CREDIT CARD FRAUD DETECTION USING MACHINE LEARNING: A STUDY

Pooja Tiwari
Department of Computer Applications
National Institute of Technology
Kurukshetra, Haryana 136119
pooja_51710011@nitkkr.ac.in

Simran Mehta
Department of Computer Applications
National Institute of Technology
Kurukshetra, Haryana 136119
simran_51710060@nitkkr.ac.in

Nishtha Sakhuja
Department of Computer Applications
National Institute of Technology
Kurukshetra, Haryana 136119
nishtha_51710077@nitkkr.ac.in

ⓘ **Jitendra Kumar**
Department of Computer Applications
National Institute of Technology
Tiruchirappalli, Tamilnadu 620015
jitendra@nitt.edu

ⓘ **Ashutosh Kumar Singh**
Department of Computer Applications
National Institute of Technology
Kurukshetra, Haryana 136119
ashutosh@nitkkr.ac.in

ABSTRACT

As the world is rapidly moving towards digitization and money transactions are becoming cashless, the use of credit cards has rapidly increased. The fraud activities associated with it have also been increasing which leads to a huge loss to the financial institutions. Therefore, we need to analyze and detect the fraudulent transaction from the non-fraudulent ones. In this paper, we present a comprehensive review of various methods used to detect credit card frauds. These methodologies include Hidden Markov Model, Decision Trees, Logistic Regression, Support Vector Machines (SVM), Genetic algorithm, Neural Networks, Random Forests, Bayesian Belief Network. A comprehensive analysis of various techniques is presented. We conclude the paper with the pros and cons of the same as stated in the respective papers.

1 Introduction

Credit card being one of the most used financial products is designed to make purchases such as gas, groceries, TVs, traveling, shopping bills and so on because of non-availability of funds at that instance. Credit cards are of most value that provides various benefits in the form of points while using them for different types of transactions. Usually major hotels as well as various car-renting firms require the buyer to own a credit card for the same. Towards the end of 2005, huge amounts of sales were generated that is approximately around $190.6 billion just by circulating around 56.4 million credit cards in Canada. Means of achieving money or services and goods by illegal or unethical means is said to be a fraud. Banking fraud is basically "The unauthorized use of an individual's confidential information to make purchases, or to remove funds from the user's account." According to survey of statista [2], there were about 792.6 million of digital consumers in around 2011 with the number rising to 903.6 million in the following year. In 2013, around 41.3% of users that use internet started buying products online, this expecting to having reached 46.4% by 2017. With e-commerce increasing rapidly, and with the world moving towards digitization, towards cashless transactions, use of credit-card users has increased rapidly, and with that, the number of frauds associated with it is also increasing.

There are several categories of credit card frauds that are observed:

1.1 Card/Account Holder

The "base level" of fraud activity accounts for the lost and stolen card and the economic conditions size of this base-level (e.g., high levels of unemployment lead to increase in fraud because of lost and stolen cards). Counterfeit cards fraud, being a more structured problem in comparison with stolen and lost cards, is a growing problem, even after sophisticated card manufacturing technologies available like the presence of holograms and magnetic stripes on the card with some information to encrypt.

Another category of fraud of cards that is stealing cards from the mail, the non-receipt of issue (NRI) fraud affects buyers issuing both new and the ones for re-issues and this problem has increased so severely that some issuers have started using other card delivery options like courier instead of mail and also special card activation programs in which bank keeps the card blocked (the ones which are included in list as an account whose transaction requests will be denied) until the customer verifies card receipt. The customer calls and bank use it to account for the fact that he caller is genuine cardholder by asking few questions about the background of the customer using the card application or its cardholder information file and these have led to a decrease in NRI losses.

Other frauds include sending of illegitimate applications for a card because of which criminals send applications using one's personal background and financial information to specify a mail for receiving the card. In such cases, even the activation of the card member cannot stop the card being misused and fall into wrong hands. Another type of fraud is mail-ordered telephone order fraud in which card imprint cannot be obtained as the buyer is not present there during the transaction.

