IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Special Issue-14, May 2019 E-ISSN: 2347-2693

Machine learning Classifiers for Credit Card Fraud Detection: A Brief Survey

Vidyashree V[1*], Akram Pasha[2], Udayarani V[3], Vinay Kumar M[4]

[1,2,3,4]School of Computing and Information Technology, REVA University, Bangalore, India

Corresponding Author: vvidyashree95@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7si14.436442 | Available online at: www.ijcseonline.org

Abstract: Utilization of credit cards encourages individuals to buy products online via the Internet. Individuals tend to do much of purchasing online or offline by utilizing the credit card facility provided by the bankers to their customers. Credit cards have turned out to be the most prominent facility available to the people around the globe to encourage paperless trades at an enormous speed. Whenever any such trade happens in exchanges or net marketing by using a paperless framework, it is subjected under high risk of fraudulent transactions due to many pitfalls in the security system of the usage of credit cards on the networks. This paper presents a brief survey of important and basic linear and non-linear machine learning algorithms that are focused to predict the fraudulent transactions by studying the patterns present in the credit card transactional datasets. The authors provide the methodology of Random Forest (RF), Support Vector machine (SVM) and Artificial Neural Network (ANN) classifiers to accurately classify whether a unseen credit card transaction is fraudulent or not.

Keywords: Credit Card Fraud Detection, Random Forest, Support Vector Machine, Artificial Neural Networks

I. INTRODUCTION

The advent of the Internet has created many opportunities in the banking sector to offer the best online service to its customers. [1] [2]. Among the many services that are offered by banks to its customers, the credit card facility offered to the customers is been utilized as one of the best services [3] [4]. However, the credit card service has given rise to various security threats [5] [6]. Among many such threats, the fraudulent transactions caused after the theft of the credit cards or hacking of the network has created many issues in the usage of credit cards [7] [8]. Therefore the key issues and challenges that are to be faced by the banking personnel are to convince the customer about the secured networks and to classify any fraudulent transactions that may have caused due to misuse or theft of the credit card in real time [9] [10].

The early detection of credit card fraud using different algorithms enables the cyber community stakeholders to gain insights about the patterns that could be used as the guidelines to protect safer transactions. However, it varies from a bank to bank in the incorporation of decoding the styles of the patterns discovered in interpretation. These

Methods apply in each internet offerings and data mining strategies. Using this method many machine learning algorithms have set up collaborative schemes for credit score card fraud detection. Further enhancement on these methods in many internet offerings-based collaborative schemes can also be seen currently in many establishments and industries [13] [14].

There is a fast boom within the wide variety of credit card transactions which has caused a massive rise in fraud [11] [12]. Fraud of credit card is an extensive-ranging term for robbery and fraud committed by the usage of a credit card that is mostly detected as a fraudulent transaction based on the range of the price in any particular transaction. Generally, the statistical techniques and plenty of record mining algorithms are used to resolve this fraud detection trouble. A Visa extortion happens when a particular rogue uses other people's card for their own use without the learning of its proprietor. At the point when such kind of cases happens by fraudsters, it is utilized until it's detected by the proprietor of the card through keen observations of the billing data.

This paper presents a brief survey of a few methods that are targeted to solve the issues and challenges in classifying the credit card fraudulent transaction. The key machine learning algorithms that are focused in this paper are RF, SVM and ANN that can perform the detection of fraudulent credit card transactions using a variety of machine learning paradigms.

The rest of the sections in the paper are organized in the following structure: Section-II describes the Fraudulent datasets and the distortion terminology, Section-III reviews the related work in the field of Machine Learning applications used for credit card fraud detection, Section-IV introduces the approaches that incorporate machine learning paradigms for fraud detection, Section-V enumerates the issues and challenges in the problem of detecting the fraudulent credit card transaction, and finally in Section-VI concludes the overall study performed and reported in this paper.

II. FRAUDULENT DATASETS AND THEIR DISTORTION

The datasets generally contain exchanges made by credit cards by any cardholders. The dataset is profoundly expected to be on one side of the class, the negative class; and with least number of transactions having positive class, that is that the fraudulent transaction. The transactions would be generally skewed and highly imbalanced. There could be various attributes in such transactions. There would be at least one attribute specifying the amount spent through the credit card, which would be of pertinent interest to be investigated during analytics of fraudulent transaction data analytics.

