FINANCIAL FRAUD DETECTION USING BIO-INSPIRED KEY OPTIMIZATION AND MACHINE LEARNING TECHNIQUE

Ajeet Singh^{1*} and Anurag Jain²

^{1,2}University School of Information Communication & Technology
Guru Govind Singh Indraprastha University, Delhi, India.

¹ajeetsinghiet@gmail.com, ²anurag@ipu.ac.in

Abstract— Financial fraud (FF) is a serious issue, a big concern for financial institutes and requires more attention. Financial frauds are a variety of theft or credit card stealing that occurs when someone takes money with the purpose of personal gain. In the current scenario, a highly accurate system is required to detect financial fraud and prevent financial loss. In this paper, new FF detection model has been proposed for accurate detect financial frauds using one of the Bio-inspired optimization algorithms as particle swarm optimization (PSO), feature selection (CFS) method and adaptive three machine learning techniques (as SVM, KNN, and AdaboostM1). The proposed model is capable to reduce the false-positive rate, training & testing time and enhanced accuracy. Therefore, the proposed PSOS algorithm applied as a features optimization method for selecting the best subset features from the highly imbalanced dataset to increased detection accuracy. The experiment results point out that the PSOS algorithm is the most excellent features optimization method and selected 7 features out of 15 features. The proposed model has been enhanced accuracy (from 82.90% to 85.51%), TPR (from 80.50 % to 90.20 %), FPR (from 0.151% to 0.191%), and decreased Error Rate (14.92 % to 17.10%) compared to RIG method. The findings of this study clearly illustrate that the Bio-inspired algorithm (PSOS) gives more appropriate results compared with the non-Bio-inspired algorithm (RIG).

Keywords— Fraud detection, Bio-Inspired computing, PSO, InfoGain

1. INTRODUCTION

The financial frauds are the criminal activity to obtain money fraudulently for personal gain. Financial frauds are increasing day by day because of rapid increasing electronic commerce service. There is a need for an efficient fraud detection system to detect financial frauds. According to the IC3 (“Internet Crime Complaint Centre”) report 2018, the IC3 received 301508 complaints and 1418.7 million USD losses [www.ic3.gov]. Financial frauds are divided into Insurance Fraud, Banking Fraud (Credit Card, Money Laundering), Telecommunication Fraud, and Web Network.

This paper is focused on credit card fraud (CCF). The credit card (CC) is the most fashionable form of payment for online, offline purchases. A CC grants credit services to the cardholder. The credit limit has to be constant with the financial capabilities of the cardholders and their payment behavior. The CC frauds have been also increased with the increased CC transaction popularity [1]. The CC frauds are split into two groups such as

Received: September 18, 2019

Reviewed: November 21, 2019

Accepted: December 6, 2019

* Corresponding Author

application frauds and transaction frauds [2]. This is the most important problem with the e-commerce service provider organizations. Fraud is called an application fraud when a fraudster is used stolen or fake documents to apply for new credit cards and loans. Application frauds are divided into loan and CC application frauds. Due to these frauds, more money has been a loss. Fraudsters are applied various techniques to commits frauds. Techniques are site cloning, phasing, fake card, and mail theft. To address the issue of quickly arising financial fraud, financial institutions have using various fraud prevention approaches such as CVV (“card verification value”), one-time password (OTP), address verification system (AVS), communal & spark detection, positive & negative list, and real-time credit card authorization, etc [6]. Mr. Chris Dawson, Police Commissioner was announced that the number of card frauds increased radically, as presented in Table I [3].

Table I. Statistics of CC frauds, June 2017- June 2018

2017	CC Frauds	2018	CC Frauds
June	753	January	2441
July	1770	February	2392
August	1935	March	2632
September	1948	April	2150
October	2125	May	2556
November	2237	June	2051
December	1914		

It is a requirement of good the CCF detection method that can help to detect a fraud type, emerging fraud patterns, trends, illegal and legal CC application fraud, Also detection of CC fraud is the main task. Keeping these facts in mind, we design a model based on a PSO, Correlation-based Feature Selection (CFS) method and MLTs (“Machine learning techniques”) to detect and minimize CCF (i.e. financial frauds) as quickly as possible [4].

The bio-inspired optimization technique is an optimization approach to optimize the data set problems using computer systems based on the principles of biology and the natural world. The bio-inspired optimization technique can be used to overcome issues like overfitting & underfitting and optimize in a better way using evolutionary techniques. Particle Swarm Optimization (PSO) is one of the Meta-heuristics and Evolutionary algorithms that work on how Swarm (Credit card) optimized their Path of movement(in case of Credit card- optimize the process of finding the credit card fraud).

