Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 7, July 2021: 14085-14098

Prediction and detection analysis of bank credit card fraud using regression model: novel approach.

Varsha yadav 1 ***(Author)***
Dept. of management and finance,
Amity business school,
Amity University, Gurugram.
Varshayadav283@gmail.com

Prof. Dr. Rishi Manrai[2] (*guide),*
Assistant professor (Senior Grade)
Dept. of management and finance
Amity business school,
Amity University, Gurugram. rmanrai@ggn.amity.edu.

Abstract— financial institutions are interested in ensuring security and quality for their customers. Banks, for instance, need to identify and stop harmful transactions in a timely manner. In order to detect fraudulent operations, data mining techniques and customer profile analysis are commonly used. Thus, we propose EVA, a Visual Analytics approach for supporting fraud investigation, fine-tuning fraud detection algorithms, and thus, reducing false positive alarms. Due to the theatrical increases of fraud which results in loss of dollars worldwide each year, several modern techniques in detecting fraud are persistently evolved and applied to many business fields. The goal of this paper is to provide a security in credit card transaction using EVA technique to detect fraud. The credit card fraud detection features uses user behavior and location scanning to check for unusual patterns.

Nowadays, the use of credit cards has significantly increased on both online and offline purchases because of the fast growth of the e-commerce and online banking system. When Someone uses other persons credit card for personal benefit without the knowledge of the owner of the credit card is known as credit card fraud. The Association of Certified Fraud Examiners defines a fraud as "the use of one's occupation for personal enrichment through the deliberate Misuse or application of the employing organization's resources or assets" [63]. Individual's and government suffer large financial losses across the world every year due to the lack of sophisticated fraud detection system.

***Index Terms*— Large vessel vasculitis, Polymyalgia rheumatic, FDG-PET/CT (A), Imaging procedure,** etc.

SOURCES OF DATA

This review is based on the published academic articles as well as our statistical analysis and regression analysis experience.

BACKGROUND:

Any business or organization that intends to be far from bankruptcy or crime strives daily to ensure

crime perpetration does not occur in the organization unabated. Traditional methods of fraud detection in credit administration are available but limited in capacity to check current sophistication in fraud perpetration; those approaches did not offer the best for time-consumption and efficiency; also, frauds are better predicted rather than a detection after the deal is done. This work presents an extensive review of literature and related works in fraud prediction in credit administration. The primary focus of this research work is to identify and dwell on the major concepts and techniques used for financial fraud prediction in credit administration as well as related works that have been done in this domain of study; while the work recommends the ensemble approach as a better alternative in this domain. The existing systematic literature reviews in this domain are not in the context of credit fraud prediction alone

INTRODUCTION

In the last decade, credit card fraud has started to pose a great threat to the businesses all over the worldwide and it seems to make an impact on the economy. It has become very important for business organizations to counter these credit card frauds effectively, for which understanding the credit cards is considered to be equally important. Fig.1 Credit Card Frauds Worldwide (The Nelson Report, 2016) Credit card frauds make a greater impact on the merchants when compared to the consumers; merchants are considered to face more risks in the credit card transactions. While consumers may face trouble trying to get a fraudulent charge reversed, merchants lose the cost of the product sold, pay chargeback fees, and fear from the risk of having their merchant account closed. Increasingly, the card not present scenario, such as shopping on the internet poses a greater threat as the merchant (the web site) is no longer protected with advantages of physical verification such as signature check, photo identification, etc. In fact, it is almost

impossible to perform any of the ‘physical Coronary artery Disease is the leading cause of left Ventricular systolic dysfunction which is the hallmark of heart failure with reduced Ejection Fraction [1, 4,6-8]. World’ checks necessary to detect who is at the other end of the transaction. This makes the internet extremely attractive to fraud perpetrators. According to a recent survey, the rate at which internet fraud occurs is 12 to 15 times higher than ‘physical world’ fraud. However, recent technical developments are showing some promise to check fraud in the card not present scenario.

