Journal of Advances and Scholarly Researches in Allied Education
Vol. 16, Issue No. 1, January-2019, ISSN 2230-7540

Comparative Analysis of Various Optimization Techniques to Imbalance Credit Card Fraud Detection

Sonam Mittal[1]* Prof. (Dr.) N. K. Joshi[2] Prof. (Dr.) Mahaveer Kumar Sain[3]

[1] Department of Computer Science, MIMT, Kota, India

[2] Department of Computer Science, MIMT, Kota, India

[3] Department of Computer Science, MAISM, Jaipur

Abstract – It is the data-driven era nowadays. Many organizations, including corporations, businesses, industrial, and medical organizations around the world, plan to derive information from a large volume of data. But most of them exist in real-word databases with class imbalance issues. The concept of class imbalance is a machine learning problem, where a total number of (positive) class labels is much smaller than the number of other data classes (negative). Financial fraud involves both the financial industry and daily life significantly. Illegitimate activity in online financial transactions has been increasing dynamic and enormity today, result in huge financial risks for both clients and associations. To tackle this problem, financial firms use a range of fraud detection models. As a consequence, financial institutions have to develop their fraud detection systems consistently. Many techniques of fraud prevention and detection in the online world have been proposed. This paper aims to analyze financial fraud detection strategies, such as extreme learning machines and optimization techniques, which play an important role in detecting fraud, as they also use the extract and expose hidden truth from the very large volumes dataset.

Keywords – Imbalance Data, Credit Card Fraud, Fraud Detection, Machine Learning, Extreme Learning, Optimization Techniques

----------X----------

1. INTRODUCTION

In recently, data mining (DM) is used by many organizations like industry, medical, banking, marketing, and to derive Useful and interesting data volume information or patterns. However, the model's analytical outcome relies on the training data set. The improved number of training data allows for a more accurate classification of the model. A few years ago, many approaches to solving the imbalanced class problem have been proposed by several researchers. The overview includes three key ways of approaching the Problems of imbalanced classification: data sampling, function selection, or ensemble [1].The role of correct Target class prediction for every case throughout the data is considered as data classification. Balanced data set classification is fairly straightforward and easy to carry out, but where the information is not balanced, it becomes complicated. The problem of class Imbalance is the problem of machine learning(ML), Where the total amount of a (positive) data class is much less than the total number of other data classes (negative)[2]. The dependence on e-commerce & online pay has grown-up increasingly over the last few decades. As the field of information technology develops every day, illegal attempts at transactions have increased worldwide and, as a result, most companies experience major financial losses [3].

The growing world generally carries out financial transactions by transfer of amount over the Internet via cashless payments. The vast volume of data that resulted in the growth of big data has run to the rise of transactions. As days pass High-speed transactions as big data over the limits of transactions and diversity are explored, are gradually increasing. Fraudsters can also do something to exploit the current fraud detection system (FDS) [4]. To meet the FDS requirements, there is also a challenge to improve the current FDS with the greatest possible accuracy. When the transaction is done with credit cards, then credit cards can be misused by fraudsters. Now, to reduce the fraudulent rate to a minimum of one, it's a very urgent need to identifies fraudulent transactions as a

real-world issue for FDS and reported them to the required people/organization [5].

Fraud Detection [6] includes the detection of fraud as soon as possible after it is committed. Detection of fraud playsa major role when the prevention of fraud has failed. Also, fraud identification must be used on an ongoing basis in practice, as one would normally be unaware that fraud prevention has failed. By diligently protecting our cards to discourage credit card theft, but if the card data are still stolen, it can be identified as soon as possible that fraud is being committed.

Supervised and Unsupervised Learning are the two categories of machine learning and Artificial Intelligence. Such approaches[7]for users, buyers, and vendors, etc. who act unusually to generate, depending on the process, suspicious ratings, rules, or visual irregularities. If supervised or unsupervised are used, that strategies the outcome only provides us with an idea of the risk of fraud. A constant effort has been made to create a machine learning algorithm that can take a large amount of input and research the pattern of transactions to identify suspicious transactions based on the data. But since we all know that online transactions are carried out in various fields on a huge level, a single ML algorithm cannot be used in any other field [8]. Since the patterns of transactions are different in different fields, the algorithm had to be built only for the online retailer who supplied us with the dataset. Fraud transactions may occur on the internet, certain essential fraud card details like fraud card number, validity, cardholder name, CVV will be requested by the customer. Fraud detection can be observed by reviewing data from past transactions that help to make the card holder's spending profile. Each cardholder with a specific pattern includes information about the quantities of transactions, purchased things details, retailer information, transaction date, etc. It would be the most powerful way of countering internet fraud transactions.

2. FRAUDULENT TRANSACTION DETECTION

Fraud in the field of e-commerce is known as payment fraud which is generally any type of illegal or false transaction made in a web-shop. This type of fraud is an upcoming issue and is very common nowadays. This is given to the electronic frauds (e-frauds) and It has become a major problem in the electronic payment system.

2.1 FRAUD

Fraud is termed as a practice that includes deliberately representing a falsehood to deceive the other party. The main purpose behind this is to obtain a profit. This profit can be anything as required by the fraudster – Money, Goods, and Services, Sensitive/Valuable Information, etc. Fraud can occur with the help of words or actions. It includes information that is generally not true and is misleading. It also includes not disclosing the information that is relevant and is to be shared with the merchant [9]. The major difference between a physical and online payment fraud is that there is no need for the card to be present with the fraudster during the time of online transactions. She/he just needs the information on the card which can easily be hacked as it is often stored and used digitally.

Fig. 1. AFP report

Organizations are finding that Fraud increasing year on year in e-payment transactions. Financial Professionals Association (AFP 2012) registered a rise in the number of organizations Subject to actual and/or attempted payment fraud from 2004 to 2009, although the proportion of organizations subject to attempted and/or actual payment fraud shows a decrease in attempted and actual payment fraud from 2010 to 2011 in Fig.1.