The objective of PSOS and RIG methods is to discover the variation between the bio-inspired and non-bio inspired algorithms. The feature optimization method advantages are removed the irrelevant, redundant or noisy data; reduce feature space dimensionality, enhance algorithm speed & accuracy. The features optimization method facilitates to reduce the problem of over-fitting and also training & testing time reduce for simplifying the CC fraud detection system.

1.1 RESEARCH CONTRIBUTION

- FF detection algorithm based on a bio-inspired algorithm as a Particle Swarm Optimization (PSO), Correlation-based Feature Selection (CFS) method, and three MLTs (Support Vector Machine, k Nearest Neighbor and AdaboostM1) has been proposed.

- A Proposed algorithm namely PSOS has been used to optimize the features and It also used for the classification process.
- The PSOS algorithm has been implemented and evaluated on the Australian dataset.
- Study the impact of the Bio-Inspired feature optimization method (selected 7 features out of 15) and non-Bio-Inspired feature optimization method (selected 14 features out of 15).
- The experiment is carried out to compute the effectiveness of the proposed FF detection system.

The remaining paper is structured as follows. Section 2, explained the literary survey & proposed research work has discussed in Section 3. Section 4 presented outlines of the experiment setup and result in analysis. The research conclusion has discussed in Section 5.

2. LITERATURE SURVEY

Currently, financial fraud is becoming widespread across the world and more money lost every year. The several researchers have proposed methodologies for financial & CC fraud detection and their methodologies focus on machine learning techniques (MLTs) and Bio-Inspired algorithms. Wang et al. [5] proposed a CCF detection model based on the whale optimized algorithm and BPNN. The whale optimized algorithm first gets the optimal value after that use the BPNN algorithm to correct the error value, and finally get the optimal value. The WOA-BP algorithm was obtained good detection accuracy (96.40 % to 98.04 %).

The study [6] has presented a survey of CCF detection techniques focused on the latest MLT and Nature Inspired technique. Also, discussed challenges & characteristics faced by good CFF detection system and also explained various techniques applied by fraudsters. It provided a picture of a current trend in CC fraud detection (CCFD). Weatherford et al. [7] were recommended a BPNN, regular neural networks, and artificial immune system (AIS) technique for CC fraud detection. The performances of BPNN, regular neural networks, and (AIS) were compared. Brabazon et al. [8] also used the AIS technique to detect an Online CC fraud with help of the three algorithms are the Unmodified Negative Selection (UNS) Algorithm, the Modified Negative Selection (MNS) and Clonal Selection (CS) Algorithm. The webbiz dataset has been used in this study. The dataset contains 4 million transactions, out of which 462279 are non-fraud transactions and 5417 fraudulent transactions. The CS technique has been classified as a large percentage of fraud transactions correctly. The MNS algorithm accuracy is 98.96%. The UNS algorithm accuracy is 98.96% and CS method calculated the accuracy of 93.38%. The UNS method provides a superior result than the MNS method. Bhattacharyya et al. [9] applied three fraud detection classifiers such as RF, LR and SVM on the CC data set to find out the CC transaction frauds and this research generates the accuracy, AUC, specificity, F-measure, precision, sensitivity, weights for accuracy (wtdAcc) and G-mean of LR (0.947, 0.654, 0.979, 0.778, 0.709, 0.942, 0.77, 0.8), SVM (0.938, 0.524, 0.984, 0.782, 0.624, 0.908, 0.678, 0.716), and RF (0.962, 0.727, 0.987, 0.86, 0.787, 0.953, 0.818, 0.847). RF presented overall good performance across a performance metric. The cyber source 14th annual online fraud information in 2013 presented that the real amount of losses increased through the number of online purchases and the expected total loss has improved up to \$3.5 billion in 2012 with a 30% rise from 2010 [10]. Zareapoor et al. [11] examined the performance of NB (Naive Bayes) KNN, SVM classifiers, and bagging with decision tree algorithm for CC fraud detection the dataset holds total 100000 transactions, 97166 legal, 2834 fraud, and 3% fraud rate. Three classifiers performance has compared with the bagging classifier. A hybrid metaheuristic