CREDIT CARD FRAUD Joshi (2006) defines credit card fraud as “Unauthorized account activity by a person for which the account was not intended. Operationally, this is an event for which action can be taken to stop the abuse in progress and incorporate risk management practices to protect against similar actions in the future” (Baesens, Vlasselaer & Verbeke, 2015). In simple terms, Credit Card Fraud is defined as when an individual uses another individual s credit card for personal reasons while the owner of the card and the card issuer are not aware of the fact that the card is being used. And the persons using the card has not at all having the connection with the cardholder or the issuer and has no intention of making the repayments for the purchase they done (Namdev, Kumar & Bansal, 2015). Maes, et.al. (2002) and Ogwueleka (2008) defines credit card fraud detection as the process of identifying the legitimate transactions and fraudulent transactions.

prediction and detection analysis of bank credit card fraud using regression model: novel approach.

With the rise and swift growth of E-Commerce, credit card uses for online purchases has increased dramatically and it caused sudden outbreak in the credit card fraud. Fraud is one of the major ethical issues in the credit card industry. With both online as well as regular purchase, credit card becomes the most popular mode of payment with cases of fraud associated with it are also increasing. A clear framework on all these approaches will certainly lead to an efficient credit card fraud detection system. Currently, for simplicity reasons, all the base learners for credit card fraud detection use the same desired distribution. It would be interesting to implement and evaluate the credit card fraud detection system by using very large databases with skewed class distributions and non-uniform cost per error. This paper presents a analysis of cost incurred in credit card fraud detection on data set.

Fig.1 Credit Card Frauds Worldwide (The Nelson Report, 2016)

CREDIT FRAUD: OVERVIEW

Figure 2: credit card transaction steps

DIFFERENT TYPES OF CREDIT CARD FRAUDS

Bhatla, Prabhu & Dua (2003) classifies credit card frauds into 3 major categories such as traditional card related frauds, merchant related frauds, and internet frauds. Frauds related to traditional cards like counterfeit, application, application etc, internet frauds line generation of credit cards, fake merchant sites etc and frauds related to merchants like triangulation, merchant collusion etc are the three categories involved in credit card frauds.

MERCHANT RELATED FRAUDS

Merchant related frauds are initiated either by owners of the merchant establishment or their employees. The types of frauds initiated by merchants are described below:

i. Merchant Collusion: This type of fraud occurs when merchant owners or their employees conspire to commit fraud using the cardholder accounts or by using the personal information. They pass on the information about cardholders to fraudsters.

Triangulation: Triangulation is a type of fraud which is done and operates from a web site. The products or goods are offered at heavily discounted rates and are also shipped before payment. The customer while browse the site and if he likes the product he place the online information such as name, address and valid credit card details to the site. When the fraudsters receive these details, they order goods from a legitimate site using stolen credit card details. The fraudsters then by using the credit card information purchase the products.

INTERNET RELATED FRAUDS

The internet is the base for the fraudsters to make the frauds in the simply and the easiest way. Fraudsters have recently begun to operate on a truly transnational level. With the expansion of trans-border, economic and political spaces, the internet has become a new worlds market, capturing consumers from most countries around the world. The below described are most commonly used techniques in Internet fraud: i. Site cloning: Site cloning is where fraudsters close an entire site or just the pages from which the customer made a purchase. Customers have no reason to believe they are not dealing with the company that they

Some sites often offer a cheap service for the customers. That site requests the customer to fill his complete details such as name and address to access the webpage where the customer gets his required products. Many of these sites claim to be free, but require a valid credit card number to verify an individual s age. These kinds of sites in this way collect as many as credit card details. The sites themselves never charge individuals for the services they provide. The sites are usually part of a larger criminal network that either uses the details it collects to raise revenues or sells valid credit card details to small fraudsters.

CREDIT CARD GENERATORS

These are the computer programs that generate valid credit card numbers and expiry dates. These generators work by generating lists of credit card account numbers from a single account number. The software works by using the mathematical Luhn algorithm that card issuers use to generate other

valid card number combinations. This makes the user to allow to illegally generating as many numbers as he desires, in the form of any of the credit card formats.

ERASING THE MAGNETIC STRIP

This is the type of the fraud where the fraudsters erase the magnetic stripe by using the powerful electro-magnet. The fraudster then tampers with the details on the card so that they match the details of a valid card, which they may have attained, for example, when the fraudster begins to use the card, the cashier will swipe the card through the terminal several times, before realizing that the metallic strip does not work. The cashier will then proceed to manually input the card details into the terminal. This kind of fraud is having high risk.

CREATING A FAKE CARD

Today we have sophisticated machines where one can create a fake card from using the scratch. This is the common fraud though fake cards require a lot of effort and skill to produce it. Modern cards are having many security features, all designed to make it difficult for fraudsters to make good quality fraudulent. After introducing the Holograms in the credit cards it makes very difficult to forge them effectively.

