Journal of Information Technology Management

Print ISSN: 2008-5893

Online ISSN: 2423-5059

A Novel Fraud Detection Scheme for Credit Card Usage Employing Random Forest Algorithm Combined with Feedback Mechanism

S. KanagaSuba Raja

Department of Information Technology, Easwari Engineering College, Chennai, India. E-mail: skanagasubaraja@gmail.com

C.J. Raman

Department of Information Technology, St. Joseph's College of Engineering, Chennai, India.

S. UshaKiruthika

Department of Computer Science and Engineering, SRM Institute of Science and Technology, Kattankulathur, India.

Abstract

As electronic commerce has gained widespread popularity, payments made for users' transactions through credit cards also gained an equal amount of reputation. Whenever shopping through the web is made, the chance for the occurrence of fraudulent activities are escalating. In this paper, we have proposed a three-phase scheme to detect fraudulent activities. A profile for the card users based on their behavior is created by employing a machine learning technique in the second phase extraction of a precise communicative pattern for the card users depending upon the accumulated transactions and the user's earlier transactions. A collection of classifiers are then trained based on all behavioral pattern. The trained collection of classifiers are then used to detect the fraudulent online activities that occurred. If an emerging transaction is fraudulent, feedback is taken, which resolves the drift's difficulty in the notion. Experiments performed indicated that the proposed scheme works better than other schemes.

Keywords: Electronic commerce, Credit card, machine learning, Transactions, Classifiers, Fraudulent activities.

DOI: 10.22059/jitm.2021.80615

Introduction

The widespread fame of mobile devices has done online shopping a standard mode of day to day purchases. Since the Internet environment is wide open, the possibility for the occurrence of bugs and utilization of lamentable practices like Trojan by black hat is more, which increases the number of fraudulent activities committed. When a black hat gloms or frauds a genuine user's credit card details (Bahnsen, et al 2016 & Behera, & Panigrahi, S. 2015, May), the same can be utilized wrongly. Based on a report taken in January 2019 by Nilson, it is projected that in the year 2027, roughly 882.08 billion transactions are involved with a credit card, up by 198.4% compared with the number of transactions performed in the year 2017. In the preceding year, more fun had dispatched around 2.5 million POS terminals. Specifically, the Asia-Pacific region had completed 102.50 billion transactions in the year 2017.

To prevent the consequences of fraudulent activities, it becomes very much essential to detect deceitful actions during credit card transactions (Van Vlasselaer, et al 2015 &Wei, Q., et al 2009). Detection of the deceptive act is further classified into two categories: detection of anomalies and detection based on the classifiers. Anomalies are detected by determining the variation between the currently executing trade and the user's profile, which was defined earlier (Brzeziński, D. 2010). Any transaction that is inconsistent with the regular dealings of the user is separated as an anomaly (Shen, A., 2007 &Srivastava, A., et al 2008). The next approach employs supervised learning schemes to teach appropriate classifiers on collecting trades involving genuine and fraudulent cases (Liu, Q., et al 2018). The directed learning scheme works by removing out the swindle features from deceptive marketing. Both techniques have their reservations (Quah, J. T., & Sriganesh, M. 2008). While the first scheme cannot reveal deceitful features, albeit it shows users' trade demeanors, the second scheme flops in differentiating the various unexciting trade demeanors of diverse user groups, albeit it catches the deceitful conducts. Transaction behaviors vary from user to user as users are inclined towards their earnings, assets, ages, and personalities, and hence the dispersion of users grows over some time. This may be termed as a difficulty of variation in concept, which is difficult to resolve by the schemes mentioned above.

Alternatively, both techniques are not vigilant of the adaptive volume of the model. For instance, consider the scenario where a user may perform some incipient transaction behaviors in a categorical interval which never transpired in the past (Randhawa, K., 2018). The majority of the schemes proposed believe only the latest occurrences for training the data and do not bother about the model's adaptive nature (Valecha, H., et al 2018). To address the concerns mentioned above, the card user's transactional behaviors are extracted by considering the transactional data from the past, combined with feedback to acclimate to the user's seasonal transactional demeanors. The proposed scheme is summarized as follows.