Many customized strategies have been utilized in the literature to investigate the information that contributes in distinguishing the facts that cause the hacking or any intruder in a banking security systems. This demands the sophisticated investigations that manage diverse areas of information like economic of financial aspects, commercial practices, and law [50] [51] [52] [53]. Many efforts in the research of data examination systems have been reported in the literature to balance distortion caused by the telephone associations, the protection offices and the banks [54] [55] [57].

Some efforts can also be seen in the literature where the researchers are trying it hard in solving problems related to the retail organizations that are experiencing the immoral impacts of frauds at Point OF Sale (POS) [58] [59]. The distortion that incorporates telephones, insurance claims, cost structure claims, MasterCard trades, etc. address basic issues for governments and associations, nonetheless yet recognizing and neutralizing coercion is authentically not a fundamental endeavor Distortion is an adaptable bad behavior that is demanding the development of clever systems for scrutinizing the data to gain insights from it. These procedures exist in the topics Knowledge Discovery in Databases (KDD), Data Mining, Machine Learning, and Statistics. They offer appropriate and productive game plans in different areas of deception bad behaviors. Examples of quantifiable data examination techniques as seen in the literature are as listed below [60] [61]:

Data pre-processing systems for area, endorsement, botch change and fixing off of missing or off base data are considered to be more relevant while dealing with the data sets to detect frauds. Matching counts is one of the data preprocessing techniques to recognize irregularities in the patterns of the business transactions. Such methodologies in the literature exist that combat the false alarms and many of the critical business and security systems that are driven on the information. The most general approach of handling any of the problems comprises:

(a) Data or Information gathering,
(b) Recording the current status of data,
(c) Scrutiny of Data or Information, and
(d) Tabulating and reporting the findings

The primary step in any data analytics application is to collect as much of the data or information as possible. The second step stands to perceive the status of data and keep the record of the status of the data for further understanding. Then the data is milled with any machine learning methodology to gain insights from the data. The final step asks to report the results of the model to either enhance the model or to fine tune the overall performance of the machine learning model.

The guidelines used in many strategies used for dealing with the data to detect fraud include Data mining to organize, group, and section the data and normally find the interesting patterns that discover frauds.

III.RELATED WORK

There are different strategies and procedures for recognizing Credit Card extortion; both supervised and unsupervised techniques. Numerous papers utilized RFs, SVMs, and ANNs [15].

Misuse identification and information discovery are the two principle access utilized for credit card misrepresentation location. The accentuation on abuse location access is more often than not after applying order strategies the exchange level. In the work of [16], common validation among client and trader is the most imperative element of the present system. All extra security frameworks are commonly found on cardholder confirmation yet overlook the trader check which makes the exchange framework defenseless against vendor related and Internet-related cheats, for example, website cloning, dealer conspiracy, triangulation and so on.

In the work of [17], the casual issue of credit card extortion identification utilizing abnormality recognition strategies has been presented, by misusing the grouping of exchanges in building cardholders bio-data’s. Their work explored how this influences recognition execution. The attention is on extortion cases which can be identified at the exchange matched.

In the work of [18], a viable meta-classifier display that works on two preparing levels is presented. Flash-based usage has been utilized to deal with the idea of the space. Investigations were led with credit card information and examinations had been achieved with Fraud Prospector and more advantageous Fraud Prospector. In any case, the created model displays moderate dimensions of data, which are adjusting parts, particularly for inequality information.

In the work of [19], own introduced investigation on the execution of customized models in foreseeing misrepresentation of credit card exchange when contrasted with amassed models. The examinations were performed utilizing genuine MasterCard exchange from three people and furthermore, the exchanges were gathered via an online poll. Their test results demonstrate that the precision of the customized replica is commonly more terrible than the amassed replicas.

In the work of [20], the random forest algorithm is used for classification.

In the work of [21] centers around different grouping systems (AI based) utilized in information extracting and an examination on every one of them. Since characterization takes the most pervasive area among information mining errands, an examination of three methods is utilized in Visa extortion discovery system and is exhibited. Every one of these techniques has its very own benefits and negative marks relying upon the application.

Many works have also been reported in the [22] [23] Where neural networks have been used for credit card fraud detection and offer an interface for commercial databases. The main goal of this method was to train a neural network with the beyond statistics of a selected customer. Then allow the community method the present day spending styles to recognize viable anomalies. The thief needs to shop for things like an awful lot as feasible. On that time a few credit card like VISA makes use of neural community and increase alarm bells when a curious contributing pattern occurs on a client's credit score card account. The benefit of this method is it could capable of work on commercial databases without potential limitations. It has a complicated graphical user interface. It is readily adaptable to join with other sensible techniques for credit score card fraud detection [24] [25].