1.2 Merchant Fraud

Another type of fraud is the merchant fraud involving the "laundering" of merchant receipts gaining huge amounts by showing illegal transactions that never occurred [21]. Many a times, during admissible transactions, legal information is stolen which is then used to illegally produce copies of cards to perform illegal transactions. Here the dealer is a "point of compromise" as all these cards have transaction histories that establishing the dealer (merchant) legally.

1.3 Abuse

Card holder making purchases on card that he/she has no intention of paying gives another type of fraud called abuse. Here card-bearer may pre-mediate+ activity just before they file for personal bankruptcy. These losses that are caused due to this "bankruptcy fraud" are a part of charge-off losses. Causing adverse effects on business and society, and accounting for about billions of dollars of lost revenue each year [5], credit card frauds have become a major issue worldwide. While some statistics show about $400 billion cost of a year, some other figures show about 1.6 billion pounds total yearly loss of UK insurers due to such fraudulent attempts. By 2005 with market splitting in two groups based on transaction types namely the credit group, that leads the market, including countries like Spain, Belgium, Italy, and Greece. With two countries, namely the United Kingdom and Ireland lacking competitors in terms of transaction product. Whereas, other group is of debit card users example Sweden. However, Germany being underserved by credit cards earlier, the market there was estimated to potentially increase by 23.3% from 2004 to 2009, reaching an approximate of €56,477 million (Euromonitor International, 2006) [37].
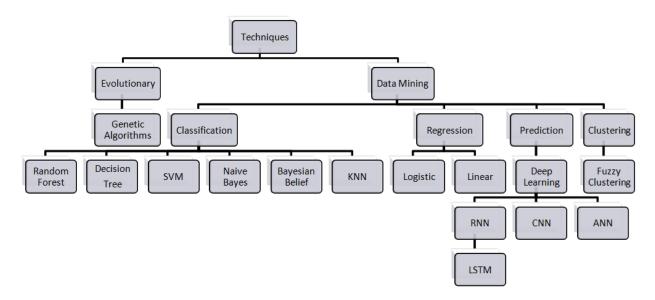
Figure 1: Taxonomy of fraud detection techniques

The observed patterns in behavior of the customers regarding payments are related with the assumptions that customers use cards instead of cash (Euromonitor International, 2006). Now the loss is actually affecting everyone even if one hasn't been defrauded, paying of credit and charge debts increases the cost of goods and services.

Hence the need of the hour is a fraud Detection system that can distinguish an incoming transaction request as a fraudulent or non-fraudulent and hence alarm the banks [31]. Various machine learning techniques can be used for prediction [41].

The rest of the paper is organized as: Section II consists of brief review of methodologies that have been proposed for a fraud detection system. The following Fig.1. depicts the methodologies that we have reviewed in this paper. Section III summarizes the techniques with their corresponding results and Section IV gives the conclusion.

2   FRAUD DETECTION APPROACHES

Machine learning finds its usage across the applications such as prediction, optimization, detection, classification etc. [38–55].

2.1   Hidden Markov Model(HMM)

A Hidden Markov Model is a stochastic model that has a set of states that are finite with a set of transition possibilities and rate parameters for those transitions [22]. The basis of the HMM Model is the Markov property that states that future events do not depend on the earlier states and only on the current ones. This property makes it useful in predictive modelling and probability forecasting. Detection of fraud using this model as specified in [1]. In this, they model the human behavior based on card holders spending habits and a state in the model is the type of the purchase. Only three price ranges that is l-low, m-medium, h-high are considered that make 3 observation symbols. For instance, letting l= (0, $200], m= [$200, $400], and h= [$400, credit card limit]. Metrics used by this model are True Positive, TP- False Positive, FP and Accuracy. Accuracy that is proposed remains close to 80 percent for all inputs large or small.

But when there is no information available about the profile, there is some degradation in performance in TP-FP metrics. And when there is slight difference between genuine and malicious transactions, then also the FDS suffers degradation in its performance by a decrease in number of TPs or a rise in FPs.