2.2 WHAT DOES A FRAUDULENT TRANSACTION LOOK LIKE?

The transactions made on an e-commerce website generally comprise some hints that can help us to recognize them as possibly fraudulent/non-fraudulent transactions. Although if there is only one or two of the specified signs, there is no need to worry if there are several signs for a particular transaction, then it might be a sign of danger to the online retailer because he might be in a stage of being tricked by the fraudster. Now, we will study the various signs [10] of a potentially fraudulent transaction:

i. Shoppers making the transaction for the first time

ii. Huge orders

iii. Quick shipping

iv. Abnormal location

v. Numerous shipping addresses

vi. Mismatch in the shipping address and the IP address

vii. Multiple orders from a unique IP address

viii. Many transactions in a short period

ix. Abnormal usage of capital letters and punctuation

2.3 CHALLENGES IN ONLINE TRANSACTIONS FRAUD DETECTION

The online fraud detection (FD) in the following characteristic and challenges [11] are:

1) The data set is large & highly imbalanced

for e.g., only 5 cases of fraud present in the big dataset which is more than 300 000 transactions in a day, resulting in this job of identifying very unusual fraud spread amongst a vast amount of legitimate transactions.

2) FD needs to be real-time

Taking into consideration that time with a deposit received by a customer in the payment. It has been transferred to his destination account is typically too short; a fraud identification warning should be created as soon as possible to avoid imminent money loss. This includes a higher degree of success in the identification of broad and imbalanced data theft.

3) The fraud behavior is dynamic

Fraud detection is constantly advancing the tactics to beat net banking protections with regular advancements in information technology.

4) The customer behavior patterns are diverse

Fraudsters tend to mimic actual client activity in this sense. They often alter their actions frequently to compete them in detecting fraud. It is all difficult to characterize and makes it even harder to distinguish between fraud and genuine performance.

5) The online banking system is fixed

Customers have access to the same banking infrastructure that can contribute to strong references to characterize typical sequences of legitimate activity and to recognize concerns of illegal net banking.

The above things mentioned are very difficult to fraud detection, which stands why are several techniques in machine learning developed to solved these problems.

2.4 CREDIT CARD FD

A credit card is a payment card that does not automatically debit payments or cash withdrawals from the current accounts. Not all banks that offer credit cards seem to be the only ones. Major corporations, for instance, grocery store chains and airlines, also have issues with credit cards. When there are growing numbers of credit card transactions, financial fraud also rises every year due to misusing credit cards. Based on statistics[12] and a press release by the BBC, Credit card fraud is projected to grow to $31 billion by 2020, costing $21 billion worldwide in 2015.

Credit card theft is a big issue that includes payment cards as an illegal channel of transaction funds, such as credit cards. The purpose of such an illegitimate transaction may be to obtain goods from the account without payment or invoice of an illegitimate fund. It is a daunting challenge to detect such deception that may place company and business organizations at risk. The strategies used to change cardholder spending actions over time and for theft. This transaction by credit card adjustment is referred to as the principle of drift [13][14]. It is also impossible to spot credit card fraud most of the time.

Card fraud detection is the application of the prediction analysis. Fraud is estimated based on historical credit card transaction details to detect credit card fraud. Training set for detecting fraud transactions[15] would be the historical details for card transactions. Today, credit cards are very widely used in our everyday lives to buy several items and to use different services. If the loss of the card is not detected by the cardholder, the big loss will be faced by the credit card business [16]. The intruder needs a relatively limited amount of information to perform any illegal transaction in online account transactions. Credit card theft remains one of the major risks that company organizations face today. Initially, the methods that result in inducing fraud must be perceived so that they can be managed efficiently. If the credit card of someone else is used for personal purposes and the card owner has no knowledge of it, credit card fraud is introduced [17].

3. MACHINE LEARNING & EXTREME LEARNING MACHINE

Researchers have provided various feedbacks to enhance the efficiency of algorithms for ML and lots of work has been done quickly to improve machine intelligence. Learning[18] is a normal phenomenon of human activity that is also an integral feature of machines. Machine learning methods[19] play a

most significant role in fraud detection. As hidden truths are always extracted by uncovered data behind very large volumes of data.

3.1 MACHINE LEARNING IN FRAUD

In the identification and prediction of fraud, ML and deep learning play a central role. To effectively identify fraudulent transactions ML algorithms needed an increased capacity to manage massive databases along with fast processing or computational resources that help network transaction detection[20]. Manually searching and identifying patterns in data take a lot of time for suspicious transactions with the database that containing lakhs of transaction data rows. ML and DL algorithms provide quick and simple solutions to problems such as fraud detection, medical diagnosis, email spam, etc.

The three most important factors behind the importance of Machine Learning are described below [21].

- Speed
- Scale
- Efficiency

3.2 HOW DOES AN ML SYSTEM WORK FOR FD?

The working [22] basic structure of FD algorithms using ML is shown in fig 2.

Fig. 2. The basic working structure of FD algorithms using ML

Feeding data: firstly, input the data into the model. The model consistency is contingent on the amount of data on that it has done training, if we have more data than the model can achieve better. You must include increasing data amounts to detect fraud specific to a given business inside of your model. This will train your model to perfectly recognize fraud-specific activities for your company.

Extracting Features: Effectively, every extra feature works to delete data from a thread linked to a transaction process. There are the location of the transaction, the identity of the client, the payment system & the network utilized for the transaction.

- **Identity**: This is used to verify the email address, telephone number, etc. of a client and it will check the bank account's credit score if the client applied to the loan.
- **Location:** It checks the IP address of the client and fraud data on the IP address and the client sending address.
- **Payment mode:** it is used to verify credit card usage in the transaction, the cardholder's name, the cards from various countries, and the bank account fraud rates used.
- **Network**: to check used mobile numbers &emails for the transaction on the network.

Training the Algorithm: You have to need training the data **when** you generated the FD algorithm first. This is done by giving clients information. It will be useful to tell how to FD algorithm differentiate 'fraudulent' & 'genuine' transactions by learning.

Creating a Model: If you have trained a specific data set on your FD algorithm. You can detect 'fraudulent' and 'non- fraudulent transactions in your enterprise using a model that works.

Machine learning is an advantage of fraud detection algorithms and it tends to boost exposure to more information. In Machine Learning, several methods are used to detect fraud.

