Future Computing and Informatics Journal

Volume 4
Issue 2 *2019 Volume 4, Issue 2*

Article 5

2019

Machine Learning Techniques for Credit Card Fraud Detection

Hossam Eldin Mohammed Abd El-Hamid Ahmed Abdou
Computers & Information Technology - Ain Shams University, eng.hossameldinm.abdelhamid@gmail.com

Wael Khalifa
Ain Shams University, Wael.Khalifa@cis.asu.edu.eg

Mohamed Ismail Roushdy
Professor & Dean of Faculty of Computers & Information Technology, Future University in Egypt, Mohamed.Roushdy@fue.edu.eg

Abdel-Badeeh M. Salem
Ain Shams University, abmsalem@yahoo.com

Recommended Citation

Abd El-Hamid, Hossam Eldin Mohammed Ahmed Abdou; Khalifa, Wael; Roushdy, Mohamed Ismail; and Salem, Abdel-Badeeh M. (2019) "Machine Learning Techniques for Credit Card Fraud Detection," *Future Computing and Informatics Journal*: Vol. 4 : Iss. 2 , Article 5.
Available at: https://digitalcommons.aaru.edu.jo/fcij/vol4/iss2/5

Digital Commons
ELSEVIER
Future Computing and Informatics Journal
https://digitalcommons.aaru.edu.jo/fcij/

Machine Learning Techniques for Credit Card Fraud Detection

Hossam Eldin M. Abd Elhamid[a], Wael Khalifa[b], Mohamed Roushdy[c], Abdel-Badeeh M. Salem[d]

[a]Faculty of Computers & Information Sciences, Ain Shams Cairo, Egypt, eng.hossameldinm.abdelhamid@gmail.com
[b]Faculty of Computers & Information Sciences, Ain Shams University, Cairo, Egypt , Cairo. Egypt, Wael.khalifa@cis.asu.edu.eg
[c] Faculty of Computers & Information Technology, Future University in Egypt New Cairo, Egypt Mohamed.Roushdy@fue.edu.eg
[d] Faculty of Computers & Information Sciences, Ain Shams University , Cairo, Egypt abmsalem@yahoo.com

Abstract

The term “fraud”, it always concerned about credit card fraud in our minds. And after the significant increase in the transactions of credit card, the fraud of credit card increased extremely in last years. So the fraud detection should include surveillance of the spending attitude for the person/customer to the determination, avoidance, and detection of unwanted behavior. Because the credit card is the most payment predominant way for the online and regular purchasing, the credit card fraud raises highly. The Fraud detection is not only concerned with capturing of the fraudulent practices, but also, discover it as fast as they can, because the fraud costs millions of dollar business loss and it is rising over time, and that affects greatly the worldwide economy. . In this paper we introduce 14 different techniques of how data mining techniques can be successfully combined to obtain a high fraud coverage with a high or low false rate, the Advantage and The Disadvantages of every technique, and The Data Sets used in the researches by researchers

Keywords:Machine Learning, Computational Intelligence, Data Mining, Credit Cards Fraud Detection

1. INTRODUCTION

Although the Credit Card transactions of the USA are the highest, it has a minimum fraud rate. The tops of the list is Ukraine with astounding 19% fraud rate and it is followed by Indonesia with 18.3% rate of fraud amid the countries of high risk Credit Card which facing Fraud threat, in other countries like Yugoslavia (17.8%), Turkey (9%) and Malaysia (5.9%). [1] Authorized users are allowed for credit card transactions by using some measurement factors such as credit card number, card holder’s address, signatures, the expire date, etc. The illegal use of the card information without the owner’s knowledge itself is an act of criminal deception which refers to the Credit card fraud. Credit card fraud detection is quite classified and not easily disclosed in public. The most common used fraud detection methods are Decision Trees, Support Vector Machines (SVM), Rule-Induction Techniques, LR, ANNs and The Meta-Heuristics such as k-means Clustering, The Genetic Algorithms, and nearest neighbor algorithms. The Fraud is kind of the human behavior that relates to stealing, misrepresenting misunderstanding, misrepresenting, cunning, cheating, and the false proposition, etc. Most of the time the companies are dealing with many and millions of parties, it is prohibitively expensive to check all the plurality of these parties' activities and to identity them manually. So certainly, for the investigating of every suspicious transaction, they afford a direct overhead cost for each of them, so ,if the transaction amount is smaller than the overhead cost, the examination is not worthwhile even if it is a suspicious transaction.

The Types of Fraud

(a)Telecommunication Fraud

The use of telecommunication services such as its tool to defraud and it affects businesses, consumers and the provider of communication service. Here we introduce credit card its different types and some related works used to solve it and the models used to fraudulent transaction detecting. Due to being a definition which is as the Entering Act without Invitation or Warrant; and also that means "Potential Possibility of Unauthorized Attempt to Access Information, Manipulate Information Purposefully." The Intruders maybe from any environment, a person from outside "The Outsider or Hacker" and someone from inside 'The Insider' who is knowing the system layout. There are three categories of Computer Intrusion and it classified into misuse intrusions, network intrusions, and host intrusions. The Misuse intrusions: analyzing the gathering of information and compare it to big databases of attack signatures.The Network intrusions: analyzing the flowing packets through network individually. Passive intrusions: it detects a potential security violation, register information and gives an alert.

(b)Application Fraud

It is happen when someone applies for a credit card but with false information that is called as application fraud. To detect the application fraud, we have to classify two different situations. First, when applications come from the same user with the same details, which is called duplicates, and second, when the applications are from different individuals but with similar details, that is named as identity fraudsters. In Phua et al. (2006), it describes application fraud as "demonstration of identity crime, occurs when application forms contain possible, and synthetic (identity fraud), or real but also stolen identity information (identity theft)." In most banks, in order to increase the quality of the credit card, the applicants need to complete an application form, the application form is mandatory except for the social fields, and the bank asks for some certain details as the contact details, mobile phone number, e-mail address and the land-line number, then, all of this confidential information will be your password.