REVIEW OF LITERATURE, ROL:

Since last two decades, research on the data mining techniques for credit card fraud detection has been started; Chan, et.al. (1999) addressed the growing credit card transactions in the US payment system that is considered to be leading to greater stolen credit card accounts. In the early years of credit card usage, banks faced a huge problem in analysing massive amounts of transaction data that efficiently compute fraud detectors in a timely manner. There are also several problems associated with the skewed distributions of training data and non-uniform cost per error. Chan, et.al (1999) conducted a study to address the three most important problems associated with the credit card transactions especially in e-commerce such as scalability, efficiency and technical issues. Chan, et.al (1999) proposed a fraud detection model that has the combination of multiple fraud detectors referred as distributed data mining of models demonstrates a significant reduction in credit card frauds.

FRAUD DETECTION METHODS

On doing the literature survey of various methods for fraud detection we come to the conclusion that to detect credit card fraud there are multiple approaches like

- **REGRESSIN MODEL.**
- **Bayesian networks**
- **Hidden markov model**
- **Genetic algorithm**
- **A fusion approach using dempster shafer theory and bayesian learning.**

- **Machine learning and AI .**
- **Neural network**
- **Logistic Regression**

Difficulties of Credit Card Fraud Detection Fraud detection systems are prune to several difficulties and challenges enumerated bellow. An effective frauddetection technique should have abilities to address these difficulties in order to achievebest performance. • Imbalanced data:The credit card fraud detection data has imbalanced nature. It means thatvery small percentages of all credit card transactions are fraudulent. This cause the detection of fraud transactions very difficult and imprecise. • Different misclassification importance: in fraud detection task,

different misclassification errors have different importance.Misclassification of a normal transaction asfraud is not as harmful as detecting a fraud transaction as normal. Because in the first case the mistake in classification will be identified in further investigations. • Overlapping data: many transactions may be considered fraudulent, while actually they are normal (false positive) and reversely, a fraudulent transaction may also seem to be legitimate (false negative). Hence obtaining low rate of false positive and false negative is a key challenge of fraud detection systems[4, 5, and 6]. • Lack of adaptability: classification algorithms are usually faced with the problem of detecting new types of normal or fraudulent patterns. The supervised and unsupervised fraud detection systems are inefficient in detecting new patterns of

normal and fraud behaviors, respectively. • Fraud detection cost: The system should take into account both the cost of fraudulent behavior that is detected and the cost of preventing it. For example, no revenue is obtained by stopping a fraudulent transaction of a few dollars [5, 7].

PROPOSED METHODOLOGY:

Artificial Immune System (AIS) the natural immune system is a highly complex system, comprised of an intricate network of specialized tissues, organs, cells and chemical molecules. These elements are interrelated and act in a highly co- ordinate and specific manner when they recognize, remember disease causing foreign cells and eliminate them. Any element that could be recognized by the immune system is named an antigen. The immune system‟s detectors are the antibodies that are capable to recognition and destruction harmful and risky antigens [27]. The immune system consists of the two main response of immune and defense: innate immune response and acquired immune response. The body‟s first response for defense is made of the outer, unbroken skin and the „mucus membranes‟ lining internal channels, such as the respiratory and digestive tracts. If the harmful cells could pass through innate immune defense the acquired immunity will defense. In fact, adaptive immune response performs based on antigen-specific recognition of almost unlimited types of infectious substances, even if previously unseen or mutated. It is worth mentioning that the acquired immune response is capable of “remembering” every infection, so that a second exposure to the same pathogen is dealt with more efficiently.

Negative Selection: Negative Selection Algorithm or NSA proposed by [34] is a change detection algorithm based on the T-Cells generation process of biological immune system. It is one of the earliest AIS algorithms applied in various real-world applications. Since it was first conceived, it has attracted many researchers and practitioners in AIS and has gone through some phenomenal evolution. NSA has two stages: generation and detection. In generation stage, the detectors are generated by some random process and censored by trying to match self-samples. Those candidates that match (by affinity of higher than affinity threshold) are eliminated and the rest are kept as detectors. In detection stage, the collection of detectors (or detector set) is used in checking whether an incoming data instance is self or non-self. If it matches (by affinity of higher than affinity threshold) any detector, it is claimed as non-self or anomaly. Brabazonet.al [35] proposed an AIS based model for online credit card fraud detection. Three AIS algorithms were implemented and their performance was standardized against a logistic regression model. Their three chosenalgorithms were the unmodified negative selectionAlgorithm, the modified negative selection algorithm andthe Clonal selection algorithm.They proposed the Distance Value Metric for calculating distance between records. This metric is based on the probability of data occurrence in the training set. Where the detection rate increased, but the number of false alarms and missed frauds remained.

