

ML Based Algorithmic Strategies for Effective Credit Card Fraud Detection

Dr. S.S.Aravinth¹, Nallamothu Deepthi², Mahammad Rubeena Afreen³, Gorla Mythri⁴ and Shyam Kumar⁵

¹⁻⁵Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Guntur, Andhra Pradesh, India

Email: aravinthkrithick@gmail.com, deepthinallamothu2004@gmail.com, mahammadrubeenaafreen@gmail.com, mythrigorla@gmail.com

Abstract—This article delves into the intricate realm of "credit card fraud," a term denoting the compromise or loss of private credit card information. The research focuses on deploying an array of machine learning methodologies to effectively detect such fraudulent activities. A substantial credit card fraud dataset is used to make this possible, and the SMOTE approach is applied to support oversampling in order to address the issue of imbalance in the dataset. This project's primary objective is to carefully assess and compare the efficacy of various machine learning approaches after meticulous feature selection and dataset partition. Among the noteworthy methods examined are support vector machines (SVM), random forests, decision trees, and logistic regression. These algorithms are examined from several angles, including important performance measures like recall, accuracy, precision, and F1-score. The credit card fraud dataset used as the basis for the analytical methodology is one that is made publicly available and was carefully selected to provide information that is critical to financial institutions and other stakeholders. The outcome of this project is poised to guide decision-making processes, enabling these entities to make informed choices when selecting the most optimal machine learning paradigm for bolstering credit card fraud detection mechanisms.

Index Terms— SVM, SMOTE technique, Random Forest Algorithm, Accuracy, Credit Card.

I. INTRODUCTION

Fraud occurs when someone who isn't the account owner uses a credit card without authorization or legal justification. By taking the required precautionary steps, this misuse can be stopped. It is also possible to investigate the behavior of such fraudulent operations in order to avoid and lessen their occurrence going forward. Using someone else's credit card for personal expenses is referred to as credit card fraud. Spending without that person's consent or the consent of the credit card's issuing company. Monitoring user population behavior is a key component of fraud detection since it makes it possible to spot and stop fraud, intrusion, and defaults [1]. This crucial issue communities like Situations that call for an automated response must be addressed via machine learning and data science. believable. This problem is extremely challenging from a learning perspective because it displays several characteristics, such as class inequality. Trades that are honest outnumber those that are dishonest. Furthermore, the statistical characteristics of the transaction patterns change over time on a regular basis. However, putting implementing Real-world fraud detection systems face a number of difficulties. Real-world examples highlight how quickly automated technology sorts through the enormous

amount of payment requests to decide which ones should be authorized. All authorized transactions are analyzed using machine learning techniques to find those that may be questionable [2]. To find out if the transaction was real or fraudulent, investigators looking into these claims talk with the cardholders. The automated method gradually improves the efficacy of fraud-detection over time by training and adjusting the algorithm based on feedback from the investigators. Methods for identifying fraud are always being developed in order to prevent con artists from altering their misleading tactics.. These con artists fall under the following categories: Credit card fraud, both Account insolvency, device hacking, application fraud, counterfeit cards, and card theft and telecom fraud are only a few examples of crimes committed both online and offline. of the many distinct forms of fraud. Current methods for detecting this kind of Artificial Genetic Algorithms, fuzzy logic, neural networks, logistic regression, and decision trees are examples of fraudulent practices [3]. Unusual approaches have often worked well on medium-sized online transactions, such as Complex network classification methods that mix data mining and network reconstruction to create representations of how one instance varies from a reference group. Using actual card transaction data, these techniques can spot instances of illicit activity. Initiatives to move forward entirely differently have also been made [4]. When a fraudulent transaction takes place, the alert feedback exchange has been improved. If a transaction was fraudulent, the approved system would be notified and it would be suggested that the present transaction be declined. Among the methods they provided was a synthetic genetic algorithm.

