Volume 8, Issue 4
August 2019

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

Fraud Detection of Credit Cards Using ABC Methodology Based on SVM Algorithm

[1]T. Pavithra and [2] Dr. K. Thangadurai

[1] PG and Research Department of Computer Science, Research Scholar, Govt.Arts College, Karur

[2]PG and Research Department of Computer Science, Assistant Professor & Head, Govt.Arts College, Karur

E-mail: [1]pavithrakrishnaveni2011@gmail.com, [2] ktramprasad05@gmail.com

ABSTRACT

The fast contribution in online based transactional activities raises the fake cases all over the world and causes incredible losses to the individuals and financial industry. Though there are several criminal activities happening in financial industry, credit card fraud is among the most common and worried about by online users. Therefore, countering the fraud behavior during data mining and machine learning is one of the famed approaches introduced by scholars intending to avoid the losses caused by these illegal acts. Mainly, data mining techniques were employed to examine the patterns and characteristics of doubtful and non-suspicious transactions based on normalized and anomalies data. On the other hand, machine learning (ML) systems were employed to expect the suspicious and non-suspicious transactions mechanically by using classifiers. Unnecessary features contribute to the incorrect classification of the credit card fraud detection. So, eliminating the redundant features reduces the size of the data and computation complexity. Identifying a best feature subset for winning classification is a non-trivial job. This needs complete search over the example space of the fraud detection dataset. The important objective of this work is to apply a Swarm intelligence based Artificial Bee Colony (ABC) algorithm is used to discover the best features in the credit card fraud classification. This study contains the data mining classification of fraud detection dataset using data mining Support Vector Machine algorithm (SVM). The credit card fraud detection data results show that SVM can be successfully used for financial data set namely credit card fraud detection diagnosing. The algorithm of efficient diagnosis and the advantages of data preparation on machine learning based routine financial based scheme are recommended by the outcomes.

Keywords: ***Credit card fraud, Artificial Bee Colony, Support Vector Machine algorithm***

1. INTRODUCTION

Credit Card Fraud is dispersal all over the world, as the information technology and communication channels increase more and more, causing huge financial losses. Financial institutions pay a great concentration to rapid solutions of fake activities detection. Credit card Fraud detection is a essential tool and maybe the best way to stop the financial fraud, due to its direct power on the institutions' costumer service, decrease of ready costs and residual a dependable financial service supplier. Beside, because of the wealth and development of electronic banking and electronic payment, the credit card fraud is dispersion in credit cards; thus, banks and credit cards issuing organizations are creation grave efforts to stop the mistreatment of costumers' accounts by taking security events.

Data mining is recognized as the procedure of gaining interesting, novel and perceptive patterns as well as discovering comprehensible, descriptive and predictive models from huge scale of data collections [1]. The aptitude of data mining systems to extract productive information from huge scale of data using statistical and mathematical techniques would help credit card fraud detection based on differentiate the characteristics of ordinary and doubtful credit card transactions. While data mining focused on discovering expensive intelligence, machine learning is rooted in knowledge the aptitude and developing its own copy for the reason of classification, clustering or so on.

The submission of machine learning systems spreads extensively all through computer sciences domains such as spam filtering, web searching, ad placement, recommender systems, drug design, credit scoring, fraud detection, stock trading, and several other applications. Machine Learning classifiers function by building a model from instance inputs and using that to create predictions or decisions, rather than next severely static program instructions. There are many special types of machine learning approaches obtainable with the intentions to resolve heterogeneous problems. Due to the nature of this learn which was focused on classification, the discussion that follows is based on this topic. Machine learning classification refers to the procedure of learning to allocate instances to predefined classes. Officially, there are more than a few types of learning such as supervised, semi-supervised, and unsupervised, reinforcement, transduction and learning to learn [2]. As the attention of this learn was to behavior supervised based machine learning classification, the discussions concerning the rest of the methods are surplus from additional elaboration. In mainly classification studies, supervised based learning is favored more than other systems due to the aptitude to control the classes of the instances with the interventions of human. In supervised learning, the classes of the instances would be labeled previous to feeding into classifiers. after that, by using confident evaluation metrics, the presentations of the classifiers could be measured.