2 Clonal selection: Clonal selection theory is used by the immune system to explain the basic features of an immune response to an antigenic stimulus. The selection mechanism guarantees that only those clones (antibodies) with higher affinity for the encountered antigen will survive. On the basis of clonal selection principle, clonal selection algorithm was initially proposed in [36] and formally explained in [37]. The general algorithm was called CLONALG. Gadiet.al in

[36] applied the AIRS in fraud detection on credit card transactions. AIRS is a classification algorithm that is based on AIS whichapplies clonal selection to create detectors.AIRS generatesdetectors for all of the classes in the database and in detectionstage uses k Nearest Neighbor algorithm (also called K-NN)in order to classify eachrecord.They compared their method with other methods like the neural networks, Bayesian networks, and decision trees and claimed that, after improving the input parameters for all the methods, AIRS has show the best results of all, partly perhaps since the number of input parameters for AIRS is comparatively high.

3 Immune Network: The nature immune system is applied through the interactions between a huge numbers of different types of cells. Instead of using a central coordinator, the nature immune systems sustain the appropriate level of immune responses by maintaining the equilibrium status between antibody suppression and stimulation using idiotypes and paratopes antibodies [38],

[39].The first Artificial Immune Network (AIN) proposed by [40]. Neal M.et.al [41] introduced the AISFD, which adopted thetechniques developed by CBR (case based reasoning) communityand applied various methods borrowed from genetic algorithm andother techniques to clone the B cells (network nodes) for mortgage fraud detection.

Danger Theory: The novel immune theory, named Danger Theory was proposed in 1994 [42]. It embarked from the concept that defined "self-non-self" in the traditional theories and emphasizes that the immune system does not respond to "non-self" but to danger. According to the theory a useful evolutionarily immune system should focus on those things that are foreign and dangerous, rather than on those that are simply foreign [43]. Danger is measured by damage inflicted

to cells indicated by distress signals emitted when cells go through an unnatural death (necrosis). Dendritic cells (DCs), part of the innate immune system, interact with antigens derived from the host tissue; therefore, the algorithm inspired by Danger Theory is named Dendritic cell algorithm. Dendritic cells control the state of adaptive immune system cells by emitting the following signals: • PAMP (pathogen associated molecular pattern) • Danger • Safe • Inflammation

Bank credit card fraud detection using regression analysis

Hybrid AIS or methods Some researchers applied different algorithms (i.e. vaccination algorithm, CART and so on) by AIS algorithm which are presented below: Wong presents the AISCCFD prototype proposed to measure and manage the memory population and mutate detectors in real time. In their work both the two algorithms the vaccination and negative selection were combined. The results were tested for different fraud types. The proposed method demonstrated higher detection rates when vaccination algorithm was applied, but it failed to detect some types of fraud precisely. Huang et.al [45] presented a novel hybrid Artificial Immune inspired model for fraud detection by combining triplealgorithms: CSPRA, the dendritic cell algorithm (DCA), and CART. Though their proposed method had high detection rate and low false alarm, their approach was focused on logging data and limited to VoD (video on demand) systems and not credit card transactions. Ayaraet.al [46] applied AIS to predict failures of ATM1 . Their approach is enriched by adding a generation of new antibodies from the antigens that correspond to the unpredicted failures.

Hidden Markov Model (HMM) A Hidden Markov Model is a double embedded stochastic process which is applied to model much more complicated stochastic processes as compared to a traditional Markov model. The underlying system is assumed to be a Markov process with unobserved states. In simpler Markov models like Markov chains, states are definite transition probabilities are only unknown parameters. In contrast, the states of a HMM are hidden, but state dependent outputs are visible. In credit card fraud detection a HMM is trained for modeling the normal behavior encoded in user profiles [52]. According to this model, a new incoming transaction will be classified to fraud if it is not accepted by model with sufficiently high probability.Each user profile contains a set of information about last 10 transactions of that user liketime; category and amount of for each transaction [52, 53, and 54].HMM produces high false positive rate [55].V. Bhusari et al. [56] utialized HMM for detecting credit card frauds with low false alarm. The proposed system was also scalable for processing huge number of transactions. HMM can also be embedded in online fraud detection systems which receive transaction details and verify whether it is normal or fraudulent.If the system confirms the transaction to be malicious, an alarm is raised and related bank rejects that transaction. The responding cardholder may then be informed about possible card misuse.