(c)Behavioral Fraud

The Behavioral fraud happens in the sales processes when the cardholder presents the basis and details of legitimate cards obtained fraudulent basis.

(d)Bankruptcy Fraud

The Bankruptcy fraud is the using a credit card while its owner is being absent. This type of fraud is one of the most complicated fraud types to be predict. Some techniques or methods may help in the prevention of fraud. The bank sends its customers an order to pay, and the users also will be recognized as they are being in a state of a personal bankruptcy and not able to regain their unwanted loaning, so the bank has to cover the losses itself. Foster & Stine (2004) presented a model to forecast the personal bankruptcy among the users of credit card, and it is by doing a pre-check with the credit office to be informed and have knowledge about the history of bank's customers which is one of the possible tries to prevent bankruptcy fraud.

(e)Theft Fraud/ Counterfeit Fraud

It focuses on theft and the fraud of rigging, which are related to other one. Theft fraud is using a fake credit card once the owner of the card gives any feedback and contact with the bank, the bank will take the measures to check the thief as soon as possible can be. By the same way, counterfeit fraud happens when the credit card is remoted used; the use of your copied card number and the codes via different websites, where there is no physical cards or signature is required, it's only needed the credit card details. Due to Pago Report issues (2005), ((there also in European E-commerce which seems to be quite low, at only 0.83 percent along with the average chargeback ratio, important concerns notified in a detailed analysis.)) For the listed credit card, the customers are being contacted quickly and if they do not react within a certain specific time then the card blocked.Here introduce the paper, and put a nomenclature if necessary, in a box with the same font size as the rest of the paper. The paragraphs continue from here and are only separated by headings, subheadings, images and formulae. The section headings are arranged by numbers, bold and 9.5 pt. Here follows further instructions for authors.

2. Machine Learning Techniques

2.1. The Neural networks:

Due to Aleskerovet al. "Developing a system, for the data extraction, based on the neural network to detect fraud in the credit cards. And also, the (CARD WATCH) proposed system contains three layers of automatic binding structures. And they used a set of structured data to train and test the system. Consequently, the results were showing high successful fraud detection rates." In, P-RCE's the neural network was applied to detect the fraud in the credit card: P-RCE is a type of the radial base function networks that are applied commonly to the tasks of pattern recognition. Krinker et al. is another model that was proposed to detect fraud in real-time, and it based on the bidirectional neural networks. In this method, they used telephone transaction data of a wide range provided by the credit card company. And it supposed that the system outperforms the algorithm based on the rule in terms of the false-positive rate. In a parallel Granular Neural Network (GNN) is proposed to speed up the data mining and the knowledge discovering to detect the fraud in the credit cards. And it is a type of indefinite neural network which is based on knowledge discovery (FNNKD). So, the basic data set was extracted from the SQL Server database containing Visa Card transactions and then pre-processed for fraud detection. As a result, they received less training errors on average in the presence of a larger training data set.

Hybrid supervised and unsupervised techniques [26]

In addition to supervised and unsupervised learning models from neural networks, some researchers have applied hybrid models. According to John Chong Lait. "Proposed Hybrid (SICLN) and Unsupervised Learning Network (ICLN) to detect credit card fraud. They have improved the bonus base only from the SICLN model to ICLN, to update the weights due to the penalty, and the reward. And this improvement was appeared in terms of stability increasing and reduced the time of training. In addition, the number of final groups of the ICLN is independent of the number of primary neurons in the network. As a result, non-operable neurons can be deleted from the blocks by applying penalty rule. So, the results specify that both of the ICLN and the SICLN are performance highly, but the SICLN outperforms the known unsupervised aggregation algorithms.

Advantages:

Capacity to gain from an earlier time/ absence of should be reinvented/Ability to concentrate runs and anticipate future exercises dependent on the present circumstance/ High precision/ Portability/ fast in discovery/ the capacity to create code to be utilized progressively frameworks/ the effortlessness to be fabricated and worked/Effectiveness in managing loud information, in foreseeing designs, in taking care of complex issues, and in handling new occasions/ Adaptability/ Maintainability/ (information)

Disadvantages:

Trouble to affirm the structure/high preparing time for huge neural systems furthermore, inordinate preparing/poor clarification capacity/hard to set up and work/ high cost/ non-numerical information should be changed over and standardized/Sensitivity to information design.

2.2. The Decision Tree:

After the introducing of the concept of the learning system, the method decision tree was developed, the C4.5 technique (Quinlan, 1993) and the ID3 method (Quinlan, 1986), which could handle continuous data. A decision tree is a tree shape table with attached lines to the nodes that are available. Every node is a sub node followed by more nodes or only one node that is assigned by the classification.

. Due to, (van et al., 2001), similarity trees yielded proven results worked on trees decision especially on the other type of the fraud, inductive decision tree in order to create a system of intrusion detection.

Advantages :

High adaptability/ great soundness/ logical/ simple to actualize/ simple to show and to get it

Disadvantages:

The Prerequisites to check every condition one by one.

In the extortion recognition, the condition is exchange.

2.3. Genetic Algorithms:

Recently, they applied optimization of the parameters of the support vector machine, inspired from natural evolution were first introduced by Holland (1975), for predicting bankruptcy, hybrid with neural network for detecting credit card fraud with high accuracy [96], then it has been used along, with the Artificial Immune System, for reducing the number of false alarm in credit card fraud detection.GA is used in data mining mainly, for variable selection [95], and mostly coupled with other DM algorithms [48]. The present estimations of these parameters have been resolved, and the basic qualities are contrasted, and the informational index parameters and the augments of the number of genuine alarms given that the quantity of cautions does not surpass a specific dimension

Due To ***K.RamaKalyani, D.UmaDevi***In Their Research **“Fraud Detection of Credit Card Payment System by Genetic Algorithm”[49]**They Represent These High

Advantages:

Functions admirably with boisterous information/simple to coordinate with other frameworks/ typically consolidated into different systems to increment the presentation of those strategies, and enhance their parameters/ simple in manufacture and work/ quick in identification/ Versatility/ Maintainability/ information disclosure and information emulating.