2.2   Decision Tree

A supervised learning algorithm [14], A decision tree which is in the form of tree structure, consisting of root node and other nodes split in a binary or multi-split manner further into child nodes with each tree using its own algorithm to perform the splitting process, until no more splitting is required that will make a difference in our model, associating

each attribute with a value that is input variables related to the method that is being used as described by Y. Sahin and E. Duman [3]. With the tree growing, there may be possibilities of overfitting of the training data with possible anomalies in branches, some errors or noise. Hence pruning is used for improving classification performance of the tree by removing certain nodes. Ease in the use, and the flexibility that the decision trees provide to handle different data types of attributes make them quite popular [27].

2.3 Random Forests

The instability in single trees and sensitivity to some training data led to development of another model that is random forests. With each tree being built independent of each other computational efficiency of random forest is comparatively better [36]. It is basically an ensemble of regression and/or classification trees with it obtaining variance amongst its trees and hence are easy to use because of use of only two randomness sources or parameters that is building trees using trained data separate bootstrapped along samples with considering only a random data attribute subset to build each tree as specified [5].

2.4 Bayesian Belief Networks

This technique uses Bayes Theorem to compute the probability of a hypothesis and identify it to be true or false. A classifier is used to calculate the conditional probabilities for all the possible classes and insert it into the class that has the highest value of conditional probability for a particular value of X [26]. Graphically, it is depicted in the form of a directed graph that is acyclic in nature, where the samples are represented by the nodes of the graph and the dependencies between them are reflected through the directed edges. Two variables are said to be independent if there are no connecting edges between them. It also gives a specification and factorization of the joint probability distribution [8].

2.5 Genetic Algorithm

This algorithm puts forth the idea of natural evolution, where the survival chances of the stronger or fitter individuals of the population is more than the weaker individuals of the population [35]. The stronger members are chosen to reproduce and thus the mean fitness of the entire population improves. The fitter members of a certain generation are chosen as the parents for the next generation and the lesser fit members are discarded. It depends on many parameters like number of parents & children, reproduction, fitness & selection functions and some termination criteria [11].

2.6 Logistic Regression

It is an appropriate technique that can be used in predictive analysis when the dependent variable is dyadic or binary [25]. Since the categorization of transactions being fraud is a double-edged variable, this technique can be used. This statistical classification model based on probabilities detects the fraud using logistic curve. Since the value of this logistic curve varies from 0 to 1, it can be used to interpret class membership probabilities.

The dataset fed as input to the model is being classified for training and testing the model. Post model training, it is tested for some minimum threshold cut-off value for prediction. Then the most significant variables are selected and the model is tuned accordingly. The accuracy of prediction came out to be 70%. Since the logistic regression, based on some threshold probabilities can divide the plane using a single line and divides dataset points into exactly two regions. Hence, the outlier points are not handled effectively [14]. It uses natural logarithmic function to calculate probability and to show that the results fall under a particular category [5].

2.7 Support Vector Machines

Support vector machines or SVMs are linear classifiers as stated in [5] that work in high dimensionality because in high-dimensions, a non-linear task in input becomes linear and hence this makes SVMs highly useful for detecting frauds. Due to its two most important features that is a kernel function to represent classification function in the dot product of input data point projection, and the fact that it tries finding a hyperplane to maximize separation between classes while minimizing overfitting of training data, it provides a very high generalization capability [28].

2.8 K-Nearest Neighbours

This is a supervised learning technique that achieves consistently high performance in comparison to other fraud detection techniques of supervised statistical pattern recognition [24]. Three factors majorly affect its performance:

distance to identify the least distant neighbors, some rule to deduce a categorization from k-nearest neighbor & the count of neighbors to label the new sample. This algorithm classifies any transactions that occurred by computing the least distant point to this particular transaction and if this least distant neighbor is classified as fraudulent then the new transaction is also labeled as a fraudulent one. Euclidean distance is a good choice to calculate the distances in this scenario. This technique is fast and results in fault alerts. Its performance can be improved by distance metric optimization [19].