model is proposed in [12] for anomaly detection from extremely imbalanced data. The hybrid algorithm is a combination of simulated annealing and PSO algorithm namely PSOSA. Authors are used Brazilian bank dataset to experiment. The results are compared with HPSO. It observed that the PSOSA algorithm showed better accuracy while compared with HPSO. The hybrid PSOSA algorithm is performed effectively for anomaly detection. Massimiliano Zanin et. al. [13], introduced a first hybrid data mining and complex network classification (Parenclitic Network Analysis) approach that capable to detect fraud instances in a CC dataset. Most recent MLTs and ANNs techniques used for financial fraud detection under the IoT environment are reviewed from 2016 to 2018 in [14]. The real financial data of Korea was used to experiment. The entire process consists of four phases such as feature selection method, sampling method, clustering and classification techniques. The MLTs and ANNs outcomes are compared based on accuracy and f-measures. The ANN has the lowest fraud detection rate than the machine learning method. A new approach for variable selection namely VS-VNS has proposed in [15] based on the variable-neighborhood-search method. The set of important variables has selected for the data classification. This method is combined with a BN to build models for generate a credit score and also six search methods such as K2, Hill climbing(LS), repeated Hill climbing (LS), Tabu search, Simulated annealing and Tree augmented naive Bayes are used. Five different datasets are used for experimentation. The VS-VNS approach has achieved good results compared with other methods.

3. PROPOSED RESEARCH WORK

This section illustrates the process of the research methodology. The proposed model presents a complete process for the detection of financial frauds (as CC frauds). The proposed work includes several steps: data collection, data clean, feature selection, PSOS, and adaptive machine learning techniques.

3.1 THE FLOW OF CREDIT CARD FRAUD DETECTION

The main elements of the CCFD system are shown in figure 1. There are four elements in the detection model include data cleaning, features selection, database, and MLTs for classification. This section explains the relationship between each of them and the aim of each phase.

Fig. 1 Proposed FF Fraud Detection system based on PSOS (or PSO-CFS) and InfoGain

3.2 DATASET DESCRIPTION

The sketch of the Australian financial dataset is given in Table II. The Australian dataset holds 690 CC applications (called instances) and 14 features with one class feature. The dataset contains 6 numerical and 8 categorical features. The dataset contains a total of 15 features that are used for the features optimization.

Table II. Australian dataset description [16]

Total Application	Good Application	Bad Application	Features
690	307 (44.5%)	383 (55.5 %)	14 +1class feature

Table III. Statistics of Quantitative Features of the Australian Dataset

Features	Min	Max	Mean	StdDev
A2	13.75	80.25	31.568	11.853
A3	0	28	4.759	4.978
A7	0	28.5	2.223	3.347
A10	0	67	2.4	4.863
A13	0	20000	184.014	172.159
A14	1	100001	1018.396	5210.103

Table III gives the summary statistics of the quantitative features of the dataset and some features have a non-numeric value such as string those are not presented in table 3. So, the 8 categorical (non-numeric) features are A1, A4, A5, A6, A8, A9, A11, and A12. The column Min gives the minimum value of features, the column Max is the maximum value, the column Mean is the average value and the column stdDev is the standard deviation of features: The order of quantitative features are A2, A3, A7, A10, A13, and A14.

Data cleaning: Data processing is a process before launching any classification task. In this work, data processing is performed in the data cleaning phase to remove irrelevant and noise data removed from the dataset before the features selection stages.

3.3 INFORMATION GAIN (INFO GAIN)

The Info Gain measure is the feature selection technique [22] to find the important feature concerning the target class from feature space. The info Gain (also called entropy) is computed for each credit card feature. The feature values 0 represent no information gain and 1 represents maximum information gain. Those credit card features contain high info-gain value that can be selected and those features very less info-gain (lower score) can be removed. General form calculating information gain

$$\text{Entropy (A)} = - \sum P_i \log_2 P \quad (1)$$

Here $p(i)$ means the probability of class i in the data group A . A is a sample of training samples. P is the proportion of the negative and positive sample in A . Entropy (A) mean average amount of info-gain mandatory to classify the transaction label of a tuple A . We used the info gain method [17] to compute the entropy of each feature of credit card and 14 features are selected from 15 features.

$$\text{InforGain (B)} = \text{Entropy (A)} - \sum_{i=0}^n \frac{A_i}{A} \text{Entropy (A}_i\text{)} \quad (2)$$

Where Entropy (A) is the total entropy of the dataset and $\text{Entropy (A}_i\text{)}$ is the entropy of the i^{th} subset computed by partitioning A based on feature B.

3.4 MACHINE LEARNING METHODOLOGY

The Machine Learning technique (MLT) is the scientific study of heuristic algorithms and statistical models used for prediction and also known as Predictive modeling tool that automates the analytical model building for data analytics. In this paper, credit card fraud dataset is used to get learnt the ML system, identity the unobserved patterns and predict the abnormality during the credit card analysis without human intervention. The MLTs are three types of learning approaches like Supervised Learning, Unsupervised Learning, and Semi-Supervised Learning. This section describes three Supervised Machine Learning techniques (MLTs) such as AdaBoostM1, SVM, K-nearest neighbors. All techniques are employed on a best-selected subset of features from the Australian dataset by the PSOS algorithm to identify the CC frauds.

