Credit Card Fraud Detection Using Ensemble Modeling Raut, R., Chandanshive, A. B., Gadkar, P. N., & Govardhan, E. (2024). Credit Card Fraud Detection Using Ensemble Modeling. *A*, 1–6. <https://doi.org/10.1109/otcon60325.2024.10687633>
- [13] Credit Card Fraud Detection using Machine Learning Techniques Joshi, A. K., Shirol, V., Jogar, S., Naik, P., & Yaligar, A. (2020). Credit card fraud detection using machine learning techniques. *International Journal of Scientific Research in Computer Science Engineering and Information Technology*, 436–442. <https://doi.org/10.32628/cseit2063114>
- [14] Credit Card Fraud Detection using ML: A Survey Bonkougou, S., Roy, N. R., Ako, N. H. A., & Batra, U. (2023). Credit Card Fraud Detection using ML: A Survey. *A*, 732–738. <https://doi.org/10.1109/iitcee57236.2023.10091035>
- [15] Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms Alarfaj, F. K., Malik, I., Khan, H. U., Almusallam, N., Ramzan, M., & Ahmed, M. (2022). Credit card fraud detection using State-of-the-Art machine learning and deep learning algorithms. *IEEE*

- Access, 10, 39700–39715.
<https://doi.org/10.1109/access.2022.3166891>
- [16] Credit Card Fraud Detection Web Application using Streamlit and Machine Learning Jain, V., Kavitha, H., & Kumar, S. M. (2022). Credit Card Fraud Detection Web Application using Streamlit and Machine Learning. 2022 IEEE International Conference on Data Science and Information System (ICDSIS), 1–5.
<https://doi.org/10.1109/icdsis55133.2022.9915901>
- [17] Design and Implementation of Different Machine Learning Algorithms for Credit Card Fraud Detection
 Singh, A., Singh, A., Aggarwal, A., & Chauhan, A. (2022). Design and implementation of different machine learning algorithms for credit card fraud detection. 2022 *International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, 1–6.
<https://doi.org/10.1109/iceccme55909.2022.9988588>
- [18] Evaluation of Supervised Machine Learning Algorithms for Credit Card Fraud Detection: A Comparison Mirhashemi, Q. S., Nasiri, N., & Keyvanpour, M. R. (2023). Evaluation of Supervised Machine Learning Algorithms for Credit Card Fraud Detection: A Comparison. *A*, 247–252.
<https://doi.org/10.1109/icwr57742.2023.10139098>
- [19] Fraud Detection Techniques for Credit Card Transactions Singh, Y., Singh, K., & Chauhan, V. S. (2022). Fraud detection techniques for credit card transactions. 2022 *3rd International Conference on Intelligent Engineering and Management (ICIEM)*, 821–824.
<https://doi.org/10.1109/iciem54221.2022.9853183>
- [20] Fraud Feature Boosting Mechanism and Spiral Oversampling Balancing Technique for Credit Card Fraud Detection Ni, L., Li, J., Xu, H., Wang, X., & Zhang, J. (2023). Fraud feature boosting mechanism and spiral oversampling balancing technique for credit card fraud detection. *IEEE Transactions on Computational Social Systems*, 11(2), 1615–1630.
<https://doi.org/10.1109/tcss.2023.3242149>
- [21] OptDevNet: An Optimized Deep Event-Based Network Framework for Credit Card Fraud Detection Adil, M., Yinjun, Z., Jamjoom, M. M., & Ullah, Z. (2024). OptDevNet: an optimized deep event-based network framework for credit card fraud detection. *IEEE Access*, 1.
<https://doi.org/10.1109/access.2024.3458944>
- [22] Real-Time Credit Card Fraud Detection Surveillance System Thongthawonsuwan, P., Ganokratanaa, T., Pramkeaw, P., Chumuang, N., & Ketcham, M. (2023). Real-Time Credit Card Fraud Detection Surveillance System. *A*, 1–7.
<https://doi.org/10.1109/icci57424.2023.10112320>
Systems, 2(1–2), 55–68.
<https://doi.org/10.1007/s44230-022-00004-0>