1) Usage of all cardholders' previous transaction records to create the behavior profile and, based on it, the measurement of deviation in each transaction.

2) Training a collection of classifiers for each group based on the behavioral demeanors and mined fraudulent features after preprocessing.

3) Assignment of the trained classifier set to each card user in the collection as the behavioral pattern and the classifier having the utmost value is considered as the topical behavioral pattern

We suggest a detection scheme for finding out the fraudulent activities in credit card usage, which employs a feedback mechanism to resolve the concept drift issue. The organization of the paper is as follows: Section II of the paper analyses the cognate works. Section III of the paper presents the proposed scheme, while section IV presents the experimental outcomes. The conclusion of the article is presented in section V.

Literature Review

Studies performed previously indicated that the researchers could categorize the transactions conducted as deceitful or candid based on recognizing the transaction history's unusual transaction behavior. A unique modified prediction scheme based on a support vector machine (SVM) and an artificial neural network (ANN) (Chen, R. C., et al 2005)was suggested to detect fraudulent activity. When the various techniques to detect fraudulent activities were all ranked, it was evident that the prediction based on neural network and logistic regression were placed at a higher rank than the prediction based on decision trees. To sense the credit card holders' fraudulent activities, the self-organization map was employed, which interprets, screen, and scrutinizes the cardholders' demeanors (Flitman, A. M. 1997).

In the Markov chain prediction method, fraudulent activities were all detected by investigating each card's card usage pattern and decoding the inconsistent pattern concerning the consistent patterns. Although the scheme mentioned above had considered the time, it does not pay attention to drift quandary. Since the model reminisces the cardholder's past behavioral patterns the deportments that may not emerge recently cannot be forgotten (Wong, M. A., &Hartigan, J. A. 1979).

In another method based on the theory of Dempster-Shafer, pieces of evidence from various usage patterns were all amalgamated, and credence was determined. The suggested fraud detection method is comprised of four significant portions. The profile of the cardholder is used to portray the transaction styles (Whitrow, C., et al 2009). Based on some well-defined rules, the number of inbound transactions based on the cardholder's profile was measured. A general perception was later developed by fusing the indications by the Dempster-Shafer

adder. Finally, a Bayesian learner can either debilitate or reinforce the computed credence by utilizing the historical data.

Based on the prediction performed on the accurate data investigation, it was identified that transactions possessed sporadic edifices. K-means algorithm was utilized to extract a week's usage pattern form the data which wad preprocessed earlier. In the following stage, when a new transaction was performed, the model determines the deviation between the completed transactions with the historical data based on the cardholder's profile. The proposed scheme had amended correctness and speed of discovery and reduced the cost in some scenarios.

More recently, the prediction of fraudulent activities based on machine learning techniques had been the topic of interest and supervised learning methods are broadly employed (Dal Pozzolo, A., 2017 & Dal Pozzolo, A., 2014). For training, machine learning-based methods utilized the basic transactional information and the features like accumulation plan, the importance of the application, amount of skew between the data, etc.; in addition to the expansion of the transaction accumulation policy, the cost sensitivity predicament is also addressed to produce an emerging collection of features using the von Mises distribution (Panigrahi, S., 2009).

Unsupervised methods do not require any previous obligation to anomalies, and hence they are favorable for those transactions where there are no labels. In the credit card fraudulent activity forecasting, outlier detection had gained significant attention (Gurjar, R. N., 2014). An outlier finding strategy based on the forecasting the affinity of the association concerning the proximity of the data point to its neighbors to upgrade the efficacy and the enactment of the data collection involving groups having unique shapes like either lines or circles was proposed. In the SODRNN approach, the inversion k most proximate neighbor algorithm was employed to find the outliers for fraud recognition. The strategy used a data stream system to examine the data only once multiple times, which was an additional mundane (Jiang, C., et al 2008).