II. LITERATURE SURVEY

TABLE I. COMPARISON OF VARIOUS MODELS AND THEIR RESULTS

S. NO	AUTHOR	MODEL	FINDINGS	LIMITATIONS
1	FAWAZ KHALED ALARFAJ.E.T.A.L[10]	Deep Learning Algorithms, Machine Learning	Out of the 284,807 transactions in the dataset, 492 were scams that occurred within the last two days.	The highly imbalanced distribution of the dataset
2	Amlan Kundu,E.T.A.L[11]	BLAST-SSAHA Hybridization	For evaluating the efficacy of detection of credit card fraud systems, there are no benchmark statistics available. Additionally, credit card firms are refusing to provide private transactional data.	The absence of benchmark statistics for evaluating credit card fraud detection systems and the unavailability of private transactional data from credit card firms.
3	SP Maniraj.E.T.A.L[12]	Machine Learning and Data Science	This is used to determine the algorithms' precision and accuracy. The component of the dataset we used for expedited testing accounted for 10% of the entire dataset	A subset comprising ten percent of the total dataset was utilized for expedited testing purposes.
4	Vaishnavi Nath Dornadula.E.T.A.L [13]	Machine Learning Algorithms	On the original dataset as well as the SMOTE dataset, we have tested a few models. Even better for binary class datasets, we employed one-class SVM.	Particularly suited for binary class datasets, we also employed the one-class in the evaluation.
5	Emmanuel Ileberi.E.T.A.L [14]	GA algorithm for feature selection	There were two phases to the experimentation. In the first step, a classification procedure was completed using F = v1, v2, v3, v4, and v5. Each feature vector in F. It was trained and evaluated using the RF, DT, ANN, NB, and LR algorithms.	It relies on a simulated dataset, which may not fully capture the intricacies and nuances of real-world credit card fraud scenarios.
6	Vaishnavi Nath Dornadula [15].	Machine Learning Algorithms	Finally, we discovered that the algorithms that produced the best results were those that used logistic regression, decision trees, and random forests.	Evaluation may not fully account for potential variations in credit card fraud patterns across different time periods or geographical regions.
7	Swarna Deep Sarkar Shadab Ahmed [16]	Machine Learning and Data Science	Despite the fact that the algorithm's accuracy is above 99.6%, its precision is only 28% when only a tenth of the data set is taken into account.	Indicating potential challenges in handling smaller and more targeted samples.
8	Yanxia Sun & Zenghui Wang [17]	Gentic algorithm	The results of the trial demonstrated that the GA-DT had a 100% accuracy rate and an AUC of 1. backed up by the GA-	Evaluation focused on a specific set of datasets, potentially limiting the generalizability of the

			ANN, which had a 100% accuracy rate and an AUC of 0.94. We want to evaluate our system using more datasets in further research.	system's performance.
9	Ibtissam Benchaji, Samira Douzi, [18]	attention mechanism and LSTM deep model	Our model was run on two separate credit card datasets to confirm our findings, and it demonstrates its capacity to provide a high sensitivity performance during the identification of fraudulent cases, which are of major importance in this domain.	The focus on only two distinct credit card datasets, potentially limiting the comprehensiveness of our model's validation.
10	Selvani Kavila [19]	Machine Learning	It achieves 90.0, 94.3, and 95.5 percent accurate for logistic regression, decision tree, and random forest classifier, respectively	Comparison may overlook potential nuances and contextual factors that influence the algorithms.

III. MODEL REQUIREMENTS

A. Platform Requirements

The approach this study suggests uses state-of-the-art machine learning techniques to spot outliers or unusual behaviors. The basic rough architecture diagram is shown in the following picture.

