International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-3, February 2020

Fuzzy Particle Swarm Optimization Feature Selection and Aggrandized Classifier for Uncovering Frauds in Credit Card Deals

Jisha.M.V, D.Vimal Kumar

Abstract: ***In today's economy, credit card plays a very important role. The rise of credit card customers improved, credit card scam cases were also on the rise. Numerous procedures are anticipated to challenge the evolution of the frauds in credit cards. In this research work, proposed an innovative fraud detection method which utilizes the similar cardholder's behavioral patterns to construct a current cardholder's interactive profile in order to stay away from the credit card scams. However, the selection of optimal features from the samples and the decision cost for accuracy becomes main important problem. To illuminate these issues this proposed research work presents an innovative fraud detection technique that makes out of four phases: 1. To augment a cardholder's behavioral styles, first we divide all cardholders into distinctive groups making use of the cardholder's historical transaction data such that the members of each group have the similar transaction behavior by K-means. 2. Introduces a new Fuzzy Particle Swarm Optimization (FPSO) feature selection for the amplification of fraud detection in credit cards. 3. By means of a prolonged wrapper method, an ensemble classification are performed by Aggrandized Kernel based Support Vector Machine (AKSVM).4.Refreshing the cardholder's social profile with an input system. This Proposed work adopts the external quality metrics as Accuracy, Recall, Concept drift rate and Fraud feature rate. The UCI dataset is used and is done in MATLAB framework. The analytical measures were used to estimate the routine of the mentioned fraud detection technique. The simulation results show that this proposed innovative fraud detection method provides better accuracy results than other fraud detection techniques. The low concept drift rate results the gain of the innovative method to classify the transactions accurately.***

Keywords: Aggrandized Kernel based Support Vector Machine, Credit Card Fraud detection, Fuzzy Particle Swarm Optimization, K-Means.

I. INTRODUCTION

In the present era, financial organizations had magnified the financial facilities by using innovative services such as credit cards, web and portable financial transaction services and Automated teller machines (ATM) [1]. Furthermore, the utilization of credit card is now more accessible and crucial part of business life with the prompt progress of e-commerce. The Master card is an installment payment card provided to customers for easy life. There are numerous advantage in using credit cards such as: ease of purchase, keeping customer credit history, protection of purchases [2]. In spite of all referenced benefits, the issue of misrepresentation might be a difficult issue in e-banking administrations that compromise MasterCard exchanges particularly and enormous budgetary misfortunes, not just for vendors, singular clients are additionally influenced [3].Fraud deals done by credit cards remains highlighted to a theft and also a fake supply of money. In general, the fraudulent transactions are occurred with the theft of the credit card details. Credit Card Company faces a massive loss when the cardholder is not aware of the loss of their card. A very little amount of information is required by the attacker for conducting any fraudulent transaction in online transactions [4]. For buying services and products online, the internet or telephonic devices are used. In few cases, the pattern in which transactions are made by the customer is the only way through which it is possible to identify that the credit card is stolen. A fraud recognition technique wants to be applied to decrease the rate of successful credit card frauds. In general, various data mining procedures and statistical analytical methods are used to solve this fraud detection issue. To prevent fraud events there are generally two procedures: Classification method and Abnormality identification. In the first method, a classifier is trained with the given patterns of normal and fraud transactions using supervised procedures [6].Second method is having the ability to filter the new deals that is uneven against the profile of the card holder by computing the distance of the inward transactions with the profile [5]. The two above methods have its own drawbacks. The classification method can identify the fraud but cannot differentiate normal behavior from diverse cardholder's [8].The abnormality identifier have the ability to disclose the behavior of the cardholder [7], but cannot depict the fraud. Overall we may declare that the age, the behavior, income and resources changes the transactional behavior of cardholder. The rise of innovative attacks advances over time which do influence the patterns of transactions. Concept drift problem is a task which is not solved by the mentioned methods [9].Facing above challenges, with the view of analogous cardholder's and their ancient transactions, abstract the behavioral pattern of a cardholder. This research effort is briefly given by the subsequent ways:

- Preprocessing via grouping the behavioral patterns using K-means;
- Feature selection behavioral patterns by Fuzzy Particle Swarm Optimization;

Revised Manuscript Received on February 05, 2020.
* Correspondence Author
Jisha M.V*, Ph. D Scholar, Department of Computer Science, Nehru Arts and Science College, T.M Palayam, Coimbatore, Tamilnadu, India.
Dr. D. Vimal Kumar , Associate Professor, Department of Computer Science, Nehru Arts and Science College, T.M Palayam, Coimbatore, Tamilnadu, India.

- Classifying behavioral patterns and assignment using Aggrandized Kernel based Support Vector Machine (AKSVM).
- Refreshing the cardholder's social profile with an input system.

The research work is structured as: Section I explains the benefits of the credit card transaction and its issues, importance of fraud detection technique. Section II presents the previous study done on fraud detection. Section III familiarizes the future fraud detection technique and its classification method. Section IV & V exhibits the tentative results. Finally, conclusion of the research work in Section VI.