The primary concern in credit card transactions was that the class's distribution was exceedingly unhinged as the number of fraudulent activities committed was fewer than 1% of the total transactions performed. In recent times, learning in the presence of class inequity had gained significant consideration as the customary learning strategies produced classifiers that were not suited for the marginal class's operation, which had a significant role in detecting predicaments. Among the several methods proposed to cope with the categories' imbalances, two strategies, namely the sampling strategy and the cost predicted strategy, were given importance. Sampling strategies employed customary learning procedures to stabilize class distribution; on the other hand, cost-predicted strategies allocated the marginal type with a

massively colossal misclassification cost by altering the cognition procedure (Masud, M., 2010).

Sampling methods were further classified as under sampling and oversampling. By abstracting the samples from the mainstream class in the training set, under-sampling methods attained balance in the class proportion. In contrast, the oversampling methods achieved the goal by replicating the models employed for marginal class training. In the case of the cost predicted strategies maintaining an equilibrium in the amount of training data was not essential as they adopted various other measures to cope with the errors in classification occurring in the multiple classes. In detecting the credit card fraud, the worth of an unexploited fraud was presumed to be that of the transaction cost, and hence it was tolerated to have an error classified wrongly rather than the risk of being missed. Therefore these procedures might produce false positives when exact alerts were the need.

For the vast majority of the above-specified schemes, supervised learning is essential before the method can be employed. The user's transaction demeanors are not a fixed one, and it keeps on changing over some time. To overcome this, retraining the model becomes mandatory, which is a time-consuming process and results in deferment in detecting fraudulent activities.

The work proposed by Malekian, D., &Hashemi, M. R. (2013, August) makes use of a transitory profile to remember the incipient ideas; it also employed the initial profile to recollect all the past transaction behavior of the user to deal with the concept drift. The scheme utilized the appropriate profile to presage the exact result whenever a substance in the users' transaction behavior. Srivastava, A., et al 2008 &Ye, N., et al 2004 had presented a scheme based on the Hidden Markov model (HMM) to sense the fraudulent activities. The method fine-tuned the window's size, which was used to determine the KL discrepancy value between the current sequence and the up to date sequence (NilsonReport, 2019). If the determined value were preeminent, then the clear-cut brink alert would be reported by the system; otherwise, it would update the present HMM to the most latest HMM. Because of the cardholders' thought drift, all of the schemes mentioned above could not report the fraudulent activities exactly. In our work, we have employed a method for the timely alteration of the cardholder's profile to suit the current exchange practices, which accomplish remarkable results after some time (Ganji, V. R., &Mannem, S. N. P. 2012).

Proposed Method

In the process of shaping out a classifier by using all the transactions, there exist various quandaries. Consider the instance; in an authentic world, a user of the credit card owes behavioral patterns; however, a classifier qualified through all transactions overlooks the card user's adapted demeanors. Outstandingly, binary relegation cannot tag all behavioral pattern

of the card user. The absence of the relegated label information made it difficult to resolve the notion of drift quandary. Table 1 lists all the basic features of the transactions made through credit cards.

The suggested approach mines behavioral pattern from the collected data and tags each pattern by the grouping method. Thus, the approach shapes each user's transactional behavior pattern through organized behavioral patterns and promptly adapts to the user's transaction manners. The architecture of the proposed approach is depicted in Figure 1. The approach involves four steps which are listed below

1) Creation of a Pin for secured feedback scheme;

2) Creation of behavioral patterns;

3) Classification of the transaction as either fraudulent or genuine;

4) Updation of the behavioral profile of the users by employing the feedback scheme.

Table 1. Basic features of transactions made through credit card

Attribute name	Description
Transaction ID	Identification number of the transaction
Cardholder ID	Identification of the cardholder
Amount	Transaction Amount
Time	Transaction’s date and time
Category	Category of the good transaction
Location	Location coordinates of cardholder
Label	The genuine/fraudulent transaction

Creation of a Secure Pin

In our proposed method, once the cardholder applies for a credit card and the bank dispatches the credit card after the confirmation and verification processes, through the internet banking or with the help of the ATM (Automatic teller machine), the cardholder needs to create a pin of 3 digits at first which is considered as the static pin and is required during the feedback process and for completion of a transaction if it is detected as a fraudulent one. This pin is permanent and is used for all the transactions, and due to any issues, it can be changed only through the consent of the cardholder and bank's authentication and authorization. A static pin

with the dynamically generated pin from the server explained below is used for verification purposes during the fraud detection and even for the feedback mechanism.