Bayesian Network A Bayesian network is a graphical model that represents conditional dependencies among random variables. The underlying graphical model is in the form of directed acyclic graph. Bayesian networks are

usefulfor finding unknown probabilities given known probabilitiesin

the presence of uncertainty [66]. Bayesian networks can play an important and effective role in modeling situations where some basic information is already known but incoming data is uncertain or partially unavailable [67], [68], [69].The goal of using Bayes rules is often the prediction of the class label associated to a given vector of features or attributes [70].Bayesian networks have been successfully applied to various fields of interest for instance churn prevention[71] in business,pattern recognition in vision[72], generation of diagnostic in medicine[73]and fault diagnosis [74] as well as forecasting [75] in power systems.Besides, these networks have also been used to detect anomaly and frauds in credit card transactions or telecommunication networks [76, 77, and 5].

Inductive logic programming (ILP) ILP by using a set of positive and negative examples uses first order predicate logic to define a concept. This logic program is then used to classify new instances. Complex relationship among components or attributes can be easily expressed,in this approach of classification.The effectiveness of the system improves by domain knowledge which can be easily represented in an ILP system [87].Muggleton et al.[88] proposed the model applying labeled data in fraud detection which using relational learning approaches such as Inductive Logic Programming (ILP) and simple homophilybased classifiers on relational databases. Perlich, et al. [89] also propose novel target-dependent detection techniques for converting the relational learning problem into a conventional one. 4.10 Case-based reasoning (CBR) Adapting solutions in order to solve previous problems and use them to solve new problems is the basic idea of CBR. In CBR, cases introduce as descriptions of past experience of human specialists and stored in a database which uses for later retrieval when the user encounters a new case with similar parameters. These cases can apply for classification purposes. A CBR system attempts to find a matching case when face with a new problem. In this method the model defined as the training data, and in test phase when a new case or instance is given to the model it looks in all the data to discover a subset of cases that are most similar to new case and uses them to predict the result. Nearest neighbor matching algorithm usually applied with CBR, although there are several another algorithms which used with this approach such as [90]. Case-based reasoning is well documented both as the framework for hybrid frauddetection systems and as an inference engine in [91].

Bank credit card fraud detection using regression analysis

STATISITCAL ANALYSIS BY SPSS SIMULATION TOOL:

Statistical analysis was performed using IBM SPSS version 20.0 software. Categorical variables were expressed using frequency and percentage. Numerical variables were presented using mean and standard deviation. Chi-square test was used to test the statistical significance of the association of all Demographic and clinical parameters between management groups. A p value of <0.05 is considered to be statistically significant.

Data set and evaluation The mentioned methods in any field definitely need a creditable data set to test upon it, and examine efficiency in compare to other‟s related work. The lack of publicly available database has been a limiting factor for the publications on financial fraud detection [36], particularly credit card transactions. On the other hand, credit card is inherently private so, creating a proper data set for this purpose is very difficult and there are no standard techniques.

SAMPLE SIZE ESTIMATION:

The data description for credit card fraud detection in banking system have considered on the basis of unbalancing data along with excel format after that convert into CSV file. The research work done using KAGGLE real data set in form of rows and Tables format for detection and count of credit card fraud detection system.

The data description is also given below:

Real data set taken form KAGGLE sites along with form of excel and convert in to CSV files.

UN balancing data set taken after that we are going to convert in form of training and testing phase. Testing and training data set phase performed.

UN BALANCING DATA SET:

The UN balance data set simply perform the target variable for performing observation of class attributes for some cases. For credit card fraud detection the UN balancing data set also taken due to lot of transaction are there. The credit card fraud detection system using un balance data set keep tracks of transaction.

CREDIT CARD FRAUD DATA SET:

We are performing the following data set which is considered as KAGGLE sites. THE FOLLOWING REAL DATA SET is given below:

Credit card fraud data set considered for performing various operation on it.