II. LITERATURE REVIEW

Halvaiee et al [10] addressed detection of fraud using Artificial Immune System in credit cards. They have induced novel prototypical AIS centered fraud detection model (AFDM). In this work, they have used an immune system motivated algorithm (AIRS) which is used to improve detection of fraud. Using this approach, the accuracy is increased to 25%, the budget is reduced to 85%, and compared to the base algorithm decreases response time of the system to 40%.

Zareapoor et al [11] presented the best classification algorithm, bagging classifier constructed on decision tree, for fraud detection. They have highlighted the common classification algorithms like Naïve Bayes (NB), Support Vector Machines (SVM), K-Nearest Neighbor algorithms (KNN) and found that these can be ensemble to construct new model classifier. To validate the advantage of bagging ensemble method, the recital estimation is prepared taking place at real time dataset of the credit card deals.

Şahin et al [12] developed fraud prevention mechanisms, the necessary device and perhaps the finest method to break many such frauds. The work developed various decision tree and support vector machine based classifiers and used to detect frauds in credit cards. The real time dataset is used to relate the presentation of decision tree and SVM models.

Whitrow et al [13] proposed an aggregation framework for transaction-level detection, employing different classification methods. These ways are applied using real dataset in two case studies. The extent of the gathering epoch includes the massive influence on its performance. Transaction aggregation is found to be profitable in numerous circumstances. Also, when random forest classifier is used the aggregation appears significantly active. Meanwhile, random forests are pledge to achieve better results than alternative classifiers, including KNN, SVM and logistic regression. Aggregation do have the benefit to acquire better results from the population drift.

Dal Pozzolo et al [14] developed an efficient fraud detection algorithm that reduces the loss, and further methods depend on the progressive machine learning techniques to support fraud detectors. It gives a solution from the expert's perspective by converging on disputes such as imbalanced, non-stationary assessment. A real time dataset from a business partner were used for investigation.

Jha et al [15] utilized a deal aggregation policy to identify frauds in credit card usage. The aggregate transaction for measuring purchaser ordering deeds for every deal and also used to spot fraudulent transactions. During this work, real time deals of an international company were used to estimate the model and for aggregating the deals.

Bahnsen et al [16] proposed algorithmic rule with von mises distribution for generating fresh features supporting and evaluating the interrupted performance of the transaction time. A European card company real data are used. Related to different detection methods, measured the manner they work and produce better results. The results showed a mean increase in savings by including the planned intervallic features into the models.

Van Vlasselaer et al [17] proposed Anomaly prevention using advanced transaction Exploration (APATE), a unique methodology to spot fraudulent credit card deals lead in on-line purchasing. This methodology associates crucial options resulting from the inward deals feature, thus arrive to the history of the deals of client by the fundamentals of Regency, Frequency, and Monetary (RFM). Also introduced a network-based sorts with the manipulation of the links of credit card holders and traders thus achieving a time-dependent suspicion mark for every network object. The outcomes displays that each intrinsic and network-based feature is to robustly intertwined sides of identical image. The arrangement of the two classes of features leads to the simplest execution prototypes that can give better AUC-scores greater than 0.98.

Quah et al [18] focused to construct a real time system by analyzing the behavioral features to interpret the fraud cases. It makes use of self-organization map for detecting the frauds by interpreting, removing and studying the purchaser behavior. Now a days, it has become easier to commit frauds through net by new mechanisms.

Sahin et al [19] introduced decision tree technique that minimizes classification prices by the selection of splitted attribute at each non terminal node. Using the real time dataset, this model performance is related to other classifiers. During this approach, cost of misclassification is the fluctuating parameter.The developed approach performs efficiently than other strategies.

Srivastava et al [20] introduced hidden Markov model (HMM) and is applied for detecting the fraud. This model is trained initially using usual behavior of an original cardholder. If the HMM does not acknowledge the arriving deal of a credit card by high probability, it is reflected as a fraud. By equivalent time, it should confirm that true deals are not removed. Thus the tentative result shows the efficiency of the method and compared against other strategies.

From above methods, researcher's concentrated on classifying transactions into genuine or fraud by analyzing the rare behaviors from their ancient transactions. As to the above work the approach could be done only after a usage of a supervised procedure.

To address this problem, the proposed methodology provides the ensemble based classification model which leads to high accuracy fraud detection system.

III. PROPOSED METHODOLOGY

This proposed credit card fraud detection system marks each behavioral pattern by specifically mining the behavioral patterns from the gathered data. Finally, based on the above strategy a time-to-time updated cardholder's profile is generated [21]. This method contains four steps as shown in Fig. 1:

- Initially preprocessing the raw features of the card holder is done by dividing the cardholder's into three groups on the basis of the amount transactions done that is, low, medium and high respectively via clustering method.
- Introduces new Fuzzy Particle Swarm Optimization (FPSO) feature selection for the augmentation of credit card fraud detection.
- An extended wrapper method is used for selecting the most effective feature and then an ensemble classification is accomplished by Aggrandized Kernel Support Vector Machine (AKSVM).
- Refreshing the cardholder's social profile with an input system.