Creation of Behavior Profile

In this stage, a clarification about the ideas of exchange record and exchange log utilized in the development of behavior profile is referenced. The m characteristics of an exchange record r is represented by r ={a1,a2,...,am|a1 ∈A1,a2 ∈ A2,...,am ∈ Am} where Ai ={ai 1,ai 2,...,aini} is the arrangement of estimations of the ith property and ni =|Ai|. Consider a card user u, the exchange log of the user is the slice of the user's exchange archives at a particular instant of time which is represented as Lu = {ru1, ru2,...,ru nu} in which nu =|Lu|. Six exchange archives of a user who bought products from the TaoBao website are shown in Table I. The transaction archive ru infers that the user bought everyday supply (DS) within the cost range of (0,200) Chinese Yaun in the evening (NI) at Shanghai Jiading (SJ) to be transported to Anhui Xuancheng (AX).

A portion of the data is preprocessed in the first records. Classification of the products and the exchange time is done. Since the exchange time is unusual, no two records can be similar. However, a few records in Lu are conceivably equivalent in light of the fact that their exchange times are put into a similar fragment of their merchandise have a place with a similar class. These equivalent records are altogether maintained in Lu in control to portray the cardholder's conduct. To speak to a few conditions advantageously, we mean ru as the arrangement of every single, distinctive record in Lu. Truth be told, ru is a set, and Lu is a multiset.

A transaction log is shown in Table 2, which includes the following fields (i) Time of Transaction, (ii) Location of Transaction, (iii) Category of goods, and(iv) Amount. The transaction is further classified as into four categories follows, Transaction_time = {Early Morning: [0, 6], Morning: (6, 12], Afternoon: (12, 18], Night: (18, 24]} and the transaction amount can be classified as Amount = {(0, 200], (200, 500], (500, 1000], (1000, ∞)}. A few features in each record are clearly subject to the related tasks (occasions) executed in the outline. These occasions/tasks can be completely requested. For instance, Transaction_location can be passed to the Category of goods on the grounds that a user can choose merchandise simply after user logins.

After the user logins, the exchange time and the location are all noted. During that instance, the goods' quantity is obtained, and the delivery address is specified in the end. Few credits are also identified with a card user's behavior propensity. For instance, when the user logins in the morning or evening, the user is at the office, and when the user logins in the night, the user is at home. In this way, we expect that Transaction_time is former to

Transaction_location. In light of such certainties and examinations, we make a behavioral profile for an individual client utilizing the exchange logs.