Disadvantages:

Requires broad device learning to set up. Furthermore, work and hard to get it.

2.4. Case Based Reasoning:

Adjusting arrangements, to take care of past issues and use them to take care of new matters, is the basic thought of CBR. In CBR, cases present as portrayals of experience of the customers, furthermore, put away in a database which uses for later recovery when the client experiences another case with comparable parameters, and these cases can apply for order purposes. A CBR framework endeavours to discover a matching situation when faced with another issue. In this technique, the model characterized as the preparation information; in the test stage, when another case or example is given to the model, it looks in every one of the information to find a subset of cases that are almost like a new case, and uses them to anticipate the outcome. However, the nearest neighbor matching algorithm typically connected with CBR, besides, there are a few other algorithms which utilized with this methodology, for example, Case-based thinking is very much archived both as the structure for half breed fraud detection frameworks.

Additionally, E.b. Reategui connected cross breed methodologies of CBR, and NN which partition the undertaking of fraud detection into two separate parts, then found that this numerous methodology was progressively powerful than any either approach [92]. In this model, CBR, searches for the best matches to the situation base; while an Artificial Neural Net (ANN) learns the examples of utilization and abuse of Visas, the case base included data, for example, exchange sums, dates, spot and type, and MCC (Merchant Category Code), the CBR and ANN frameworks announced an arrangement precision of 89% on a case base of 1606 cases.

Advantages:

Helpful in area that has an enormous number of models/ can work with deficient or uproarious information/ powerful/ adaptable/ simple to refresh and keep up/ can be utilized in a cross breed approach.

Disadvantages:

May experience the ill effects of the issue of inadequate data.

2.5. Clustering Techniques:

Two clustering techniques have been recommended for social fraud by Bolton and Hand (2002).((Friend bunch investigation is a framework that permits recognizing accounts which are carrying on uniquely, in contrast to others at one minute, they were acting the equivalent. Then these records are identified as suspicious, at that point fraud examiners have been utilized to reveal those cases.)) The hypothesis behind companion bunch examination is that, if accounts that we're carrying on the equivalent for a specific timeframe, and after that one record, and yet acting altogether in an unexpected way, at that point this record must be reported. Another methodology, Breakpoint examination utilizes an alternate hypothesis which expresses that if a difference in card utilization is told on an individual premise, the record must be researched. Or on the other hand, we can say that the Breakpoint examination based on the exchanges of a solitary card, and it can distinguish suspicious conduct. Signs of suspicious conduct are an abrupt exchange for a high sum and a high recurrence of use with no learning to cardholders.

Advantages:

- A cluster of data items can be treated as one gathering.
- Versatile to change and help single out valuable highlights that recognize various gatherings of data.
- Scalability: we need highly versatile clustering calculations to manage huge databases.
- Capacity to manage various types of attributes.
- ((Revelation of clusters with attribute shape: the clustering techniques ought to be fit for identifying bunches of subjective shape. They ought not to be limited to just separation estimates that will in general discover round cluster of little sizes.))
- High dimensionality: the clustering techniques ought to not exclusively have the option to deal with low-dimensional data yet, besides, the high dimensional space.
- Capacity to manage noisy data: Databases contain noisy, absent or mistaken data. A few calculations are touchy to such data and may prompt low quality clusters.
- Interpretability: the clustering results ought to be interpretable, coherent, and usable.

Disadvantages:

- While doing cluster techniques, we first parcel the arrangement of data into groups dependent on data closeness and afterward dole out the names to the gatherings.

2.6. Inductive Logic Programming:

ILP, by utilizing a lot of positive and negative models, utilizes first request predicate logic to characterize an idea. And it is used to order new occasions. Complex relationships among parts or traits can be effectively communicated, in this methodology of characterization. The adequacy of the framework improves by space information, which can be effectively approached to in an ILP framework [87]. Muggleton et al. [88] proposed the model that applying the name of the information in misrepresentation detection, which utilizing social learning methodologies, for example, Inductive Logic Programming (ILP) and the straightforward based classifiers on social databases. Perlich, et al. [89] Also proposed novel target-subordinate detection techniques for changing over the social learning issue into a customary one.

Advantages:

Incredible in procedure various data types/ ground-breaking displaying language that can demonstrate complex connections/ innovative in handling the missing information.

Disadvantages:

Has low prescient precision/ amazingly touchy to commotion/ their presentation disintegrates quickly within sight of fake information.

2.7. K-Nearest Neighbor Algorithm:

The idea of nearest neighbor algorithm has been utilized in a few peculiarity detection techniques. A standout amongst the best classifier algorithms that have been utilized in the credit card fraud detection is the k-nearest neighbor algorithm, which is a supervised learning algorithm, where the aftereffect of new case inquiry is ordered based on greater part of K-Nearest Neighbor classification. It was first presented by Aha, Kibler, and Albert (1991).

The exhibition of KNN algorithm is affected by three fundamental variables [Mohammed J. Islam]:

- The separation metric used to find the nearest neighbors.
- The separation rule used to get a characterization from k-nearest neighbor.
- The quantity of neighbors used to characterize the new example. Due To Joseph Pun, Yuri Lawryshyn , In Their Research "**Improving Credit Card Fraud Detection using a Meta-Classification Strategy"**[47]They Gave Ranking To The K-N. Algorithm As Following:k-nearest neighborWith Diversity Value was DT, kNN, NB Was 0.394858

And Giving It Score Of 36% reached Score 91% Meta classifier Probability In 800 Accounts Investigated in a day

Advantages:

It can be connected to the data from any conveyance for example, data doesn't need to be distinct with a linear boundary. Very basic and instinctive. In the case of large no. of samples, it made a good classification.

Disadvantages:

Higher dependence of K value. Test stage is costly. No preparation organize, all the work is finished during the test arrange.

