Received: 5 February 2022 | Revised: 27 April 2022 | Accepted: 28 April 2022 | Published on: 22 May 2022

DOI: 10.1002/spy2.239

RESEARCH ARTICLE

WILEY

Predicting credit card fraud using multipurpose classification based on evolutionary rules

Mahmut Dirik

Department of Computer Engineering, Sirnak University, Şırnak, Turkey

Correspondence
Mahmut Dirik, Department of Computer Engineering, Sirnak University, Şırnak, Turkey.
Email: mhmd.dirik@gmail.com

Abstract

Due to advances in Internet technology, credit card transactions are increasing faster than ever before. This has led to a fraud problem that affects businesses, cooperating institutions, and government agencies. Credit card fraud occurs when a third party uses your credit card or credit account for an unauthorized transaction. Given the increased security of credit card transactions, fraudsters are developing new tricks or exploiting new vulnerabilities. Thanks to evolving technology, it is possible to analyze the use of maliciously obtained data by studying the time and cost associated with account switching transactions. In this study, we propose the ENORA and NSGA-II methods to create rule-based classifiers that can be easily interpreted using the credit card fraud diagnosis dataset created by analyzing the time intervals of individuals' credit card usage. In this experiment, credit card payments are classified as fraudulent or nonfraudulent based on several variables. The experiments were conducted in full training mode and 10-fold cross-validation mode. The performance of the algorithm was measured by accuracy, area under the receiver operating characteristic (ROC) curve, mean square error, proportion of true positives, proportion of false positives, precision, recall, F-measure, area under the curve (AUC), and Matthews correlation coefficient. The classification performance of the model using the correct classification ratio (ACC) is as follows: NSGA-II = 94.244%, ENORA = 93.236%. The performance of the other metrics is also discussed in detail in the results section. These results illustrate the significant predictive power of the proposed credit card theft models. After a thorough statistical analysis of our results, we found that the proposed strategy is capable of producing accurate and easy-to-understand categorization models.

KEYWORDS

credit card fraud prediction, ENORA, fraud detection, machine learning, multiobjective evolutionary, NSGA-II, rule-based classifiers

1 | INTRODUCTION

Credit cards have become a means of payment that consumers can use quickly and frequently because of their widespread use and solid infrastructure. However, as credit cards have become more widely used, some problems have arisen. By facilitating access to accurate credit information, these implications can allow criminals to amass illicit wealth. Fraud is

often defined as unlawful copying with the intent to gain an advantage. With the increasing reliance on online technology, the number of credit card frauds has also skyrocketed. Credit cards are used in almost all transactions, whether online or offline. Most of the research has focused on detecting external credit card theft. Credit card fraud can be classified as either offline or online. Offline fraud occurs when a physical card is stolen from a location such as a call center. Online fraud occurs when a card is stolen over the phone, while shopping, or on the Internet. Credit card fraud is divided into two types: internal card fraud and external card fraud. Internal card fraud occurs when a false identity is used to commit fraud based on an agreement between cardholders and their bank, while external card fraud occurs when a credit card is used to obtain cash in a dubious manner.[1,2] Credit card fraud is a major problem for banks because the transaction mechanism is inherently vulnerable. Stronger security systems should be implemented to monitor credit card transactions and detect fraud as early as possible.

Machine learning has helped solve a number of important business challenges, such as identifying spam emails, making targeted product suggestions, and making accurate diagnoses. Machine learning has evolved as computing power has increased, enormous amounts of data have become available, and statistical models have been developed.[3,4] Due to the increasing number of transactions through the widespread use of payment methods (credit/debit cards, cell phones, kiosks), it has become important for banks and businesses to combat fraud. To effectively address this issue, advances have been made in detecting fraudulent methods based on machine learning and predictive analytics. Credit card fraud can be detected based on card activity or usage activity and timestamps.[2,5,6] Many significant research projects have been conducted to find new techniques to detect different types of fraud.[1-8] There are several credit card fraud detection methods offered by researchers that are effective to some extent. However, the main problems are that the datasets are not available due to security concerns, and that the datasets are extremely unstable. Many machine learning-based solutions have been proposed for credit card fraud detection.[3,4,6,7,9-12]

In this paper, we present a technique for fraud detection using a dataset of credit card transactions, which we call multipurpose evolutionary rule-based classification. the basic concept is that a new order performs transactions based on rule-based decisions, such that a significant deviation from normal trading behavior represents a fraud risk.

The machine learning algorithms used in this study are used to classify incoming credit card payments as fraudulent or nonfraudulent based on several factors. The input components shown in Figure 1 illustrate the proposed input functions of the system. The data we used was obtained from the Kaggle database.[13] We used the ENORA and NSGA-II algorithms, which are rule-based learning algorithms. These features are very informative for fraud detection. Figure 1 illustrates the rough structure of the proposed credit card fraud detection technique. The average daily transaction amount, the transaction amount, whether the credit card was declined or not, the total number of declines per day, whether the transections are international or not, whether the countries are high risk or not, the average daily chargebacks, the average chargebacks over 6 months, the average chargebacks over 6 months in each country, and the chargeback frequency are the input metrics used by the fraud detection algorithms. After a rule-based machine learning process that evaluates all of these input elements, the goal is to determine whether the transaction is fraudulent or legitimate.

As can be seen in Figure 1, the intermediate component or black box that provides the link between input and output is the machine learning component that performs learning or makes rule-based decisions in this system. This system uses supervised machine learning techniques. A subset of machine learning (ML),[14] called supervised learning, is concerned with simulating the behavior of systems in their natural environment. Given a set of historical data sets, each consisting of an input vector that often includes an output, supervised models are used to predict the future.[15] The most accurate models are those that can accurately predict the consequences of new inputs. Due to the improved capabilities of modern computers and the digitization of ever increasing amounts of data, supervised learning approaches are currently playing an increasingly important role in a variety of applications. When modeling increasingly complicated behaviors, interpretability can take a back seat. What matter in this case is the model that is to be developed to achieve the desired result. Therefore, the model has an extensive sequential network of nodes with a large number of variables, including ANN,[16] SVM,[17] and DLNN.[18] The interpretability of these systems is more difficult to determine than that of our proposed system. It is possible to describe the behavior of categorization systems in a form that is easily understood by a user,[19] and this is called interpretability. In other words, a model is said to be interpretable if the reasoning behind the prediction it provides is understandable. While there is widespread agreement on how to evaluate the performance of a classification system, and common metrics such as accuracy, area under the receiver operating characteristic curve, and root mean square error are often used, there is no universally accepted metric for evaluating the interpretability of classification models. Furthermore, there is no ideal tradeoff between interpretability and performance of classification systems; rather, the best tradeoff varies by system and application. On the contrary, as a rule, the simpler a classification system is, the easier it is to understand. RBCs (rule-based classifiers)[20,21] are among the most widely used interpretable models in use today.