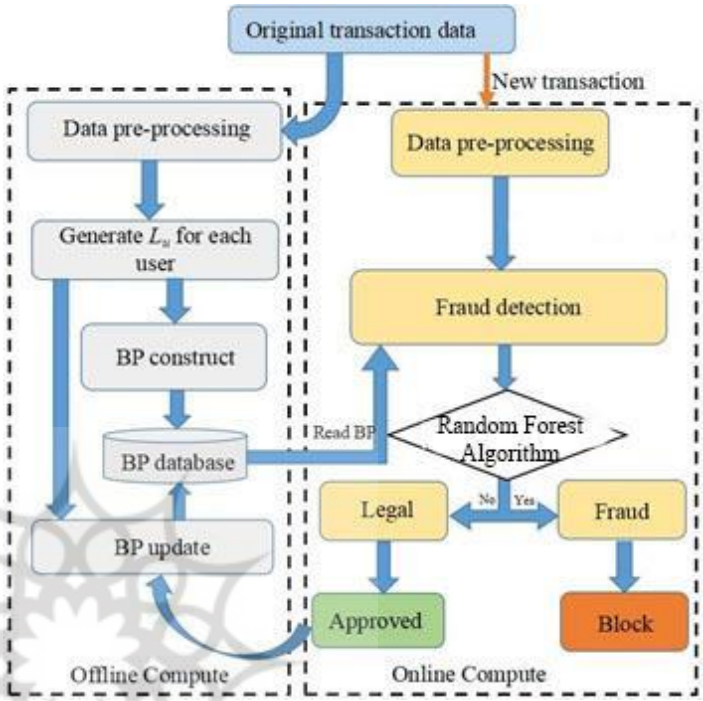

Figure 1. The architecture of the proposed approach

Table 2. Fields of the Transaction log

Transaction records	Time of Transaction	Location of Transaction	Category of goods	Amount
T1	EM	SJ	SS	(0,200)
T2	MO	AX	EP	(500,1000)
T3	AF	AX	DS	(200,500)
T4	MO	SJ	SS	(0,200)
T5	NI	AX	DS	(0,200)

EM: early morning
NI: night
AF: afternoon
SJ and AX: the abbreviations of two places' names
MO: morning
DS: daily supply
EP: electronic product
SS: school supply

Classification of the Current Transaction

By employing the random forest procedure (Breiman, L. 2001), the transactions are all categorized into genuine transactions and fraudulent transactions. Using the random forest procedure and the conduct profile, we have grouped the current and past transactions based on the classifiers. The conditions for grouping are Category of goods, location, amount of transaction, and time of the transaction

Category of Goods

The Goods purchased by the customer are categorized into various groups like Restaurant, Jewellery, and Hospitals, etc. If the customer purchases a product using a credit card in the Category mentioned above, the goods will be checked with data history. If the goods purchased are from the same Category purchased before, the transaction is legitimate; otherwise, it goes for the next classifier.

Location

This is another classifier to classify whether the transaction is legitimate or not. In this classifier, the user's location is taken into consideration by mapping the latitude and longitude of the user during the time of the transaction. A range of 3 kilometers is kept for optimized output. If the current transaction occurs outside of this range from the previous transaction records, it is classified as a fraudulent one; otherwise, it goes for the next classifier.

Amount of the transaction

This classifier is used to classify the transaction based on the user's amount of the transaction. The previous records are stored in the behavior profile, and the transaction amounts are rounded off to the nearest lower and upper bound values. During the current transaction, if the part of the transaction is present in the behavior profile, it is a legitimate transaction. Otherwise, it is considered a fraudulent transaction if the current transaction value is new and not present in the behavior profile. After this, the algorithm moves to the next classifier.

Time of the transaction

It denotes the time duration during which the user had performed the transaction. It is further categorized into four categories based on four different time assortments which are as follows Early Morning: [0, 6], Morning: [6, 12], Afternoon: [12, 18], Night: [18, 24]. If the current transaction's time is very much identical to the user's conduct profile, then it is a genuine

transaction; otherwise, it is categorized into a fraudulent transaction that requires subsequent authentication.

After the classification process, if any of the classifiers classify the transaction to be fraudulent, the system goes for the next level of authentication, which is the feedback mechanism, and it is explained below.

Updating the behavioral profile of the users by employing the feedback scheme

The feedback mechanism is used for the second level authentication and for updating the behavior profile. Whenever the algorithm detects fraud or classifies a transaction as a fraud, the system goes for the feedback mechanism, which uses a combination of the static and dynamic pin for the authentication and then it the user is authenticated, it updates the details of the current transaction in the records and updates the behavior profile. For better security and authentication purposes, we use a static and dynamic pin. During the cardholder's first transaction, the cardholder is requested to assign a static pin that needs to be remembered by the user and stays as it is till the end and is the same for further transactions. And the dynamic pin is the pin that is generated by the server during any fraud detection. During the feedback mechanism, the server generates a dynamic pin sent to the cardholder through email or notification in the application. For authentication, the cardholder needs to enter the static pin's combination, followed by the dynamic pin, referred to as OTP (One Time Password).