AdaBoost M1: AdaBoost M1 (“Adaptive Boosting”) is a well know ensemble boosting classification algorithm developed [18]. It merges the weak classifier into a strong classifier form. AdaBoostM1 could be used in combination with different kinds of learning algorithms (“weak learners”- WLs) to improve their performance. The outcome of the WLs is joined by a weighted sum which shows the ending outcome of the boosted classifier. The AdaBoostM1 technique is used for minimizing the error of learning methods that give a slightly better performance and also perform well in various dataset excluding for noisy data. AdaboostM1 could meet two conditions:

- i. The classifier must be trained correlatively on a diversity of weighed training instances.
- ii. In each iteration, it tries to give an outstanding fit for these instances by minimizing training error.

Pros: It is simple to implement & influential classification technique that improves the prediction performance. Also, run effectively on large data sets. *Cons:* It is sensitive to outliers & noisy data. It is slower compared to GBoost.

Support Vector Machine (SVM)

SVM is a supervised ML Technique used for regression & classification analysis [24]. It can handle several continuous and no continuous attributes. SVM has a hyperplane for classification tasks. The hyperplane has used as a decisions plane to separates the CC transaction/application into fraud class and legal class from multidimensional feature space. The SVM is based on the main two properties - kernel representation & margin optimization. A complex region is learned by the polynomial (homogeneous) kernel and RB kernel used to learn. In CCF detection, for each test feature, it determines if the test feature falls out the side of the learned region, it is announced as fraud otherwise as legal.

Pros: SVM algorithm needs large training dataset sizes intending to achieve its top prediction accuracy. *Cons:* The kernel choice is the biggest issue and the incorrect choice of the kernel can lead to enhance an error percentage [18, 20].

K-Nearest Neighbors (KNN)

KNN is a machine learning technique used for regression and classification tasks. It is lazy learning or of instance-based learning type classifier [24]. The KNN classifier is the store all available transactions then it classifies any new transaction based on a similarity and distance measure. Any incoming CC transaction is classified by the computing of nearest neighbor (NN) point to the new incoming transaction.

The CC transaction point outs as a fraud, if the NN is fraud, and if the NN is not a fraud, then it is pointed out as legitimate. The distance is computed by using the Euclidean distance measure method for continuous attributes and matching coefficient or hamming distance measure method for categorical attributes. The distance is calculated for every attribute and then combined (multivariate data) together. The KNN can optimize by better distance metrics.

Pros: KNN is capable to use with categorical data and robust to the noise training set. It could be learning models in real-time; there is no need for the predictive model before classification. *Cons:* It requires determining the value of K and Ineffective to feature scaling. The KNN based model accuracy depends on the distance measurement method. At the time of the transaction, fraud cannot detect by KNN [19, 20].

3.5 PARTICLE SWARM OPTIMISATION

The standard Particle swarm optimization (PSO) algorithm is discussed in this section. PSO is a population-based global optimization technique [21, 24, 27], and it is motivated with the social behavior of schooling of fish, flocking of birds or swarms of bees together for the optimization problem (finding food). The PSO strength is a fast convergence compares with genetic algorithms, simulated annealing, and other algorithms. PSO is base on the theory of particle swarm for each solution. Every particle contains a solution in the search space, represented by vector $y_i = (y_{i1}, y_{i2} \dots, y_{iZ})$ and velocity $v_i = (v_{i1}, v_{i2} \dots v_{iZ})$ where Z means the search space dimensionality. Each particle modifies its position & velocity during the movement based on its own experience and its neighbors (see Equation 2, 3). The pBest and gBest acquired by the best population in the population are called the particle best position and also help PSO to search an optimal solution. The following equation presents how to PSO searches an optimal solution. PSO algorithm is used to enhance the performance of CCF detection (financial fraud detection). According to equation 2, each particle y_i position is changed.

$$y_i^{(t+1)} = y_i^{(t)} + v_i^{(t+1)}; \quad (3)$$

According to equation 3, the velocity v_i of each particle is changed.

$$v_i^{(t+1)} = W * v_i^{(t)} + c1 * r1 * (pBest_i - y_i^{(t)}) + c2 * r2 * (gBest - y_i^{(t)}); \quad (4)$$

Where y_i is the i^{th} particle position at t time, v_i is the i^{th} particle velocity at t time, $v_i^{(t+1)}$ is the maximum velocity and $v_i^{(t+1)} \in [-v_{max}, v_{max}]$. W is the inertia weight (W) used to manage the impact of earlier velocities. $pBest_i$ is the personal best performance (local search, personal influence), $gBest$ is the best performance of the group (global search, social influence). Parameters r1 and r2 are the arbitrary numbers between 0 and 1. c1, c2 are positive acceleration constant (called self-recognition and social component/parameters). The operation is repeated till predefined criteria or the highest number of iterations satisfied and after that, the algorithm is stopped. The algorithm has been shown as the best fitness value. Generally, the PSO carries out for a fixed amount of iterations.