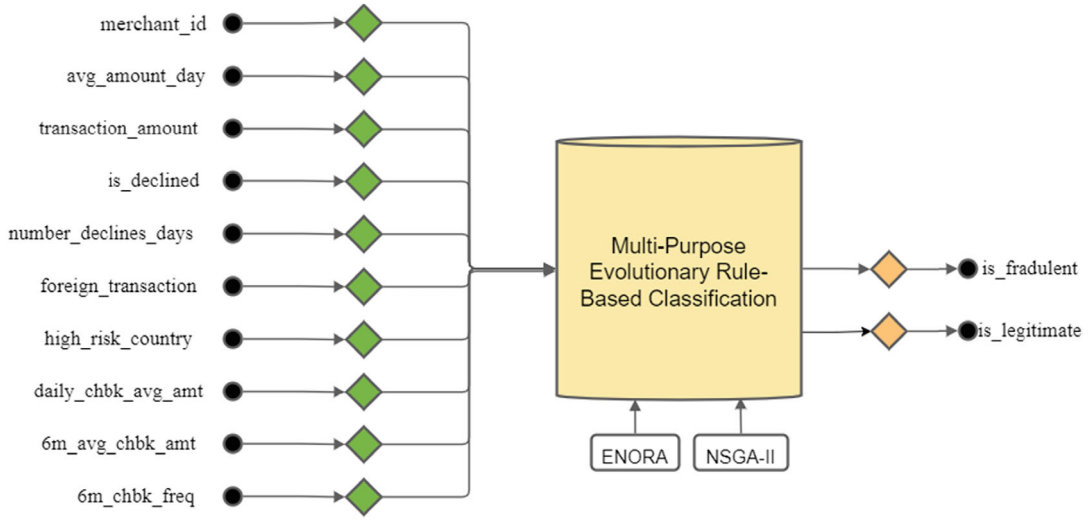

FIGURE 1 Transaction authorization flowchart for credit card fraud prediction with versatile rule-based classification

In general, RBCs develop categorization systems that are highly interpretable due to their human-like thinking. Our method explores the tradeoff between accuracy and interpretability through the lens of a multiobjective optimization problem. We construct a solution as a collection of rules (a classifier) and specify two criteria for optimization: interpretability and accuracy. We chose to solve this problem by using meta-heuristics such as multiobjective evolutionary algorithms (MOEA)[22-24] and, in particular, two well-known algorithms: NSGA-II[22] and ENORA,[25,26] which are both recognized methods. Over the years, there have been several applications and comparisons of these two state-of-the-art evolutionary algorithms.[9,27] NSGA-II is well known and has the advantage of being accessible in a wide variety of implementations, although ENORA generally performs better. MOEAs are mainly used in the present research for learning RBCs with fuzzy logic.[28-30] Fuzzy RBCs, on the other hand, are intended for use with numerical data from which fuzzy sets are formed and represented by linguistic labels. Using RBCs for categorical data, on the other hand, is something we are interested in, and this requires a different technique.

The following sections summarize the structure of this paper. Section 2, proposed methodology, and its subtitles; data set, multipurpose constrained evolutionary optimization algorithms ENORA and NSGA-II, and the performance evaluation criteria used are explained. Section 3 presents the results and discussion of our experiments conducted on the public credit card fraud dataset. Finally, Section 4 presents the results and future work.

2 | PROPOSED METHODOLOGY

Fraud detection is a two-step process that anticipates each transaction and classifies it as fraudulent or legitimate. Predicting credit card fraud using a multipurpose classification based on evolutionary rules is a classification project because the variable to be predicted is binary (not counterfeit or fraudulent). The goal is to develop a model that can be used to determine the probability that a transaction is fraudulent. The article compares the performance of the classification approaches ENORA and NSGA-II, two widely used algorithms for rule-based and multicentric classification. The next subsections provide an overview of these strategies as well as the classification techniques, datasets, and metrics used to quantify performance.

2.1 | Data set

The data used in this study are from the Kaggle database.[13] This dataset contains 11 features for 3075 payments. Table 1 shows the features in this dataset. We repeated the 10-fold cross-validation learning procedure[31] three times and considered the average value of the performance metrics "percent accuracy," "area under the ROC curve," and "serialized model size" across all results.

TABLE 1 Characteristics and descriptions of the dataset used

Features	Descriptions of features
merchant_id	ID of the merchant
avg_amount_day	Average of amount per transaction per day
transaction_amount	The amount of the transaction
is_declined	Yes = the credit card is declined, no = the credit card is not declined
number_declines_day	Total number of declines per day
foreign_transaction	Yes = it is a foreign transaction, no = it is not a foreign transaction
high_risk_country	Yes = it is a high-risk country, no = it is not a high-risk country.
daily_chbk_avg_amt	Daily average of chargeback.
6m_avg_chbk_amt	Six-months average of chargeback
6m_chbk_freq	Frequency of the 6-months chargeback
is_fradulent	Fraudulent = the payment is fraudulent, not-fraudulent = the payment is not fraudulent (target variable).

2.2 | The multiobjective evolutionary algorithms

An evolutionary learning system is presented that finds many pareto-optimal solutions (classifiers) under constrained optimization, accuracy, and comprehensibility constraints for different objectives simultaneously. In this section, the main components of the proposed evolutionary algorithm are discussed. These components include the solution representation, constraint management, initial population, and variation operators. We have developed two elite pareto-based MOEA, ENORA, and NSGA-II, using a set of alternative selection, sampling, and generation switching techniques that exploit these common components.

2.3 | ENORA

The ENORA technique was introduced for multiobjective optimization with constrained real parameters.[25] ENORA is a pareto-based elite MOEA based on $(\mu + \lambda)$ survival, where μ is the population size and λ is the number of offspring produced. ENORA was first proposed in reference 31 as an evolutionary method based on selection, adaptive mutation, and a population of size one, symbolized as $(1 + 1)$. The $(\mu + \lambda)$ method ensures the survival of the best offspring and parents and is therefore an elitist technique. ENORA optimizes evolutionary optimization with multiple objectives using $(\mu + \lambda)$-survival with $\mu = \lambda =$ population size, binary tournament selection, recombination, and adaptive mutation. Algorithm 1 illustrates a multiobjective optimization method based on the $(\mu + \lambda)$ approach. The approach starts with the initialization and evaluation of a P population consisting of N individuals.

Algorithm 1. $(\mu + \lambda)$ strategy for multiobjective optimization

Require: $T > 1$ {Number of generations}
Require: $N > 1$ {Number of individuals in the population}
1: Initialize P with N individuals
2: Evaluate all individuals of P
3: $t \leftarrow 0$
4: **while** $t < T$ **do**
5: $Q \leftarrow \emptyset$
6: $i \leftarrow 0$
7: **while** $i < N$ **do**
8: *Parent1* ← Binary tournament selection from P
9: *Parent2* ← Binary tournament selection from P
10: *Child1*, *Child2* ← *Crossover*(*Parent1*, *Parent2*)

11: *Offspring1* ← *Mutation*(*Child1*)
12: *Offspring2* ← *Mutation*(*Child2*)
13: Evaluate *Offspring1*
14: Evaluate *Offspring2*
15: $Q \leftarrow Q \cup \{Offspring1, Offspring2\}$
16: $i \leftarrow i + 2$
17: **end while**
18: $R \leftarrow P \cup Q$
19: $P \leftarrow N$ best individuals from R according to the *rank-crowding* function in population R
20: $t \leftarrow t + 1$
21: **end while**
22: **return** Non-dominated individuals from P

In addition to Algorithm 1, Algorithm 2 is used for double tournament selection, and Algorithms 3 and 4 are used for a ranking function based on pareto fronts and crowding.