2.8. Logistic Regression:

(Altman, Marco 1994; Flitman, 1997) Information mining assignments has increasingly more factual model that includes discriminant examination, regression investigation and numerous logistic regression. So, Logistic regression (LR) is helpful for circumstances in which we need to have the option to foresee the nearness or nonappearance of a trademark or result dependent on estimations of a lot of indicator factors. It is as a direct regression model, yet it is fit to models where the reliant variable is dichotomous. ((Logistic regression coefficients can be utilized to assess chances proportions for every one of the free factors in the model, and it is relevant to a more extensive scope of research circumstances than highlight investigation. (Ohlson, 1980; Martin, 1997) assessing the chances of a firm's disappointment with likelihood.))

Advantages:

- It is truly quick to get Results.
- It will work better if there's a separate

choice limit, not parallel to the center.

- Logistic regression is naturally basic, it has a low difference, as is less inclined to over-fitting.
- Better especially when you are managing exceptionally high measurement information. Content grouping is an exemplary issue.
- computing the chances of the issue as the proportion of the likelihood of having the result isolated by the possibilities of not having it.

Disadvantages:

- It's anything but a valuable apparatus, except if analysts have effectively distinguished all-important autonomous factors.
- It requires every datum point to be free of every other datum focuses.

2.9. Outlier Detection:

Outliers are an essential type of non-standard consideration that can be utilized for fraud detection. A study that goes amiss much from different perceptions and emerges doubt, that it was created by an alternative instrument, is known as the outlier, and also the Unsupervised learning Approach is utilized by this model. For the most part, the consequence of unsupervised learning is another clarification or portrayal of the watched information, which will, at that point, lead to an improved future choices.

the supervised strategies are just prepared to separate between genuine exchanges and recently known fraud. Some unsupervised credit card fraud detection procedures have been proposed by Bolton and Hand, with the assistance of utilizing social outlier detection strategies. Spending conduct unusually and recurrence of exchanges will distinguish as outliers, which are likely fraud cases.

Advantages:

- They are numerically justified. For instance, the verification of contending speculations is a traditional issue of scientific measurements, which can be connected to factual models utilized and, specifically, to the detection of outliers.
- If a probabilistic model is given, factual strategies are very efficient and make it conceivable to uncover the importance of the outliers found.
- In the wake of building the model, the data on which the design, is based, is not required. It is sufficient to store the insignificant measure of data that depicts the image.

Disadvantages:

- They require either development of a probabilistic data model dependent on empirical data, which is a somewhat confusing computational undertaking, or from the earlier information of the conveyance laws.
- If the model is parameterized, complex computational systems for finding these parameters are required.
- It isn't ensured that the data being analyzed match the accepted dispersion law if there is no gauge of the circulation thickness dependent on the empirical data.
- The development of tests, for speculation verification on account of complex combinations of dissemination, is a nontrivial task.

2.10. Support Vector Machine:

Support vector machine (SVM) is a managed learning model, with related learning Algorithms that can break down and perceive designs for grouping and relapse tasks, and it is a paired classifier.

, Ghosh and Reilly created a model that utilizing the SVMs and appreciated the neural systems. In this examination, a three-layer feed-forward RBF neural systems connected for identifying fake charge card exchanges, through just two passes required to produce a misrepresentation score in like clockwork. Tung-Shou Chen et al. proposed a paired of the support vector framework (BSVS), in which the support vectors were chosen by methods for the Hereditary Algorithms (GA). In the proposed model, self-sorting out map (SOM) was the first connected to acquire a high negative rate, and the BSVS was then used to train the information agreeing their conveyance. On the other hand, an arrangement model that depends on the choice trees and the support vector machines (SVM), was built separately for identifying Visa misrepresentation. The primary relative examination among the SVM, what's more, the choice tree strategies in charge card extortion that discovery with a genuine informational collection, were performed in this paper. However, the outcomes uncovered that the choice tree classifiers, for example, Truck beat SVM in taking care of the issue under scrutiny. ((Rongchang Chen et al. recommended a novel survey responder exchange the (QRT) approach with the SVM for charge card misrepresentation identification. The goal of this exploration was the utilization of the SVM as well as different methodologies, for example, Over-examining and greater part voting, in favour of, were exploring the forecast precision of their strategy in extortion location.)) The test results showed that the QRT approach has high level of productivity as far as expectation precision. Qibei Lu et al. set up a Visa misrepresentation recognition model dependent on Class Weighted SVM. Utilizing Essential Segment Examination (PCA); they at first decreased information measurement to less manufactured composite highlights because of the high dimensionality of information. At that point, as per awkwardness attributes of information, an improved Lop-sidedness Class Weighted SVM (ICW-SVM) was proposed.

The Support Vector Machines (SVM) is a measurable learning procedure and has fruitful application in scope of issues. Also, it was first presented by Cortes and Vapnik (1995), and it has been observed to be useful in an assortment of grouping errands. Due To Y. Sahin and E. DumanIn Their Research “Detecting Credit Card Fraud by Decision Trees and Support Vector Machines”[63] they made a Distribution of data with respect to the classes is highly Imbalanced. The time period that is used to build our sample Included 978 fraudulent records and 22 million normal ones With a ratio of about 1:22500.t

Advantage:

SVMs convey a one of a kind arrangement since the optimality issue is curved/ by picking a fitting speculation grade, SVMs can be strong, notwithstanding when the preparation test has some predisposition.

Disadvantages:

Poor in process large dataset/ expensive/has low speed of detection/ medium accuracy/ lack of transparency of results

2.11. Bayesian Network:

The Bayesian conviction network was first presented by Cooper and Herskovits (1992). Bayesian conviction networks are measurable procedures in information mining and extremely successful for displaying circumstances, where some data is now known and approaching information is uncertain or in part inaccessible. However, the objective of utilizing Bayesian principles is to accurately anticipate the estimation of an assigned discrete class variable given a vector of indicators or traits. In 1993, Sam maes et al has been recommended BN for charge card fraud recognition. With the end goal of fraud recognition, two Bayesian networks theory, for portraying the conduct of clients, are built.