2. FEATURE SELECTION METHODS

Feature is a unique and measurable characteristic of a process that is visible. Any time a credit card is used, the transaction data including a number of features (such as credit card ID, amount of the transaction, etc.) are saved in the database of the service supplier [3]. Precise features strongly influence the performance of a fraud detection system. Feature selection is the process of selecting a subset of features out of a larger set, and

leads to a successful classification. The whole search space contains all possible subsets of features, meaning that its size is 2 N , in which N is the number of features. Thus feature selection is an NP-hard problem [4]. Figure 1 depicts the concept of feature selection [5]. In classification, a dataset usually includes a large number of features that may be relevant, irrelevant or redundant. Redundant and irrelevant features are not useful for classification, and they might even reduce the efficiency of the classifier regarding the large search space, which is the so called curse of dimensionality [6].

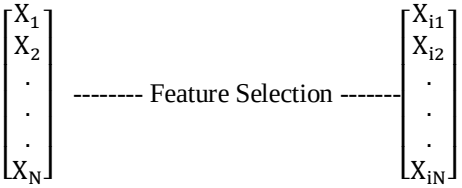

Figure 1. Feature selection (here, N represents the number of original features, and M represents the number of reduced features, i.e. M < N).

The benefits of feature selection include reducing the computational costs, saving storage space, facilitating model selection procedures for accurate prediction, and interpreting complex dependencies between variables. The features that are well selected not only optimize the classification accuracy but also reduce the number of required data for achieving an optimum level of performance of the learning process [7,8]. Feature selection methods usually include search strategy, assessment measure, stopping criterion, and validation of the results. Search strategy is a search method used for producing a subset of candidate features for assessment. An assessment measure is applied for evaluating the quality of the subset of candidate features. The objective of the stopping criterion is to determine when a decision process should stop, and validation is the study of validity of the selected features with the real world datasets. It is obvious that search strategy and assessment measure are the two key factors in the feature selection process. Filter and Wrapper methods are the most important methods of feature selection [7].

A. Filter methods

Filter approaches are independent from learning algorithm, and are cheaper and more general than the wrappers from the computational cost viewpoint. Filter methods only evaluate the relation between features, and are independent from the classification and use measures such as distance, information, dependency, and compatibility. Filter methods are classified into the feature subset selection (FSS) and feature ranking (FR) methods [7]. This classification is based on whether these methods evaluate the relation between the features separately or through feature subsets. In feature ranking methods, each feature is ranked separately, and then the features are ranked based on their relation with the objective variable. The subset selection methods explore all the subsets of features using a certain assessment measure [7].

B Wrapper methods

Wrapper methods use the classifier as a black box and its performance as objective function for features subset assessment. Wrapper approaches include a learning algorithm as assessment function [6]. Feature selection criterion in wrapper methods is a forecasting function that finds a subset with the highest performance. Sequential backward selection (SBS) and sequential forward selection (SFS) are two common wrapper methods. SFS (SBS) starts without any features (or all features), and then the candidate features are, respectively, added to (or omitted from) until adding or omission does not increase the classification performance [6].

3. RELATED WORK

A comprehensive understanding of fraud detection technologies can be helpful for us to solve the problem of credit card fraud.

Lutao Zheng [9] proposed an effective fraud detection method is important since it can identify a fraud in time when a criminal uses a stolen card to consume. One method is to make full use of the historical transaction data including normal transactions and fraud ones to obtain normal/fraud behavior features based on machine learning techniques, and then utilize these features to check if a transaction is fraud or not. In this paper, two kinds of random forests are used to train the behavior features of normal and abnormal transactions. We make a comparison of the two random forests which are different in their base classifiers, and analyze their performance on credit fraud detection. The data used in our experiments come from an e-commerce company in China.

J. Esmaily and R. Moradinezhad [10] in their paper proposed a hybrid of artificial neural network and decision tree. In their model they used a two-phase approach. In first phase the classification results of Decision tree and Multilayer perceptron were used to generate a new dataset which in second phase is feed into Multilayer perceptron to finally classify the data. This model promises reliability by giving very low false detection rate.