Algorithm 2. Binary tournament selection

Require: P {Population}
1: $I \leftarrow$ Random selection from P
2: $J \leftarrow$ Random selection from P
3: **if** I is better than J according to the *rank-crowding* function in population P **then**
4: **return** I
5: **else**
6: **return** J
7: **end if**

Algorithm 3. Rank-crowding function

Require: P {Population}
Require: I, J {Individuals to compare}
1: **if** $rank\,(P, I) < rank\,(P, J)$ **then**
2: **return** *True*
3: **end if**
4: **if** $rank\,(P, J) < rank\,(P, I)$ **then**
5: **return** *False*
6: **end if**
7: **return** $Crowding\_distance\,(P, I) > Crowding\_distance\,(P, J)$

Algorithm 4. Crowding_distance function

Require: P {Population}
Require: i {Individual}
Require: l {Number of objectives}
1: for $j = 1$ to l **do**
2: $f_j^{\max} \leftarrow \max_{I \in P} \left\{ f_j^I \right\}$
3: $f_j^{\min} \leftarrow \min_{I \in P} \left\{ f_j^I \right\}$

4: $f_j^{\sup_j^I} \leftarrow$ value of the jth objective for the individual higher adjacent in the jth objective to the individual I
5: $f_j^{\inf_j^I}$ value of the jth objective for the individual lower adjacent in the jth objective to the individual I
6: **end for**
7: **for** $j = 1$ to / **do**
8: **if** $f_j^I = f_j^{\max}$ or $f_j^I = f_j^{\min}$ **then**
9: **return** ∞
10: **end if**
11: **end for**
12: CD $\leftarrow 0.0$
13: **for** $j = 1$ to l **do**
14: CD $\leftarrow$ CD $+ \frac{f_j^{\sup_j^I} - f_j^{\inf_j^I}}{f_j^{\max} - f_j^{\min}}$
15: **end for**
16: **return** CD

2.4 | NSGA-II

The NSGA-II algorithm is an evolutionary algorithm with multiple objectives proposed by Deb et al.[32] The algorithm was developed by eliminating the shortcomings of the NSGA algorithm developed by Srinivas and Deb.[33] NSGA-II[32] is a remarkable pareto-based evolutionary multiobjective algorithm that integrates an explicit diversity approach to improve the previous NSGA algorithm. NSGA-II has many applications in the literature because it is a fast and exclusive algorithm with low computational complexity. Like ENORA, NSGA- II uses a $(\mu + \lambda)$ strategy (Algorithm 1) in conjunction with a binary tournament selection algorithm (Algorithm 2) and a ranking improvement function (Algorithm 3). Each individual in ENORA is assigned a place in the objective search space, and the rank of an individual in a population is equal to the degree of nondominance that individual has in that place. On the other hand, in NSGA-II, the rank of an individual within a population is proportional to the degree of nondominance that individual has within the population. Both ENORA and NSGA-II use the same nondominant sorting approach.[34] It compares each answer with the others and stores the results so that each pair of solutions is not compared again. The main difference between ENORA and NSGA-II is that NSGA-II never selects the dominant individual of the other as the winner of the tournament, while ENORA does.

2.5 | Evaluation of the performance

The purpose of performance evaluation is to determine the efficiency of the algorithms used to achieve the desired goal and to verify the usability of the system. To verify a categorization technique, its output values must be compared with the observed values. The confusion matrix, sensitivity, specificity, false positive rate, balanced classification rate, and Matthews correlation coefficient all serve as performance measures for evaluating fraud detection classifiers. The confusion matrix[35] of a binary classifier is shown in Table 2. The correlations between these indicators are determined using very complicated measurements. The following measures are used to estimate the performance: percent correct, TP rate, FP rate, precision, recall, F-Measure, MCC, receiver operating characteristic (ROC) area, PRC Area, and RMSE.

True positives (TP) are situations that are both expected and observed. True negatives (TN) are cases that are expected to be correspondingly negative. False positives are cases in which an outcome is perceived to be positive but is actually

TABLE 2 Confusion matrix of credit card dataset

	Predicted fraud	Predicted nonfraud
Actual fraud	TP	FN
Actual nonfraud	FP	TN

negative. False negatives are cases in which a situation is perceived as negative but is actually positive. The correlations between these indicators are determined using very complicated measurements. in addition, the sensitivity, specificity, accuracy, F-measure, and area under the curve (AUC) of the proposed methods are compared. The performance indicators used in this study and the formulas of these indicators are given in table Equations (1)–(10). These indicators have already been used in a number of studies.[36-39]

$\text{Accuracy (ACC)} = \frac{TP+TN}{TP+FP+TN+FN}$	40-42	(1)
$\text{Sensitivity (Recall)} = \frac{TP}{TP+FN}$	41,42	(2)
$\text{Specificity} = \frac{TN}{FP+TN}$	41,42	(3)
$\text{Precision} = \frac{TP}{TP+FP}$	41,42	(4)
$F-\text{measure} = 2\times\frac{\text{Precision}\times\text{Recall}}{\text{Precision}+\text{Recall}}$	41,42	(5)
$\text{MCC} = \frac{TP\times TN-FP\times FN}{\sqrt{(TP+FP)(TP+FN)(TN+FP)(TN+FN)}}$	43	(6)
$\text{AUC} = \frac{1}{2}\times(\text{Sensitivity}+\text{Specificity})$	44	(7)
$\text{Kappa statistic} = \frac{(\text{observed accuracy}-\text{expected accuracy})}{1-\text{expected accuracy}}$	45	(8)
$\text{Mean absolute error (MAE)} = \frac{1}{N}\sum_{i=1}^{N} \mid \widehat{\theta}_i - \theta_i \mid$	46	(9)
$\text{Root mean square error (RMSE)} = \sqrt{\frac{1}{N}\sum_{i=1}^{N} \mid \widehat{\theta}_i - \theta_i \mid}$	44	(10)

In these equations, TP, FP, TN, and FN represent the number of true positive, false positive, true negative, and false negative classifications (or predictions) (Equations (1)–(10)). A positive prediction means that a transaction is classified as fraudulent, while a negative prediction means that the transaction is classified as normal (ie, not fraudulent). The area under the receiver operating characteristic (AUC) curve is a statistic used to describe the ROC curve. The ROC curve can be used to evaluate the tradeoff between true-positive rate (TPR) and false-positive rate (FPR) for a threshold-based classifier. By setting the *x*-axis to the FPR and the *y*-axis to the TPR, you can create the ROC curve and calculate the area under the ROC curve (AUC). Precision and recall are important features to consider when dealing with unstable data (ie, *F*-score). Precision is a measure of the relevance of the outcome scale and the closeness to the intended response, while recall is a measure of the number of relevant outcomes. Precision and recall values above 1 mean that the classifier correctly recovered the results and recovered most of the positive results. Therefore, the precision–recall curve provides a comprehensive view of the classifier's accuracy and is robust even with unstable datasets. In addition to the above metrics, we consider AUC as a general performance metric. The AUC is a graphical representation of the FPR and the TPR at different confidence levels. Because the AUC value does not depend on a discontinuity number, it is considered a more accurate indicator of overall performance than accuracy.[47]

3 | RESULT AND DISCUSSION

Cross-validation was performed to determine the effectiveness of the proposed credit card fraud detection technique and to establish a credible performance comparison. The performance of the proposed approach was evaluated using a tenfold cross-validation of data sets (testing and training methods). The experiment was performed on a computer with an Intel Core i7 processor and 16 GB of RAM using the Weka[48] software platform. The proposed strategy and other machine learning approaches were developed and evaluated using Weka software. The performance of the classifiers created using the proposed methods was compared using the same settings and algorithm parameters, which are listed in Table 3.

TABLE 3 The performance of the algorithms used

Algorithm	batch Size	genera -tions	max Labels	max Similarity	maxV	minV	num Decimal Places	population Size	report Frequency
ENORA	100	20	5	0.4	2	30	4	100	20
NSGA-II	100	20	5	0.4	2	30	4	100	20

TABLE 4 Comparison of the performance of the rule-based learning models ENORA and NSGA-II

	Percent Correct	TP Rate	FP Rate	Precision	Recall	F-Measure	MCC	ROC Area	PRC Area	Kappa St.	MAE	RMSE
ENORA-acc	93.236%	0.603	0.011	0.9	0.603	0.722	0.7	0.796	0.6	0.6851	0.0676	0.2601
ENORA-auc	88.683%	0.804	0.099	0.581	0.804	0.674	0.62	0.852	0.495	0.6078	0.1132	0.3364
ENORA-rmse	92.911%	0.583	0.012	0.894	0.583	0.705	0.69	0.785	0.582	0.6671	0.0709	0.2663
NSGA-II-acc	92.683%	0.594	0.016	0.861	0.594	0.703	0.68	0.789	0.57	0.6626	0.0732	0.2705
NSGA-II-auc	88.878%	0.877	0.109	0.578	0.877	0.697	0.65	0.884	0.525	0.6322	0.1112	0.3335
NSGA-II-rmse	94.244%	0.672	0.011	0.909	0.672	0.773	0.75	0.83	0.659	0.7407	0.0576	0.2399