IV.MACHINE LEARNING APPROACH FOR FRAUD DETECTION

The general methodology of any machine learning paradigm is to collect the credit card related data to scrutinize a person if he is coming with the exact information. Subsequently the system asks for a Personal Identity Number (PIN) [62] [63] for authentication. The figure 1 shows the general framework of a system matching the Personal Identity Number (PIN) with the account holder's data stored in the database. The system also has a module that gets activated in the event of occurrence of the fraud based on the patterns it sees by a transaction with the help of predictive models that are attached to the system. The predictive model used is trained with several records of the transactions that are clean and fraudulent. While there is the initial load of some transactions, the system begins its verification based on some threshold number of transactions. Once the database of these many threshold number of transactions are studied the fraud detection module of the system get activated. Customers spending profile is the key data that is examined to decide if the current transaction is fraudulent. This statistics is associated with the credit card (like account number, protection query, and solution that are provided on the time of registration). If the detected transaction is fraudulent then the security statistics form will stand up. It has a fixed question wherein the consumer has to answer them successfully to do the transaction. These forms have records inclusive of private, professional, deal with; dates of birth, and so on are to be had inside the database [66] [67]. If user enrolled statistics can be matched with database information, then the transaction may be finished securely. And else person transaction will be finished and move to an online shopping website.

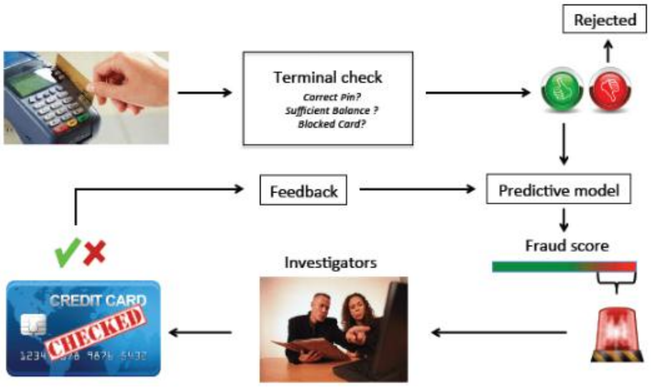


Figure 1: credit card fraud detection process

B. SUPPORT VECTOR MACHINES

SVM is categorized as a supervised machine learning algorithm as it works with the labelled data to perform the two important machine learning tasks such as classification and regression. It is mostly used in classification problems. Every record in the data set is considered as data point in n-dimensional space. Correspondingly, these data points are used to construct a hyperplane with maximum margin between the positive and negative data points. The hyperplane is just a line for a two-dimensional space. And two classes are separated as wide as possible as shown in figure 2. The two important features of any Support Vector Machine that contribute for its stability are: kernel representation and margin optimization. Kernels, such as Radial Basics Function (RBF) kernel are basically used to study the complicated regions in the search space A kernel function represents the dot product of projections of data points in a high dimensional feature area. The basic methods find out the smallest hypersphere within the kernel space that consists of all training examples, and then concludes on which aspect of hypersphere a test instance lies. If a test instance lies out of the hypersphere, it is confirmed to be suspicion SVM can have higher prediction performance than BPN (Back propagation community) in predicting the future data. But BPN contains the better performance. If g(x) is the described separate, individually portray as seeks after.

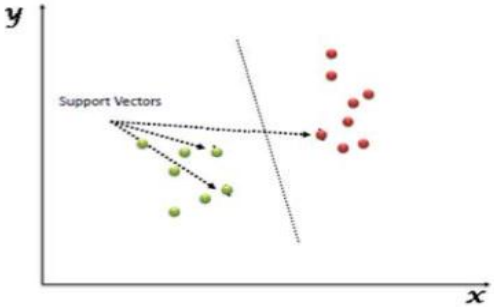
$$g(x) >= 1, V\chi \text{ € Class1}$$
$$g(x) <= -1, V\chi \text{ € Class 2}$$

The focuses that rest on the limits characterize bolster variable quantity and those help variable quantities thus characterize the separates. A large portion of the characterization calculations perform direct orders by illustration a straight line in the component area.

It is convincing to do an irregular grouping of information. Likelihood lies in the expansion of direct information calculation. They have two noteworthy advances included.

Stage 1: Alter the first information in such an approach to plot into high dimensional search space.