Tanmay Kumar and SuvasiniPanigrahi [11] proposed a hybrid approach to credit card fraud detection using fuzzy clustering and neural network. It makes use of two phases. In phase one, they used a c-means clustering algorithm to generate a suspicious score of the transaction and in next phase if a transaction is suspicious it is feed into neural network to determine whether it was really fraudulent or not.

AyushiAgrawal and others [12] proposed testing a transaction using Hidden Markov Model, Behaviour based technique and Genetic Algorithm, wherein they used the Hidden Markov Model to maintain the record of previous transactions, Behaviour based technique for grouping of datasets and lastly genetic algorithm for optimization i.e. calculating the threshold value.

Thuraya and Razooqi [13] proposed a system of fraud detection using Fuzzy Logic and Neural Network. They found out that ANN was 33% more accurate than fuzzy logic. The existing data in the system was used for decision making and using fuzzy logic each data was given a membership attribute then for the validation of results ANN was used.

PoojaChougule and others [14] proposed simple K-means and Simple Genetic Algorithm for fraud detection. In this paper they showed that how k-means algorithm grouped the transactions based on the distinct attribute values and genetic algorithm was used for optimization since with the increase in size of the input k-means algorithm produced outliers. Basically

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

k-means algorithm produced clusters which were then optimized by the genetic algorithm.

Sahil Dhankhad [15] was applying many supervised machine learning algorithms to detect credit card fraudulent transactions using a real-world dataset. Also, they employed these algorithms to apply a super classifier using collection learning methods. They recognize the most important variables that may lead to higher accuracy in credit card fraudulent transaction detection. Moreover, they compare and discuss the presentation of different supervised machine learning algorithms that exist in literature beside the super classifier that they implemented in this paper.

4. PROPOSED METHODOLOGY

Artificial bee colony (ABC) algorithm, as a population-based stochastic optimization proposed by Karaboga, recognizes the intelligent foraging behavior of honey bee swarms. It can be used for clustering and classification, and optimization learning. Pseudocode of the ABC algorithm is given as Pseudocode 1.

1.Load traning set samples
2.Generate the intial populations zi, i=1,….,SN
3.Evaluvate the fitness (fi)of the populations
4. set Cycle to 0
5.repeat
6. FOR each employeed bee{
Produce new employee bee ui by using 6
Calculate the value fi
Apply greedy solution process}
7. Calculte the probality values Pi the solutions zi by 5
8.FOR each onlooker bees{
Select the solution zi depanding upon Pi
Calculte the value fi
Apply greedy solution process}
9.If there is an abandonet solution for the scout
Then restore it with a new solution which will
Be randomly produce by 7
10. Memories the best solution so far
11.Cycle =cycle+ 1
12.until cycle=MCN

An artificial group of bees in the ABC algorithm consists of three special groups: employed bees, onlooker bees, and scout bees. In this algorithm, the number of bees employed in the colony also generation the number of viewer bees. As well, the number of employed bees or viewer bees equals the number of solutions in the population. Aonlooker bee is the bee that stays in the dance area to make the food source selection decision. Anonlooker bee is named employed bee once it leaves to a food source. An employed bee that has inspired the food source revolves into a scout bee, and its duty is to execute a random search to find out new resources. Food supply locations which signify the solution to the optimization problem and the quantity of nectar in the food source depends on the value of the related solution. This value is calculated in (1).

$$\text{fit}_i = \frac{1}{1+f_i} \qquad (1)$$

SN in the algorithm specifies the size of the population. At initial stage, the ABC algorithm produces a dispersed initial population P(C =0) f SN solutions (food source positions) randomly, where SN means the size of population. Each solution$z_i$is a D-dimensional vector for i=1, 2, 3……, SN. Here D is the numbers of cluster for each dataset. After establish, an examination is repeated on employed bees, onlooker bees, and scout bee's processes until the number of population of positions C=1, 2... MXCN) is completed. Here MXCN is the maximum cycle number.

An employed bee creates a small vary in position due to the local knowledge in its memory, and a new source is generated. This bee makes a contrast of the fitness amount of a new source with the nectar amount of earlier source and decides which one is higher. If the new position is higher than the old one, then it is incorporate into its memory and the old one is beyond. Otherwise, the location of the previous one stays in its memory. All employed bees that total the task of research split the location and nectar food source information with the onlooker bees that are in the dance area.