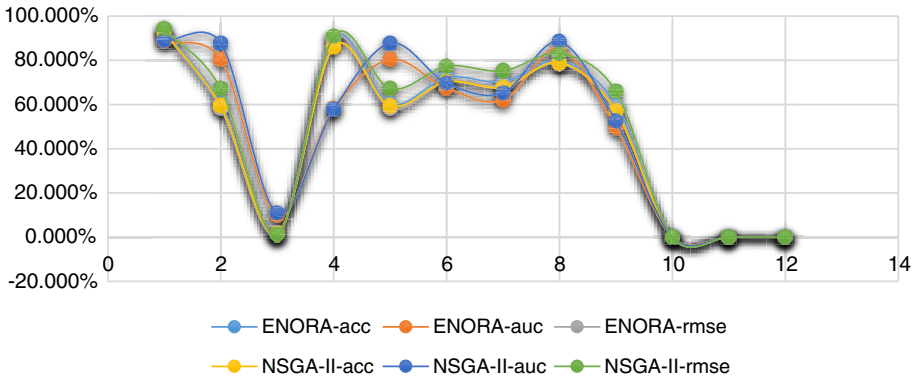

FIGURE 2 Comparing the performance of the rule-based learning models ENORA and NSGA-II using a graphical representation

Table 4 shows the results obtained using the performance metrics of the two classifiers. In this table, the most accurate results were obtained using the ENORA-acc and NSGA-II-rmse methods. These data are presented graphically in Figure 2.

Figure 3 visually illustrates the Area of ROC. A ROC curve[49,50] is a graph showing the rates of true positivity (sensitivity) and false positivity (specificity) for different thresholds. Each point on the ROC curve indicates the sensitivity and specificity values associated with a particular threshold. A ROC curve represents a probability curve for different classes. In a typical ROC curve, the *X*-axis represents the FPR, and the *Y*-axis represents the TPR. The larger the area under the ROC curve, the more accurate machine learning models are in classifying certain classes.

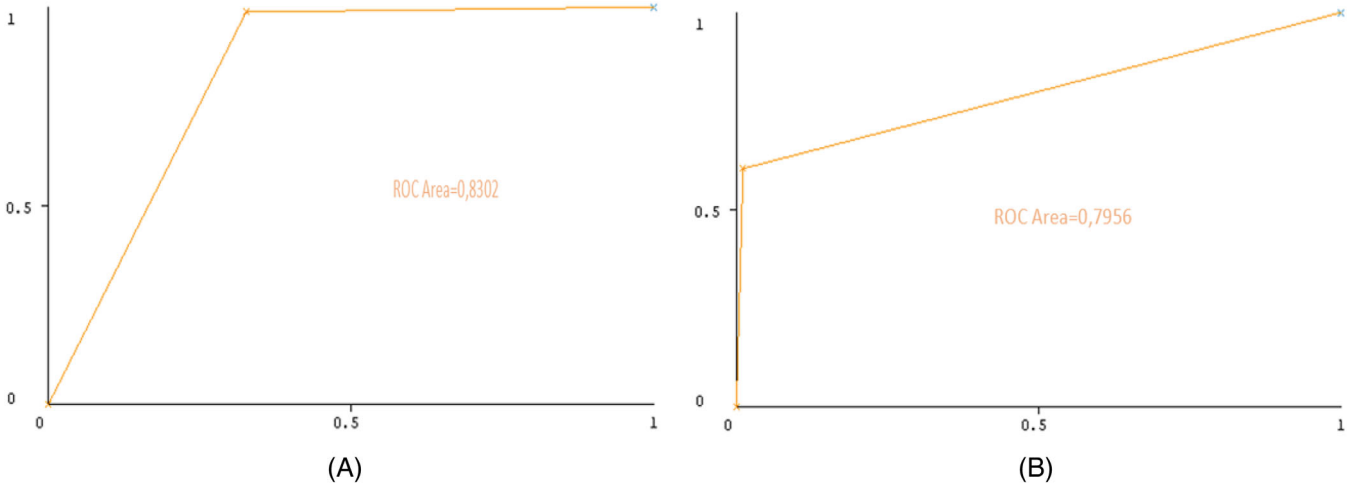

FIGURE 3 Area under the receiver operating characteristic curve (A) NSGA-II-RMSE, (B) ENORA-acc)

TABLE 5 Predicting credit card fraud with a rule-based classifier using ENORA-acc

Rule	Antecedents	Consequent
Rule 1:	IF merchan_id IS Moderately Low (Center: 4.476543124334E9, S.D.: 1.0149212032646E9) AND avg_amount_days IS Moderately High (Center: 1556.2619, S.D.: 163.0985) AND transaction_amount IS Low (Center: 14025.5451, S.D.: 12095.5783) AND is_declined IS no AND number_declines_days IS High (Center: 18.7178, S.D.: 3.1155) AND foreign_transaction IS no AND high_risk_countries IS yes AND daily_chbk_avg_amt IS High (Center: 948.3819, S.D.: 206.2265) AND 6m_avg_chbk_amt IS Moderately Low (Center: 294.5613, S.D.: 106.8123) AND 6m_chbk_freq IS Moderately High (Center: 6.7889, S.D.: 0.7632)	THEN is_fradulent IS fraudulent
Rule 2:	IF merchan_id IS High (Center: 6.5040362656435E9, S.D.: 3.9353841071358E8) AND avg_amount_days IS Moderately Low (Center: 686.7463, S.D.: 243.4995) AND transaction_amount IS Moderately Low (Center: 37546.2913, S.D.: 3600.0) AND is_declined IS yes AND number_declines_days IS High (Center: 18.7178, S.D.: 3.1155) AND foreign_transaction IS no AND high_risk_countries IS yes AND daily_chbk_avg_amt IS Medium (Center: 578.8003, S.D.: 33.2667) AND 6m_avg_chbk_amt IS Moderately High (Center: 700.7621, S.D.: 74.8512) AND 6m_chbk_freq IS Moderately Low (Center: 3.1841, S.D.: 0.8237)	THEN is_fradulent IS fraudulent
Rule 3:	IF merchan_id IS Moderately Low (Center: 4.476543124334E9, S.D.: 1.0149212032646E9) AND avg_amount_days IS Moderately Low (Center: 686.7463, S.D.: 243.4995) AND transaction_amount IS Moderately Low (Center: 37546.2913, S.D.: 3600.0) AND is_declined IS yes AND number_declines_days IS Moderately Low (Center: 7.2091, S.D.: 1.6095) AND foreign_transaction IS yes AND high_risk_countries IS yes AND daily_chbk_avg_amt IS High (Center: 948.3819, S.D.: 206.2265) AND 6m_avg_chbk_amt IS Moderately Low (Center: 294.5613, S.D.: 106.8123) AND 6m_chbk_freq IS Moderately Low (Center: 3.1841, S.D.: 0.8237)	THEN is_fradulent IS fraudulent
Rule 4:	IF merchan_id IS Moderately Low (Center: 4.476543124334E9, S.D.: 1.0149212032646E9) AND avg_amount_days IS Moderately High (Center: 1556.2619, S.D.: 163.0985) AND transaction_amount IS Moderately Low (Center: 37546.2913, S.D.: 3600.0) AND is_declined IS yes AND number_declines_days IS Low (Center: 1.5222, S.D.: 2.3268) AND foreign_transaction IS no AND high_risk_countries IS no AND daily_chbk_avg_amt IS High (Center: 948.3819, S.D.: 206.2265) AND 6m_avg_chbk_amt IS Medium (Center: 501.1621, S.D.: 43.6455) AND 6m_chbk_freq IS Moderately Low (Center: 3.1841, S.D.: 0.8237)	THEN is_fradulent IS fraudulent
Rule 5:	IF merchan_id IS Moderately Low (Center: 4.476543124334E9, S.D.: 1.0149212032646E9) AND avg_amount_days IS High (Center: 1955.4596, S.D.: 195.8723) AND transaction_amount IS Low (Center: 14025.5451, S.D.: 12095.5783) AND is_declined IS yes AND number_declines_days IS High (Center: 18.7178, S.D.: 3.1155) AND foreign_transaction IS no AND high_risk_countries IS no AND daily_chbk_avg_amt IS Moderately Low (Center: 351.7183, S.D.: 67.9211) AND 6m_avg_chbk_amt IS Moderately Low (Center: 294.5613, S.D.: 106.8123) AND 6m_chbk_freq IS Moderately Low (Center: 3.1841, S.D.: 0.8237)	THEN is_fradulent IS fraudulent
Rule 6:	IF merchan_id IS Moderately Low (Center: 4.476543124334E9, S.D.: 1.0149212032646E9) AND avg_amount_days IS Medium (Center: 1085.944, S.D.: 242.0242) AND transaction_amount IS Medium (Center: 59146.2913, S.D.: 7827.2859) AND is_declined IS no AND number_declines_days IS Moderately Low (Center: 7.2091, S.D.: 1.6095) AND foreign_transaction IS no AND high_risk_countries IS no AND daily_chbk_avg_amt IS High (Center: 948.3819, S.D.: 206.2265) AND 6m_avg_chbk_amt IS Moderately Low (Center: 294.5613, S.D.: 106.8123) AND 6m_chbk_freq IS High (Center: 8.6766, S.D.: 0.9787)	THEN is_fradulent IS fraudulent