Once the cardholder enters the pin, the pin is verified, and if the details are correct, the transaction happens. The details of the current transaction are updated in the behavior profile. If the credentials are not legit, the transaction is stopped, and the cardholder is notified about the current transaction.

Experimental Analysis

Testing the proposed approach using genuine information is very tough since the financial institutions won't convey their data to investigators; there are no standard data sets for the experiments. For the proposed work, we used a very similar system similar to those used in the related works to generate the exchange information. In our work, we classify the transactions whose drift values are incremental as genuine transactions and those with rapid variation as fraudulent ones. We inoculate two types of transactions to some card users as a fraud. 1) fraudulent transactions from hoaxers; 2) transactions that emerged in history but conflictingly varying with the recent transaction behavior. Table 3 presents a confusion matrix in which y represents the True label of the transaction, and pred is the expected label. The effectiveness of the proposed approach is measured by utilizing the typical dual cataloging metrics like True-Positive (TP), False-Positive (FP), False-Negative (FN), and True-Negative (TN).

Table 3. Confusion Matrix

	Actual positive y = 1	Actual negative y = 0
Predict positive pred = 1	True-Positive (TP)	False-positive (FP)
Predict negative pred = 0	False-negative (TP)	True-negative (TN)

True Positive denotes the number of dishonest transactions forecasted correctly as dishonest, while False Positive denotes the nurember of genuine transactions forecasted wrongly. False-Negative denotes the number of dishonest transactions that were forecasted as honest, whereas True Negative denotes the number of honest transactions forecasted as dishonest. The accuracy and recall are calculated as follows:

$$Accuracy = TP + TN + FP + FN \quad (1)$$

$$Recall = \frac{TP}{TP + FN} \quad (2)$$

Accuracy represents the complete competence of the model, and recall represents the portion of the fraudulent transactions detected fraudulent by the proposed approach.For a better result, the accuracy and recall value should be as high as possible for detecting fraudulent transactions more efficiently. Random Forest algorithm with feedback mechanism is tested with the current existing Markov chain algorithm and the classic random forest algorithm. For ease, the methods are represented as:

I. Random Forest Algorithm with Feedback mechanism (RF + FB)

II. Markov Chain (MC)

III. Random Forest Algorithm (RF)

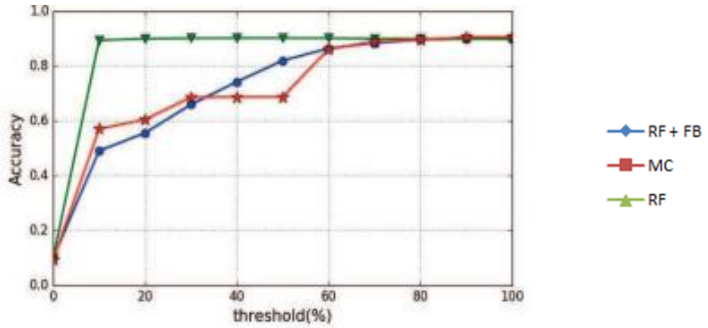

Figure 2. Comparison of accuracy

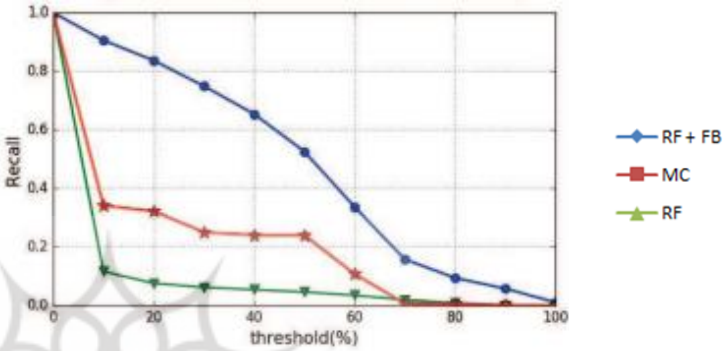

Figure 3.Comparison of recall

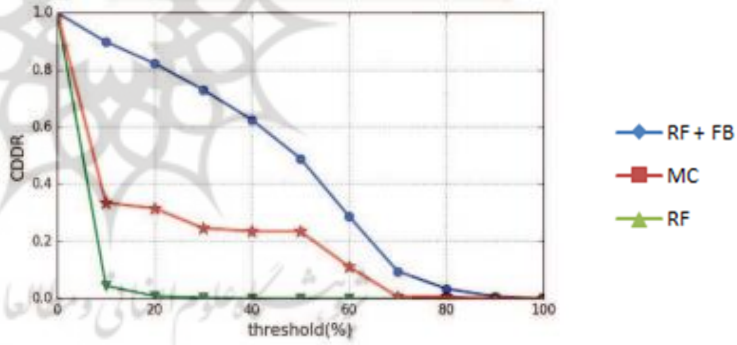

Figure 4. Comparison of CDDR

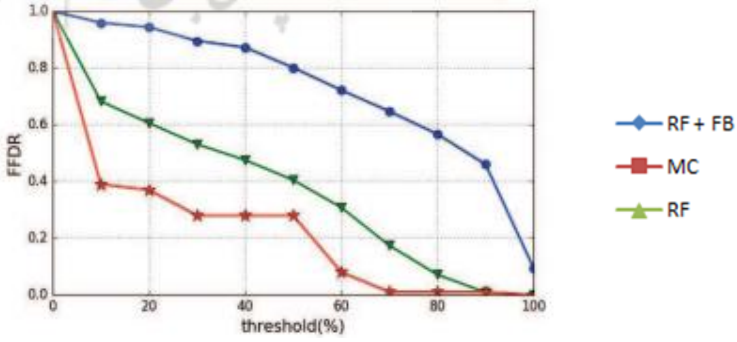

Figure 5. Comparison of FDDR

Label 1 and Label 2 are the two major variations of the fraudulent trade. While Label 1 signifies the fraudulent trade caused by deceptive features, Label 2 signifies those caused by

unexpected variation from the behavioral profile. We outline two indicators: Fraud Feature Detection Rate (FFDR) and the Concept Drift Detection Rate (CDDR). FDDR denotes the portion of the transactions. For assessing the three schemes mentioned above, identical datasets with various thresholds are used where accuracy, CDDR, recall, and FFDR act as the assessment parameters.

The dataset's assessment indicates that about 1.14% of the transactions fall under Label 1, and 8.33% falls under Label 2. The major objective is to have extraordinary CDDR and FFDR. The outcomes are publicized below. Accuracy of the RF model is found to be better than the other two schemes, whereas the recall is the worst. As far as the recall is concerned, the model trained by combined RF and FB does reasonably well. When the schemes RF and MC are compared, it is observed that the former performs better on FFDR while the later performs well on CDDR.

When considering the model trained by the combined RF and FB, it is inferred that both CDDR and FFDR have the best value. While FFDR upsurges by 97.8%, CDDR increases by 109% compared with RF and MC schemes, respectively, with the threshold set to 50%. It is understood that the development of each arc is alike because of the huge proportion of concept drift data, but in the real collection of data, there may be only a small proportion of concept drift data. From the simulation performed using four dissimilar datasets, it is observed that the drift in the transaction is observed to be 0%, 8.33%, 16.67%, and 25%, respectively. From the graph, it is also observed that the combined RF and FB scheme does perform well when compared with other schemes.

Conclusion and Future Work

We have proposed an enhanced and efficient scheme for fraud detection in this paper, which gives a solution for concept drift. The paper also proposed a more secure system and authentication mechanism for the feedback mechanism. This process can be implemented on the individual level and can create a behavior profile with more accuracy and precision at a personal level. More number of constraints can be added to the algorithm for better results and accuracy in future works.

References

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.

Behera, T. K., &Panigrahi, S. (2015, May). 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.

Breiman, L. (2001). Random forests. *Machine learning*, *45*(1), 5-32.