Real data set in form of raw and tables.

UN balance data set perform the various detection.

Data set consist CSV file for performing simulation work details.

Credit card real data set is consisting various records in form of rows and column.

Step 1: Understanding and Cleaning Your Data. There are various approaches to move toward normalization, yet it comes down to being proactive toward the information that is going into your CRM framework.

- Step 2: Knowing the Data Entry Points.
- Step 3: Choosing Data Standards.
- Step 4: Defining the Normalization Matrix.

Data splitting is basically performed the data portion for two purpose.

Cross validation.

One is used for predictive model

Second one is evaluate for model performance.

The data splitting for credit card fraud detection have performed in tow partitions.

Training phase. It consist large portion of real data set.

Testing phase: it consist for small data set.

DATA RESAMPLING:

Data inspecting is a measurable investigation method used to choose, control and dissect a delegate subset of information focuses to recognize examples and patterns in the bigger informational index being analyzed. The resampling data set performed on the basis of credit card fraud detection on keep training and testing phase.

RESEARCH METHODOLOGY:

The research methodology considered hybrid model for performing fraud detection based on machine learning and artificial intelligence based module represented.

Fraud risk management in banks can be implemented using a classification credit card fraud detection model, which is built the following way:

- **Obtaining data samplings for the model estimation and preliminary testing;**
- **Model estimation;**
- **Testing stage and deployment.**

The goal of such model is to be able to distinguish the highest possible True Positive Rate (TPR) and the lowest possible False Positive Rate (FPR) in order to offer accurate forecast and fraud monitoring in banks.

Now, here's a kick – even a slight number of FPR cases in your classification model can result in a large number of incorrectly classified results. Your model will then classify both True Positive (indeed fraudulent transactions) and a certain amount of False Positive (honest transactions that may resemble fraudulent ones) as fraudulent activity. And then, you will have to manually recheck those incorrectly classified cases. No good, right?

So the prevention of frauds in banks starts with balancing and refining your data first. Next, to train your model even further, you can use different oversampling methods to balance the data you have at hand. (I've shared the techniques we used in the case study.)

Considering that you have already given your classifier model enough samples for the initial training, let's move on to the model estimation stage.

Bank credit card fraud detection using regression analysis

REGRESSION MODEL FOR CREDIT CARD FRAUD DETECTION:

To build analytical model, German credit card fraud dataset is taken consisting of 20 attributes out of which 7 are numerical attributes and 13 are categorical attributes and almost 1000 transactions . After doing preliminary data exploratory analysis on dataset for all attributes.

For Logistic Regression Model building the input dataset is divided into train Data and test Data. Below is code of model building.

- Model <- glm (Fraud ~., data = trainData, family =

  binomial) Predict <- predict (model, type = 'response', data=testData)

In this glm, logistic analytical model is used for fraud prediction. The fraud is responses variable and all other are predictors. Once model gets trained it is tested with the test data with threshold cut-off of 0.5 for prediction. The model is tuned by choosing most significant variables as shown below

- Function: model<-glm (Fraud~

  Status.of.existing.checking.account

  +Duration.in.months +Savings.account.bonds

  +Present.employment.since

CONCLUSION AND FUTURE WORK:

In this paper, various research papers based on credit card fraud are studied and discussedbased on the finding of these papers, the various credit card frauds are classified and among them,card-not-present fraud and skimming frauds are more frequently occurred.The fraudsters mostlyused website cloning, the false merchant website, and phishing methodology to steal credit carddetail.The challenges and issues to prevent and detect the fraud have also been discussed andidentified that one of the biggest issues is benchmark dataset which has unskewed, balanced and free from the anomaly and real-world dataset.. In this paper, techniques based on machine learning are discussed. The study can be extendedfor bio-inspired algorithms which have not explored in the paper and the result can becompared with traditional MLT. More effects can be made to get the real dataset from the creditcard issuing and managing organization, so that the exact techniques can be compared on thereal dataset.

In future, this work can further be extended on the enhancement of fraud detection techniques based on the detection accuracy, precision, MCC and improvement of fraud detection evaluation criteria. Security guidelines are needed for credit card users to make them aware of how to use and secure card details.

ACKNOWLEDGEMENTS

We would like to thank the team of the regression analysis.

AND SPSS SIMULATION TOOL SOFTWARE.