TABLE 5 continued

Rule	Antecedents	Consequent
Rule 7:	IF merchan_id IS Moderately Low (Center: 4.476543124334E9, S.D.: 1.0149212032646E9) AND avg_amount_days IS Moderately Low (Center: 686.7463, S.D.: 243.4995) AND transaction_amount IS Moderately Low (Center: 37546.2913, S.D.: 3600.0) AND is_declined IS no AND number_declines_days IS Moderately Low (Center: 7.2091, S.D.: 1.6095) AND foreign_transaction IS no AND high_risk_countries IS no AND daily_chbk_avg_amt IS Low (Center: 66.1808, S.D.: 155.2055) AND 6m_avg_chbk_amt IS High (Center: 900.3621, S.D.: 116.6765) AND 6m_chbk_freq IS Medium (Center: 4.9889, S.D.: 0.4174)	THEN is_fradulent IS non-fraudulent
Rule 8:	IF merchan_id IS Moderately Low (Center: 4.476543124334E9, S.D.: 1.0149212032646E9) AND avg_amount_days IS Moderately High (Center: 1556.2619, S.D.: 163.0985) AND transaction_amount IS High (Center: 91214.434, S.D.: 18212.2611) AND is_declined IS yes AND number_declines_days IS Low (Center: 1.5222, S.D.: 2.3268) AND foreign_transaction IS no AND high_risk_countries IS no AND daily_chbk_avg_amt IS High (Center: 948.3819, S.D.: 206.2265) AND 6m_avg_chbk_amt IS Moderately Low (Center: 294.5613, S.D.: 106.8123) AND 6m_chbk_freq IS Low (Center: 1.3333, S.D.: 0.9549)	THEN is_fradulent IS non-fraudulent
Rule 9:	IF merchan_id IS Moderately Low (Center: 4.476543124334E9, S.D.: 1.0149212032646E9) AND avg_amount_days IS Moderately High (Center: 1556.2619, S.D.: 163.0985) AND transaction_amount IS Moderately Low (Center: 37546.2913, S.D.: 3600.0) AND is_declined IS yes AND number_declines_days IS Moderately Low (Center: 7.2091, S.D.: 1.6095) AND foreign_transaction IS no AND high_risk_countries IS no AND daily_chbk_avg_amt IS High (Center: 948.3819, S.D.: 206.2265) AND 6m_avg_chbk_amt IS Moderately Low (Center: 294.5613, S.D.: 106.8123) AND 6m_chbk_freq IS Low (Center: 1.3333, S.D.: 0.9549)	THEN is_fradulent IS non-fraudulent
Rule 10:	IF merchan_id IS Moderately Low (Center: 4.476543124334E9, S.D.: 1.0149212032646E9) AND avg_amount_days IS Medium (Center: 1085.944, S.D.: 242.0242) AND transaction_amount IS Moderately Low (Center: 37546.2913, S.D.: 3600.0) AND is_declined IS no AND number_declines_days IS Moderately Low (Center: 7.2091, S.D.: 1.6095) AND foreign_transaction IS no AND high_risk_countries IS yes AND daily_chbk_avg_amt IS Moderately Low (Center: 351.7183, S.D.: 67.9211) AND 6m_avg_chbk_amt IS Medium (Center: 501.1621, S.D.: 43.6455) AND 6m_chbk_freq IS Medium (Center: 4.9889, S.D.: 0.4174)	THEN is_fradulent IS non-fraudulent
Rule 11:	IF merchan_id IS High (Center: 6.5040362656435E9, S.D.: 3.935384107135E8) AND avg_amount_days IS Medium (Center: 1085.944, S.D.: 242.0242) AND transaction_amount IS Low (Center: 14025.5451, S.D.: 12095.5783) AND is_declined IS no AND number_declines_days IS High (Center: 18.7178, S.D.: 3.1155) AND foreign_transaction IS yes AND high_risk_countries IS yes AND daily_chbk_avg_amt IS High (Center: 948.3819, S.D.: 206.2265) AND 6m_avg_chbk_amt IS Low (Center: 60.5857, S.D.: 56.2056) AND 6m_chbk_freq IS High (Center: 8.6766, S.D.: 0.9787)	THEN is_fradulent IS non-fraudulent

TABLE 6 Predicting credit card fraud with a rule-based classifier using NSGA-II-RMSE