The Proposed (PSOS) Algorithm

The main objective of the proposed algorithm is capable to reduce the training & testing time, reducing overfitting problem, identify credit card fraud accurately, and enhance detection accuracy. The proposed algorithm is a fusion of PSO algorithm, feature optimization by CFS and three machine learning techniques (for classification). The PSO parameters are individual weight 0.340, iteration 20, inertia weight 0.30, population size 20, and social weight 0.330. The PSO algorithm can be terminated if met one of the criteria: the maximum iterations (for example 100 iterations), the number of iteration without enhancement, and minimum objective function error.

Algorithm: PSOS for Feature Optimization

Input: A PoS is a transaction of credit card $\mathbf{Y} = (y_1, y_2, y_3, \dots, y_d)$

Total features: **TF**. Feature set $\mathbf{F} = (f_i: i = 1, 2, 3, \dots, n)$

Objective function $f(\mathbf{y})$

Algorithm parameters: Population 20, Iteration 20, 3 MLTs

Output: $\mathbf{S}$ is the selected best features (subset of $\mathbf{F}$) by **PSOS**

$\mathbf{O}$ is the outcomes of MLTs.

1. Calculate each particle fitness function of y_i in $\mathbf{W}^0$;
 2. Setup $gBest$; $\diamond gBest$ represent the best global answer ("in the swarm").
 3. Setup $pBest_i$; $\diamond pBest_i$ represent the best local answer ("in the swarm").
 4. **Repeat**, While (termination condition is not met)
 5. Setup $t = t + 1$; $\diamond$ Making counter to be increas.
 6. **For** $i = 1$ to n do $\diamond n$ is the size of the particle swarm.
 7. New $v_i^{(t+1)} = wv_i^{(t)} + c1*r1*(pBest_i - y_i^{(t)}) + c2*(gBest - y_i^{(t)})$;
 $\diamond$ Velocities update.
 8. New $y_i^{(t+1)} = \text{Current } y_i^{(t)} + \text{New } v_i^{(t+1)}$; $\diamond$ Particle positions update
 9. Calculate the fitness function $f(y_i)$ of all particle y_i in $\mathbf{W}^t$;
 10. **If** $f(y_i) < f(pBest_i)$ **Then** $\diamond$ Solving minimization problem.
 11. $pBest_i = y_i$;
 12. **End If**
 13. **If** $f(y_i) < f(gBest)$ **Then**
 14. $gBest = y_i$;
 15. **End If**
 16. Update y_i, v_i ;
 17. **End For**
 18. **Until** the end criterion is not met
 19. Identify feature subset i.e. $FF = FF1 \cup FF2 \cup FF3 \cup \dots$ using particles
 20. Generate the best particle and Return the feature subset
-

The following flow chart (see fig 2) is presented the working flow of the proposed PSOS algorithm for the optimization of features to the detection of CCF.

Fig. 2 The Working flow of the proposed particle swarm optimization algorithm.

4. RESULTS ANALYSIS AND DISCUSSION

This section discussed the experimental setup and analysis of results based on Bio-Inspired algorithm & non-Bio-Inspired algorithm using several of the binary classification metrics as discussed in this section.

4.1 EXPERIMENTAL SETUP

All experiments were run on a window 10 OS with Intel (R) Core (TM) i-3-2310M CPU @ 2.10 GHz processors and 4 GB RAM. All experiments with default parameter value using the WEKA tool + Eclipse has performed. 10-fold cross-validation approach used to estimate the accuracy of the PSOS algorithm and other algorithms. This works can be implemented by R, MATLAB, RAPIDMINER tool, etc.