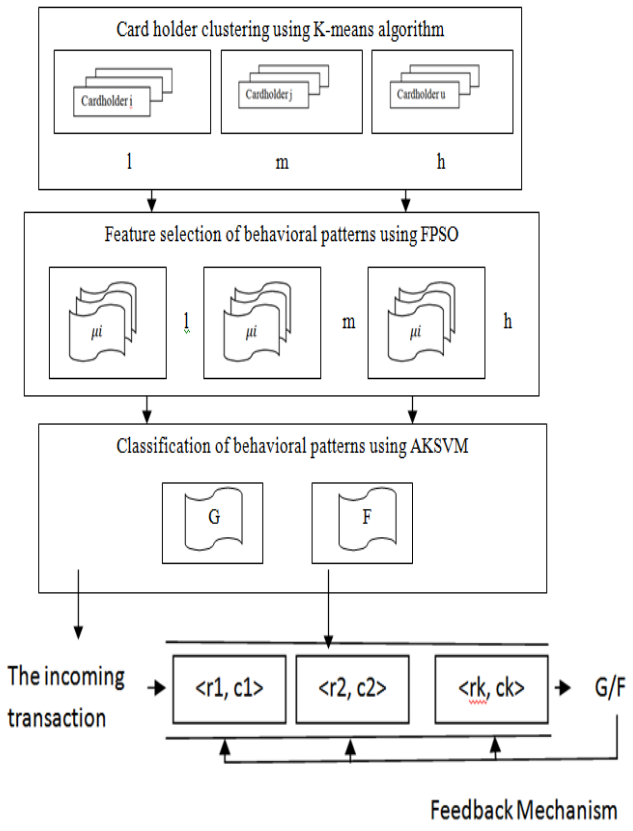

Fig .1 General framework of Detection procedure to Credit card Frauds [21].

IV. PROBLEM FORMULATION

The effort done focus on the classification problematic that is encountered during a Fraud Detection System, provided that it presents an appropriate enactment measures and proper explanation of the response interaction. Let the feature vector is denoted by x_i related to the i^{th} legal dealings and ∈ be the equivalent category, where zero denotes a illegal deal and one denotes real deals. Noting that the nature of transaction stream differs with time, each day the classifier K is newly retrained or updated. Especially, the classifier K is skilled on the supervised deals or transactions that exists till the day t-1, denoted by $K_{t-1.}$ At day t, the authorized set of deals or transactions are processed by the classifier $K_{t-1.}$

A. Preprocessing data

Data are generated from many origins in a diversity of patterns. In data mining, preprocessing is done to make over the information into an acceptable form. In Preprocessing ,there exists various activities including fusing data from multiple origins, for mining process and cleaning the data compatible information's are chose, e.g. handling outliers and missing values.. The yield of preprocessing could be a normal data matrix; i.e. a vector of instances or tuples (objects) where every instance indicates a set of attribute values [21]. If there are n instances with p attributes each, then there will be n rows and p columns in the standard data matrix. To build better model for prediction or depiction, the preprocessed knowledge is utilized in data processing method.

1) Cardholder Clustering:

Firstly, k-means clustering algorithm [22] is used to generate three similar clusters built on transaction amount by dividing all cardholder's into low (l), medium (m) and high (h) respectively. The main goal of K-means clustering is that the sum of squares is minimized within each cluster by distributing M spotted points in N coordinates into K clusters. We cannot predict always that the result will have minimal sum of squares, apart from the presence of lesser value for M, N and K. When there is no change of appoint from one cluster to another, then the solution is minimum and considered as local optima. Let us consider among the cardholders, three clusters of ids, where id implies the identification of each cardholder. Let S = {l, m, h} and |S|=3. It is more convenient to resolve the sparse problematic of data by considering the deals by all cardholder's in a set than using single cardholder's transaction. By taking into account both features, his or her past dealings and further behavioral patterns suggested via other followers in the similar set, which might occur in upcoming can help us improve a cardholder's behavior and become accustomed to attain an individual model[21].

B. Feature Selection Of Behavioral Patterns Using Fuzzy Particle Swarm Optimization

The fuzzy based features of the behavioral patterns is designated through a fuzzy matrix μ with m rows and n columns where m denotes the total of data objects and n denotes the total of clusters. The component μ_{ij} represents the extent of link or membership function of i^{th} object with the j^{th} cluster [23]. To overwhelm the limitations of fuzzy systems, the capability of global search in PSO procedure is applied in the derived algorithm. Particle Swarm Optimization (PSO) is a population based optimization tool that optimize a problem by iteratively improving a solution by considering a given degree of quality.