Rule	Antecedents	Consequent
Rule 1:	IF merchan_id IS Low (Center: 3.7987392436881E9, S.D.: 2.37 AND avg_amount_days IS Moderately High (Center: 1387.3474, S.D.: 66.5329) AND transaction_amount IS Moderately High (Center: 72163.9302, S.D.: 4261.1101) AND is_declined IS yes AND number_declines_days IS Moderately Low (Center: 5.0168, S.D.: 1.2298) AND foreign_transaction IS yes AND high_risk_countries IS no AND daily_chbk_avg_amt IS Moderately High (Center: 794.2448, S.D.: 140.1988) AND 6m_avg_chbk_amt IS Moderately High (Center: 686.9354, S.D.: 33.2667) AND 6m_chbk_freq IS Medium (Center: 4.2035, S.D.: 0.4135)	THEN is_fradulent IS fraudule
Rule 2:	IF merchan_id IS Moderately High (Center: 5.4705541848133E9, S.D.: 5.1 AND avg_amount_days IS Medium (Center: 978.9205, S.D.: 276.0485) AND transaction_amount IS Moderately Low (Center: 24417.7058, S.D.: 4815.783) AND is_declined IS no AND number_declines_days IS High (Center: 17.0979, S.D.: 2.2698) AND foreign_transaction IS yes AND high_risk_countries IS yes AND daily_chbk_avg_amt IS Medium (Center: 416.289, S.D.: 33.2667) AND 6m_avg_chbk_amt IS High (Center: 956.3957, S.D.: 149.2022) AND 6m_chbk_freq IS Moderately High (Center: 6.0035, S.D.: 0.3581)	THEN is_fradulent IS fraudule
Rule 3:	IF merchan_id IS Moderately Low (Center: 4.5573271374116E9, S.D.: 4.2 AND avg_amount_days IS High (Center: 1813.9026, S.D.: 255.8041) AND transaction_amount IS High (Center: 96840.9404, S.D.: 14135.0912 AND is_declined IS yes AND number_declines_days IS Medium (Center: 9.0168, S.D.: 0.9713) AND foreign_transaction IS no AND high_risk_countries IS no AND daily_chbk_avg_amt IS Low (Center: 105.4235, S.D.: 187.7564) AND 6m_avg_chbk_amt IS Medium (Center: 484.8946, S.D.: 48.6022) AND 6m_chbk_freq IS Moderately High (Center: 6.0035, S.D.: 0.3581)	THEN is_fradulent IS fraudule
Rule 4:	IF merchan_id IS Moderately High (Center: 5.4705541848133E9, S.D.: 5.1 AND avg_amount_days IS Medium (Center: 978.9205, S.D.: 276.0485) AND transaction_amount IS Moderately High (Center: 72163.9302, S.D.: 4261.1101) AND is_declined IS no AND number_declines_days IS Moderately High (Center: 13.0168, S.D.: 0.6667) AND foreign_transaction IS no AND high_risk_countries IS no AND daily_chbk_avg_amt IS Medium (Center: 416.289, S.D.: 33.2667) AND 6m_avg_chbk_amt IS Low (Center: 80.7377, S.D.: 78.5115) AND 6m_chbk_freq IS Medium (Center: 4.2035, S.D.: 0.4135)	THEN is_fradulent IS fraudule
Rule 5:	IF merchan_id IS Moderately High (Center: 5.4705541848133E9, S.D.: 5.1 AND avg_amount_days IS Medium (Center: 978.9205, S.D.: 276.0485) AND transaction_amount IS Moderately High (Center: 72163.9302, S.D.: 4261.1101) AND is_declined IS no AND number_declines_days IS High (Center: 17.0979, S.D.: 2.2698) AND foreign_transaction IS yes AND high_risk_countries IS yes AND daily_chbk_avg_amt IS Moderately High (Center: 794.2448, S.D.: 140.1988) AND 6m_avg_chbk_amt IS Medium (Center: 484.8946, S.D.: 48.6022) AND 6m_chbk_freq IS Low (Center: 0.8723, S.D.: 0.6416)	THEN is_fradulent IS fraudule

TABLE 6 continued

Rule	Antecedents	Consequent
Rule 6:	IF merchan_id IS Moderately Low (Center: 4.5573271374116E9, S.D.: 4.2 AND avg_amount_days IS Medium (Center: 978.9205, S.D.: 276.0485) AND transaction_amount IS Moderately High (Center: 72163.9302, S.D.: 4261.1101) AND is_declined IS no AND number_declines_days IS High (Center: 17.0979, S.D.: 2.2698) AND foreign_transaction IS no AND high_risk_countries IS no AND daily_chbk_avg_amt IS Medium (Center: 416.289, S.D.: 33.2667) AND 6m_avg_chbk_amt IS Medium (Center: 484.8946, S.D.: 48.6022) AND 6m_chbk_freq IS Medium (Center: 4.2035, S.D.: 0.4135)	THEN is_fradulent IS fraudule
Rule 7:	IF merchan_id IS Moderately High (Center: 5.4705541848133E9, S.D.: 5.1 AND avg_amount_days IS Moderately High (Center: 1387.3474, S.D.: 66.5329) AND transaction_amount IS Moderately High (Center: 72163.9302, S.D.: 4261.1101) AND is_declined IS no AND number_declines_days IS High (Center: 17.0979, S.D.: 2.2698) AND foreign_transaction IS yes AND high_risk_countries IS no AND daily_chbk_avg_amt IS Medium (Center: 416.289, S.D.: 33.2667) AND 6m_avg_chbk_amt IS High (Center: 956.3957, S.D.: 149.2022) AND 6m_chbk_freq IS Medium (Center: 4.2035, S.D.: 0.4135)	THEN is_fradulent IS non-fraudul
Rule 8:	IF merchan_id IS Low (Center: 3.7987392436881E9, S.D.: 2.3 AND avg_amount_days IS Medium (Center: 978.9205, S.D.: 276.0485) AND transaction_amount IS Medium (Center: 46017.7058, S.D.: 5166.0236) AND is_declined IS yes AND number_declines_days IS Moderately High (Center: 13.0168, S.D.: 0.6667) AND foreign_transaction IS yes AND high_risk_countries IS yes AND daily_chbk_avg_amt IS Moderately High (Center: 794.2448, S.D.: 140.1988) AND 6m_avg_chbk_amt IS Moderately Low (Center: 285.2946, S.D.: 33.2667) AND 6m_chbk_freq IS Moderately High (Center: 6.0035, S.D.: 0.3581)	THEN is_fradulent IS non-fraudul
Rule 9:	IF merchan_id IS Moderately High (Center: 5.4705541848133E9, S.D.: 5.1 AND avg_amount_days IS Moderately High (Center: 1387.3474, S.D.: 66.5329) AND transaction_amount IS Low (Center: 2817.7058, S.D.: 7764.3042) AND is_declined IS yes AND number_declines_days IS High (Center: 17.0979, S.D.: 2.2698) AND foreign_transaction IS yes AND high_risk_countries IS no AND daily_chbk_avg_amt IS Moderately High (Center: 794.2448, S.D.: 140.1988) AND 6m_avg_chbk_amt IS Moderately Low (Center: 285.2946, S.D.: 33.2667) AND 6m_chbk_freq IS High (Center: 8.1155, S.D.: 1.2658)	THEN is_fradulent IS non-fraudul
Rule 10:	IF merchan_id IS Moderately Low (Center: 4.5573271374116E9, S.D.: 4.2 AND avg_amount_days IS Medium (Center: 978.9205, S.D.: 276.0485) AND transaction_amount IS High (Center: 96840.9404, S.D.: 14135.0912) AND is_declined IS yes AND number_declines_days IS Low (Center: 1.0168, S.D.: 0.6667) AND foreign_transaction IS yes AND high_risk_countries IS no AND daily_chbk_avg_amt IS Medium (Center: 416.289, S.D.: 33.2667) AND 6m_avg_chbk_amt IS High (Center: 956.3957, S.D.: 149.2022) AND 6m_chbk_freq IS Medium (Center: 4.2035, S.D.: 0.4135)	THEN is_fradulent IS non-fraudul

TABLE 6 continued

Rule	Antecedents	Consequent
Rule 11:	IF merchan_id IS Low (Center: 3.7987392436881E9, S.D.: 2.3 AND avg_amount_days IS Moderately High (Center: 1387.3474, S.D.: 66.5329) AND transaction_amount IS Moderately Low (Center: 24417.7058, S.D.: 4815.783) AND is_declined IS no AND number_declines_days IS Moderately Low (Center: 5.0168, S.D.: 1.2298) AND foreign_transaction IS yes AND high_risk_countries IS yes AND daily_chbk_avg_amt IS Moderately High (Center: 794.2448, S.D.: 140.1988) AND 6m_avg_chbk_amt IS Moderately Low (Center: 285.2946, S.D.: 33.2667) AND 6m_chbk_freq IS Medium (Center: 4.2035, S.D.: 0.4135)	THEN is_fradulent IS non-fraudul
Rule 12:	IF merchan_id IS Moderately Low (Center: 4.5573271374116E9, S.D.: 4.2 AND avg_amount_days IS Moderately High (Center: 1387.3474, S.D.: 66.5329) AND transaction_amount IS High (Center: 96840.9404, S.D.: 14135.0912) AND is_declined IS no AND number_declines_days IS High (Center: 17.0979, S.D.: 2.2698) AND foreign_transaction IS no AND high_risk_countries IS yes AND daily_chbk_avg_amt IS Moderately High (Center: 794.2448, S.D.: 140.1988) AND 6m_avg_chbk_amt IS Medium (Center: 484.8946, S.D.: 48.6022) AND 6m_chbk_freq IS High (Center: 8.1155, S.D.: 1.2658)	THEN is_fradulent IS non-fraudul

The easiest to interpret and most accurate result for the ENORA classifier was produced by ENORA-acc with 11 rules (see Table 5).