- Regression of logistics
- Decision Tree
- Random Forest
- Neural Networks

Table I. Contribution and limitation of ML techniques applied to credit card fraud

S. No.	Technic	Real-Time	Data set		Validation			Observations
			Size	Type	Accuracy (%)	TP (%)	Sensitivity (%)	
1.	RI+NN +SSN [23]	R	over 200P million customers		NA	NA	NA	+ Clustering allows finding the latest hidden pattern from input data. + For further analysis, transaction filtering decreases the total cost as well as the processing time.
2.	AR +FAR [24]	R	12,107 transactions	P	NA	NA	NA	+ The method used comes with the challenge of minimizing support & confidence value, improving FAR execution times, reducing the unnecessary generation of rules & making outcomes more intuitive, thereby promoting fraud detection work.
3.	DST +NR [25]	R	NA	G	NA	MI	NA	+ The design has to be built flexibly& it is still possible to add novel rules at a later level using NR and some other effective technique.
4.	RF + AG [26]	NR	175million transactions	P	NA	NA	NA	+ The aggregating time has a major influence on the effectiveness of the fraud detection classifiers.
5.	SVM +AG [26]	NR			NA	NA	NA	
6.	LR + AG [26]	NR	1.1million transactions		NA	NA	NA	
7.	KNN+AG [26]	NR			NA	NA	NA	
8.	SVM [27]	NR	2420 fraudulent transactions	G	95.30	NA	72.7	+ While sensitivity and accuracy decreased with less fraudulent training data, accurate data indicate the opposite trend.
9.	RF [27]	NR			90.80	NA	52.4	
10.	LR [27]	NR			94.20	NA	65.4	
11.	GA + SS [28]	NR	100,000 fraudulent	P	NA	NA	NA	+ If they want to face fewer losses due to theft, bank management should improve the monitoring power.
12.	AIS [29]	NR	640 361 total transactions	P	80	88*	NA	+ The efficiency of the AIS is substantially enhanced by three mechanisms (new representation in payments and algorithm of r-contiguous bit matching of variable width, vaccine protocol, and process in the evolution of such memory cells).

13.	SVM [30]	NR	970 fraudulent	P	NA	90	NA	•And without class distribution
14.	CART [30]	NR	records 22		NA	83.1	NA	and impurity evaluation in cost
15.	CSDT [30]	NR	million normal transactions		NA	92.1	NA	calculations, we could use misclassification prices.
16.	SOM [31]	NR	10,000 accounts of a selected credit card [1.01.2005-1.03.2005)	P	100	NA	NA	• non-experts can effectively examine and view high-dimensional datasets projected into the two- dimensional space.
17.	AIRS +LC [32]	NR	3.74% fraudulent transactions	P	NA	83*	NA	• Improving the generation of memory cells increases the rate of detection. • changes in distance function perform better-concerning FP.
18.	DT [33]	NR	NSL-KDD dataset	S	91.03	NA	NA	• Reduce host analysis engine complexity.
19.	NB [33]	NR			91.02	NA	NA	
20.	ANN+MPL [33]	NR			99.47	NA	NA	• Propensity to rely on the server's inherent logging and tracking capabilities.
21.	PN+ANN +MPL [34]	NR	Transactions 01-2011 →12-2012.	P	NA	NA	NA	•Addition of par ecclitic characteristics to raw data set increases produced results, reducing error from MPL 19.2 to 12.23%
22.	SVM [35]	NR	NSL-KDD	S	98.8	NA	NA	• The dataset of NSL-KDD shows it is a good candidate data set for IDS performance simulation and testing.
23.	NB [35]	NR			74.9	NA	NA	•Correlation, based on the Feature Selection approach is used for Reduction in dimension, time reduction, and identity of detection.
24.	DBSCAN+ HMM+ LR [36]	R	5 dataset, 10,000,, 1,000,000 Within one year	G	NA	NA	NA	•The Detection Layer and Batch Training Layer should be finally moved to enhance the overall performance during actual machine implementation of the device streaming or computing services.
25.	KNN+OD [37]	NR	NA	P	NA	NA	NA	•OD work quickly and the online huge datasets. •With memory limitations, KNN can easily be used for fraud detection.
26.	FL+ ID3 [38]	NR	NA	P	89	NA	NA	• decreases Irrelevant processing therefore we can achieve detection in the optimal time.

NA: Not Addressed, P: public, G: global, S: synthetic, R:real, NR: not real, CC: cloud computing

Proxim: Accident occurred between the date of issue of legislation and the effective date of starting, 1; otherwise 0.0. Calculated*:

3.3 EXTREME LEARNING MACHINE

ELM [39] is a simple, fast, and effective random algorithm built for training hidden neural networks with the single hidden layer (SLFNs). In the ELM, the weight of the input & hidden layer is distributed at random and the bias value of hidden nodes is distributed at random, while the weights of the hidden and output layer are distributed at random are calculated analytically. The SLFN architecture is defined by three (d, m, k), in which d is Input layers nodes, i.e. the dimension of input data, m is the hidden layers node count and k is the output layers node which is the final class for input data. Given a training set D={(xi, yi)| xiϵ Rd, yi ϵ Rk}, 1≤i≤ n, The following equation (1) can be designed on the SLFN[40] with form (d, m, k).

$$f(x_i) = \sum_{j=1}^{m} \beta_j g(w_j * x_i + b_j) \qquad (1)$$

Where,

βj = weight vector for jth-hidden node to connect the o/p node g(*) = activation function

w_t = weight vector that links jth-hidden node to input nodes, jth = bj hidden node bias values.

& b_1 are randomly generated given in Equation (1) and β_j can be achieved to solve the following linear system in eq. (2).

$$\sum_{j=1}^{m} \beta_j g(w_j * x_i + b_j) = y_i \qquad (2)$$

Eq. (2) can be written in that matrix format like:

$$H\beta = Y \qquad (3)$$

$$H = \begin{bmatrix} g(w_1 * x_1 + b_1) \dots g(w_m * x_1 + b_m) \\ \vdots \quad \vdots \quad \vdots \\ \vdots \quad \vdots \quad \vdots \\ g(w_1 * x_n + b_1) \dots g(w_m * x_n + b_m) \end{bmatrix}$$

$$Y = [y_1^T, y_2^T, \dots, y_m^T]^T$$

$$\beta = [\beta_1^T, \beta_2^T, \dots, \beta_m^T]^T$$

H is the SLFN input & output layer matrix. This is usually defined as a non-square matrix. By solving the following optimization dilemma, the approximate solution of Eq. (3) can be obtained by

$$\min_{\beta} \|H\beta - Y\| \qquad (4)$$

The approximate solution of Eq.(4) is given as

$$\hat{\beta} = H^{\dagger}Y \qquad (5)$$

$H^{\dagger}$=Moore-Penrose generalized H inverse matrix.