- ***Funding: No funding sources.***
- ***Conflict of interest: None declared***
- ***Ethical approval: Not required.***
- ***SPSS AALYSIS BY IBM TECHNIQUES.***

prediction and detection analysis of bank credit card fraud using regression model: novel approach.

- ***Regression model peroformed.***

REFERENCES:

1. Abdallah, A.; Maarof, M. A.; Zainal, A.(2016). Fraud detection system: A survey, Journalof Network and Computer Applications, 68, 90-113, 2016.
2. Agrawal, A.; Jain,A.; Kumar, B. S.(2019). Deep Learning Based Classification for Assessmentof Emotion Recognition in Speech, Available at SSRN 3356238.
3. Alam, F.; Pachauri, S. (2017). Detection using weka, Advances in Computational Sciences and Technology, 10(6), 1731-1743, 2017.
4. Awoyemi, J. O.; Adetunmbi, A. O.; Oluwadare, S. A. (2017). Credit card fraud detectionusing machine learning techniques: A comparative analysis, 2017 International Conferenceon Computing Networking and Informatics (ICCNI), IEEE, 1-9, 2017.
5. Bai, B.; Yen, J.; Yang, X. (2008). False financial statements: characteristics of China's listedcompanies and cart detecting approach, International journal of information technology & decision making, 7(2), 339-359, 2008.
6. Bhattacharyya, S.; Jha, S.; Tharakunnel, K. Westland, J. C. (2011). Data mining for credit card fraud: A comparative study, Decision Support Systems, 50(3), 602-613, 2011.
7. Bhusari, V.; Patil, S.(2011). Application of hidden markov model in credit card fraud detection, International Journal of Distributed and Parallel systems 2(6), 203, 2011.
8. Brabazon, A.; Cahill, J.; Keenan,P.; Walsh,D.(2010).Identifying online credit card fraud using artificial immune systems, Evolutionary Computation (CEC), 2010 IEEE Congress on IEEE, 1-7, 2010.
9. Chan, P. K.; Fan, W.; Prodromidis, A. L.; Stolfo, S. J.(1999). Distributed data mining incredit card fraud detection, IEEE Intelligent Systems and Their Applications, 67-74, 1999.
10. Chandola, V.; Banerjee, A.; Kumar, V. (2009). Anomaly detection: A survey, ACM computing surveys (CSUR), 41(3), 1-72, 2009.
11. Charleonnan, A. (2016). Credit card fraud detection using RUS and MRN algorithms,2016 Management and Innovation Technology International Conference (MITicon), IEEE, MIT73-MIT76, 2016.
12. Chaudhary, K.; Yadav, J.; Mallick, B. (2012). A review of fraud detection techniques: Credit
13. card, International, Journal of Computer Applications , 45
14. , 39-44, 2012.
15. **Bank credit card fraud detection using regression analysis**
16. Chen, R.C.; Chiu, M.L.; Huang, Y.L.; Chen, L.T. (2004). Detecting credit card fraudby using questionnaire responded transaction model based onsupport vector machines, international Conference on Intelligent Data Engineering and Automated Learning, Springer, 800-806, 2004.
17. Chen, R.C.; Luo, S.T.; Liang, X.; Lee, V.(2005). Personalized approach based on svm andann for detecting credit card fraud, International Conference on Neural Networks and Brain,IEEE, 810-815, 2005.. [15] Cortes, C.; Vapnik, V.(1995). Support-vector networks, Machine learning, 20(3), 273-297.
18. Craciun, M.; Ratiu, C.; Bucerzan, D.; Manolescu, A. (2013). Actuality of Bankruptcy PredictionModels used in Decision Support System, International Journal of Computers Communications& Control, 8(3), 375-383, 2013.
19. Duman, E.; Ozcelik, M.H.(2011). Detecting credit card fraud by genetic algorithm andscatter search, Expert Systems with Applications, 38(10), 13057-13063, 2011.
20. Falaki, S.; Alese, B.; Adewale, O.; Ayeni, J.; Aderounmu, G.; Ismaila, W.(2012). Probabilisticcredit card fraud detection system in online transactions, Int. J. Softw. Eng. Appl, 6 ,69-78, 2012.
21. Gadi, M. F. A.; Wang, X.; do Lago, A. P. (2008). Credit card fraud detection with artificialimmune system, in:International Conference on Artificial Immune Systems, Springer, 119-131, 2008.
22. Ghosh, S.; Reilly, D. L.(1994). Credit card fraud detection with a neural-network,In System Sciences, Proceedings of the Twenty-Seventh Hawaii International Conference on, IEEE, 3,621-630, 1994.
23. Guo, T.; Li, G.Y. (2008). Neural data mining for credit card fraud detection, 2008 InternationalConference on Machine Learning and Cybernetics, IEEE, 7, 3630-3634, 2008.
24. Halvaiee, N. S.; Akbari, M. K.(2014). A novel model for credit card fraud detection usingartificial immune systems, Applied Soft Computing, 24, 40-49, 2014.
25. Huang, R.; Tawfik, H.; Nagar, A.K. (2010). A novel hybrid artificial immune inspired approachfor online break-in fraud detection, Procedia Computer Science, Elsevier, , 1(1), 2733-2742, 2010.