B. Module Description

First of all, Kaggle, a data analysis service that provides datasets, is where we got our dataset. This dataset consists of 31 columns altogether, 28 of which have the labels "v1-v28" on them to safeguard sensitive information. Time, quantity, and class are indicated in the other columns. How much time passed between the first and second transactions is shown by the time indicator. The total amount of money traded is the amount. If a transaction is lawful, it is categorized as Class 0, and if it is fraudulent, it is labeled as Class 1 [20–22]. This graph allows you to visually understand the dataset and look for any anomalies. It displays the times at which transactions were completed over a period of two days. It's clear that the most transactions occurred during the Below is a heatmap of this area:

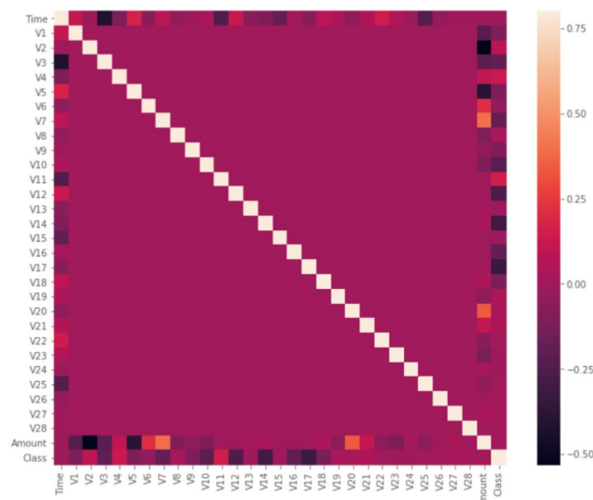


Fig 1: Missing value imputation area's heat map

From fig 1: A missing value imputation area's heat map provides a visual representation of missing data patterns within a dataset, enabling analysts to identify and address areas with significant data gaps. A missing value imputation area's heat map is a powerful exploratory tool for understanding the distribution and patterns of missing data within a dataset. It aids in identifying areas of concern, formulating imputation strategies, and making informed decisions about data preprocessing and analysis.

From fig 2: Transaction Class Distribution Frequency vs. Class" refers to a graphical representation that illustrates the frequency distribution of different classes within a transaction dataset. This type of visualization is commonly used in fields such as finance, fraud detection, and machine learning, where transactions are categorized into different classes based on certain criteria. Transaction Class Distribution Frequency vs. Class



Fig 2: Transaction class distribution frequency vs. class

visualization is a useful tool for understanding the distribution of different classes within a transaction dataset. It helps in making informed decisions about data analysis, model building, and addressing class imbalance in various applications, including fraud detection and machine learning.

IV. DESIGN AND IMPLEMENTATION

A. Algorithms (*K-Nearest Neighbour*)

- K-Nearest Neighbor is a machine learning method based on supervised learning that is among the simplest.
- Assuming that the new case/data and the prior cases are identical, the K-NN technique classifies the new instance in the category to which the available examples are most similar.

The K-NN method maintains all of the old data while classifying new data based on similarity. This shows that the K-NN method can rapidly and accurately identify fresh data.

While both classification and regression problems may be solved by trying the K-NN method, classification problems are the ones where it is most typically applied.

Since K-Nearest Neighbor is a non-parametric technique, no presumptions are made on the underlying data.

Because it saves the training dataset rather than instantly learning from it, the technique is often described as a slow learner algorithm. Instead, while categorizing data, it uses the dataset to carry out an operation.

The sklearn Programme contains this algorithm. Classification, regression, and outlier identification ensemble-based approaches and algorithms are included in the ensemble module of the sklearn package. The NumPy, SciPy, and matplotlib modules, which provide many simple and useful tools for data analysis and machine learning, were used to construct this free and open-source Python library. It comes with a range of classification, clustering, and regression methods and is designed to work with scientific and numerical libraries. We developed a Python program that demonstrates the methods suggested in this paper using the Jupiter Notebook platform. The Google Collaboration platform allows this software to be executed in the cloud as well. It enables any file created with Python Notebook.