The Bayesian Network needs preparing the information to work and require a high handling rate. The BN is more exact

and a lot quicker than the neural network[98], however, BBN’s are slower when connected to new occurrences

In other research, two methodologies are proposed for charge card misrepresentation location utilizing Bayesian network; To start with, the fake client conduct and in the second the genuine (ordinary) client conduct are displayed by Bayesian network. The deceitful conduct net is built from expert learning, while the authentic net is set up, in regard to accessible information from non-fake clients, the legitimate net is adjusted to a particular client dependent on rising information. Characterization, of new exchanges, was just led by embedding it to both networks sand, then determine the kind of conduct as indicated by comparing probabilities. Applying Bayes' rule gives the likelihood of misrepresentation for new exchanges. Once more, Ezawa and Norton built up a four-arrange of the Bayesian network; They asserted that bunches of prominent techniques, for example, relapse, K-closest neighbour and neural networks, set aside too long effort to be appropriate in their information. [79]

Advantages : High preparing and discovery speed/ high exactness.

Disadvantages : Extreme preparing need/ costly.

2.12. Hidden Markov Model:

A Hidden Markov Model is a twofold installed stochastic process, which is utilized to model significantly more confused stochastic processes when contrasted with a conventional Markov model. On the off chance that, an approaching credit card exchange isn't acknowledged by the prepared Hidden Markov Model with adequately high likelihood, it is viewed as fraudulent exchanges

V. Bhusari et al. utilized Gee for identifying credit card frauds with low false caution High alarm for false [55]. However, the proposed framework was moreover versatile for processing the immense number of exchanges. Also, the Gee can likewise be installed in online fraud detection frameworks that get exchange subtleties and check whether it is typical or fraudulent. And, if the framework affirms the exchange to be vindictive, an alert is raised and the related bank rejects that exchange. The reacting cardholder, then, may educate about conceivable card abuse.

Advantages : Detection is fast.

Disadvantages : It is very expensive/ the accuracy is low / cannot deal with large size data sets scalability.

2.13. The Fuzzy Logic Based System:

FLBS is the Network based on fuzzy rules, and it addresses the vulnerability of the info and yield factors by characterizing fuzzy sets and numbers, to express values as etymological factors, for example, little, medium and enormous. And there are two significant sorts of these Networks are Fuzzy Neural Network (FNN) and Fuzzy Darwinian System (FDS).

2.13.1 Fuzzy Neural Network (FNN)

The point of FNNs is to process the huge volume of dubious data, which is broadly connected in our life [61]. ((According to **Syeda et al (2002)** [21] "propose fuzzy neural networks on parallel machines to accelerate rule creation for client explicit credit card fraud detection. And his work can be identified with Information mining and the Knowledge Discovery in the information bases (KD)." In this technique, **Syeda** et al utilized the GNN (Granular Neural Network) strategy that utilizations a fuzzy neural network based on knowledge discovery (FNNKD), for how quick, we can prepare the network and how quick various clients can be processed for detection in parallel.)) There are different fields in the exchange table that incorporate the exchange sums, the time between exchanges, the proclamation date, the exchange code, the posting date, the and exchange portrayal. As always, for the execution of this credit card fraud detection technique, the applicable fields from the database were removed into a straightforward content experience by applying a proper SQL investigation.

2.13.2 Fuzzy Darwinian System (FDS)

This strategy utilizes Genetic programming to advance fuzzy logic rules, and to fit for characterizing of the credit card exchanges into "suspicious" and non-suspicious classes. It portrays the utilization of a transformative fuzzy framework fit for arranging suspicious and non-suspicious credit card exchanges. So, the structure involves two primary components: a Genetic Programming (GP) look algorithm and a fuzzy master framework.

Advantages:

Fuzzy Neural Network: The Detection is Very fast /the accuracy is good.

Fuzzy Darwinian System: The accuracy is Very High/ Also, its' Maintenance easy.

Disadvantages:

Fuzzy Neural Network : It is Highly Cost.

Fuzzy Darwinian System: The speed of the detection is very low / Very expensive.

2.14. Artificial Immune System:

Artificial immune systems (AIS) speak to a significant technique roused by biological systems, and created by Neal et al in 1998 [99]. ((Be that as it may, one of the primary preferences of the AIS model is that the model just needs positive guides to prepare on, producing finders (ALCs) with negative selection method.)) Artificial Immune Systems (AIS) are a class of bio inspired versatile or learning algorithms, which incorporates the artificial immune acknowledgment system [39]; a supervised discovering that has indicated huge accomplishment on the characterization issue in the credit card fraud detection, and this method can take care of the grouping issue in neural network. In 2002, the Diary Nature published an article on AIS, where it demonstrated that the AIS had numerous kinds of utilizations, including the detection of fraudulent monetary exchanges. Also, the AIS detection motors actualizes the AIS based algorithms which can group input information as typical or fraudulent. ((The system discretionarily produces an ALC, test it against the arrangement of self-examples and in the event that it doesn't coordinate any of oneself examples, it is incorporated into the arrangement of develop ALCs. The AIS comprises of artificial-lymphocytes (ALCs) that ready to characterize any example as self or non-self by distinguishing just non-self-examples.)) And The AIS has effectively been utilized in PC security to identify network interruption, clustering information for the information mining, distinguishing PC infections, and idea learning. Then, the Abnormal state model of AIS has been connected for credit card fraud detection that was affected principally by Hofmeyr and Forrest (1999) and Wightman (2003) .The fundamental improvements inside AIS have concentrated on five principle immunological theories: clonal selection, immune networks, danger theory, hybrid AIS and negative selection.

Advantage:

High capacity in example acknowledgment/ amazing in Learning and memory/ Self-association/ simple in coordination with different frameworks/progressively evolving inclusion/self-Identity/multi-layered/has decent variety/ clamour resilience/ adaptation to internal failure/ predator-prey elements/ Inexpensive/ no compelling reason to preparing stage in DCA.