26. Iyer, D.; Mohanpurkar, A.; Janardhan, S.; Rathod, D.; Sardeshmukh, A. (2011). Credit card fraud detection using hidden markov model, Information and Communication Technologies (WICT), World Congress on, IEEE, 1062-1066, 2011.
27. Jha, S.; Guillen, M.; Westland, J. C. (2012). Employing transaction aggregation strategy todetect credit card fraud, Expert systems with applications, 39(16), 12650-12657, 2012.
28. Kirkos, E.; Spathis, C.; Manolopoulos, Y.(2007). Data mining techniques for the detectionof fraudulent financial statements, expert systems with applications , 32(4), 995-1003, 2007.
29. Kohonen, T. (1990). The self-organizing map, Proceedings of the IEEE, 78(9), 1464-1480,1990.
30. Kokkinaki, A. I. (1997). On atypical database transactions: identification of probable fraudsusing machine learning for user Profiling, Knowledge and Data Engineering Exchange Workshop,IEEE proceedings, 107-113, 1997.
31. Kou, G.; Peng, Y.; Shi, Y.; Wise, M.; Xu,W. (2005). Discovering credit cardholders behaviorby multiple criteria linear programming, Annals of Operations Research, 135, 261-274, 2005.
32. Lu, Q.; Ju, C. (2011). Research on credit card fraud detection model based on class weightedsupport vector machine, Journal of Convergence Information Technology, 6, 2011.
33. Maes, S.; Tuyls, K.; Vanschoenwinkel, B.; Manderick,B.(2002) . Credit card fraud detectionusing bayesian and neural networks, Proceedings of the 1st international naiso congress on neuro fuzzy technologies, 261-270, 2002.
34. Mahmoudi, N.; Duman, E.(2015). Detecting credit card fraud by modified Fisher discriminant analysis, Expert Systems with Applications, 42(5), 2510-2516.
35. Makki, S.; Assaghir, Z.; Taher, Y.; Haque, R.; Hacid, M. S.; Zeineddine, H. (2019). An Experimental Study With Imbalanced Classification Approaches for Credit Card Fraud Detection, IEEE Access, 7, 93010-93022, 2019.
36. Meyer, A.; Zimmermann, H.-J. (2011). Applications of Fuzzy Technology in Business Intelligence,International Journal of Computers Communications & Control, 6(3), 428-441, 2011.
37. Minegishi, T.; Niimi, A. (2011). Detection of fraud use of credit card by extended VFDT,Internet Security (WorldCIS), 2011 World Congress on, IEEE, 152-159, 2011.
38. Nami, S.; Shajari, M. (2018). Cost-sensitive payment card fraud detection based on dynamic **Bank credit card fraud detection using regression analysis** random forest and k-nearest neighbors, Expert Systems with Applications, 110, 381-392, 2018.
39. Nguwi, Y.Y.; Cho, S.Y. (2010). An unsupervised self-organizing learning with support vectorranking for imbalanced datasets, Expert Systems with Applications , 37, 8303-8312, 2010.
40. Nunes, C. L.; De Castro, L. N.; Timmis, J. (2002). Artificial immune systems: a newcomputational intelligence approach, Springer Science and Business Media, 2002.
41. Olszewski, D.(2014). Fraud detection using self-organizing map visualizing the user profiles, Knowledge-Based Systems, 70, 324-334, 2014.
42. Paasch, C. A. (2008). Credit card fraud detection using artificial neural networks tuned bygenetic algorithms, Hong Kong University of Science and Technology, Hong Kong, 2008.

****
**********.