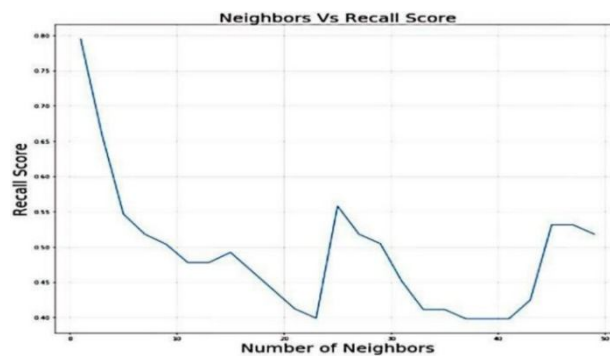


Fig 3: Neighbors Vs Recall Score

The relationship between the number of neighbors in the K-Nearest Neighbors (KNN) algorithm and the recall score is a pivotal consideration in binary classification. Adjusting the 'k' value in KNN impacts the recall score; lower 'k' values can enhance recall by correctly classifying nearby positive instances, potentially leading to overfitting and reduced precision, while higher 'k' values promote generalization, potentially improving precision but potentially missing nearby positive instances and lowering recall. Striking the right balance between 'k' and recall involves a trade-off between capturing immediate positive instances and achieving better overall model performance, necessitating a careful selection of 'k' based on data characteristics and desired outcomes.

B. Implementation

It is challenging to implement this idea since banks must cooperate yet are hesitant to do so because of market competitiveness, legal concerns, and the need to secure customer data. We worked on the machine learning methods of logistic regression, Support Vector Machine (SVM), Random Forest, Decision Tree, and KNN during the implementation. Using all these methods, analysis of credit card fraud detection gave accurate values. From the dataset which is downloaded the data is split into training and testing data. Both the training and testing data all the machine learning algorithms are implemented and which gave individual accuracies. All the accuracies are compared and it is found that KNN gave the highest accuracy among all the other implemented methods. Since banking information is sensitive, just an overview of the results is given here. There are very few occurrences of this strategy on the level 1 list, but they are almost certainly scammers. The requirement is more difficult for the other list. The level 2 list is still narrow enough to take into account every distinct situation. At least half of the cases on this list, according to credit and collections authorities, might have involved questionable fraudulent activity. passwords, phone numbers, and email addresses in order to reduce overhead costs and increase productivity. The level 2 and level 3 lists could be utilized with these additional questions.

V. COMPARITIVE ANALYSIS, RESULTS AND DISCUSSIONS

A. Comparison of Sampling Methods across Various Classifiers

From the training dataset, four distinct selected datasets were produced, which were then used to train each classifier. Each classifier starts with a dataset that hasn't been sampled. F1, Precision, and Recall are the assessment measures that are employed. The four classifiers that have been developed to use the four distinct sampling techniques are the Gradient Boosting Machine (GBM), Stacked Ensemble (SE), Distributed Random Forest (DRF), and Artificial Neural Network (ANN) (RUS, SMOTE, DBSMOTE, SMOTEENN). For each sample strategy used, the findings reported in this section detail the classifier in question. Each classifier concludes with a detailed explanation of the crucial evaluation metrics F1, Precision, and Recall score. the employing makes it simpler to comprehend how the classifier performed with each of the sample approaches and the confusion matrix.

B. Artificial Neural Networks

The ANN architecture in this instance was configured with two layers: the output layer, which had 200 neurons, and the hidden layer, which contained 30 neurons. Rectified Linear Unit (ReLU) was the activation function that was employed. The model went through 61 rounds of the training dataset before reaching peak performance. A dropout of 40% was used to Programme the model to automatically remove the neurons from the hidden layer. For this case, the model's learning rate was set at 0.005. As the harmonic mean of the two measurements, the F1 measure, the highest F1 score on an unsampled dataset is 0.8116, which is ideal when accuracy and recall are equally relevant or significant. However, recall is more important than precision in the case of FDS of all the datasets under consideration, the RUS sampling strategy received the lowest accuracy rating and highest recall (0.8311). Despite having a recall that is lower than the ANN with SMOTE's second-highest recall of 0.7635, The ANN using unsampled data has largest f1 score (0.8116), which was best. As a result, SMOTE sampling is a superior model for ANN.