4.2 PERFORMANCE MEASURES

The various performance measures are discussed in this subsection to validate the proposed model. These performance measures are derived from the confusion matrix [18,20,22,23].

$$\text{Precision / Hit rate} = \text{TP} / (\text{TP} + \text{FP}) \quad (5)$$

$$\text{Recall/Sensitivity/TPR} = \text{TP} / (\text{TP} + \text{FN}) \quad (6)$$

$$\text{F-Measure} = (2 * \text{Recall} * \text{Precision}) / (\text{Recall} + \text{Precision}) \quad (7)$$

$$\text{Accuracy} = (\text{TP} + \text{TN}) / (\text{TP} + \text{FP} + \text{TN} + \text{FN}) \quad (8)$$

$$\text{Misclassification Rate} = (\text{FP} + \text{FN}) / (\text{TP} + \text{FP} + \text{TN} + \text{FN}) \quad (9)$$

$$\text{Specificity/TNR} = \text{TN} / (\text{FP} + \text{TN}) \quad (10)$$

$$\text{Mean absolute error (MAE)} = \frac{1}{n} \sum_{i=1}^n (E_i - O_i)^2 \quad (11)$$

Root Mean Squared Error

$$\text{RMSE} = \sqrt{\frac{1}{n} \sum_{i=1}^n (E_i - O_i)^2} \quad (12)$$

4.3 EXPERIMENTAL RESULT ANALYSIS

The Proposed algorithm (PSOS) has been performed on the Australian dataset to optimization features and find out credit scoring. The 7 features are optimized out of 15 features and the order these features are A4, A5, A7, A8, A10, A13, A14 whereas ranker (Info Gain) method has selected 14 features out of 15 features and the order of these features are A8, A10, A9, A14, A7, A5 A,6, A3, A13 A,4 A,2, A12, A11, and A1. After selected the best subset of features by PSOS then AdaBoostM1, SVM, and KNN classifiers are applied on these selected features to classification performance based on TPR, FPR, recall, precision, f-measures, Accuracy, MAE, RMSE and error rate evaluation metrics.

The PSOS algorithm and RIG algorithm performance are presented in Tables V & VI according to three MLTs. We compared the outcomes of the BioInspired algorithm and other algorithms. As shown in Table V, TPR has increased while the FPR has decreased. Table VI summarizes the results of the proposed approach & RIG method based on accuracy; detection time, error rate, mean absolute error (MAE), and root mean squared error (RMSE) measures. These outcomes reveal that the proposed algorithm minimizes the error rate by 1.25% and 1.18% compared to the other algorithms.

The SVM classifier on the PSOS algorithm has excellent detection performance with an accuracy of 85.51%, TPR 92.5%, F- measures 85.00%, and Error Rate 14.4928%. The experimental result indicates that the features optimization method is more effective for

CCF detection (see Table V & VI). Finally, the results reflect the performance of the PSOS algorithm has been increased. Varied abbreviations are presented in Table VII which used in this paper.

Table V. Detection outcomes of PSOS and RIG

Technique	Model	Parameters					
		TPR	FPR	P%	R%	F %	BSF
Proposed (PSOS)	AdaBoostM1	90.20	0.191	79.10	90.20	84.30	7
	SVM	92.50	0.201	78.70	92.50	85.00	
	KNN	80.50	0.151	81.00	80.50	80.70	
RIG	AdaBoostM1	83.10	0.146	82.00	83.10	82.50	14
	SVM	91.20	0.206	78.00	91.20	84.10	
	KNN	78.20	0.149	80.80	78.20	79.50	

Table VI. Accuracy, Errors, and Duration (Sec) to build a model of PSOS and RIG

Technique	Model	Parameters				
		Acc %	MCR %	MAE	RMSE	Ts
Proposed (PSOS)	AdaBoostM1	85.07	14.9275	0.2095	0.3279	0.03
	SVM	85.51	14.4928	0.1449	0.3807	0.27
	KNN	82.90	17.1014	0.1757	0.4122	0.01
RIG	AdaBoostM1	84.35	15.6522	0.2081	0.3217	0.06
	SVM	84.64	15.3623	0.1536	0.3919	0.82
	KNN	82.03	17.971	0.1807	0.4232	0.01

Table VII. Used Abbreviation

Abbreviation	Name	Abbreviation	Name		
P	Precision	Ts	Time in seconds		
R	Recall	Acc	Accuracy		
F	F-measures	BSF	Best selected features		
FS	Feature Selected	MCR: Misclassification Rate			
CFS	Correlation-based feature selection method				
PSOS	Particle Swarm Optimization algorithm with feature selection				
RIG	Ranker with Information Gain				
MAE	Mean Absolute Error				
RMSE	Root Mean Squared Error				

Figure 3 demonstrates the comparison between proposed and existing methodologies based on recall, F-measure, and precision. Figure 3 shows the outcomes that reveal the advantage of the PSOS algorithm. The proposed PSOS algorithm yields superior to the existing methodology. It has confirmed that the proposed algorithm gives better outcomes than the other approach in terms of enhanced precision, recall, and F-measure value. Precision value is described as the correctly predicted outcomes over an entire number of predicted outcomes.