An onlooker bee assesses the nectar information of all employed bees and decides a food source depending on the probability of the nectar amount. This probability value (p_i) is considered in (2). Just like the employed bees, the onlooker bee changes the condition from memory and it checks the nectar amount of the candidate source. If its nectar amount is higher than the previous one and the new position is incorporate into memory and the old one is beyond, then

$$P_i = \frac{fit_i}{\sum_{n=1}^{SN} fit_i} \qquad (2)$$

Where SN is the amount of food sources which is equivalent to the number of employed bees and the fitness of the fit_isolution given in (1). ABC uses (3) for creating a candidate food position:

$$u_{ij} = z_{ij} + \phi_{ij} (z_{ij}\text{-}z_{kj}) \qquad (3)$$

Here, k□{1,2…,SN} and j□{1,2,…,D} are randomly chosen indexes. k is a random value dissimilar from i. □_ij is a random number among [1,-1] which controls the manufacture of neighboring food sources about z_ij and represents evaluation of two food sources to a bee.

While viewer and employed bees achieve use in the search area, scout bees control the discovery process and change the consumed nectar food source with a new food source in the ABC algorithm. If the location cannot be improved as a before determined cycle number, this food source is conventional as abandoned. The before determined cycle number is defined as the "limit" for desertion. In this case, there are three control parameters in ABC: the number of food sources (SN) which is equivalent to the number of employed and viewer bees, the maximum cycle number (MXCN), and the maximum value.

If an abandoned source is assumed to be z_i and j□{1,2,…,D}, the scout looks for a new source to replace 〖z〗_i . This process is described by (4):

$$z_i^j = z_{min}^j + \text{rand}(0,1) (z_{max}^i - z_{min}^i) \qquad (4)$$

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

After (u_{ij}) which is each candidate location is produced, the location is evaluated by ABC and its performance is compared with earlier one. The performance is compared with the earlier one. If the new food source has the same quantity or more nectar than the old one, the new one gets place instead of the old food source in memory. If not, the old one stays in its place in memory. So a greedy selection method is used to make selections between the old source and one of the candidates.

SVM is an efficient supervised learning algorithm used in classification and regression study for applications like pattern recognition, data mining, and machine learning application. This algorithm was developed in 1995 by Cortes and Vapnik [6]. Several studies have been performed on SVM: a flexible support vector machine for regression, an evaluation of flyrock phenomenon stand on blasting operation by using support vector machine.

In this algorithm, there are two different groups alienated by a linear plane. The training of the algorithm is formative the procedure for the parameters of this linear plane. In multiclass applications, the problem is classified into groups as belonging also to one class or to others. SVM's use in pattern recognition is explained below.

An n-dimensional pattern (object) x has n coordinates $x = x_{1,}x_{2,\ldots\ldots,}x_n)$ where each x is a real number, x∈R for $i = 1,2 \ldots, n$. Each pattern xj belongs to a class $y_j \in\{-1, +1\}$. Believe a training set T of m patterns jointly with their classes, $T = \{(x_1, y_1), (x_2, y_2), \ldots\ldots, (x_m, y_m)\}$. Believe a dot creation space S, in which the patterns x are embedded, $x_1, y_1 \ldots\ldots x_m \in S$. Any hyperplane in the space S can be writing as

$$\{x \in S \mid w.x + b = 0\}, w \in S, b \in R \qquad (5)$$

$$w.x = \sum_{i=1}^{n} w_i\, x_i (6)$$

A training set of patterns can be alienated as linear if there be presents at least one linear classifier expressed by the pair (w, b)which properly classifies all training patterns as can be seen in Figure 1. This linear classifier is stand for by the hyperplane H$(w.x + b = 0)$and describes a region for class +1 patterns $(w.x + b > 0)$ and another region for class −1 patterns $(w.x + b < 0)$

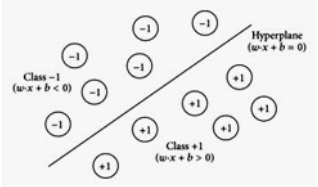

Figure 1 Linear classifier defined by the hyperplane(w.x+b=0)

After the preparation process, the classifier becomes complete for prediction of the class membership on new patterns, different from training. The class of a pattern x_k is establishing from the following equation:

$$\text{Class } (x_k) = \begin{cases} +1\ if\ w.x_k + b > 0 \\ -1\ if\ w.x_k + b < 0 \end{cases} \qquad (7)$$

Thus, the classification of new patterns relies on only the sign of the term. $x + b$.