4. OPTIMIZATION TECHNIQUES FOR FRAUD DETECTION

By applying a sparse sample set direct to the model using existing data mining algorithms, we cannot achieve good detection results with such algorithms. Such existing algorithms also contribute to concerns such as under-learning, over-fitting, and optimal local solutions. Therefore, improving the detection process is critical [41]. Therefore, further research includes methods to further enhance the accuracy of credit card fraud identification and speed-up detection. Conventional networking algorithms have slow rates of convergence and are susceptible to local minima for networks. To optimize the credit card, various optimization methods are used:

1) Particle Swarm Optimization

Dr. Kennedy and Dr. Eberhart in 1995, developed a population based stochastic optimization strategy called PSO that was inspired by social activity Particle Swarm Optimization of the fish school or the flocking of birds [42]. The particles update their

speed and location with the following equations (6) & (7).

$$vi[t]=vi[t-1]+c1*r1*(pbest[t]-xi[t-])+c2*r2*(gbest[t]-xi[t-1]) \quad (6)$$

$$xi[t+1]=xi[t]+vi[t+1] \quad (7)$$

where,

vi[t] =particle speed,

xi[t] = current particle (solution).

pbest[t] and gbest[t] = defined as local best position and global best position at iteration t,

r1, r2 = random numbers between (0,1).

c1, c2 = learning factors. Usually c1 = c2 = 2.

To vary the c1 & c2 values, we can balance the exploitation & exploration efficiency of the PSO method

2) IPSO

Improved PSO (IPSO) [43] is an adaptive PSO algorithm for optimizing particle swarms. Since the momentum costs (i.e. weight) decrease gradually with the rises of generations, the search area is decreased and the efficiency of IPSO is higher than the PSO.

3) Bat Algorithm

The Bat algorithm [44] is the effective algorithm for finding the optimized solution based on the bat's echolocation behavior.

4) Genetic Algorithm (GA)

Real-world optimization problems are often challenging for NP and an important hyperspace search approach is genetic algorithms [45]. Like several methods, such as the gradient descent method, the algorithms are designed to neglect local optima to locate the optimum solution. Although the principle is easy to learn, the algorithms require a high level of experience in the problem of encoding and fitness function evaluation.GA[46] is a method to find the best solution that parallels the mechanism of natural selection & biological evolution. Selection, crossover, and mutation operators are the main operations where the crossover is a very critical operation that determines convergence.

5) Simulated Annealing

Simulated Annealing (SA) has been used in a wide search space to achieve the global optimal solution for a particular objective cost function. SA[47] shows its effective estimation in real-time for different application areas.

6) Whale Optimization Algorithm

A new form of swarm intelligence optimization algorithm suggested by Australian scholar Mirjaliliet in 2016 is the whale optimization algorithm (WOA). It was developed by whale population quest, encirclement, and hunting attacks from the simulation of the predatory behavior of whales in nature. Search optimization is achieved through Prey and other methods. WOA[48] is a modern algorithm for heuristic optimization inspired by humpback whale hunting. WOA provides superior results in terms of accuracy and rate of convergence.

7) Dandelion Algorithm (DA)

Intelligent algorithms are all related to the optimal solution search. Though, in the search method, individuals use the same process them. The Dandelion Algorithm a new swarm- intelligence algorithm (DA), was proposed to improve complex functions to achieve optimal solutions globally, which was Sowing dandelion inspired by action. In DA [49], the population of Dandelions is split into two sub-populations, which are appropriate for sowing & inappropriate for sowing, and after this apply different ways of sowing to the different sub-population. Meanwhile, a different method of sowing is to follow the appropriate for sowing sub-population to avoid slipping into the ideal local optima.

8) Dandelion Algorithm with Probability-based Mutation

A DA (dandelion algorithm) is an intelligent optimization algorithm. recently suggested that indicates excellent success in solving optimization problem function. Although, it converges slowly like most other intelligent algorithms, and slips rapidly into local optima. To solve both faults, A mutation-based on probability (DAPM) [50] dandelion algorithm is proposed. In DAPM, according to a given probability model, It can be used interchangeably for both Gaussian & levy mutations. Exploitation & exploration both can be balanced well by DAPM. 3A Gaussian mutations are used in probability models, namely linear, binomial and exponential.

5. LITERATURE REVIEW

A few supervised and semi-supervised approaches to fraud detection are used, but there are three important issues of card data, namely strong class imbalances, inclusion, and measurement capacity for the number of transactions and samples that are marked and undecided. The researchers analyzed the effects of several techniques.

H. Li and M. Wong (2015) suggested a new methodology depends upon GBGP (Grammar-based Genetic Programming), multi-objective

optimization & ensemble learning to solve problems of FFD. Decision Trees (DTs), Bayesian Networks (BNs), Bagging, Ada Boost & Logit Boosts on 4 FFD datasets, LR (Logistic Regression), NNs (Neural Networks), SVM (Support Vector Machine), the statistic is thoroughly contrasted with the proposed method. The experimental findings demonstrated the efficacy of the new method, including two real-life issues, in the given FFD issues. The main significance and importance of the analysis may be generalized concretely on a 2 basis. First, the real-life classification issues are evaluated by a variety of data mining techniques. Second, A new methodology is given based on GBGP, NSGA-II, and ensemble learning [51].