Brzeziński, D. (2010). Mining data streams with concept drift. *Cs Put Pozna*, *89*.

Chen, R. C., Luo, S. T., Liang, X., & Lee, V. C. (2005, October). Personalized approach based on SVM and ANN for detecting credit card fraud. In *2005 International Conference on Neural Networks and Brain* (Vol. 2, pp. 810-815). IEEE.

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.

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.

Flitman, A. M. (1997). Towards analysing student failures: neural networks compared with regression analysis and multiple discriminant analysis. *Computers & Operations Research*, *24*(4), 367-377.

Ganji, V. R., &Mannem, S. N. P. (2012). Credit card fraud detection using anti-k nearest neighbor algorithm. *International Journal on Computer Science and Engineering*, *4*(6), 1035-1039.

Gurjar, R. N., Sharma, N., &Wadhwa, M. (2014, February). Finding outliers using mutual nearness based ranks detection algorithm. In *2014 International Conference on Reliability Optimization and Information Technology (ICROIT)* (pp. 141-144). IEEE.

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.

Liu, Q., Li, P., Zhao, W., Cai, W., Yu, S., & Leung, V. C. (2018). A survey on security threats and defensive techniques of machine learning: A data driven view. *IEEE access*, *6*, 12103-12117.

Malekian, D., &Hashemi, M. R. (2013, August). An adaptive profile based fraud detection framework for handling concept drift. In *2013 10th International ISC Conference on Information Security and Cryptology (ISCISC)* (pp. 1-6). IEEE.

Masud, M., Gao, J., Khan, L., Han, J., &Thuraisingham, B. M. (2010). Classification and novel class detection in concept-drifting data streams under time constraints. *IEEE Transactions on Knowledge and Data Engineering*, *23*(6), 859-874.

NilsonReport, 2019, The Nilson Report: https:// www.nilsonreport.com/ upload/ content promo/ The Nilson Report 01-17-2019.pdf .

Panigrahi, S., Kundu, A., Sural, S., &Majumdar, A. K. (2009). Credit card fraud detection: A fusion 363.

Quah, J. T., &Sriganesh, M. (2008). Real-time credit card fraud detection using computational intelligence. *Expert systems with applications*, *35*(4), 1721-1732.

Randhawa, K., Loo, C. K., Seera, M., Lim, C. P., & Nandi, A. K. (2018). Credit card fraud detection using AdaBoost and majority voting. *IEEE access*, *6*, 14277-14284.

Shen, A., Tong, R., & Deng, Y. (2007, June). Application of classification models on credit card fraud detection. In *2007 International conference on service systems and service management* (pp. 1-4). IEEE.

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.

Valecha, H., Varma, A., Khare, I., Sachdeva, A., &Goyal, M. (2018, November). Prediction of consumer behaviour using random forest algorithm. In *2018 5th IEEE Uttar Pradesh Section*

International Conference on Electrical, Electronics and Computer Engineering (UPCON) (pp. 1-6). IEEE.

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.

Wong, M. A., &Hartigan, J. A. (1979). Algorithm as 136: A k-means clustering algorithm. *Journal of the Royal Statistical Society. Series C (Applied Statistics)*, *28*(1), 100-108.

Wei, Q., Yang, Z., Junping, Z., & Yong, W. (2009, August). Mining multi-label concept-drifting streams using ensemble classifiers. In *2009 Sixth international conference on fuzzy systems and knowledge discovery* (Vol. 5, pp. 275-279). IEEE.

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.

Ye, N., Zhang, Y., &Borror, C. M. (2004). Robustness of the Markov-chain model for cyber-attack detection. *IEEE Transactions on Reliability*, *53*(1), 116-123.

Bibliographic information of this paper for citing:

Raja, S. KanagaSuba; Raman, C.J. &Kiruthika, S. Usha (2021). A Novel Fraud Detection Scheme for Credit Card Usage Employing Random Forest Algorithm Combined with Feedback Mechanism. *Journal of Information Technology Management*, Special Issue, 21-35.