Particle swarm optimization (PSO) is a residents based stochastic optimization procedure motivated by flocking birds and schooling of fish and are established by reiterations. The PSO algorithm begins with a populace of particles which are

allowed to move on a particular space where the positions denotes the prospective results for the particular problem, and velocities are erratically reset in the search space. By apprising particle velocity and position, the optimal position search is carried out in each iteration. Thus, by means of a fitness function, the fitness value of all particle's positions are calculated [24]. The velocity of every particle is reorganized by best two positions, individual finest position and global finest position. The individual or private best position, is the finest position the particle had visited denoted by pbest and gbest denotes the finest position the swarm had visited later the first step time. The particle's velocity and position are modernized as "equation (1)" and "equation (2)".

$$V(t+1) = w.V(t) + c_1 r_1 \left(pbest(t) - X(t)\right) + c_2 r_2 \left(gbest(t) - X(t)\right); \quad k = 1,2,\ldots..P \qquad (1)$$

$$X(t+1) = X(t) + V(t+1) \qquad (2)$$

where the position and velocity of particle are given by X and V respectively. The inertia weight is given by w, acceleration coefficients are c_1 and c_2 ,are positive constants, that on the process of search switch the impact of pbest and gbest, P is the quantity of particles in the swarm, r_1 and r_2 are random values in range [0, 1]. In anticipated FPSO technique the position and velocity of particles reconstructed to signify the fuzzy relation among variables. The Fuzzy Particle Swarm Optimization (FPSO) algorithm, denotes the position of particle X which illustrates the fuzzy relation from the set of data objects, $o = \{o_1, o_2, \ldots\ldots, o_n\}$, to set of cluster centers, $Z = \{z_1, z_2, \ldots\ldots, z_c\}$. X is conveyed by "equation (3)".

$$X = \begin{bmatrix} \mu_{1l} & \cdots & \mu_{1c} \\ \vdots & \ddots & \vdots \\ \mu_{nl} & \cdots & \mu_{nc} \end{bmatrix} \qquad (3)$$

Where μ_{ij} is the membership function of the i^{th} object with the j^{th} cluster with constraints. Hence we may notice that the position matrix of every particle is identical to fuzzy matrix μ. Moreover, a matrix with m rows and n columns, members of which are in the range [-1, 1] specifies the velocity of every particle. Using the matrix calculations, we acquire equations for apprising the positions and velocities of the particles.

$$V(t+1) = w \otimes V(t) \oplus (c_1 r_1) \otimes \left(pbest(t) \ominus X(t)\right) \oplus (c_2 r_2) \otimes \left(gbest(t) \ominus X(t)\right) \qquad (4)$$

$$X(t+1) = X(t) \oplus V(t+1) \qquad (5)$$

After apprising the position matrix, it may disrupt the restrictions represented in (4) and (5). Thus we have to normalize the position matrix. For this, in the matrix every elements of negative value are assigned zero. If in a row of matrix, every elements are zero, they must be re-calculated by sequence of arbitrary numbers in the interval [0, 1] and without violating the constraints, the matrix experiences the resulting changes:

$$Xnormal = \begin{bmatrix} \mu_{11}/\sum_{j=1}^{c}\mu_{1j} & \cdots & \mu_{1c}/\sum_{j=1}^{c}\mu_{1j} \\ \vdots & \ddots & \vdots \\ \mu_{n1}/\sum_{j=1}^{c}\mu_{nj} & \cdots & \mu_{nc}/\sum_{j=1}^{c}\mu_{nj} \end{bmatrix} \qquad (6)$$

The FPSO algorithm like former algorithms, requires a function for estimating the general results called fitness function. In this work "equation.(6)" is used for evaluating the solutions.

$$f(X) = \frac{K}{J_m} \qquad (7)$$

where K represents a constant and J_m denotes objective function. The reduced Jm, improves the clustering effect and makes the individual fitness f(X) efficient.

Algorithm 1. Fuzzy PSO for feature selection

1. The constraints considering the population size P,1c,2c,w are initialized and indicate the highest iterative count.
2. Create a swarm with **P** particles (X, pbest, gbest and V are n× c matrix).
3. Initialize X, V, pbest for every particle and gbest for the swarm.
4. Compute cluster centers for every particle.
5. Compute fitness value of every particle with "equation (7)".
6. Compute pbest for every particle.
7. Compute gbest for the swarm.
8. Apprise the velocity matrix for every particle with "equation (4)".
9. Apprise the position matrix for every particle with "equation (5)".
10. Go to step 4 if the algorithm's stopping condition is not met.

If no enhancement in gbest in further iterations, then it is assumed as the termination condition of the developed algorithm.We can generate a set of standard features for each cluster by considering all cardholder's normal feature set as in "equation (8)".

$$G_j = \cup_{id \in j} G^{id}, \forall j \in V \qquad (8)$$

The characterization of interactive arrangements may be opaque once resolved by human knowledge. As such it is difficult to classify precise behavior sets into standard feature sets in the real world. To unify high level abstract knowledge, it is appropriate to use classification methods to solve the supervised learning problems.