Sequential Minimal optimization is used in the training phase of SVM. SMO algorithm is an accepted optimization method used to train the support vector machine (SVM). The dual appearance of an SVM primal optimization problem is specifying in (8):

$$\max_{\propto} \quad \Psi(\propto) = \sum_{i=1}^{N} \propto_i - \frac{1}{2}\sum_{i=1}^{N}\sum_{j-1}^{N} y_i\ y_j k(x_i, x_j) \propto_i \propto_j$$

……(8)

$$subject\ to \sum_{i=1}^{N} y_i \propto_i = 0 \quad 0 \leq \propto_i \leq C, i = 1, \ldots, n,$$

Where $x_i$is a training example, $y_i \in \{-1, +1\}$is the equivalent target value, $\propto_i$is the Lagrange multiplier, and is a real value cost parameter.

5. EXPERIMENTATION AND RESULT DISCUSSIONS

The credit card fraud dataset, in the form provided by Prof. Hofmann, encloses definite/symbolic attributes and is in the file "german.data". For algorithms that require numerical attributes, Strathclyde University formed the file "german.data-numeric". This file has been edited and some pointer variables added to make it appropriate for algorithms which cannot cope with definite variables. Some attributes that are ordered categorical (such as attribute 17) have been coded as an integer. Number of Attributes german: 20 (7 numerical, 13 categorical). The purpose of the research is to mine the subset of attributes so as to recover the prediction accuracy of credit card fraud detection. The explanation of the dataset is listed in Table 1.

Volume 8, Issue 4
August 2019

ITEE Journal
Information Technology & ElectricalEngineering

ISSN: - 2306-708X

	Attribute Name	Description	Data Type
1	over_draft	Status of an existing checking account	Qualitative
2	credit_usage	Duration in month	Numerical
3	credit_history	Credit history	Qualitative
4	purpose	Purpose	Qualitative
5	current_balance	Credit amount	Numerical
6	Average_Credit_Balance	Savings account/bonds	Qualitative
7	employment	Present employment since	Qualitative
8	location	Installment rate in percentage of disposable income	Numerical
9	personal_status	Personal status and sex	Qualitative
10	other_parties	Other debtors/guarantors	Qualitative
11	residence_since	Present residence since	Numerical
12	property_magnitude	Property	Qualitative
13	cc_age	cc_age in months%	Numerical
14	other_payment_plans	Other installment plans { bank, stores, none}	Qualitative
15	housing	Housing (rent, own,' for free')	Qualitative
16	existing_credits	Number of existing credits at this bank	Numerical
17	job	job	Qualitative
18	num_dependents	Number of people being liable to provide maintenance for	Numerical
19	own_telephone	Telephone	Qualitative
20	foreign_worker	foreign worker	Qualitative
	class		

TABLE 1

Description of Credit Card Fraud Dataset

Computational environment All the experiments have been conducted on a computer with Intel Core I5-2600 3.4 GHz and 4-GB RAM. The Artificial Bee Colony feature selection algorithm was implemented using Swing Java programming language with Weka and LibSVM libraries to execute the data classification. The proposed ABC algorithm is developed as a software program in JAVA using eclipse tool in figure 2.