Stage 2: Examine the data for a separate hyperplane that well characterizes the information in new huge dimensional space



Applications of SVMs for Credit Card Fraud Detection:

In the work of [25], examines the Supervised based on the classification. The dataset utilizing standardization and Principal Component Analysis, every one of the classifiers accomplished over 95.0% precision contrasted with results came to before pre-handling the dataset.

In the work of [26], behavior-based Classification type approach using Support vector machine is applied. The implemented methods to use of SVM offer effective working of overall performance in fraud detection. Generally, SVM supply a completely unique solution by the usage of the kernels. The implemented method gives higher accuracy of detection and also easy to maintain the large volumes of transactions.

In the work of [27], a survey of many strategies in credit card fraud detection is performed. The study also evaluates every methodology such as Decision Tree, Neural Network, Bayesian Network, a genetic set of rules, assist vector gadget, k nearest neighbor and Artificial Immune System, Hidden Markov Model, fuzzy neural community and fuzzy Darwinian gadget. The key focus in this work was based on certain design standards of every machine learning algorithm.

In the work of [28], a whole composition of systems for efficient fraud detection was studied. The work studies the use of clustering & outlier detection methods in detecting the fraudulent transactions.

In the work of [29], examines the fraud by using the data stored in the banks and working with several data mining equipment that contains the initial detection.

In the work of [30], evaluation of SVM and deep learning in coping with the credit card fraud detection problem faced has been implemented.

In the work of [31], performs a survey of cutting-edge techniques in credit card fraud detection. The purpose of their paper is to support a complete evaluation of various methods to locate fraudulent transaction.

In the work of [32], utilization of simulated pattern of 200k credit card transactions is used to check two systems gaining knowledge of algorithms for fraud detection: Logistic Regression (LR) and Random Forest (RF).

In the work of [33], the issue of credit card fraud detection is done by using datasets and judgment standards. The benefits and drawbacks of fraud detection methods are enumerated and compared. Furthermore, a category of stated techniques into fundamental fraud detection methods in mainly, misuses (supervised) and anomaly detection (unsupervised) are provided. Again, a category of methods is proposed based on the functionality of the method the numerical and express datasets.

In the work of [34], the diverse forms of frauds are examined using data mining tools for early detection of frauds. They investigated the supervised techniques Support Vector Machines with Spark (SVM-S) to build a model representing ordinary and odd customer conduct and evaluated the validity of the recent transaction. The consequences acquired from databases of credit card transactions display that those methods are effective inside the banking fraud transaction.

C. RANDOM FOREST

Random Forest is an ensemble learning method that builds many decision trees during training to classify the data in to two or more classes. Random Forests can be used either for classification or regression tasks.

Figure 3 shows the working process of random tree in a Random Forest algorithm.

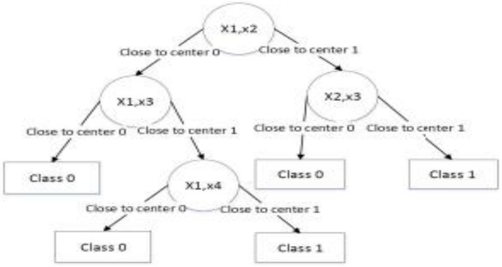


Fig 3 Random Tree Process

Basic advantages of utilizing Random Forest are:

- runs successfully on generous tables
- higher factual classifier
- successfully negotiates with a considerable number appearance

Applications of RF for Credit Card Fraud Detection:

In the work of [35], the comparative study of the classification algorithms that are classifying the credit score card transaction's records as fraudulent or not is performed using several machine learning algorithms including the Random Forest. Supervised category algorithms consisting of the decision tree, Random Forest and Support Vector Machines (SVM) are used to exactly find the records and also their precision is tabulated.

In the work of [36], random forests are used to discover the conduct features of legal and fraudulent transactions for the data sets taken from the E-trade business enterprise in China. In this work, they make a contract of the two random forests which may be different in their base classifiers and analyze their overall performance on credit fraud detection.

In the work of [37], machine learning approach like Logistic regression, Decision Tree and Random Forest have been used to detect the fraud in credit card device. Sensitivity, accuracy and error price is used to assess the performance of th proposed machine learning algorithms. The accuracy for logistic regression, Decision tree, and random forest classifier are found to be significantly good. By evaluating all of the three-technique, it has been determined that random forest classifier is better than the logistic regression and decision tree.

In the work of [38], a study was made to identify numerous category strategies for the usage of different metrics for judging supervised classifiers used for the credit card fraud detection. This model aims at reconstructing fraud detection in preference to misclassifying an absolute transaction as fraud.