F. Ghobadi & M. Rohani (2016) developed a CCFD-based ANN and Meta Cost Credit card Fraud detection (CCFD) model to reduce the probability, risk of losing credibility. ANN was used by credit card to deter and detect fraud. As there are unequal data (fraud and non-fraud cases), it is difficult to identify fraudulent transactions. Meta Cost procedure is applied to solve an imbalanced data query. The model proposed is based on CSNN's approach to the detection of misuse. The model demonstrated cost savings and higher rates of detection compared to the AIS model. Actual transaction data from major Brazilian issuers of credit cards are taken from this survey [52].

N. Jalinus et. al. (2017)) proposed a paper where the accurate performance metrics used for the detection of fraud were first clarified. A novel learning methodology has been structured by the authors that can overcome drift concept, latency verification, and class imbalance issues. The paper also showed the effect on real credit card transactions of the given problems [53].

A.G.C. de Sá et. al. (2018) proposed an algorithm for the real problem of credit card fraud detection to Customizable BNC (Bayesian Network Classifier), Fraud-BNC. A hyper-heuristic evolution algorithm (HHEA) was used to produce fraud-BNC. The BNC algorithms were ordered in the taxonomic system and a particular collection is searched for the best-combined data. To develop BNC fraud, data from the popular Brazilian Pag Seguro online payment service was tested & created by 2 costly classification techniques. Compared to 7 other algorithms, results have been evaluated on the given problem of data classification and e-economic performance of the method. Fraud-BNC was the best algorithm for great gaps between two perceptions, improving the organization's current economic success by up to 72.64% [54].

P. Singh (2017) proposed to use different classification models to assess the accuracy and other output parameters of the fraudulent transaction based on machine learning methods. to test the performance objectively, classification algorithms have been applied such as the K-NN), ELM, Random Forest, the MLP and Bagging Classifier. They recommended an ensemble of five separate algorithms that offered improved forecasting efficiency to a predictive classification model [55].

Z. Wang et al. (2017) implemented Weighted ELM (WELM) to manage imbalanced classification problems. It was found that its two parameters greatly influence its performance. The purpose of this paper was to apply different intelligent optimization methods to optimizing the WELM & evaluate its efficiency in imbalanced classification. Experimental studies indicated that WELM with a genetic algorithm, Bat algorithm, self-learning dandelion algorithm &dandelion algorithm with improved particle swarm optimization, a probability-based mutation dandelion algorithm can do better than WELM. Furthermore, the proposed algorithm relates to the FD card. The findings indicated that high detection efficiency can be obtained [56].

Sun, J. et. al. (2018) To test class-imbalanced credit risk, a new ensemble model was proposed, which integrated various sampling, multiple self-organizing kernel fuzzy maps, and local precision ensembles. Different sampling methods were expanded and integrated (SMOTE, under-sampling,& hybrid sampling) to obtain balanced data sets for pre-processing imbalanced credit risk sample sets. To create a more effective based classification, several kernel functions (that are Gaussian, Sigmoid & Polynomial) to boost fuzzy self-organizing maps have been included. To achieve various prediction values, the improved base classifiers would then process the balanced sample sets. The local precision ensemble method was used to synthesize these estimation effects dynamically to achieve final results. As a consequence, the current ensemble model reduced over fitting and lack of data and be more appropriate for managing. This analysis described financial data of Chinese listed companies and also allows a comparative review of the relative analysis of the data collection, including various financial criteria, and provides a reliable & satisfactory predictive result for imbalanced credit risk assessment. Findings showed that the classified ensemble model given through this work provides good results in comparison to other models for assessing imbalance credit likelihood [57].

M. K. Mishra and R. Dash (2014) attempted the 2 ANN classifier methods namely MLP& ELM added to the credit card fraud data set to identify fraudulent transactions. The efficiency of both classifier methods measured based on precision, recall, accuracy, and time of classification. The findings showed that 97.84% & 95.46% accuracy of both the

MLP and ELM classifiers, respectively. ELM can predict new fraudulent transactions very easily [58].

A. C. Bahnsen et. al. (2015) proposed a system focused on DECSP for the detection of credit card frauds. The system included DECSP with numerous feature extraction methods such as PSO, GA, PCA, and Recursive Feature Elimination techniques. By experimenting, the results have been obtained and compared based on accuracy, precision, F1 score & AUC. With GA, DECSP beats other strategies by given four-efficiency metrics. Also, based on statistical tests, they checked the results [59].

I. Benchaji et. al. (2018) presented an approach namely optimized XG Boost (OXG Boost) to cope with the class imbalance in datasets without resampling techniques. The Randomized Search CV hyper parameter optimization technique was used in this presented solution to find the optimized XG Boost parameters. To achieve the performance of the model, data sampling methods were combined with XG Boost. The experiment was carried out based on two real-world datasets of credit cards. The experimental result revealed that the incorporation of data sampling does not affect the performance of XG Boost. The presented solution has outperformed on the higher accuracy in contrast to the existing one [60].

N. Balasupramanian et. al. (2017) future a deep-forest approach for fraud detection online transactions combining the process of differentiation generation of features and models based on deep-forest. As the details of the single-time transaction that does not involve information such as user behavior, it has insufficiently implemented a time-based distinction mechanism in our scheme to detect fraudulent transaction. The Degree of Personal Credit (ICD) and Degree in Group Anomaly (GAD) differentiate between legitimate and fraudulent transactions. Furthermore, the proposed algorithm was used to identify fraud transactions to address extreme inequalities in online transactions. Despite the absence of external transactions from the raw deep- forest model, crude DEF was improved with the outliers detection method, and increased attention was provided to outliers to promote fraud detection model accuracy. They checked the transaction details of one bank, lastly. This approach boosts the accuracy rate by 15% and the alarming rate by 20% over the random forest detection model [61].

Here we look at algorithms based on the detection of fraud and credit cards. Also, it is introduced and worked. We analyzed those algorithms now in Table II.