C. DistributedRandomForest(DRF):

With a maximum tree depth of 20, there were to be 43 trees. The minimum tree depth, which lessens model complexity, prevents overfitting. When the value for the min rows option is set to 5, each leaf must have at least 5 observations. The row sampling rate, set at 63%, is determined by the sample rate. As 0.8 was chosen as the column sample rate, 80% of the columns must be sampled in order to construct one tree. More varied trees with strong regularisation qualities will be produced when the column sample rate is decreased. The maximum accuracy provided at 0.9286 had an impact on the F1 score, which was highest for the DRF's unsampled

dataset. For SMOTE sampling, which we believe to be a more significant and important metric, the highest recall is at 0.8176 with an acceptable precision of 0.86. SMOTE sampling has an exceptional recall rating, making it the ideal sampling model for DRF. It should be noted that the DRF classifier received the second-best recall score from SMOTEENN sampling. The SMOTEENN technique uses the Nearest Edited Neighbor strategy to reduce data or eliminate noise, which removes any sample that has been incorrectly classified by its three closest neighbors. Because the recall score was lower than with the initial SMOTE sampling, this result demonstrates that noise reduction is unsuccessful.

D. Gradient Boosting Machine (GBM):

There were 116 trees in total with a 15-foot maximum tree depth. As a result, over fitting may be prevented and model complexity may be reduced. Since the column sampling rate was set at 0.8, and a minimum of 100 rows were sampled from each tree, each tree will consume 80% of the columns. Two sample methods, SMOTE and SMOTEENN, were discovered to produce the highest recall score, which was 0.81. The model which has largest level of accuracy is represented by the F1 score. May be used as a choice criterion when two classifiers produce recall scores that are equivalent consequently, is the best model for the GBM classifier. An accuracy score of 0.90 and a recall score of 0.81 were achieved via SMOTE sampling. Although the model with the greatest F1 score (DBSMOTE) had the highest accuracy (0.94), when compared to the other models, it had a lower recall score (0.79), which kept it from being regarded as the best model.

E. Stacked Ensemble (SE):

For the Ensemble stacked, there aren't many variables to specify. All trained models (30 models) make up the composite model known as the SE, which also includes a In order to enhance model performance, generic linear models (GLMs) act as meta-learners. To offer a 5-fold cross-validated model training utilizing stratified sampling, the meta-learner folds were set to 5. The stacked ensemble model, which combines ANN, GBM, and DRF, is a Super Learner. The Random under Sampling (RUS) technique is the least efficient approach. accuracy score and a key metric score of 0.68. The method known as SMOTEENN, which combines the Edited Nearest Neighbor (ENN) algorithm and SMOTE oversampling and noise reduction, has the greatest observed recall score. This model is the most effective sampling technique for the Stacked Ensemble, with an accuracy score of 0.85. Because the unsampled dataset is fully based on the original data and no artificial samples have been added, it has less noise than the sampled dataset, which is how it was able to get the highest accuracy score of 0.94.

TABLE II. ACCURACY OF THE VARIOUS MACHINE LEARNING TECHNIQUES

Classifier	Trainin g	Accurac y
Logistic Regression	0.99902	0.99888
Support Vector Machine	0.80147	0.83088
KNN	0.99845	0.99833
Naïve Bayes	0.66051	0.66176
ANN	0.99944	0.99833
Gaussian NB	0.99326	0.99376

From table 2 the classifiers' performance varies across the dataset. Logistic Regression, K-Nearest Neighbor, Artificial Neural Network, and Gaussian Naive Bayes show high accuracy in both training and testing, while Support Vector Machine and Naive Bayes perform moderately. Logistic Regression exhibits exceptional accuracy of around 99.9%, demonstrating strong generalization. K-Nearest Neighbor and Artificial Neural Network also achieve impressive accuracies at about 99.8%, showcasing effective pattern recognition. Gaussian Naive Bayes yields solid results with accuracies near 99.3%, particularly suited for Gaussian-distributed data. Further model optimization and consideration of computational complexity and interpretability are advised for selecting the best-suited classifier.