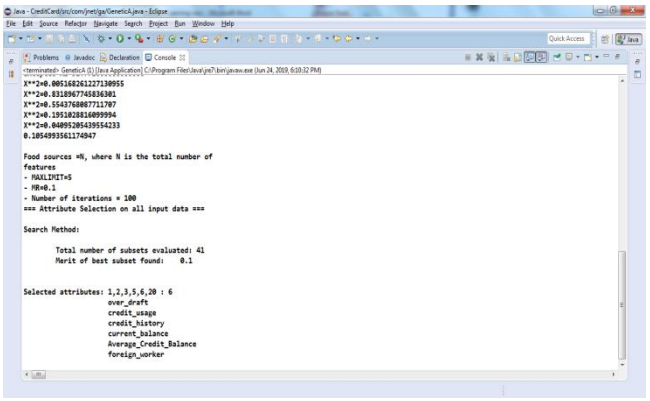

Figure 2 The proposed ABC algorithm

In order to evaluate the performance of the proposed method, the following control parameters are used.

- Number of dimensions =14
- Total Number of onlooker bees and employed bees =12
- Maximum number of iterations =100
- Limit=10

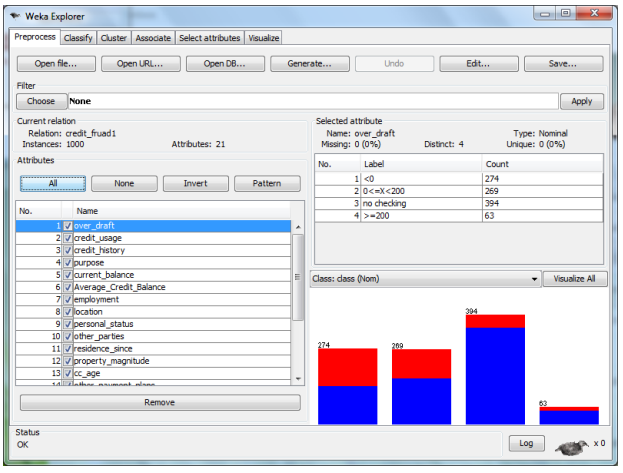

Figure 3 Credit Card fraud dataset with all 21 features

Volume 8, Issue 4
August 2019

ITEE Journal
Information Technology & ElectricalEngineering

ISSN: - 2306-708X

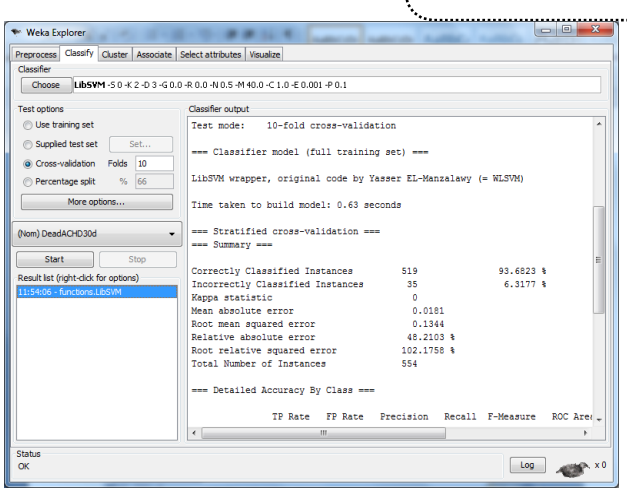

Figure 4 The accuracy obtained by the SVM classifier

Figure 1. shows the loading of Create card fraud dataset with all 21 features followed by the results obtained by the SVM classifier without ABC in Figure 2. The accuracy obtained by the SVM classifier with 21 features is 70%. The correctly classified instances are 700. The parameters of the ABC feature selection algorithm are set as follows: number of dimension is 4, Number of employed bees and onlooker bees =12, Maximum number of iterations =100, Limit=10. The classification accuracy obtained by the proposed PSO-SVM classifier is 96.3% with 963 correctly classified instances Fig.3. depicts the loading of ABC-SVM feature subset followed by the accuracy obtained by the sub set of ABC-SVM features in Figure 4.