2.9 Fuzzy Clustering

Based on the past activities of the users or customers this technique helps determine normal usage patterns of the users [34]. Whenever there is a deviation in the normal patterns, a suspicion score is calculated, accordingly the transactions are categorized as legitimate or fraudulent or suspicious. Further the suspicious transactions need to be recognized as fraudulent or occasional deflection from the usual patterns by the genuine customers itself. This is achieved by applying learning techniques through the neural networks, which effectively helps reduce false alarms [18].

2.10 Neural Networks

A neural network is a network of neurons, comprising of perceptron which is a linear binary classifier which helps to classify the inputs data. Each perceptron consists of four parts: Input layer, Weights and Bias, Weighted Sum and Activation Function [32]. Our analysis covers three different neural networks:

2.10.1 Artificial Neural Network (ANN)

An ANN is composed of of three types of layers: input, hidden and output. The data to be trained travels from the input to intermediate hidden and then to the output layer, termed as Forward Propagation. The network is initially trained with normal behavior of the cardholder. The transactions that seems to be fraud are then Backpropagated through the network and are then classified as the fraudulent and non-fraudulent transactions. This technique was found to be quite efficient as a Neural Network doesn't need to be reprogrammed so its processing speed is high [23].

2.10.2 Convolution Neural Network (CNN)

CNN contains neurons with learnable values weights and biases with each neuron receiving various input vectors, and then calculate sum that is weighted over them, pass the value through an activation function and deliver an output [29, 30]. Krishna and Reshma [13] proposed a model in which they trained their model using CNN. Initially, feature selection algorithm was applied on the original data. Then, to overcome the imbalance in the data or the skewed distribution, SMOTE (Synthetic minoring oversampling technique) helps generating synthetic transactions that are fraud for balancing the dataset. The next step involved feature transformation and then the features were converted into a matrix which was given as input. They used soft-max activation function.

2.10.3 Recurrent Neural Network (RNN)

RNNs are networks with loops in them having the ability to hold information. It can be thought of as a multilayer perceptron, where each of them passes an information to its successor [33]. RNN has internal states which are updated after each unit time. Though, RNN being a powerful and simple model, still training them properly with gradient descent is hard. There are problems like Vanishing and Exploding Gradient Descent associated with it [15]. These problems tell as the length of the input sequence grows, the gradient may either increase or decrease exponentially. These problems can be overcome using techniques like by removing the dependency of the sequence state vectors on the weight matrix and introducing memory cells which was termed as LSTM (Long Short-Term Memory) Network as proposed by Bayer [17, 43].

3 Summary

Table 1 summarizes some of the significant solutions proposed for the fraud detection using machine learning. The study shows that the Fraud Bayesian Network Classifier followed by probability threshold is more beneficial than Naïve Bayes, Tree Augmented Naïve Bayes, Support Vector Machines and Decision Trees on the PagSeguro dataset when precision, recall and economic efficiency are taken into account [16]. Bayesian Learning when taken with Dempster-Shafer Theory resulted in 98% True Positives and less than 10% False Positives [7]. Genetic Algorithms along with Scatter Search improves the performance by 200% when applied on the existing systems of a major bank of Turkey [11]. Although ANN detects frauds faster, but Bayesian Belief is better as it is able to detect 8% more frauds

as recorded on data provided by Serge Waterschoot at Europay International [8]. When dataset is highly imbalanced and independent of the rate of frauds Bagging Ensemble Classifier is one of the most stable approaches and has a high fraud catching rate [9]. As observed on the German dataset using Big Data Analytical Framework with Hadoop it was observed that Random Forest Decision Tree outperforms Logistic Regression, Decision Trees and Decision Tree Random Forest in terms of precision and accuracy [14]. Whereas Deep Networks training approach handled data granularity with high accuracy on the same dataset [12]. Long Short-Term Memory improves upon transactions that are face to face, but is more likely to overfit i.e. layers have fewer nodes [15]. The results on the Nation banks credit card warehouse showed that Decision Tree worked better than Support Vector Machines in terms of accuracy [3]. The behaviour certificate model that was tested on the data generated using simulator performed well overall in comparison to Support Vector Machines [10]. A lot of financial resources were saved when Cost-Sensitive Decision Tree approach was used. It also outperformes traditional classifiers in terms of total number of frauds detected [6]. Convolutional Neural Networks along with SMOTE performs better than Neural Networks [13]. The True Positives accounted for 93.9% and False Positives around 6.10% when Fuzzy Clustering and Neural Networks where implemented on data developed by Panigrahi [18]. A real world credit card data by US bank put forth the better performance of Distributed deep learning than the non-privacy baseline approaches [4]. Other important factors are further discussed in Table 1.