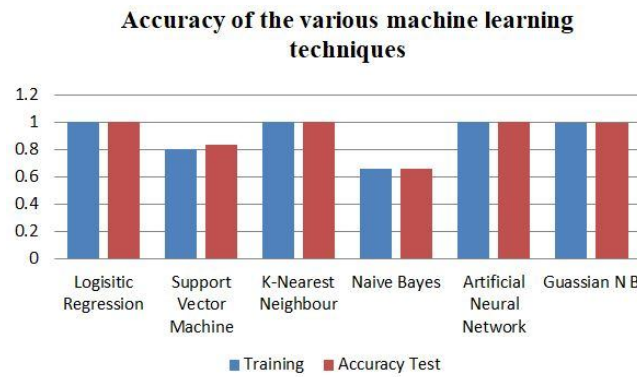


Fig 4: Accuracy of several machine learning methods for detecting credit card fraud

TABLE III. PERFORMANCE ANALYSIS OF CLASSIFIERS: RECALL AND F-SCORE COMPARISON FOR BINARY CLASSIFICATION

Classifier	Class	Precision	Recall	F1 Score	Support
Logistic Regression	0	1	1	1	852
	1	0.74	0.56	0.64	149
K- NN	0	1	1	1	852
	1	1	0.05	0.09	149
ANN	0	1	1	1	852
	1	0.34	0.82	0.07	149
Guassian NB	0	1	0.99	1	852
	1	0.17	0.64	0.26	149

From table 3 the classifiers' performance is evaluated the Precision, Recall, and F-score for two classes (0 and 1). Logistic Regression, K-Nearest Neighbor, and Gaussian Naive Bayes achieve high precision, recall, and F-scores for class 0 (close to or equal to 1), indicating strong performance in correctly identifying this class. However, for class 1, their performance varies significantly. While Logistic Regression has decent precision (0.74), K-Nearest Neighbor exhibits perfect precision but low recall and F-score, implying its effectiveness in capturing true positives but struggling with missed positive cases. The Artificial Neural Network demonstrates higher recall (0.82) but lower precision and F-score for class 1, suggesting it identifies more relevant instances but with a higher rate of false positives. Gaussian Naive Bayes shows balanced performance with respect to precision, recall, and F-score for class 1, maintaining a trade-off between correct identification and false positives. Careful consideration is needed when selecting the appropriate classifier based on the desired trade-offs between precision, recall, and F-score for both classes.

VI. CONCLUSION AND FUTURE WORK

Credit card fraud is unquestionably a criminal violation. This essay lists the most common fraud strategies and describes how to recognize them. It also discusses recent academic studies conducted in the field. This paper has also given a thorough explanation of how machine learning may be used to enhance fraud detection, along with the methodology, pseudocode, implementation details, and experiment results. When only a tenth of the data set is considered, the algorithm's precision is only 28%, despite its accuracy of over 99.9%. When the entire dataset is provided to the computer, the accuracy rises to 33%. If this study's findings were to be applied commercially, only a small subset of the dataset—made up of only two days' worth of transaction records—could be made available to the public. The accuracy, when implemented in the Decision tree, is 96.4, and in the random forest is 98.1. While the program is based on machine learning principles, its efficiency will only increase with time.

Though we fell short of our target, we were still able to create a system that might potentially approach 100% accuracy in fraud detection given enough time and data. As with any project of this nature, this one may be made better. The way the project is organized makes it possible to integrate numerous algorithms as modules and integrate their outputs to increase the accuracy of the result. Other algorithms could be added to this model to make it even better. These algorithms' output, though, needs to follow a specific format that is compatible with the other algorithms. It's easy to add the modules after that condition is met, as the code indicates. Due to this, the project is very flexible and adaptable. The dataset offers additional potential for growth. When was it demonstrated that algorithm accuracy increases with dataset size? Therefore, adding unquestionably, with more data, the model's fraud detection efficiency will increase while the number of false positives will be reduced. However, the banks themselves must give their own formal approval.