Table II. Analysis of CCFD Methods

Sr. No.	Title, Publication & year	Learning Paradigm	Method	Challenges
(i)	Title-"The Novel Model for Artificial Immune System Detections of Credit Card Fraud" [62] Published in: ELSEVIER (Journal) 2014	Supervised	Artificial Immune System	- Fields of the weighting of data. - Cloud computing misuse of AIRS. - Function of distance is dependent on the data set. - Phases of memory generation and affinity calculation take time.
(ii)	Title-"Detection of credit card fraud by modified analyses of fish discrimination" [63] Published in: ELSEVIER (Journal) 2015	Supervised	Profit based modified discriminant linear classifier	- Can't handle false negatives effectively.
(iii)	Title-"APATE: Novel Approach for Automated Credit Card Transaction Fraud Detection using Network-based Extensions" [64] Published in: ELSEVIER (Journal) 2015	Supervised	Online fraud transaction automatic detection model Extraction of intrinsic feature Extraction Network	- Data is too high an imbalance.
(iv)	Title-"Fraud detection application based on the Bagging Ensembles classification Credit Card application" [65] Published in: ELSEVIER (Conference) 2015	Supervised	Complete bagging classification architecture to increase the stability of machine analysis algorithms.	- Classification slow. - Imbalanced Data set. - The Dataset of large size. - The methods of evaluation are to be determined.
(v)	Title-"Feature Engineering Strategies for Credit Card Fraud Detection" [66] Published in: ELSEVIER (Journal) 2016	Supervised	LR, Von Mises Supply for periodic behavior analysis	- Response and time of calculation of the various characteristics.
(vi)	Title-"Horse Race Analysis in Credit Card Fraud – Deep Learning, Logistic Regression, and Gradient Boosted Tree" [67] Published in: IEEE (Conference) 2017	Supervised	LR, Decision Tree, ANN	- Prediction power is less. - Data set size is large. - Feature selection.
(vii)	Title-"Adversarial Learning in Credit Card Fraud Detection" [68] Published in: IEEE (Conference) 2017	Supervised	LR	- the use of velocity parameter to find more algorithm features. - Retraining classification cost.

6. CONCLUSION

The dependence on electronic commerce & net payments is grown increasingly over the past decades. To be better over time, the field of information technology is evolving every day. Financial fraud impacts both the financial market and daily life greatly. Fraud will decrease industry trust, destabilize savings and impact living costs. Nowadays, Illegal acts have become ever more complicated and unrestricted to deal with online transactions that causes led all consumers and associations to substantial financial losses. To combat this issue, financial institutions use a range of models for mitigating fraud. Many methods to prevent and detect fraud in the online world have been discussed. However, in regards to providing the same purpose of detecting and preventing illegal online transactions, all these strategies come with their features, benefits, and challenges.

With this sense, this paper discusses the existing fraud detection analysis to define extreme learning & optimization algorithms that are used to analyze each algorithm according to specific criteria. Detecting credit card fraud is a grave issue. Companies are now spending trillions of dollars to create new algorithms to help to identify fraudulent transactions and avoid them. The goal of the overall study is to identify credit card- related frauds using various machine learning, ELM, and optimization techniques.

REFERENCES

[1] A. Hanskunatai (2018). "A New Hybrid Sampling Approach for Classification of Imbalanced Datasets", 2018 3rd International Conference on Computer and Communication Systems (ICCCS), Nagoya, pp. 67-71.

[2] P. Shukla and K. Bhowmick (2017). "To improve classification of imbalanced datasets", 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, pp. 1-5.

[3] Sumit Chandra et. al. (2018). "A STUDY OF CASHLESS TRANSACTION BEHAVIOR OF BANK CUSTOMERS IN DISTRICT MATHURA, UP", Scholarly Research Journal for Humanity Science & English Language, UGC Approved Sr. No.48612, VOL- 6/26.

[4] S. Isabella et. al.: "An Efficient Study of Fraud Detection System Using Ml Techniques".

[5] K. Joshi (2018). "Cashless Transaction Challenges and Remedies", International Journal of Creative Research Thoughts (IJCRT), pp. 167-172.

[6] J. Zhao (2016). "Extracting and reasoning about implicit behavioral pieces of evidence for detecting fraudulent online transactions in e-Commerce", Decision support systems 86: pp. 109-121.

[7] K. Anupriya, Mrs. C. Kanimozhi (2016). "Scam Detection for Online Shopping using Deep Learning", International Journal of Engineering Research & Technology (IJERT), Vol. 4, No. 11, pp. 1-6.

[8] Lakshmi S. V. S. S. and Selvani Deepthi Kavila (2018). "Machine Learning For Credit Card Fraud Detection System", International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 24, pp. 16819-16824.

[9] L. Fernandes (2013). "Fraud In Electronic Payment Transactions: Threats and Countermeasures", Asia Pacific Journal of Marketing & Management Review, Vol. 2, No. 3, pp. 23-32.

[10] Apapan Pumsirirat, Liu Yan (2018). "Credit Card Fraud Detection using Deep Learning based on Auto-Encoder and Restricted Boltzmann Machine", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 9, No. 1.

[11] Viktor Shpyrkoand Bohdan Koval (2018). "Models of Fraud Detection and Analysis of Payment Transactions Using Machine Learning", pp. 38-53.

[12] K. Chaudhary, J. Yadav, B. Mallick (2012). "A review of Fraud Detection Techniques: Credit Card", International Journal of Computer Applications, Vol. 45, No. 1.

[13] N. Jalinus, R. A. Nabawi, & A. Mardin (2017). "The Seven Steps of Project-Based Learning Model to Enhance Productive Competences of Vocational Students", In 1st International Conference on Technology and Vocational Teacher (ICTVT 2017), Atlantis Press. Advances in Social Science, Education and Humanities research, Vol. 102, pp. 251-256.

[14] S. Kiran, J. Guru, R. Kumar, N. Kumar, D. Katariya (2018). "Credit card fraud detection using Naïve Bayes model-based and KNN classifier", Int. Journal of Adv. Research, Ideas, and Innovations in Technology, Vol. 4.

[15] A.N Agrawal, N. Dermala (2016). "Credit card fraud detection using SVM and Reduction of false alarms", International Journal of Innovations in Engineering and Technology (IJIET), Vol. 7, No. 2, pp. 176-182.

[16] C. Phua, V. Lee, Smith, K.R. Gayler (2010). "A comprehensive survey of data mining-based fraud detection research", arXiv preprint arXiv:1009.6119.