Disadvantages:

Need high preparing time in NSA/ poor in handle missing information in Clonal G and NSA

3.The Data Sets

The referenced strategies in any field certainly need a noteworthy informational index to test upon it and inspect effectiveness in contrast with other related work. The absence of an openly accessible database has been a restricting component for the distributions of money related to misrepresentation recognition, especially Visa

Table 1: Datasets Used By Researchers For Artificial Neural Network

Technique	Source Of Data	Data Sets Sizes	Advantages	Dis Advantages
Artificial Neural Network	Mellon Bank (Real Data set)	About 1,100,000 of transactions/ Which Licenced in a period of 8 weeks – 2 Months [47]	Capacity to gain from an earlier time/ absence of should be reinvented/Ability to concentrate runs and anticipate future exercises dependent on the present circumstance/ High precision/ Portability/ fast in discovery/ the capacity to create code to be utilized progressively frameworks/ the effortlessness to be fabricated and worked/Effectiveness in managing loud information, in foreseeing designs, in taking care of complex issues, and in handling new occasions/ Adaptability/ Maintainability / (information)	Trouble to affirm the structure/high preparing time for huge neural systems furthermore, inordinate preparing/poor clarification capacity/hard to set up and work/ high cost/ non-numerical information should be changed over and standardized/Sensitivity to information design.
	Synthetically generated data	These data were extracted into a flat file from SQL server database which contain sample oftransactions of Visa Card and at that point proceeded.[21]		
	Vesta Corporation (Vestacorporation is aninnovator and worldwide leader in virtual commerce (Real Data set)	Exactly 206,541 different transactions, 204,078 Of them are Tyical and The other 2463 are fake fraudulent [17]		

TABLE II :Datasets Used By Researchers For Artificial Immune System

Technique	Source Of Data	Data Sets Sizes	Advantages	Dis Advantages
Artificial Immune System	Big Brazilian bank, its registers within The time between Jul/14/2004 - Sep/12/2004. (Real Data set)	Exactly 41647 financial transactions with 3.14% fake fraudulent transactions [50]	High capacity in example acknowledgment/ amazing in Learning and memory/ Self-association/ simple in coordination with different frameworks/progressively evolving inclusion/self-Identity/multilayered/has decent variety/ clamor resilience/ adaptation to internal failure/ predator-prey elements/ Inexpensive/ no compelling reason to preparing stage in DCA.	Need high preparing time in NSA/ poor in handle missing information in Clonal G and NSA
	Financial institute in Ireland (WebBiz) (Real Data set)	More than 4 million credit card transactions from462279 unparalleledclient , 5417 of them are fake fraudulent transactions [19]		
	Large Australian bank (Real Data set)	Total of 640361 different transactions, of 21746 different credit cards [51]		

TABLE III :Datasets Used By Researchers For Genetic Algorithm

Technique	Source Of Data	Data Sets Sizes	Advantages	Dis Advantages
Genetic Algorithm	Synthetically generated data	320000000 different transactions of 1050 credit card with different 42 different features [49]	Functions admirably with boisterous information/simple to coordinate with other frameworks/ typically consolidated into different systems to increment the presentation of those strategies, and enhance their parameters/ simple in manufacture and work/ quick in identification/ Versatility/ Maintainability/ information disclosure and information emulating.	Requires broad device learning to set up. Furthermore, work and hard to get it.
	Synthetically generated data	About 1000000 transactions with 20 different features [25]		

Table IV : Data Sets Used By Researchers In Another Data Mining Techniques:

Data mining techniques	First Union Bank and Chase Bank (Real Data set)	Each bank provided 500,000 Of records traversing one year With 20% fraud and 80% non fraud distribution for Chase Bank/ 15% versus 85% for First Union Bank [48]
	Synthetically generated data	10000 financial transaction [41]
Artificial Neural Network tuned by genetic algorithm/ Data mining techniques	Hong Kong bank, registers within the time between January2006- January 2007 (13month) (Real Data set)	More about 50 million transactions of credit cards on more onemillion (1,167,757 credit cards) credit cards from One country [42]
Multiple criteria linear programming	Major US bank (Real Data set)	More than 6000 credit card data with 64 indicator variables plus 1class variable, 84% of these data were just normal accounts and the other 16% were false records or fraudulent accounts [52]

4. Comparison Of The Used Techniques

We Present A Comparison of 14 recent different techniques used in the fraud credit card detection, Due to the study of Masoumeh Zareapoor,Seeja.K.R and M.Afshar.Alam "Analysis of Credit Card Fraud Detection Techniques: based on Certain Design Criteria" They classified the techniques in the following, Most High Accuracy techniques were Fuzzy Darwin System, with very low detection speed and expensive cost , The Bayesian Network, with very high speed and expensive too, Case Based Reasoning a Medium cost and high speed Technique and The Logistic Regression with high speed and low general cost. Other Systems Represents Good Accuracy like Artificial Immune System, a very high speed and low general cost system, and Fuzzy Neural Network a very high speed and high cost system. Either Techniques like: The Neural Network, a high speed and cost, The Decision Tree too, K-Nearest Neighbor with medium speed and high cost, Support Vector Machine, slow and costly high, The Self-Organizing Map, high speed also high cost and The Genetic Algorithm which costs low and with medium speed shows Medium Accuracy, The rest Of techniques like Hidden Makrov Model, a high speed and high cost technique, The Back Propagation, which is slow and costly high Expert System, The Inductive Logic Programming, medium cost/speed Technique and The Outlier Detection , All of them represented Low Accuracy.