REFERENCES

- [1] P. Y. Prasad, A. S. Chowdary, C. Bavitha, E. Mounisha and C. Reethika, "A Comparison Study of Fraud Detection in Usage of Credit Cards using Machine Learning," 2023 7th International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2023, pp. 1204-1209, doi: 10.1109/ICOEI56765.2023.10125838.
- [2] " V. Jain, H. Kavitha and S. Mohana Kumar, "Credit Card Fraud Detection Web Application using Streamlit and Machine Learning," 2022 IEEE International Conference on Data Science and Information System (ICDSIS), Hassan, India, 2022, pp. 1-5, doi: 10.1109/ICDSIS55133.2022.9915901
- [3] Y. Singh, K. Singh and V. Singh Chauhan, "Fraud Detection Techniques for Credit Card Transactions," 2022 3rd International Conference on Intelligent Engineering and Management (ICIEM), London, United Kingdom, 2022, pp. 821-824, doi: 10.1109/ICIEM54221.2022.9853183.
- [4] Q. S. Mirhashemi, N. Nasiri and M. R. Keyvanpour, "Evaluation of Supervised Machine Learning Algorithms for Credit Card Fraud Detection: A Comparison," 2023 9th International Conference on Web Research (ICWR), Tehran, Iran, Islamic Republic of, 2023, pp. 247-252, doi: 10.1109/ICWR57742.2023.10139098.
- [5] A. Singh, A. Singh, A. Aggarwal and A. Chauhan, "Design and Implementation of Different Machine Learning Algorithms for Credit Card Fraud Detection," 2022 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), Maldives, Maldives, 2022, pp. 1-6, doi: 10.1109/ICECCME55909.2022.9988588.
- [6] Z. Li, G. Liu and C. Jiang, "Deep Representation Learning With Full Center Loss for Credit Card Fraud Detection," in IEEE Transactions on Computational Social Systems, vol. 7, no. 2, pp. 569-579, April 2020, doi: 10.1109/TCSS.2020.2970805.
- [7] A. A. Taha and S. J. Malebary, "An Intelligent Approach to Credit Card Fraud Detection Using an Optimized Light Gradient Boosting Machine," in IEEE Access, vol. 8, pp. 25579-25587, 2020, doi: 10.1109/ACCESS.2020.2971354.
- [8] H. Tingfei, C. Guangquan and H. Kuihua, "Using Variational Auto Encoding in Credit Card Fraud Detection," in IEEE Access, vol. 8, pp. 149841-149853, 2020, doi: 10.1109/ACCESS.2020.3015600.
- [9] Y. Xie, G. Liu, C. Yan, C. Jiang and M. Zhou, "Time-Aware Attention-Based Gated Network for Credit Card Fraud Detection by Extracting Transactional Behaviors," in IEEE Transactions on Computational Social Systems, vol. 10, no. 3, pp. 1004-1016, June 2023, doi: 10.1109/TCSS.2022.3158318.
- [10] S. N. Kalid, K. -H. Ng, G. -K. Tong and K. -C. Khor, "A Multiple Classifiers System for Anomaly Detection in Credit Card Data With Unbalanced and Overlapped Classes," in IEEE Access, vol. 8, pp. 28210-28221, 2020, doi: 10.1109/ACCESS.2020.2972009.
- [11] S. Han, K. Zhu, M. Zhou and X. Cai, "Competition-Driven Multimodal Multiobjective Optimization and Its Application to Feature Selection for Credit Card Fraud Detection," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 52, no. 12, pp. 7845-7857, Dec. 2022, doi: 10.1109/TSMC.2022.3171549.
- [12] D. Cheng, X. Wang, Y. Zhang and L. Zhang, "Graph Neural Network for Fraud Detection via Spatial-Temporal Attention," in IEEE Transactions on Knowledge and Data Engineering, vol. 34, no. 8, pp. 3800-3813, 1 Aug. 2022, doi: 10.1109/TKDE.2020.3025588.
- [13] S. Han, K. Zhu, M. Zhou and X. Cai, "Information-Utilization-Method-Assisted Multimodal Multiobjective Optimization and Application to Credit Card Fraud Detection," in IEEE Transactions on Computational Social Systems, vol. 8, no. 4, pp. 856-869, Aug. 2021, doi: 10.1109/TCSS.2021.3061439.
- [14] J. Cui, C. Yan and C. Wang, "ReMEMBeR: Ranking Metric Embedding-Based Multicontextual Behavior Profiling for Online Banking Fraud Detection," in IEEE Transactions on Computational Social Systems, vol. 8, no. 3, pp. 643-654, June 2021, doi: 10.1109/TCSS.2021.3052950.
- [15] L. Zheng, G. Liu, C. Yan, C. Jiang, M. Zhou and M. Li, "Improved TrAdaBoost and its Application to Transaction Fraud Detection," in IEEE Transactions on Computational Social Systems, vol. 7, no. 5, pp. 1304-1316, Oct. 2020, doi: 10.1109/TCSS.2020.3017013.
- [16] C. Phua, K. Smith-Miles, V. Lee and R. Gayler, "Resilient Identity Crime Detection," in IEEE Transactions on Knowledge and Data Engineering, vol. 24, no. 3, pp. 533-546, March 2012, doi: 10.1109/TKDE.2010.262.