[17] A. Stojanovic, D. Aouada, B. Ottersten, A.C. Bahnsen (2013). "Cost-sensitive Credit Card Fraud Detection using Bayes minimum risk", in 12th International Conference on Machine Learning and Applications (ICMLA), pp. 333-338.

[18] Maryam M Najafabadi et. al. (2015). "Deep learning applications and challenges in big data analytics", Journal of Big Data, 2, Article number: 1.

[19] Dahee Choi and Kyungho Lee (2017). "Machine Learning based Approach to Financial Fraud Detection Process in Mobile Payment System", IT Co Nvergence PR Actice (INPRA), Volume: 5, Number: 4 (December 2017), pp. 12-24.

[20] Suman, Dharminder Kumar (2016). "Performance Analysis of Various Credit

Card Fraud Detection Approaches: A Review", International Journal of Advance Research in Science and Engineering, Vol. 5, No. 9.

[21] Abdallah, Aisha & Maarof, Mohd & Zainal, Anazida. (2016), "Fraud Detection System: A survey", Journal of Network and Computer Applications, 68. 10.1016/j.jnca.2016.04.007.

[22] CLIFTON PHUA et. al. (2010). "A Comprehensive Survey of Data Mining-based Fraud Detection Research".

[23] J. Quah, M. Sriganesh (2008). "Real-time credit card fraud detection using computational intelligence", Elsevier, Expert Systems with Applications, Vol. 35, No. 4, pp. 1721-1732.

[24] D. Sa´nchez, M.A. Vila, L. Cerda, J.M. Serrano (2009). "Association rules applied to credit card fraud detection", Elsevier, Expert Systems with Applications, Vol. 36, No. 2, Part 2, pp. 3630-3640.

[25] S. Panigrahi, A. Kundu, S. Sural, A.K. Majumdar (2009). "Credit card fraud detection: A fusion approach using Dempster–Shafer theory and Bayesian learning" Elsevier, Information Fusion, Vol. 10, No. 4, pp. 354-363.

[26] C. Whitrow, D. J. Hand, P. Juszczak, D. Weston, N. M. Adams (2009). "Transaction aggregation as a strategy for credit card fraud detection", Springer, Data Mining and Knowledge Discovery, Vol. 18, No. 1, pp. 30-55.

[27] S. Bhattacharyya, S. Jha, K. Tharakunnel, J.C. Westland (2011). "Data mining for credit card fraud: A comparative study", Elsevier, Decision Support Systems, Vol. 50, No. 3, pp. 602- 613.

[28] E. Duman, H. Ozcelik (2011). "Detecting credit card fraud by genetic algorithm and scatter search", Elsevier, Expert Systems with Applications, Vol. 38, No. 10, pp. 13057-13063.

[29] N. Wong, P. Ray, G. Stephens, L. Lewis (2012). "Artificial immune systems for the detection of credit card fraud: an architecture", prototype, and preliminary results, Information Systems Journal, Vol. 22, No. 1, pp. 53-76.

[30] Y. Sahin, S. Bulkan, E. Duman (2013). "A cost-sensitive decision tree approach for fraud detection", Elsevier, Expert Systems with Applications, Vol. 40, No. 15, pp. 5916-5924.

[31] D. Olszewski (2014). "Fraud detection using self-organizing map visualizing the user profiles", Elsevier, Knowledge- Based Systems, Vol. 70, pp. 324- 333.

[32] N.S. Halvaiee, M.K. Akbari (2014). "A novel model for credit card fraud detection using artificial Immune Systems", Elsevier, Applied Soft Computing, Vol. 24, pp. 40-49.

[33] A. Mubalik (Mubarek), E. Adali (2017). "Multilayer Perception Neural network technique for fraud detection", IEEE, Computer Science and Engineering (UBMK), International Conference, pp. 383-387.

[34] M. Zanin, M. Romance, S. Moral, R. Criado (2017). "Credit card fraud detection through parenclitic network analysis", pp. 1-8.

[35] L. Dhanabal, Dr. S.P. Shantharajah (2015). "A Study on NSL- KDD Dataset for Intrusion Detection System Based on Classification Algorithms", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, No. 6, pp. 446-452.

[36] Y. Dai, J. Yan, X. Tang, H. Zhao, M. Guo (2016). "Online Credit Card Fraud Detection: A Hybrid Framework with Big Data Technologies", IEEE, Trustcom/BigDataSE/ISPA, pp. 1644-1652.

[37] N. Malini, M. Pushpa (2017). "Analysis on Credit Card Fraud Identification Techniques based on KNN and Outlier Detection", IEEE, Advances in Electrical, Electronics, Information, Communication, and Bio-Informatics (AEEICB), Third International Conference.

[38] S. Askari, A. Hussain (2017). "Credit Card Fraud Detection Using Fuzzy ID3", IEEE, Computing, Communication and Automation (ICCCA), pp. 446-452.

[39] "New learning scheme of feed forward neural networks", Proceedings of International Joint Conference on Neural Networks (IJCNN2004), Vol. 2, pp. 985-990, 2004.

[40] C. Shen, S. Zhang, J. Zhai, D. Luo, and J. Chen (2018). "Imbalanced Data Classification Based on Extreme Learning Machine Auto encoder," 2018 International Conference on Machine Learning and

Cybernetics (ICMLC), Chengdu, pp. 399-404.

[41] N. Homem and J. Paulo Carvalho (2008). “Optimizing a Fraud Detection Process”, IPMU, Vol. 3, pp. 1-8.

[42] D. Sharma, N. Kumar Yadav, Gunjan, and A. Bala (2016). “Impact of distributed generation on voltage profile using different optimization techniques”, 2016 International Conference on Control, Computing, Communication and Materials (ICCCCM), Allahabad, pp. 1-6.

[43] F. Han, Y. Hai-Fen, L. Qing-Hua (2013). “An improved evolutionary extreme learning machine based on particle swarm optimization”, Neurocomputing, Vol. 116, pp. 87-93, 2013.

[44] X.S. Yang (2010). “A new met heuristic bat-inspired algorithm”, Proceedings of the Nature Inspired Cooperative Strategies for Optimization (NICSO 2010), Springer, Berlin, Heidelberg, pp. 65–74.