C. Ensemble Classification Is Performed By Aggrandized Kernel Based Support Vector Machine

The most important scheme of ensembling is to arrive to a global model with high accuracy and reliable estimates rather with a single model[24]. The global model is originated by merging models with similar functioning capability. In this work, Bagging and AdaBoost ensembling methods were analyzed and compared with the prediction done by single classifier alone[25].

Aggrandized Kernel based Support Vector Machine (EKSVM)

Support Vector Machine model is a machine learning approach that is constructed on theories of statistics. A group of support vectors are used to signify data patterns thereby classify the data. To derive a discriminant function f(x), such that $y_i = f(x_i)$ given N data samples$(x_1, y_1) \ldots (x_i, yi) \ldots (xN, yN)$ a common two class classification strategy is applied.

A potential linear discriminant function is given by f(x) = sgn(w · x − b) where w · x − b = 0 is the splitting hyper plane in the data space. Selecting a better discriminant function should provide a hyper plane possessing maximum splitting margin with respect to two classes [26]. Finally f(x) = sgn(PI i=1 $\alpha_i y_i(x_i \cdot x - b)$ represents the absolute linear discriminant function, where I is the total training records, x_i is the support vectors and $y_i \in \{-1, +1\}$ is the label linked with the training data, $0 \leq \alpha_i \leq C$ (constant C > 0). When the area splits the two classes into non-linear, the data points are linearly separated by renovating data points to high dimensional space. The nonlinear discriminant function of SVM is:

$$f(x) = sgn(\sum_{i=1}^{l} \alpha_i y_i K(x_i, x) + b), \quad (9)$$

where $K(x_i, x)$ is the kernel function which is mainly used to change data points. The sigmoid function, polynomial function, radial basis function and linear function are the general kernel functions. The kernel function is not used to differentiate the data features. In the kernel function of SVM K(xi, x), all features of the training and test datasets are equally preserved. Considering all features likewise may lead to inefficient process and will upset the accurateness of SVM[26]. The best method to treat different features is by adding weights to the respective kernel function [27]. The importance of every feature is highlighted by the given weights. The proposed kernel function is expressed by K (wx_i, wx), where w is a vector containing feature weights of data set. A non-linear discriminant function with feature weights is developed by "equation (10)",

$$f(x) = sgn(\sum_{i=1}^{l} \alpha_i y_i K(wx_i, wx) + b), \quad (10)$$

This enhanced kernel is independent on any other kernel functions. A Kernel function is derived by different weights assigned to the features. From a training data, we may compute and derive feature weights by using rough set strategy. The main rules used are 1) A weight 0 is assigned, if a feature is not in any reducts; 2) a feature is defined essential, if its occurrence in the reducts is more; 3) if a reduct has less number of features, the most required is considered. The needed feature for a reduct is also represented by the only one feature of a reducts.

Algorithm 2: Estimation of Feature Weight.

Input : The derived features.
Output: The weight vector W.
Determines all reducts of D by rough sets;
$M_{feature}$ ← total features in D;
M_{reduct} ← total of reducts of D;
//Initialize the weight of each feature.
for (i ← 0 to $M_{feature}$) do
    w_i ← 0;
endfor
// Compute the weight of every feature.
for (i ← 0 to $M_{feature}$) do
    for (j ← 0 to M_{reduct}) do
        if (feature i in the j^{th} reduct R_j) then
            n ← number of features in R_j ;
            w_i ← w_i + 1 n ;
        endif
    endfor
endfor

Considering above principle, an Algorithm 2 depicts the method to calculate feature weights and to assign rank to features by using the rough set strategy. With the completion of the estimation of ranking, the features with a weight 0 are removed. Feature selection and ranking is done with the same Algorithm 2.

D. Response Methodology to Apprise the Cardholder's Behavior Profile.

To refresh the summary of the cardholder, the true or normal data in given experimental set is not considered. On the grounds that it could mirror indirectly the progressions of the cardholder's deal practices, the true labels or data are used. Henceforth, this projected technique utilizes a criticism component to refresh the profile of every cardholder once a fresh deal comes [21]. Every cardholder u in cluster j has a set $C_j^u = \{ c_1, c_2, \ldots \ldots, c_k \}$.

A ranking score is allocated to every group, and the summary of cardholder is articulated to as a 2-tuple < >, where:

- c_i is one of the interactive conduct standard in set C_j^u.
- r_i is one of the evaluation score of the group c_i.