Table 1: A detailed comparison fraud detection approaches

Work	Technique used	Dataset used	Pre- Processing	Performance Metrics	Result
[16]	Bayesian Network Classifier (HHEA), instance reweighing and probability threshold analysis.	PagSeguro (Brazilian Online Payment Service)	✓	HM between Precision and Recall, and Economic Efficiency.	Fraud BNC following Probability threshold - more beneficial than NB, TAN, SVM, Decision Trees, Logistic Regression
[11]	Genetic Algorithm and Scatter Search.	Major Bank of Turkey (industrial partner).	✓	Misclassification cost based on TP, TN, FP, FN, TFL, S, r., No. of frauds, Ratio of legitimate transactions, Class Imbalance	Improved existing performance by 200%.
[1]	Hidden Markov Model	NA	✓	TP, FP	80% accurate
[8]	Bayesian Belief, ANN	Provided by Serge Waterschoot at Europay International	✓	TP, FP	Bayesian Belief, better than ANN. 8% more frauds detected. But ANN detects faster.
[9]	Bagging Ensemble Classifier	Real world credit card dataset obtained from USCO-FICO competition.	✓	Fraud Catching Rate, False Alarm Rate, Balanced Classification Rate, Mathews Correlation coefficient.	Stable, Fraud catching rate is high, Independent of rate of frauds, suitable for highly imbalanced dataset.
[14]	Big Data Analytical Framework with Hadoop	German Dataset	✓	FP, TP.	Random Forest Decision Tree performs best in terms of accuracy and precision among LR, DT & DTRF.

[15]	LSTM, State of art methods.	Dataset Recorded from March to May 2015.	✓	Robustness against imbalance classes, Attention to business specific interests.	LSTM's more accurate as compared to RF, improves upon face to face transactions, but LSTM is prone to overfit (layers have fewer nodes).
[12]	Deep Networks by training a deep network	German Credit Data		Accuracy, Variance	High Accuracy handing data granularity
[5]	Logistic Regression, SVM, Random Forests	From international credit card operation of study in ANN tuned by Genetic Algorithm (GAs) to detect fraud		Accuracy, sensitivity, Specificity, precision, F-measure, G-mean, wtdAcc.	Random Forest-better performance overall. Logistic Regression- better performance through different datasets.
[3]	Decision Trees, SVM	Nation banks credit card warehouse	✓	Accuracy	Decision tree outperforms SVM
[4]	Distributed deep learning	real-world credit card data by a US bank	✓	AUC comparison.	Better performance than non-privacy baseline.
[10]	Behavior certificate model	Generated using simulator	✓	Accuracy, Recall, Specificity, precision, F-measure, G-mean	Overall better performance than SVM
[7]	Dempster-Shafer theory and Bayesian learning	Transaction history repository (THD) built using simulator		FP-TP	Upto 98% TP and less than 10% FP
[6]	Cost-sensitive Decision Tree	Banks credit card data warehouses	✓	Saved Loss Rate (SLR)	Saved much more financial resources, outperforms traditional classifier in number of frauds detected.
[13]	Convolutional Neural Network	Credit card fraud data	✓	TP-FP, FN-TN, Precision and Recall with their HM.	With SMOTE, outperforms NN.
[18]	Fuzzy clustering and neural networks	Developed by Panigrahi [7]		FP, TP/Sensitivity, TN/Specificity	Upto 93.9% TP and less than 6.10% FP
[20]	K-Nearest Neighbor	Real data from private bank	✓	Recall, F-measure, Specificity, Accuracy, Precision,	Performance is evaluated on the basis of the metrices.