The classifier NSGA-II was developed using NSGA-II -rmse with 12 rules, resulting in the most accurate and easy to understand output for the classifier (see Table 6).

We tabulated the rules and results generated by our system to illustrate its potential. To test our system, we created a cross-validated experiment for the credit card fraud detection dataset, in which we ran the 10-fold cross-validation learning process four times and then ran the experiment. Finally, we performed a statistical analysis of the data to determine if there was a statistically significant difference. We performed a performance comparison between the two algorithms under the same conditions and with the same data set. Specifically, we used the ENORA and NSGA-II algorithms in conjunction with the acc, auc, and rmse objective functions and plotted the rules for the algorithms that performed best in this scenario. The rule tables for ENORA-ACC and ENORA-RMSE can be found in Tables 5 and 6, respectively, as they contain the results of the optimal combination with ENORA-ACC and ENORA-RMSE. It can be seen that the result changes positively when the number of rules of the classifier increases. The data seem to indicate that the classifiers are more accurate when the optimization model is controlled by the RMSE, which means that, on average, optimization models controlled by accuracy are preferred over other optimization models. The study showed that ENORA-acc achieved a success rate of 93.236% in cross-validation with 11 rules, while NSGA-II -rmse achieved a success rate of 94.244% with 12 rules. After statistical tests, it was concluded that the results obtained according to the performance measurement model of the proposed method are meaningful and applicable.

4 | CONCLUSIONS AND FUTURE WORKS

It is important to detect credit card theft as early as possible. Financial institution losses and the increasing complexity of credit card fraud detection require the development and deployment of increasingly effective systems for detecting fraudulent credit card transactions. This paper describes an intelligent method for credit card fraud detection by developing a rule-based fuzzy classifier using the multiobjective evolutionary fuzzy classifier (NSGA-II, ENORA) and applying it to credit card transactions. According to our concept, a classifier learning problem is defined as a multiobjective optimization problem that is solved by adapting an evolutionary algorithm to the specific requirements of the task. We tested our proposal on a public dataset using two different evolutionary algorithms. We performed a series of experiments on a real dataset. By comparing the results of the two approaches, we found that the proposed strategy performs better. The results of the evaluation are presented in the form of a 10-fold cross-validation of the datasets. Our original goal was to develop a classifier learning system that provides interpretable yet accurate classifiers. We believe that this goal was achieved since interpretability is a direct function of the number of rules in the document. Experimental results show that the proposed technique works well and achieves the best overall performance in terms of accuracy, AUC, precision, and F1 score, as well as other metrics and ratios. The results demonstrate the feasibility and usefulness of using an effective parameter optimization technique to improve the prediction performance of the proposed approach.

CONFLICT OF INTEREST

The authors declare that they have no known financial or personal conflicts of interest that may have influenced the work in this study.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are openly available in Kaggle Repository at https://www.kaggle.com/datasets/shubhamjoshi2130of/abstract-data-set-for-credit-card-fraud-detection.[13]

ORCID

Mahmut Dirik https://orcid.org/0000-0003-1718-5075

REFERENCES

1. Kundu A, Panigrahi S, Sural S, Majumdar AK. BLAST-SSAHA hybridization for credit card fraud detection. *IEEE Trans Depend Secure Comput*. 2009;6(4):309-315. doi:10.1109/TDSC.2009.11
2. Lucas Y, Portier PE, Laporte L, et al. Towards automated feature engineering for credit card fraud detection using multi-perspective HMMs. *Futur Gener Comput Syst*. 2020;102:393-402. doi:10.1016/j.future.2019.08.029

3. Kim E, Lee J, Shin H, et al. Champion-challenger analysis for credit card fraud detection: hybrid ensemble and deep learning. *Expert Syst Appl*. 2019;128:214-224. doi:10.1016/j.eswa.2019.03.042
4. Wang D, Chen B, Chen J. Credit card fraud detection strategies with consumer incentives. *Omega (United Kingdom)*. 2019;88:179-195. doi:10.1016/j.omega.2018.07.001
5. Makki S, Assaghir Z, Taher Y, Haque R, Hacid MS, Zeineddine H. An experimental study with imbalanced classification approaches for credit card fraud detection. *IEEE Access*. 2019;7:93010-93022. doi:10.1109/ACCESS.2019.2927266
6. Itoo F, Meenakshi, Singh S. Comparison and analysis of logistic regression, Naïve Bayes and KNN machine learning algorithms for credit card fraud detection. *Int J Inf Technol*. 2021;13(4):1503-1511. doi:10.1007/s41870-020-00430-y. https://link.springer.com/article/10.1007/s41870-020-00430-y. Accessed January 30, 2022.
7. Venkata Suryanarayana S, Balaji GN, Venkateswara Rao G. Machine learning approaches for credit card fraud detection. *International Journal of Engineering and Technology(UAE)*. 2018;7(2):917-920. doi:10.14419/ijet.v7i2.9356
8. Ata O, Hazim L. Comparative analysis of different distributions dataset by using data mining techniques on credit card fraud detection. *Tehnicki Vjesnik*. 2020;27(2):618-626. doi:10.17559/TV-20180427091048
9. Jiménez F, Sánchez G, Juárez JM. Multi-objective evolutionary algorithms for fuzzy classification in survival prediction. *Artif Intell Med*. 2014;60(3):197-219. doi:10.1016/j.artmed.2013.12.006
10. Vanam MK, Amirali Jiwani B, Swathi A, Madhavi V. High performance machine learning and data science based implementation using Weka. *Mater Today Proc*. 2021. doi:10.1016/j.matpr.2021.01.470. https://reader.elsevier.com/reader/sd/pii/S2214785321005617?token=A46DCBE156F8228DD40B9DE4C563823FE7BDE9CC480CCC3042C7CAA1A7D943125538F7A620C945C827878041BD516D2B&originRegion=eu-west-1&originCreation=20220513071659. Accessed January 30, 2022.
11. Jiménez F, Martínez C, Miralles-Pechuán L, Sánchez G, Sciavicco G. Multi-objective evolutionary rule-based classification with categorical data. *Entropy*. 2018;20(9):684. doi:10.3390/e20090684. https://www.mdpi.com/1099-4300/20/9/684. Accessed January 30, 2022.
12. Singh A, Jain A. An empirical study of AML approach for credit card fraud detection-financial transactions. *Int J Comput Commun Control*. 2019;14(6):670-690. doi:10.15837/IJCCC.2019.6.3498
13. Credit card fraud detection | Kaggle. https://www.kaggle.com/shubhamjoshi2130of/abstract-data-set-for-credit-card-fraud-detection?select=creditcardcsvpresent.csv. Accessed January 30, 2022.
14. Janiesch C, Zschech P, Heinrich K. Machine learning and deep learning. *Electron Markets*. 2021;31:685-695. doi:10.1007/s12525-021-00475-2/Published
15. A. Ferrario and E. Zurich, Algorithm, Machine Learning and Artificial Intelligence.
16. S. Ghosh and D. L. Reilly, Credit card fraud detection with a neural-network. Paper presented at: Proceedings of the Hawaii International Conference on System Sciences, 1994, vol. 3, pp. 621–630. doi: 10.1109/hicss.1994.323314
17. Poongodi K, Kumar D. Support vector machine with information gain based classification for credit card fraud detection system. *Int Arab J Inf Technol*. 2021;18(2):199-207. doi:10.34028/IAJIT/18/2/8
18. T. T. Nguyen, H. Tahir, M. Abdelrazek, and A. Babar, Deep learning methods for credit card fraud detection.
19. Gacto MJ, Alcalá R, Herrera F. Interpretability of linguistic fuzzy rule-based systems: an overview of interpretability measures. *Inf Sci*. 2011;181(20):4340-4360. doi:10.1016/j.ins.2011.02.021
20. Hajek P, Novotny J. Fuzzy rule-based prediction of gold prices using news affect. *Expert Syst Appl*. 2022;193:116487. doi:10.1016/j.eswa.2021.116487
21. Liu H, Gegov A. Collaborative decision making by ensemble rule based classification systems. In: Pedrycz W, Chen SM, eds. *Granular Computing and Decision-Making. Studies in Big Data*. Vol 10. Cham: Springer; 2015:245-264. doi:10.1007/978-3-319-16829-6_10
22. A. Seshadri, Multi-objective optimization using evolutionary algorithms (MOEA).
23. Carreño Jara E. Multi-objective optimization by using evolutionary algorithms: the p-optimality criteria. *IEEE Trans Evol Comput*. 2014;18(2):167-179. doi:10.1109/TEVC.2013.2243455
24. P. Dueholm Justesen, Multi-objective optimization using evolutionary algorithms, 2009.
25. F. Jiménez, A. F. Gómez-Skarmeta, G. Sánchez, and K. Deb, An evolutionary algorithm for constrained multi-objective optimization. Paper presented at: Proceedings of the 2002 Congress on Evolutionary Computation, *CEC 2002*, 2002, vol. 2, pp. 1133–1138. doi: 10.1109/CEC.2002.1004402
26. F. Jimenez, An evolutionary algorithm for constrained multi-objective optimization. Paper presented at: Proceedings of the 2002 Congress on Evolutionary Computation. CEC'02 (Cat. No.02TH8600), IEEE 2002, pp. 1133-1138 vol.2.
27. Jiménez F, Jódar R, Martín M d P, Sánchez G, Sciavicco G. Unsupervised feature selection for interpretable classification in behavioral assessment of children. *Expert Syst*. 2017;34(4):Aug. doi:10.1111/EXSY.12173
28. Gorzałczany MB, Rudziński F. A multi-objective genetic optimization for fast, fuzzy rule-based credit classification with balanced accuracy and interpretability. *Appl Soft Comput J*. 2016;40:206-220. doi:10.1016/j.asoc.2015.11.037
29. Ducange P, Lazzerini B, Marcelloni F. Multi-objective genetic fuzzy classifiers for imbalanced and cost-sensitive datasets. *Soft Comput*. 2010;14(7):713-728. doi:10.1007/s00500-009-0460-y
30. Rey MI, Galende M, Fuente MJ, Sainz-Palmero GI. Multi-objective based fuzzy rule based systems (FRBSs) for trade-off improvement in accuracy and interpretability: a rule relevance point of view. *Knowl-Based Syst*. 2017;127:67-84. doi:10.1016/j.knosys.2016.12.028
31. R. Kohavi, A study of cross-validation and bootstrap for accuracy estimation and model selection, 1995. http://robotics.stanford.edu/˜ronnyk
32. Deb K. Multi-objective optimisation using evolutionary algorithms: an introduction. In: Wang L, Ng A, Deb K, eds. *Multi-objective Evolutionary Optimisation for Product Design and Manufacturing*. London: Springer; 2011:3-34. doi:10.1007/978-0-85729-652-8_1