In the preceding stage, a Priority Queue is utilized to pick a group with the most noteworthy ranking gain featured by a grey block. When this technique identifies a erroneous guess then the latest transactions will not be conform to the cardholder's profile. The rating score of the classifier is changed by utilizing the true label of the incoming transactions. Subsequently, propose an input system for refreshing the rank. The classifier is rewarded if it predicts correctly (i.e., ri = ri+1) in the event, else it will be rebuffed (i.e., rj = rj-1). By utilizing this criticism component, the following exchange can be estimated by a group c* to such an extent that r* is the most elevated ranking gain in $\{r_1, r_2 \ldots . r_k\}$. It is described in Algorithm 3.

Algorithm 3: Classifier's rating score is apprised.

Input: Exclusive *id* of a cardholder, a set of 2-tuples $\{< r_i, c_i > | i = 1, \ldots\ldots, k\}$ and an inward deal with p -1 earlier deals
Output: A fresh set of 2-tuples $\{< r_i', c_i > | i = 1, \ldots\ldots, k\}$

```
1. Xid: = a vector of inward deal with p - 1
   preceding deals gained from Algorithm 1;
2. c* := a group acquired peak rate score
   via a Priority Queue;
3. pred := forecast tag of X^id with c*;
4. label := Accurate tag of the inward deal;
5. if pred ≠ tag and tag = 0 then
6.     for (i := 1; i ≤ k; i++) do
7.         pred_i = forecast tag of X^id using c_i;
8.         if pred_i ≠ tag then
9.             r_i' := r_i − 1;
10.        else
11.            r_i' := r_i + 1;
12.        endif
13.    endfor
14. endif
```

V. RESULTS AND DISCUSSIONS

This proposed method provides the best framework to detect the fraud and the result shows that Aggrandized Kernel Support Vector Machine (SVM) performance is excellent. The anticipated fuzzy particle swarm optimization (FPSO) increases enactment of the classifier when related to the present fraud detection methods. The performance of the fraud detection technique is measured with the help of the UCI dataset for analytical measurements. The proposed work adopts the external quality metrics such as Accuracy, Recall, Concept drift detection rate (CDDR) denotes the segment of genuine deals labelled as 2 recognized to be fraud and Fraud feature detection rate (FFDR) denoting the segment of the illegal deals labelled as 1 recognized to be fraud.

Table 1. Simulation results of the proposed and existing techniques.

Metrics	ARF+FM	FPSO+SVM	FPSO+AKSVM
Accuracy(%)	78.51	85.59	92.25
Recall (%)	81.15	87.19	93.61
CDDR	0.4322	0.3168	0.1971
FDDR	0.9394	0.9589	0.9860

The Fig. 2 illustrates the accuracy evaluation between the proposed and existing fraud detection technique. From the simulation results the proposed FPSO-AKSVM provides better accuracy compared to the existing ARF and FPSO+SVM fraud detection technique. It concludes that the proposed ensemble based classifier technique provides best credit card fraud detection.

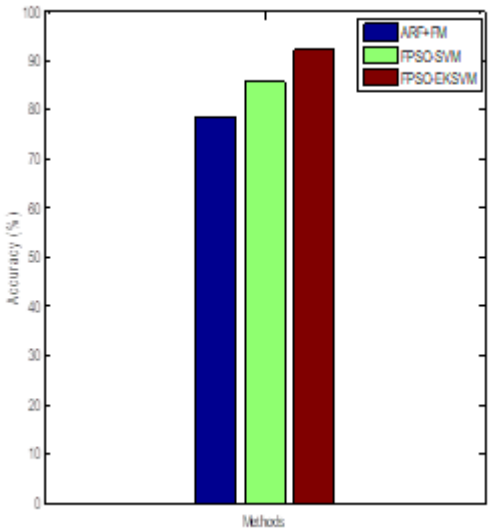

Fig.2. Accuracy evaluation between the proposed and present fraud detection technique

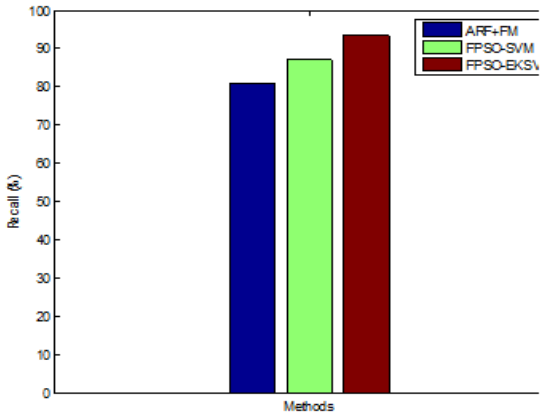

Fig. 3. Recall evaluation among the proposed and present fraud detection technique.

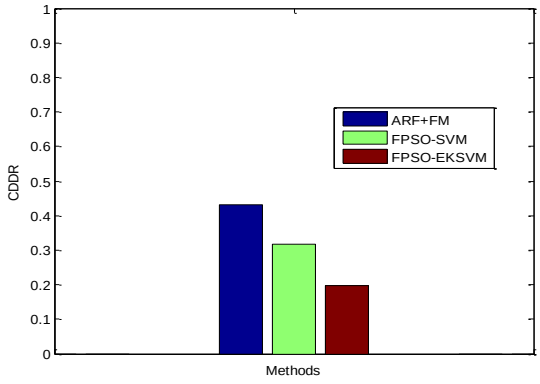

Fig.4. Concept Drift Detection Rate evaluation among the proposed and present fraud detection technique.