4   Conclusions

We have come across various fraud detection techniques that exists today but none of them were competent enough to detect the fraud at the time it actually took place. They detected the frauds which happened in the past. The setback of all the techniques discussed so far give accurate results only when performed on a particular dataset and sometimes with some special features only. But we need to establish a technology that works equally precisely and accurately under all circumstances and with various datasets. Techniques like SVM works better than Logistic Regression when there is a class imbalance and comparatively Random Forest performs better among all three [5, 14].

Bagging Ensemble Classifier is suitable for highly imbalanced dataset [9]. Some techniques like Decision Tress and SVM gives better results on raw unsampled data whereas techniques like ANN and Bayesian Belief Network have high

accuracy and detection rate but are expensive to train [8]. Similarly, KNN and SVM gives better results with small datasets but are not preferable with large datasets.

Among all the techniques discussed, it is found that Neural Networks detects frauds with high precision and performs best. But as they are expensive to train and can also be over trained in case of fewer nodes as in case of LSTM [15]. So, in order to minimize this cost, we can pair neural network with some augmentation techniques like Genetic Algorithms or Artificial Immune Systems by selecting optimized weight edges and eliminating those weights that causes error.

References

[1] A. Srivastava, A. Kundu, S. Sural and A. Majumdar, "Credit card fraud detection using hidden markov model," In: IEEE transactions on dependable and secure computing, vol. 5, no. 1, Jan.-March 2008, pp. 37-48.

[2] Statista the statistic portal, https://www.statista.com/topics/871/online-shopping/, March 14, 2017.

[3] S. Yusuf, E. Duman, "Detecting credit card fraud by decision trees and support vector machines," IMECS 2011- International multiconference of Engineers and Computer Scientists 2011, 1, 442-447, 2011.

[4] Y. Wang, S. Adams, P. Beling, S. Greenspan, S. Rajagopalan, M. Velez-Rojas, S. Mankovski, S. Boker, D. Brown, "Privacy preserving distributed deep learning and its application in credit card Fraud detection," 1070-1078, 2018.

[5] S. Bhattacharyya, S. Jha, K. Tharakunnel, J. Westland, "Data mining for credit card fraud: A comparative study," Decision Support Systems, 50, 602-613, 2011.

[6] Y. Sahin, S. Bulkan, E. Duman, "A cost-sensitive decision tree approach for fraud detection" Expert Syst. Appl., 40, 5916-5923, 2013.

[7] S. Panigrahi, A. Kundu, S. Sural, A. Majumdar, "Credit card fraud detection: a fusion approach using demp-ster–shafer theory and bayesian learning," Information Fusion, 10, 354-363, 2009.

[8] S. Maes, K. Tuyls, B. Vanschoenwinkel, B. Manderick, "Credit card fraud detection using bayesian and neural networks, 2002.

[9] M. Zareapoor, P. Shamsolmoali, "Application of credit card fraud detection: based on bagging ensemble classifier," Procedia Computer Science, 48, 679-686, 2015.

[10] L. Zheng, et al, "A new credit card fraud detecting method based on behavior certificate," IEEE 15th international conference on Networking, Sensing and Control (ICNSC), Zhuhai, pp. 1-6, 2018.

[11] E. Duman, M. Özçelik, "Detecting credit card fraud by genetic algorithm and scatter search," Expert Syst. Appl., 38, 13057-13063, 2011.

[12] A. Roy, J. Sun, R. Mahoney, L. Alonzi, S. Adams, P. Beling, "Deep learning detecting fraud in credit card transactions," Systems and Information Engineering Design Symposium (SIEDS), Charlottesville, VA, 2018, pp. 129-134, 2018

[13] F. Kang, C. Dawei, T. Yi, Z. Liqing, "Credit card fraud detection using convolutional neural networks," 483-490, 2016.

[14] P. Suraj, N. Varsha and S. P. Kumar, "Predictive modelling for credit card fraud detection using data analytics," Procedia Computer Science, 132, 385-395, 2018.