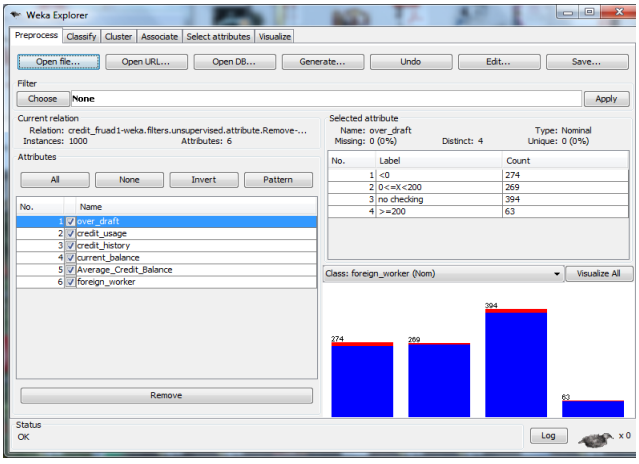

Figure 5 Correctly classified instances

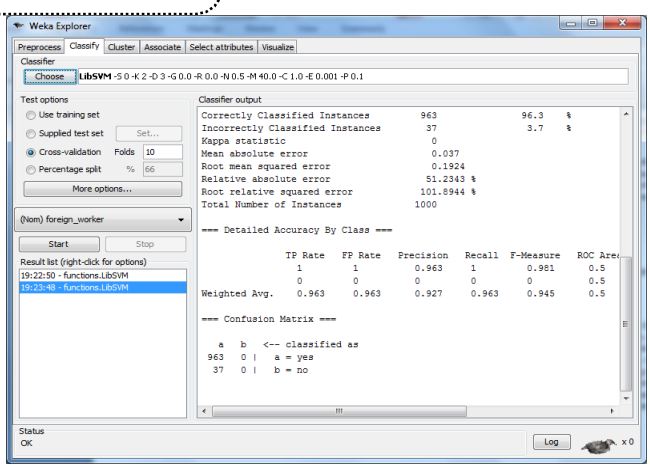

Figure 6 The Accuracy obtained by the sub set of ABC-SVM features.

Table II gives the comparison of result between the support vector machine and ABC with SVM methods. SVM yielded an accuracy of 93.6% with fourteen features. For the same dataset, in the second experiment it produced an accuracy of 96.3 % with six features. The results demonstrated that, ABC with SVM performs better than all the methods in terms of accuracy. The algorithm produced good accuracy with six features namely over_draft, credit_usage, credit_history, current_balance, Average_Credit_Balance, foreign_worker.

TABLE II
THE COMPARISON OF RESULT BETWEEN THE SUPPORT VECTOR MACHINE AND ABC WITH SVM METHODS

Algorithm	Accuracy	Precision	Recall	F-Measure
Traditional Dataset with SVM	70	0.7	1	0.824
ABC with SVM	96.3%	0.963	1	0.945

The graphic demonstration of the ABC-SVM feature selection comparative results is presented in Figure 7.

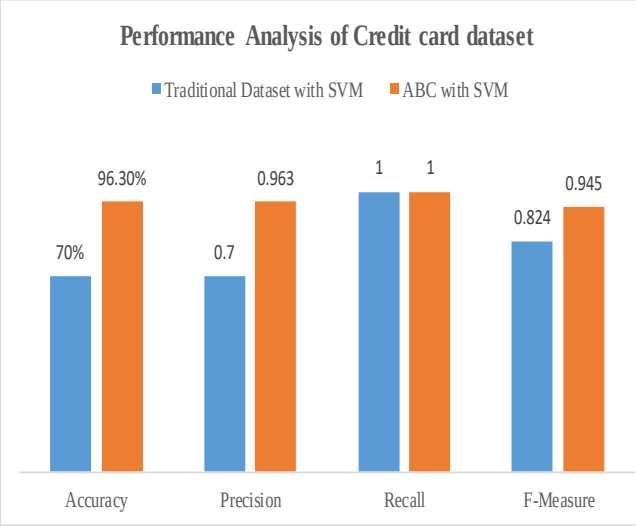

Figure 7 The graphic demonstration of the ABC-SVM

6. CONCLUSION

This method presents a feature selection technique based on ABC algorithm. The results show that a reduced number of features can attain classification accuracy superior to that using the full position of features. ABC is a met heuristic algorithm that share information among the bees in the population and select possible solutions, which can satisfy the defined criteria. ABC has a unique solution update mechanism (updating in two phases), which allows the results to converge to the optimal solution quickly. Also, it is simple and easy to implement because it has fewer control parameters to configure. In this paper, ABC-SVM used the wrapper technique for classification and the experimental results of the algorithm with the Credit card fraud data showed improvement in accuracy when comparing to the conventional forward selection and back elimination feature selection. The algorithm identified six features for disease identification.