- [17] L. Zheng, G. Liu, C. Yan and C. Jiang, "Transaction Fraud Detection Based on Total Order Relation and Behavior Diversity," in *IEEE Transactions on Computational Social Systems*, vol. 5, no. 3, pp. 796-806, Sept. 2018, doi: 10.1109/TCSS.2018.2856910.
- [18] Z. Yuan, H. Chen, T. Li, X. Zhang and B. Sang, "Multigranulation Relative Entropy-Based Mixed Attribute Outlier Detection in Neighborhood Systems," in *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 52, no. 8, pp. 5175-5187, Aug. 2022, doi: 10.1109/TSMC.2021.3119119.
- [19] Y. -J. Lee, Y. -R. Yeh and Y. -C. F. Wang, "Anomaly Detection via Online Oversampling Principal Component Analysis," in *IEEE Transactions on Knowledge and Data Engineering*, vol. 25, no. 7, pp. 1460-1470, July 2013, doi: 10.1109/TKDE.2012.99.
- [20] A. Jung and P. H. J. Nardelli, "An Information-Theoretic Approach to Personalized Explainable Machine Learning," in *IEEE Signal Processing Letters*, vol. 27, pp. 825-829, 2020, doi: 10.1109/LSP.2020.2993176.
- [21] Y. Li et al., "Automated Anomaly Detection via Curiosity-Guided Search and Self-Imitation Learning," in *IEEE Transactions on Neural Networks and Learning Systems*, vol. 33, no. 6, pp. 2365-2377, June 2022, doi: 10.1109/TNNLS.2021.3105636.
- [22] D. Y. Harvey and M. D. Todd, "Automated Feature Design for Numeric Sequence Classification by Genetic Programming," in *IEEE Transactions on Evolutionary Computation*, vol. 19, no. 4, pp. 474-489, Aug. 2015, doi: 10.1109/TEVC.2014.2341451.
- [23] S. Deveraju and Ramakrishnan, "Entropy-based feature selection for network intrusion detection systems," in *Methods, Implementation, and Application of Cyber Security Intelligence and Analytics*, 10.4018/978-1-6684-3991-3.ch012
- [24] Pumsirirat, A. and Yan, L. (2018). Credit Card Fraud Detection using Deep Learning based on Auto- Encoder and Restricted Boltzmann Machine. *International Journal of Advanced Computer Science and Applications*, 9(1).