[15] J. Jurgovsky, M. Granitzer, K. Ziegler, S. Calabretto, P.E. Portier, L. He, O. Caelen, "Sequence classification for credit-card fraud detection," 10.1016/j.procs.2015.04.201, 2018.

[16] A. De Sá, A. Pereira, G. Pappa, "A customized classification algorithm for credit card fraud detection," 2018.

[17] J. S. Bayer, München, Technische Universität München, Diss., "Learning Sequence Representations," 2015.

[18] T. K. Behera, S. Panigrahi, "Credit card fraud detection: a hybrid approach using fuzzy clustering, neural network," Second International Conference on Advances in Computing and Communication Engineering, Dehradun, pp. 494-499, 2015.

[19] T. R. C. Sudha, "Credit Card Fraud Detection in Internet using K Nearest Neighbour Algorithm," IPASJ international journal of computer science, vol. 5, no. 11, 2017.

[20] M. Sanaz, S. Mehdi, "Cost-sensitive payment card fraud detection based on dynamic random forest and k-nearest neighbors.," 2018.

[21] R. Patidar and L. Sharma, "Credit card fraud detection using neural network," International Journal of Soft Computing and Engineering (IJSCE), 1(32-38),2011.

[22] S. Fine, Y. Singer and N. Tishby, "The hierarchical hidden Markov model: Analysis and applications." Machine learning, 32(1), 41-62, 1998.

[23] J. Kumar and A. K. Singh, "Workload prediction in cloud using artificial neural network and adaptive differential evolution," Future Generation Computer Systems, 81, 41-52, 2018.

[24] M. L. Zhang and Z. H. Zhou, " A lazy learning approach to multi-label learning. Pattern recognition, " 40(7), 2038-2048, 2007.

[25] J. Pearce and S. Ferrier, "Evaluating the predictive performance of habitat models developed using logistic regression," Ecological modelling, 133(3), 225-245, 2000.

[26] J. Cheng and R. Greiner, "Learning bayesian belief network classifiers: Algorithms and system," In Conference of the Canadian Society for Computational Studies of Intelligence, pp. 141-151, Springer, Berlin, Heidelberg, June-2011.

[27] P. H. Swain and H. Hauska, "The decision tree classifier: Design and potential," IEEE Transactions on Geoscience Electronics, 15(3), 142-147, 1977.

[28] C. J. Burges, "A tutorial on support vector machines for pattern recognition," Data mining and knowledge discovery, 2(2), 121-167, 1998.

[29] R. S. Reshma, "Deep Learning Enabled Fraud Detection in Credit Card Transactions," International Journal of Research and Scientific Innovation (IJRSI), July 2018.

[30] Y. Pandey, "Credit card fraud detection using deep learning," International Journal of Advanced Research in Computer Science, May – June 2017.

[31] A. Dal Pozzolo, G. Boracchi, O. Caelen, C. Alippi and G. Bontempi, "Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy," in IEEE Transactions on Neural Networks and Learning Systems, vol. 29, no. 8, pp. 3784-3797, Aug. 2018.

[32] Z. Kazemi and H. Zarrabi, "Using deep networks for fraud detection in the credit card transactions," IEEE 4th International Conference on Knowledge-Based Engineering and Innovation (KBEI), Tehran, 2017, pp. 0630-0633.

[33] Z. C. Lipton, J. Berkowitz, and C. Elkan, "A critical review of recurrent neural networks for sequence learning," arXiv preprint arXiv:1506.00019, 2015.

[34] X. L. Xie and G. Beni, "A validity measure for fuzzy clustering," IEEE Transactions on Pattern Analysis & Machine Intelligence, (8), 841-847, 1991.

[35] K. S. Shin, and Y. J. Lee, "A genetic algorithm application in bankruptcy prediction modeling," Expert Systems with Applications, 23(3), 321-328, 2002.

[36] T. K. Ho, "Random decision forests," In Proceedings of 3rd international conference on document analysis and recognition, Vol. 1, pp. 278-282, IEEE, August-1995.