[45] N. F. Ryman-Tubb, P. Krause, W. Garn (2018). “How Artificial Intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark,” Engineering Applications of Artificial Intelligence, Vol. 76, pp. 130-157.

[46] D. Whitley (1994). “A genetic algorithm tutorial, Statist. Comput., Vol. 4, No. 2, pp. 65–85.

[47] S. Madichetty, M. Rambabu and A. Dasgupta (2014). “Selective harmonic elimination: Comparative analysis by different optimization methods”, 2014 IEEE 6th India International Conference on Power Electronics (IICPE), Kurukshetra, pp. 1- 6.

[48] C. Wang, Y. Wang, Z. Ye, L. Yan, W. Cai, and S. Pan (2018). “Credit Card Fraud Detection Based on Whale Algorithm Optimized BP Neural Network”, 2018 13th International Conference on Computer Science & Education (ICCSE), Colombo, pp. 1-4.

[49] X. Li, S. Han, L. Zhao, C. Gong, X. Liu (2017). “New Dandelion Algorithm Optimizes Extreme Learning Machine for Biomedical Classification Problems”, Computational Intelligence and Neuroscience, Vol. 2017, Article ID 4523754.

[50] Xiguang Li, Shoufei Han, Liang Zhao, Changqing Gong, Xiaojing Liu (2017). "New Dandelion Algorithm Optimizes Extreme Learning Machine for Biomedical Classification Problems", Computational Intelligence and Neuroscience, vol. 2017, 13 pages. https://doi.org/10.1155/2017/4523754.

[51] H. Li and M. Wong (2015). “Financial fraud detection by using Grammar-based multi-objective genetic programming with ensemble learning”, 2015 IEEE Congress on Evolutionary Computation (CEC), Sendai, pp. 1113-1120.

[52] F. Ghobadi and M. Rohani (2016). “Cost-sensitive modeling of credit card fraud using neural network strategy”, 2016 2nd International Conference of Signal Processing and Intelligent Systems (ICSPIS), Tehran, pp. 1-5.

[53] N. Jalinus, R. A. Nabawi, & A. Mardin (2017). “The Seven Steps of Project-Based Learning Model to Enhance Productive Competences of Vocational Students”, In 1st International Conference on Technology and Vocational Teacher (ICTVT 2017). Atlantis Press. Advances in Social Science, Education and Humanities research, Vol. 102, pp. 251-256.

[54] D. Sá, et. al. (2018). “A customized classification algorithm for credit card fraud detection”, Engineering Applications of Artificial Intelligence, Vol. 72, pp. 21–29.

[55] P. Singh (2017). "Comparative study of individual and ensemble methods of classification for credit scoring," 2017 International Conference on Inventive Computing and Informatics (ICICI), pp. 968-972, DOI: 10.1109/ICICI.2017.8365282.

[56] Z. Wang et. al. (2017). "Distributed and weighted extreme learning machine for imbalanced big data learning," in Tsinghua Science and Technology, vol. 22, no. 2, pp. 160- 173, DOI: 10.23919/TST.2017.7889638.

[57] Sun, J. et. al. (2018). “Imbalanced enterprise credit evaluation with DTE-SBD: Decision tree ensemble based on SMOTE and bagging with differentiated sampling rates.” Inf. Sci. 425: pp. 76-91.

[58] M. K. Mishra and R. Dash (2014). "A Comparative Study of Chebyshev Functional Link Artificial Neural Network, Multi- layer Perceptron and Decision Tree for Credit Card Fraud Detection," 2014 International Conference on Information

Technology, pp. 228-233, DOI: 10.1109/ICIT.2014.25.

[59] A. C. Bahnsen, D. Aouada, A. Stojanovic and B. Ottersten (2015). "Detecting Credit Card Fraud Using Periodic Features," 2015 IEEE 14th International Conference on Machine Learning and Applications (ICMLA), pp. 208- 213, DOI: 10.1109/ICMLA.2015.28.

[60] I. Benchaji, S. Douzi and B. ElOuahidi (2018). "Using Genetic Algorithm to Improve Classification of Imbalanced Datasets for Credit Card Fraud Detection," 2018 2nd Cyber Security in Networking Conference (CSNet), pp. 1-5, DOI: 10.1109/CSNET.2018.8602972.

[61] N. Balasupramanian, B. G. Ephrem and I. S. Al- Barwani (2017). "User pattern based online fraud detection and prevention using big data analytics and self-organizing maps," 2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), pp. 691-694, DOI: 10.1109/ICICICT1.2017.8342647.

[62] N. Halvaiee, M. Akbari (2014). "A novel model for credit card fraud detection using Artificial Immune System", Elsevier Applied Soft Computing, pp. 40-49.

[63] N. Mahmoudi, E. Duman (2015). "Detecting credit card fraud by Modified Fisher Discriminant Analysis", Elsevier Expert System with Application, pp. 2510-2516.

[64] V. Vlasselaer, C. Bravo, O. Caelen, T. Eliassi-Rad, L. Akoglu, M. Snoeck, B. Baesens (2015). "APATE: A Novel Approach for Automated Credit Card Transaction Fraud Detection using Network-based Extensions", ELSEVIER Decision Support Systems, pp. 38-48.

[65] M. Zareapoor, P. Shamsolmoali (2015). "Application of Credit card Fraud Detection: Based on Bagging Ensemble Classifier", Elsevier International Conference on Intelligent Computing, Communication & Convergence, pp. 679-685.

[66] A. Bahnsen, D. Aouada, A. Stojanovic, B. Ottersten (2016). "Feature Engineering Strategies for Credit Card Fraud Detection", ELSEVIER Expert System with Applications, pp. 134-142.

[67] G. Rushin, C. Stancil, M. Sun, S. Adams, P. Beling (2017). "Horse Race Analysis in Credit card Fraud- Deep Learning, Logistic Regression, and Gradient Boosted Tree", IEEE, pp. 117-121.

[68] M. Zeager, A. Sridhar, N. Fogal, S. Adams, D. Brown, P. Beling (2017). "Adversarial Learning in Credit card Fraud Detection", IEEE, pp. 112-116.

Corresponding Author

Sonam Mittal*

Department of Computer Science, MIMT, Kota, India

sonammittalkota@gmail.com