The Fig.3 describes the Recall comparison between the proposed and existing fraud detection technique. From the simulation results the proposed FPSO-AKSVM provides better recall compared to the existing ARF and FPSO+SVM fraud detection technique. It concludes that the proposed ensemble based classifier technique provides best credit card fraud detection. Fig.4 illustrates the CDDR comparison between the proposed FPSO-AKSVM and existing ARF and FPSO+SVM fraud detection technique. It concludes that the proposed ensemble based classifier technique provides best credit card fraud detection.

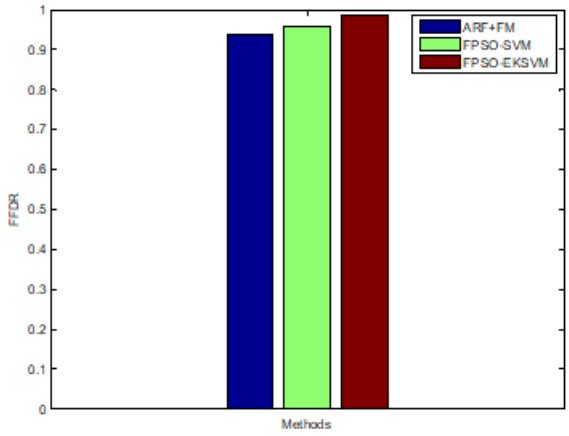

Fig 5. Fraud Features Detection Rate evaluation among the proposed and present fraud detection technique.

The Fig.5. illustrates the FFDR comparison between the proposed FPSO-AKSVM and existing ARF and FPSO+SVM fraud detection technique. It concludes that the proposed ensemble based classifier technique provides best credit card fraud detection method.

VI. CONCLUSION

In this research approach, an innovative fraud detection method has been developed and evaluated. To construct a fresh interactive profile of a cardholder, the mode of the interactive arrangements from the similar cardholders are selected. This technique gives accuracy in finding out fraudulent transactions and minimizing the number of false alerts. Aggrandized Kernel-based Support Vector Machine (AKSVM) algorithm in a credit card fraud detection system results in detecting or predicting fraud probably in a very short period after the transactions have been made. This will ultimately avoid the banks and customers from huge money losses which will decrease risks. The experimental outcome illustrate the recital and success of the anticipated method and achieves good accuracy compared with the other two methods at the detection of transactions. Also, we are going to propose a bank club alarm system like an IPS (Intrusion Prevention System) as a preventive measure against fraud and employ the proposed method in other banking areas.