33. Siinivas N, Deb K. Muiltiobjective optimization using nondominated sorting in genetic algorithms. *Evol Comput*. 1994;2(3 Fall):221-248. doi:10.1162/evco.1994.2.3.221
34. Deb K, Pratap A, Agarwal S, Meyarivan T. A fast and elitist multiobjective genetic algorithm: NSGA-II. *IEEE Trans Evol Comput*. 2002;6(2):182-197. doi:10.1109/4235.996017
35. Deng X, Liu Q, Deng Y, Mahadevan S. An improved method to construct basic probability assignment based on the confusion matrix for classification problem. *Inf Sci*. 2016;340–341:250-261. doi:10.1016/j.ins.2016.01.033
36. Harandizadeh H, Armaghani DJ. Prediction of air-overpressure induced by blasting using an ANFIS-PNN model optimized by GA. *Appl Soft Comput*. 2021;99:106904. doi:10.1016/j.asoc.2020.106904
37. Chai T, Draxler RR. Root mean square error (RMSE) or mean absolute error (MAE)? -arguments against avoiding RMSE in the literature. *Geosci Model Dev*. 2014;7(3):1247-1250. doi:10.5194/gmd-7-1247-2014
38. Harandizadeh H, Armaghani DJ, Mohamad ET. Development of fuzzy-GMDH model optimized by GSA to predict rock tensile strength based on experimental datasets. *Neural Comput Applic*. 2020;32(17):14047-14067. doi:10.1007/s00521-020-04803-z
39. Sun D, Lonbani M, Askarian B, et al. Investigating the applications of machine learning techniques to predict the rock brittleness index. *Appl Sci (Switzerland)*. 2020;10(5):1691. doi:10.3390/app10051691. https://www.mdpi.com/2076-3417/10/5/1691. Accessed January 30, 2022.
40. Josephine Isabella S, Srinivasan S, Suseendran G. An efficient study of fraud detection system using Ml techniques. In: Peng S.-L., et al (eds.), *Intelligent Computing and Innovation on Data Science, Lecture Notes in Networks and Systems*. Vol 118. Singapore: Springer Nature Singapore Pte Ltd; 2020:59-67. doi:10.1007/978-981-15-3284-9_8. https://www.researchgate.net/publication/341392687_An_Efficient_Study_of_Fraud_Detection_System_Using_Ml_Techniques. Accessed January 30, 2022.
41. Dornadula VN, Geetha S. Credit card fraud detection using machine learning algorithms. *Procedia Comput Sci*. 2019;165:631-641.
42. Taha AA, Malebary SJ. An intelligent approach to credit card fraud detection using an optimized light gradient boosting machine. *IEEE Access*. 2020;8:25579-25587. doi:10.1109/ACCESS.2020.2971354
43. Chicco D, Tötsch N, Jurman G. The Matthews correlation coefficient (mcc) is more reliable than balanced accuracy, bookmaker informedness, and markedness in two-class confusion matrix evaluation. *BioData Mining*. 2021;14:1-22. doi:10.1186/s13040-021-00244-z
44. Mahmut Dirik, Mehmet Gül. Dynamic Optimal ANFIS Parameters Tuning with Particle Swarm Optimization Sırnak University, Department of Computer Engineering.
45. Viera AJ, Garrett JM. Understanding interobserver agreement: the kappa statistic. *Fam Med*. 2005;37(5):360-363
46. DİRİK M, GÜL M. Dynamic optimal ANFIS parameters tuning with particle swarm optimization. *Eur J Sci Technol*. 2021;28:1083-1092. doi:10.31590/ejosat.1012888
47. Lin TH, Jiang JR. Credit card fraud detection with autoencoder and probabilistic random forest. *Mathematics*. 2021;9(21):2683. doi:10.3390/math9212683. https://www.mdpi.com/2227-7390/9/21/2683. Accessed January 30, 2022.
48. Weka 3—Data Mining with Open Source Machine Learning Software in Java. https://www.cs.waikato.ac.nz/ml/weka/. Accessed April 22, 2022
49. Fawcett T. An introduction to ROC analysis. *Pattern Recogn Lett*. 2006;27(8):861-874. doi:10.1016/j.patrec.2005.10.010
50. Powers DMW. Evaluation: from precision, recall and F-measure to ROC, informedness, markedness & correlation. *J Mach Learn Technol*. 2011;2(1):37-63. https://api.semanticscholar.org/CorpusID:55767944#id-name=S2CID

How to cite this article: Dirik M. Predicting credit card fraud using multipurpose classification based on evolutionary rules. *Security and Privacy*. 2022;5(5):e239. doi: 10.1002/spy2.239