5. Conclusion

We present in this Study a relative investigation of Fifteen different misrepresentation identification techniques dependent on credit card (Neural Network, Decision Tree, genetic algorithm, case Based Reasoning, Bayesian Network, Support Vector Machine, K-nearest neighbor and Artificial Immune System, Hidden Markov Model, fuzzy neural network and fuzzy Darwinian system , Inductive Logic programming , Clustering Techniques, Logistic Regression, and Outlier Detection). The fundamental goal of this research is to survey procedure of various discovery techniques dependent on Visa. By considering the most significant parameter in various techniques, Like the exactness, the Method speed and its cost. An examination table of comparison was set up so as to look at different charge card misrepresentation identification instruments. Every one of the strategies of charge card extortion recognition depicted in table 1 has its very own qualities and shortcomings. We found this outcome is referenced in following table from the references that we have referenced in end. Also, we detect the advantages and the disadvantages of every technique used for them to have its good point and its weakness.

A table was set to differentiate the data sets used on the different researches too, to detect the accuracy and efficiency of every system used.

References

[1] KhyatiChaudhary, JyotiYadav, BhawnaMallick, " A review of Fraud Detection Techniques: Credit Card", International Journal of Computer Applications Volume 45– No.1 2012.

[2] Michael Edward Edge, Pedro R, Falcone Sampaio, "A survey of signature based methods for financial fraud detection", journal of computers and security, Vol. 28, pp 3 8 1 – 3 9 4, 2009.

[3] Linda Delamaire, Hussein Abdou, John Pointon, "Credit card fraud and detection techniques: a review", Banks and Bank Systems, Volume 4, Issue 2, 2009.

[4] Salvatore J. Stolfo, David W. Fan, Wenke Lee and Andreas L. Prodromidis, "Credit Card Fraud Detection Using Meta-Learning: Issues and Initial Results"; Department of Computer Science- Columbia University; 1997.

[5] Maes S. Tuyls K. Vanschoenwinkel B. and Manderick B., "Credit Card Fraud Detection Using Bayesian and Neural Networks"; Vrije University Brussel – Belgium; 2002.

[6] Andreas L. Prodromidis and Salvatore J. Stolfo; "Agent-Based Distributed Learning Applied to Fraud Detection"; Department of Computer Science- Columbia University; 2000.

[7] Salvatore J. Stolfo, Wei Fan, Wenke Lee and Andreas L. Prodromidis; "Cost-based Modeling for Fraud and Intrusion Detection: Results from the JAM Project"; 0-7695-0490-6/99, IEEE 1999.

[8] Soltani, N., Akbari, M.K., SargolzaeiJavan, M., "A new user-based model for credit card fraud detection based on artificial immune system," Artificial Intelligence and Signal Processing (AISP), 2012 16th CSI International Symposium on., IEEE, pp. 029-033, 2012.

[9] S. Ghosh and D. L. Reilly, "Credit card fraud detection with a neural-network", Proceedings of the 27th Annual Conference on System Science, Volume 3: Information Systems: DSS/ Knowledge- Based Systems, pages 621-630. IEEE Computer Society Press, 1994.

[10] MasoumehZareapoor, Seeja.K.R, M.Afshar.Alam, "Analysis of Credit Card Fraud Detection Techniques: based on Certain Design Criteria", International Journal of Computer Applications (0975 – 8887) Volume 52– No.3, 2012.

[11] Fraud Brief – AVS and CVM, Clear Commerce Corporation, , http://www.clearcommerce.com, 2003.

[12] All points protection: One sure strategy to control fraud, Fair Isaac, http://www.fairisaac.com, 2007.

[13] Clear Commerce fraud prevention guide, Clear Commerce Corporation, http://www.clearcommerce.com, , 2002

[14]RaghavendraPatidar, Lokesh Sharma, "Credit Card Fraud Detection Using Neural Network", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1, 2011.

[15] M.JeevanaSujitha, K. RajiniKumari, N.Anuragamayi, "The Credit Card Fraud Detection Analysis With Neural Network Methods", IJCST Vol. 3, Issue 1, Spl. 5, Jan. - March 2012.

[16] A. Krenker, M. Volk, U. Sedlar, J. Bester, A. Kosh, "Bidirectional Artificial Neural Networks for Mobile-Phone Fraud Detection," Journal of Artificial Neural Networks, Vol. 31, No. 1, pp. 92-98, 2009.

[17] John Zhong Lei, AliA.Ghorbani, "Improved competitive learning neural networks for network intrusion and fraud detection ",Neuro computing 75135–145. (2012)

[18] S. Hofmeyr. "An immunological model of distributed detection and its application to computer" security. PhD thesis, University Of New Mexico, 1999.

[19] A. Brabazon, et.al. "Identifying Online Credit Card Fraud using Artificial Immune Systems", IEEE Congress on Evolutionary Computation (CEC), Spain, 2011

[20] M. Gadi, X. Wang, A. Lago, "Credit Card Fraud Detection with Artificial Immune System", Springer, 2008 Van der Geer, J., Hanraads, J. A. J., & Lupton, R. A. The art of writing a scientific article. Journal of Science Communication, 163, 51–59. (2000).

[21] J. Tuo, S. Red, W. Lid, X. Li. B. Li, L. Lei, "Artificial Immune System for Fraud Detection", 3th International Conference on Systems, Man and Cybernetics, pp 101-107, 2004.

[22] N. Wong, P. Ray, G. Stephens, L. Lewis, "Artificial Immune Systems for Detection of Credit Card Fraud: an Architecture, Prototype and Preliminary Results," Journal of Information Systems, Vol. 22, No.1, pp. 53–76, 2012.

[23] James V. Hansena, , Paul Benjamin Lowrya, Rayman D. Meservya, , Daniel M. c Donald ," Genetic programming for prevention of cyber terrorism through dynamic and evolving intrusion detection "Journal Decision Support Systems, Volume 43, Issue 4, , Pages 1362–1374, August 2007.

[24] EkremDuman, M. HamdiOzcelik," Detecting credit card fraud by genetic algorithm and scatter search", Expert Systems with Applications 38 13057–13063. (2011)

[25] K.RamaKalyani, D.UmaDevi," Fraud Detection of Credit Card Payment System by Genetic Algorithm", International Journal of Scientific & Engineering Research Volume 3, Issue 7, -2012.