REFERENCES

1. Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C., & Bontempi, G. (2017). Credit card fraud detection: a realistic modeling and a novel learning strategy. IEEE transactions on neural networks and learning systems, 29(8), 3784-3797.
2. Zojaji, Z., Atani, R. E., & Monadjemi, A. H. (2016). A survey of credit card fraud detection techniques: Data and technique oriented perspective. arXiv preprint arXiv:1611.06439.
3. Raj, S. B. E., & Portia, A. A. (2011, March). Analysis on credit card fraud detection methods. In 2011 International Conference on Computer, Communication and Electrical Technology (ICCCET) (pp. 152-156). IEEE.
4. Zareapoor, M., Seeja, K. R., & Alam, M. A. (2012). Analysis on credit card fraud detection techniques: based on certain design criteria. International journal of computer applications, 52(3).
5. Jiang, C., Song, J., Liu, G., Zheng, L., & Luan, W. (2018). Credit card fraud detection: A novel approach using aggregation strategy and feedback mechanism. IEEE Internet of Things Journal, 5(5), 3637-3647.
6. Muruti, G., Rahim, F. A., & bin Ibrahim, Z. A. (2018, November). A Survey on Anomalies Detection Techniques and Measurement Methods. In 2018 IEEE Conference on Application, Information and Network Security (AINS) (pp. 81-86). IEEE.
7. Panigrahi, S., Kundu, A., Sural, S., & Majumdar, A. K. (2009). Credit card fraud detection: A fusion approach using Dempster–Shafer theory and Bayesian learning. Information Fusion, 10(4), 354-363.
8. Ngai, E. W., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decision support systems, 50(3), 559-569.
9. Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C., & Bontempi, G. (2015, July). Credit card fraud detection and concept-drift adaptation with delayed supervised information. In 2015 international joint conference on Neural networks (IJCNN) (pp. 1-8). IEEE.
10. Halvaiee, N. S., & Akbari, M. K. (2014). A novel model for credit card fraud detection using Artificial Immune Systems. Applied soft computing, 24, 40-49.
11. Zareapoor, M., & Shamsolmoali, P. (2015). Application of credit card fraud detection: Based on bagging ensemble classifier. Procedia computer science, 48(2015), 679-685.
12. Şahin, Y. G., & Duman, E. (2011). Detecting credit card fraud by decision trees and support vector machines.
13. Whitrow, C., Hand, D. J., Juszczak, P., Weston, D., & Adams, N. M. (2009). Transaction aggregation as a strategy for credit card fraud detection. Data mining and knowledge discovery, 18(1), 30-55.
14. Dal Pozzolo, A., Caelen, O., Le Borgne, Y. A., Waterschoot, S., & Bontempi, G. (2014). Learned lessons in credit card fraud detection from a practitioner perspective. Expert systems with applications, 41(10), 4915-4928.
15. Jha, S., Guillen, M., & Westland, J. C. (2012). Employing transaction aggregation strategy to detect credit card fraud. Expert systems with applications, 39(16), 12650-12657.
16. Bahnsen, A. C., Aouada, D., Stojanovic, A., & Ottersten, B. (2016). Feature engineering strategies for credit card fraud detection. Expert Systems with Applications, 51, 134-142.
17. Van Vlasselaer, V., Bravo, C., Caelen, O., Eliassi-Rad, T., Akoglu, L., Snoeck, M., & Baesens, B. (2015). APATE: A novel approach for automated credit card transaction fraud detection using network-based extensions. Decision Support Systems, 75, 38-48.
18. Quah, J. T., & Sriganesh, M. (2008). Real-time credit card fraud detection using computational intelligence. Expert systems with applications, 35(4), 1721-1732.
19. Sahin, Y., Bulkan, S., & Duman, E. (2013). A cost-sensitive decision tree approach for fraud detection. Expert Systems with Applications, 40(15), 5916-5923.
20. Srivastava, A., Kundu, A., Sural, S., & Majumdar, A. (2008). Credit card fraud detection using hidden Markov model. IEEE Transactions on dependable and secure computing, 5(1), 37-48.
21. Jiang, C., Song, J., Liu, G., Zheng, L., & Luan, W. (2018). Credit card fraud detection: A novel approach using aggregation strategy and feedback mechanism. IEEE Internet of Things Journal, 5(5), 3637-3647.
22. Viji, D., & Banu, S. K. Z. (2018). An improved credit card fraud detection using k-means clustering algorithm. International Journal of Engineering Science Invention (IJESI).
23. Bai, Q. (2010). Analysis of particle swarm optimization algorithm. Computer and information science, 3(1), 180.
24. Lingras, P., & Jensen, R. (2007, July). Survey of rough and fuzzy hybridization. In 2007 IEEE International Fuzzy Systems Conference (pp. 1-6). IEEE.

25. Dzelihodzic, A., & Donko, D. (2016). Comparison of ensemble classification techniques and single classifiers performance for customer credit assessment. Model Artif Intell, 11(3), 140-150.
26. Kobayashi, K., & Komaki, F. (2006). Information criteria for support vector machines. IEEE transactions on neural networks, 17(3), 571-577.
27. Chung, K. M., Kao, W. C., Sun, C. L., Wang, L. L., & Lin, C. J. (2003). Radius margin bounds for support vector machines with the RBF kernel. Neural computation, 15(11), 2643-2681.

AUTHORS PROFILE

Mrs. Jisha.M.V presently is a full-time Ph.D. Scholar in Computer Science under the guidance of Dr.Vimal Kumar, Associate Professor, Department of Computer Science at Nehru Arts and Science College, T.M.Palayam, Coimbatore, Tamilnadu, India. Her research area is data mining. She has 8 years of teaching experiences from colleges under Calicut University. She has presented papers in National and International Conferences. She has published four papers in UGC approved journals, one in Scopus and 16 in peer reviewed, National and International journals. Her area of interest is in data mining, artificial intelligence, compilers and theory of computation. She is a proud recipient of Outstanding Researcher of the year 2019 award by IARDO.
Email: jisharudhra@gmail.com.

Dr. D. Vimal Kumar received MCA degree at KSR College of Technology, Periyar University from the Department of Master of Computer Applications, India, in 2002. He received his M.Phil. Computer Science degree at Kongu arts & Science College, Bharathiar University in the Year 2007. He received his doctorate in Anna University in the year 2014. He has 14 years of teaching experience. He is one of the approved supervisor of Bharathiar University currently guiding 6 scholars. He has published 25 articles in National /International journals. He has also presented papers in National and International Conferences. His area of interest includes data mining, network, software engineering, mobile computing and image processing. He is currently working as Associate Professor in department of computer science in Nehru Arts and Science College, T.M Palayam, Coimbatore, Tamilnadu, India. He is a proud recipient of Best Faculty Award in Computer Science Stream at Nehru Arts and Science College for the Academic Year 2018-19 and Best College Teacher of the Year 2019 by IARDO. Email-id: drvimalcs@gmail.com.