[37] L. Delamaire, H. A. H. Abdou, and J Pointon, "Credit card fraud and detection techniques: a review," Banks and Bank systems, 4(2), 57-68, 2009.

[38] J. Kumar, A. K. Singh, A. Mohan, "Resource-efficient load-balancing framework for cloud data center networks," ETRI Journal, 43 (1), pp. 53-63, 2021.

[39] D. Saxena, I. Gupta, J. Kumar, A. K. Singh, X. Wen, "A Secure and Multiobjective Virtual Machine Placement Framework for Cloud Data Center," IEEE Systems Journal, 2021. (Article in Press) DOI: 10.1109/JSYST.2021.3092521

[40] A. K. Singh, J. Kumar, "Secure and energy aware load balancing framework for cloud data centre networks," Electronics Letters, 55 (9), pp. 540-541, 2019.

[41] J. Kumar and A. K. Singh, "Cloud Resource Demand Prediction using Differential Evolution based Learning," 2019 7th International Conference on Smart Computing & Communications (ICSCC), 2019, pp. 1-5.

[42] J. Kumar, A. K. Singh, "Dynamic resource scaling in cloud using neural network and black hole algorithm," Proceedings on 5th International Conference on Eco-Friendly Computing and Communication Systems, ICECCS 2016, pp. 63-67.

[43] J. Kumar, R. Goomer, A. K. Singh, "Long Short Term Memory Recurrent Neural Network (LSTM-RNN) Based Workload Forecasting Model for Cloud Datacenters," Procedia Computer Science, 125, pp. 676-682, 2018.

[44] A. K. Singh, D. Saxena, J. Kumar, V. Gupta, "A Quantum Approach towards the Adaptive Prediction of Cloud Workloads," IEEE Transactions on Parallel and Distributed Systems, 32 (12), pp. 2893-2905, 2021.

[45] J. Kumar, A. K. Singh, "Performance Assessment of Time Series Forecasting Models for Cloud Datacenter Networks' Workload Prediction," Wireless Personal Communications, 116 (3), pp. 1949-1969, 2021.

[46] J. Kumar, A. K. Singh, R. Buyya, "Self directed learning based workload forecasting model for cloud resource management," Information Sciences, 543, pp. 345-366, 2021.

[47] J. Kumar, A. K. Singh, "Decomposition Based Cloud Resource Demand Prediction Using Extreme Learning Machines," Journal of Network and Systems Management, 28 (4), pp. 1775-1793, 2020.

[48] J. Kumar, D. Saxena, A. K. Singh, A. Mohan, "BiPhase adaptive learning-based neural network model for cloud datacenter workload forecasting," Soft Computing, 24 (19), pp. 14593-14610, 2020.

[49] J. Kumar, A. K. Singh, "Adaptive learning based prediction framework for cloud datacenter networks' workload anticipation," Journal of Information Science and Engineering, 36 (5), pp. 981-992, 2020.

[50] J. Kumar, A. K. Singh, R. Buyya, "Ensemble learning based predictive framework for virtual machine resource request prediction," Neurocomputing, 397, pp. 20-30, 2020.

[51] J. Kumar, A. K. Singh, "Cloud datacenter workload estimation using error preventive time series forecasting models," Cluster Computing, 23 (2), pp. 1363-1379, 2020.

[52] J. Kumar, A. K. Singh, "Workload prediction in cloud using artificial neural network and adaptive differential evolution," Future Generation Computer Systems, 81, pp. 41-52, 2018.

[53] J. Kumar, "Machine Learning Models for Cloud Resource Management," PhD dissertation, National Institute of Technology Kurukshetra, 2019.

[54] S. Singh, T.K. Madan, J. Kumar, A. K. Singh, "Stock Market Forecasting using Machine Learning: Today and Tomorrow," 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies, ICICICT 2019, pp. 738-745.

[55] V. Sharma, S. Kaur, J. Kumar, A. K. Singh, "A fast parkinson's disease prediction technique using PCA and artificial neural network," 2019 International Conference on Intelligent Computing and Control Systems, ICCS 2019, pp. 1491-1496.