[26] Abhinav Srivastava, AmlanKundu, ShamikSural, Arun K. Majumdar. "Credit Card Fraud Detection using Hidden Markov Model", IEEE Transactions on dependable and secure computing, Volume 5 (37-48), ; (2008)

[27] Anshul Singh, Devesh Narayan "A Survey on Hidden Markov Model for Credit Card

Fraud Detection”, International Journal of Engineering and Advanced Technology (IJEAT) Volume-1, Issue-3; (49-52) , (2012)..

[28] B.SanjayaGandhi ,R.LaluNaik, S.Gopi Krishna, K.lakshminadh “Markova Scheme for Credit Card Fraud Detection”. International Conference on Advanced Computing, Communication and Networks; (144-147), (2011).

[29] S. Benson Edwin Raj, A. Annie Portia “Analysis on Credit Card Fraud Detection Methods”. IEEE-International Conference on Computer, Communication and Electrical Technology (152-156), ; (2011).

[30] V. Bhusari, S. Patil, “Application of Hidden Markov Model in Credit Card Fraud Detection”, International Journal of Distributed and Parallel Systems (IJDPS) Vol.2, No.6, November (2011)

[31]Siddhartha Bhattacharyya, SanjeevJha, KurianTharakunnel, J. Christopher Westland “Data mining for credit card fraud: A comparative study”. Elsevier, Decision Support Systems 50; (602–613), (2011).

[32] P. Ravisankar, V. Ravi, G. RaghavaRao, I. Bose, “Detection of financial statement fraud and feature selection using data mining techniques” , Decision Support Systems 50 491–500. (2011)

[33] Y. Sahin and E. Duman,” Detecting Credit Card Fraud by Decision Trees and Support Vector Machines”, proceeding of international multi-conference of engineering and computer statistics Vol. 1, 2011.

[34] Qibei Lu, ChunhuaJu, “Research on Credit Card Fraud Detection Model Based on Class Weighted Support Vector Machine”, Journal of Convergence Information Technology, Vol. 6, Number 1, 2011.

[35] Inigo Monedero, Felix Biscarri, Carlos Leon, Juan I. Guerrero, Jesus Biscarri, RocioMillan, “Detection of frauds and other non-technical losses in a power utility using Pearson coefficient, Bayesian networks and decision trees”, journal of Electrical Power and Energy Systems 34 pp 90–98. (2012)

[36] SuvasiniPanigrahi, AmlanKundu, ShamikSural, A.K. Majumdar “Credit card fraud detection: A fusion approach using Dempster–Shafer theory and Bayesian learning”. Elsevier, Information Fusion10; (354–363), (2009).

[37] Lee KC, Jo NY. Bayesian network approach to predict mobile churn motivations: emphasis on general Bayesian network, Markov blanket, and what-if simulation, LNCS, 6284;, pp 304–13, 2010.

[38] Riascos LAM, Simoes MG, Miyagi PE. A Bayesian network fault diagnosis system for proton membrane exchange fuel cells. J. Power Sources; 165:267–78 2007

[39] M.R. Harati Nik, "FUZZGY: A hybrid model for credit card fraud detection", Sixth International Symposium on Telecommunications (IST),PP. 1088 - 1093, 2012.

[40] Adnan M. Al-Khatib, “Electronic Payment Fraud Detection Techniques”, World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 2, No. 4, 137-141, 2012.

[41] T. Guo, G.yang LI, “neural data mining for credit card fraud detection”, Proceedings of the Seventh International Conference on Machine Learning and Cybernetics, 2008.

[42] C. Paasch, Credit Card Fraud Detection Using Artificial Neural Networks Tuned by Genetic Algorithms, Hong Kong University of Science and Technology (HKUST), Hong Kong, Doctoral Dissertation, 2007.

[43]Kim, M., & Han, I. The discovery of experts’ decision rules from qualitative bankrupcy data using genetic algorithms. Elsevier, Expert Systems with Applications., 25; (637–646) (2003).

[44] Joseph Pun, Yuri Lawryshyn “Improving Credit Card Fraud Detection using a Meta-Classification Strategy”International Journal of Computer Applications (0975 – 8887)Volume 56– No.10, October 2012.

[45]S. Maes, K. Tuyls, B. Vanschoenwinkel, B. Manderick “Credit card fraud detection using Bayesian and neural networks”. Proceedings of the First International NAISO Congress on Neuro Fuzzy Technologies; (261-270), (1993).

[46]Nicholas Wong, Pradeep Ray, Greg Stephens & Lundy Lewis). “Artificial immune systems for the detection of credit card fraud”. Info Systems, Volume 22; (53–76). (2012)

[47]Sushmito Ghosh, Douglas L. Reilly:Credit Card Fraud Detection with a Neural-Network. HICSS (3): 621-630 1994.

[48]Philip Chan profile imagePhilip K. ChanDistributed Data Mining in Credit Card Fraud Detection, Wei imageWei FanAndreas Leonidas Prodromidis L. ProdromidisSalvatore Stolfo profile imageSalvatore J. StolfoPublication:IEEE Intelligent SystemsNovember 1999.

[49] M. Hamdiozcelik et al.Detecting credit card fraud by genetic algorithm and scatter search Expert Systems with Applications 38(10):13057-13063 · September 2011.

[50] Manoel Fernando Alonso Gadi,Credit Card Fraud Detection with Artificial Immune SystemInternational Conference on Artificial Immune SystemsICARIS: Artificial Immune Systems pp 119-131.(2008).

[51] 76Nicholas Wong, Pradeep Ray, Greg Stephens& Lundy Lewis†Artificial immune systems for the detectionof credit card fraud: an architecture,prototype and preliminary resultsisj_369 53.2011.

[52] Microarray and RT-PCR screening for white spot syndrome virus immediate-early genes in cycloheximide-treated shrimp Wang-JingLiuaYun Shiang Changa Chung-Hsiung Virology Volume 334, Issue 2, Pages 327-341 10 April 2005.