Fig. 3 Comparison between precision, recall, and F-measure

Fig. 4 Accuracy comparison between the proposed technique and RIG

The proposed PSOS algorithm illustrates high accuracy (82.90% to 85.51 %,) followed by RIG (82.03% to 84.35 %). It observed that accuracy has increased from 0.87 % to 1.16%. From figure 4, it has proved that the proposed PSOS methodology presents better outcomes than the RIG method in terms of enhanced accuracy rate. Accuracy is expressed as to how well fraud prediction is completed correctly over the set of data instances.

Fig. 5 Comparative study of MAE and RMSE

Figure 5 presents the outcomes of Mean Absolute Error (MAE), Root Mean Squared Error (RMSE) measures. Outcomes reveal that the PSOS algorithm minimizes the error rate compared to the RIG technique.

Fig. 6 Misclassification Rate of PSOS and RIG

Figure 6 presented the performance comparison of PSOS and RIG based on the Misclassification Rate. The results of the PSOS algorithm show that the Misclassification Rate (MCR or EEE) has decreased by approx 1.0 % whereas the error rate has increased by Information gain algorithm. Figure 6 clearly illustrates that the PSOS Algorithm performance is better than RIG.

5. CONCLUSION AND DISCUSSION

Nowadays, the credit card (CC) uses is growing day by day worldwide for online and offline purchases, so there is the possibility of raising the CC frauds. CC fraud is one of the varieties of financial fraud in the banking domain. Researchers are giving more concentration on Bio-Inspired algorithm since their features like simple, derivation free, voiding local minima, and flexible. In reality, the population-based techniques are fashioning these times for enhancing and resolving many engineering problems. The anonymization based algorithms performance might be improved by the optimization-based algorithms.

In this paper, the PSOS algorithm as Bio-Inspired has been introduced for feature optimization and identifies credit card frauds. The technique proposed in the study has been used one class feature as A15 (1, 0) for selecting the best subset of features from the dataset. The proposed PSOS algorithm has selected 7 best features from imbalanced & anonymous CC application dataset whereas RIG method has selected 14 best features from 15 features. The best-selected subset of features by PSOS has been utilized for classifying fraud transactions and also for enhanced classification accuracy.

The PSOS algorithm got a maximum accuracy of 85.51%, 85.07 %, & 82.90% and decreased the error rate of 14.9275%, 14.4928% % 17.1014% on SVM, AddboostM1, and KNN. The outcomes of PSOS are compared with RIG. The outcomes show that the proposed technique is better than the RIG. These outcomes indicated that the proposed Bio-Inspired algorithm as PSOS algorithm has superior detection accuracy, the time required for model building compared to RIG and also the error rate less. The impact of feature optimization has studied in this study.

This paper also, provided a picture of the current trend in CCF detection using Bio-Inspired algorithm. In the future, this work can be extended used a hybrid Bio-Inspired algorithm to detect CC frauds from the imbalanced dataset and improve the accuracy & processing speed.

ACKNOWLEDGMENT

The authors gratefully acknowledge to University School of Information Communication & Technology, Guru Govind Singh Indraprastha University, Delhi, India and The UGC of India for granting Fellowship to research work.