REFERENCES

[1] Agyapong, K. B., J. B. Hayfron-Acquah, and M. Asante. "An overview of data mining models (Descriptive and predictive)." International Journal of Software & Hardware Research in Engineering 4 (2016): 53-60.

[2] Eshghi, Abdollah, and Mehrdad Kargari. "Introducing a Method for Combining Supervised and Semi-Supervised Methods in Fraud Detection." In 2019 15th Iran International Industrial Engineering Conference (IIIEC), pp. 23-30. IEEE, 2019.

[3] Dal Pozzolo, Andrea, Olivier Caelen, Yann-Ael Le Borgne, Serge Waterschoot, and Gianluca Bontempi. "Learned lessons in credit card fraud detection from a practitioner perspective." Expert systems with applications 41, no. 10 (2014): 4915-4928.

[4] Tabakhi, Sina, Parham Moradi, and Fardin Akhlaghian. "An unsupervised feature selection algorithm based on ant colony optimization." Engineering Applications of Artificial Intelligence32 (2014): 112-123.

[5] Zhang, Yudong, Shuihua Wang, Preetha Phillips, and Genlin Ji. "Binary PSO with mutation operator for feature selection using decision tree applied to spam detection." Knowledge-Based Systems 64 (2014): 22-31.

[6] Xue, Bing, Mengjie Zhang, and Will N. Browne. "Particle swarm optimisation for feature selection in classification: Novel initialisation and updating mechanisms." Applied soft computing 18 (2014): 261-276.

[7] Bouaguel, Waad, Ghazi Bel Mufti, and Mohamed Limam. "A fusion approach based on wrapper and filter feature selection methods using majority vote and feature weighting." In 2013 International Conference on Computer Applications Technology (ICCAT), pp. 1-6. IEEE, 2013.

[8] Wang, Gang, Jian Ma, and Shanlin Yang. "An improved boosting based on feature selection for corporate bankruptcy prediction." Expert Systems with Applications 41, no. 5 (2014): 2353-2361.

[9] Xuan, Shiyang, Guanjun Liu, Zhenchuan Li, Lutao Zheng, Shuo Wang, and Changjun Jiang. "Random forest for credit card fraud detection." In 2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC), pp. 1-6. IEEE, 2018.

[10] Mubarek, Aji Mubalaike, and Eşref Adalı. "Multilayer perceptron neural network technique for fraud detection." In 2017 International Conference on Computer Science and Engineering (UBMK), pp. 383-387. IEEE, 2017.

[11] Behera, Tanmay Kumar, and Suvasini Panigrahi. "Credit card fraud detection: a hybrid approach using fuzzy clustering & neural network." In 2015 Second International Conference on Advances in Computing and Communication Engineering, pp. 494-499. IEEE, 2015.

[12] Agrawal, Ayushi, Shiv Kumar, and Amit Kumar Mishra. "Implementation of novel approach for credit card fraud detection." In 2015 2nd International Conference on

Computing for Sustainable Global Development (INDIACom), pp. 1-4. IEEE, 2015.

[13] Razooqi, Thuraya, Pansy Khurana, Kaamran Raahemifar, and Abdolreza Abhari. "Credit card fraud detection using fuzzy logic and neural network." In Proceedings of the 19th Communications & Networking Symposium, p. 7. Society for Computer Simulation International, 2016.

[14] Chougule, Pooja, A. D. Thakare, Prajakta Kale, Madhura Gole, and Priyanka Nanekar. "Genetic K-Means Algorithm for Credit Card Fraud Detection." International Journal of Computer Science and Information Technologies (IJCSIT) 6, no. 2 (2015): 1724-1727.

[15] Dhankhad, Sahil, Emad Mohammed, and Behrouz Far. "Supervised machine learning algorithms for credit card fraudulent transaction detection: a comparative study." In 2018 IEEE International Conference on Information Reuse and Integration (IRI), pp. 122-125. IEEE, 2018.