REFERENCES

- [1] Chaudhary, K., Yadav, J., Mallick, B. "A review of fraud detection techniques: Credit card." , International Journal of Computer Applications 45(1), 39-44 (2012)
- [2] Bolton, R. J. Hand, D. J. "Statistical fraud detection: a review.", Statistical Science, vol. 17, no. 3, pp. 235–255, (2002).
- [3] David, W. "Tap-and-go credit card fraud on the rise, prompting a warning from senior police." , <https://www.abc.net.au/news/2018-07-26/tap-and-go-fraud-on-the-rise/10040890>, last accessed 2019/02/20
- [4] Mareeswari, V., Gunasekaran, G. "Fraud Prevention on Credit Card Application Using Hybrid Swarm Optimization Method.", Special Issue on International Conference on Advances in Engineering (ICAE) -2016 Conference Held at Hotel Magaji Orchid, Sheshadripuram, Bengaluru, India, International Journal of Emerging Research in Management & Technology ISSN: 2278-9359 (Volume-5, Issue-5), (2016).
- [5] Wang, C., Wang, Y., Ye, Z., Yan, L., Cai, W., Pan, Sh. "Credit card fraud detection based on whale algorithm optimized BP neural network.", In: The 13th International Conference on Computer Science & Education, August 8-11, 2018, Colombo, Sri Lanka, (2018).
- [6] Adewumi, Aderemi O., Akinyelu, Andronicus A. "A survey of machine-learning and nature-inspired based credit card fraud detection techniques.", In: International Journal of System Assurance Engineering and Management, (2016).
- [7] Weatherford, M. "Mining for fraud." IEEE Intelligent Systems 17 (4), 4-6. (2002).
- [8] Brabazon, A., Cahill, J., Keenan, P., Walsh, D. "Identifying online credit card fraud using the artificial immune system." In: Evolutionary Computation (CEC), 2010 IEEE Congress on, IEEE, 2010, pp. 1-7.
- [9] Bhattacharyya, S., Jha, S., Tharakunnel, K., Westland, J. C. "Data mining for credit card fraud: A comparative study", Decision Support Systems 50 (3), 602-613, (2011).
- [10] 14th Annual Report, Cyber source issue, https://www.cybersource.com/about/news_and_events/archive/2013/2656, March 20, 2013, last accessed 2018/12/12.
- [11] Zareapoor, M., Shamsolmoali, P. "Application of credit card fraud detection: Based on bagging ensemble classifier.", Procedia Computer Science 48 679-685, (2015).
- [12] Sivakumar, N., Balasubramanian, R. "Enhanced Anomaly Detection in Imbalanced Credit Card Transactions using Hybrid PSO.", International Journal of Computer Applications (0975 – 8887) Volume 135 – No.10, February 2016, (2016).
- [13] Zanin, M., Romance, M., Moral, S., Criado, R. "Credit Card Fraud Detection through Parenclitic Network Analysis." Hindawi, Complexity, Volume 2018, Article ID 5764370, 9 pages, <https://doi.org/10.1155/2018/5764370> (2018).
- [14] Choi, D., Lee, K. "An Artificial Intelligence Approach to Financial Fraud Detection under IoT Environment: A Survey and Implementation.", Security and Communication Networks, Hindawi, Volume 2018, Article ID 5483472, 15 pages, (2018).
- [15] Boughacia, D., Abdullah A, Alkhawaldehb, K. "A new variable selection method applied to credit scoring.", Journal: Algorithmic Finance, vol. 7, no. 1-2, pp. 43-52, 2018, 21 June 2018, DOI: 10.3233/AF-180227, (2014)
- [16] UC Irvine Machine Learning Repository, <https://archive.ics.uci.edu/ml/index.php>, last accessed 2019/02/21.
- [17] Hall, Mark A., Smith Lloyd A. "Practical feature subset selection for machine learning.", Springer (1998)
- [18] Singh, A., Jain, A. "Adaptive Credit Card Fraud Detection Techniques Based On Feature Selection Method.", In: 3rd International Conference on Computer, Communication and Computational Sciences (IC4S2018), October 20-21, 2018 in Bangkok, Thailand, (2018).
- [19] Cover, T. M., Hart, P. E. "Nearest neighbor pattern classification.", IEEE Transactions on Information Theory, vol. 13, no. 1, pp. 21–27, (1967)
- [20] Seeja, K. R. Zareapoor, M. "FraudMiner: A Novel Credit Card Fraud Detection Model Based on Frequent Itemset Mining.", the Scientific World Journal, (2014).
- [21] Eberhart, R. C., Kennedy, J. "A new optimizer using particle swarm theory.", In Proceedings of the 6th International Symposium on Micro Machine and Human Science, (Nagoya city, Aichi, Japan, October 04 - 06, (1995).
- [22] Choi, D., Kyungho L. "An Artificial Intelligence Approach to Financial Fraud Detection under IoT Environment: A Survey and Implementation." Security and Communication Networks s(2018).
- [23] Gupta, S., "Deep learning vs. traditional machine learning algorithms used in credit card fraud detection". Diss. Dublin, National College of Ireland, (20160).
- [24] Mishra, K. K., Tiwari, Sh, Misra, A. K., "A bio inspired algorithm for solving optimization problems", 2nd International Conference on Computer and Communication Technology (ICCCCT-2011), IEEE, (2011).

- [25] Thennakoon, A., Bhagyani, C., Premadasa, S., Mihiranga, S., Kuruwitaarachchi, N. "Real-time Credit Card Fraud Detection Using Machine Learning". 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence) (pp. 488-493, IEEE, (2019).
- [26] Kumar, M. S., Soundarya, V., Kavitha, S., Keerthika, E. S., & Aswini, E., "Credit Card Fraud Detection Using Random Forest Algorithm", In 2019 3rd International Conference on Computing and Communications Technologies (ICCCCT) (pp. 149-153). IEEE, (2019, February).
- [27] Rai, D., Tyagi, K., "Bio-inspired optimization techniques: a critical comparative study", ACM SIGSOFT Software Engineering Notes, 38(4), 1-7, (2013).