In the work of [39], the decision tree primarily based on Meta classifier that can be used to select the fraudulent transactions in large imbalanced data is used. The developed meta-classifier primarily based on the forecast in two layers. The first level of a forecast is accomplished with the resource of Random Forest classifier, and the second forecast is completed by means of using an ensemble created with Decision Trees. The consequences obtained from the first and the second -degree prediction model are integrated to form the final predictions.

The work of [40], developed the customized models in assessment of the fashions in picking out fraud for awesome people. For this purpose, they have composed some actual transactions and some particular records through an internet questionnaire. Then, they have built customized and aggregated fashions. The performance of those models is to assess the usage of check facts set to evaluate their accuracy in identifying fraud for specific individuals. The experimental results show that aggregated fashions outperform custom designed fashions. Besides, they compared the overall performance of the random forest and Naïve Bayes in growing the models for fraud detection.

In the work of [41], the consumer credit card prediction is done through information mining. They have advanced an ensemble machine incorporating majority balloting and concerning Multilayer Perceptron (MLP), Logistic Regression (LR), choice timber (J48), Random Forest (RF), Radial Basis Function (RBF) community and Support Vector Machine (SVM).

The work of [42], performs the study on diverse famous classifier algorithms that have been most often used in detecting credit card fraud. Moreover, it specializes in the measure used to evaluate the magnificence ordinary performance and in ranking those algorithms.

D. ARTIFICIAL NEURAL NETWORK

An artificial neural network is an arrangement of the computing processes that are designed to simulate the way the human brain performs the analysis and pre-process the information. It can be considered as the foundation for artificial intelligence as it solves a problem which is too difficult to be solved by humans. The neural network is approved for the detection of fraud in credit card it will give efficient results in multiple problems. Applying the neural network on detection of fraud in credit card as same a human brain, the human brain contains the collection of information in the real life and also memories of past life, the same process also did in this algorithm. Here in credit card fraud detection, this algorithm divides the data into many categories:1) card container income, occupation of that person and 2) It will collect the payment details like, Variety of large purchasing, frequencies of more purchases, address, this information will find out the future transaction is fraud or not. The neural network mainly contains three layers. As shown in fig4

Input layer: This layer has input nodes, it will analyze the cardholder's details and check the characteristics of the transaction.

Hidden layer: Hidden nodes find out the transaction is fraud or genuine

Output layer: After examining the transaction output node will give the output like 0 or 1(fraud or not).

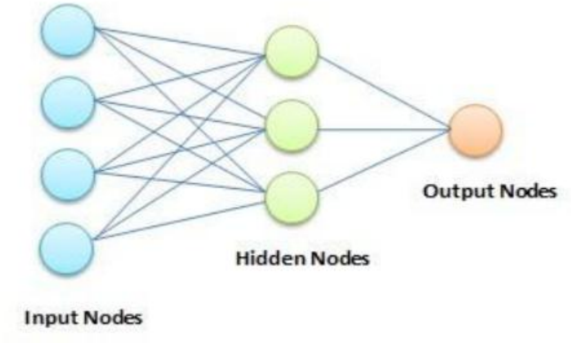


Fig4 neural network architecture

Applications of ANN for Credit Card Fraud Detection:

In the work of [23], a Cost-Sensitive credit card fraud detection device known as CSNN (Cost-Sensitive Neural Network) is used for detecting fraudulent transactions. The most important contributions of this paper was to detect the price maximization and minimization by using minimizing functions.

In the work of [24], the basic study of a case is checked concerning credit card fraud detection, wherein Cluster Analysis is used for normalization. In their work, the results obtained from the use of Artificial Neural Networks and Cluster Analysis on fraud detection has proven that neuronal inputs may be decreased through the way of clustering attributes.

The work of [25], performs a survey of diverse methods used in credit card fraud detection systems based on certain layout. Credit card fraud detection device is at most demand for any card delivering financial support to the customers. Credit card fraud detection has drawn pretty a variety of importance from the ANN and some of the strategies to counter credit fraud in the literature.

RESEARCH GAP:

Issues and Challenges in detecting the fraudulent credit card transaction:

The major issue that is found in the credit card datasets is that the datasets are extremely imbalanced and highly skewed. The actual transactions are dominated than fraudulent transactions. The fraudulent events are arise not often. So it might be tough to discover the fraudulent transaction, if it is kept in mind as the criminal will be motivated to make an attempt in invalid transactions and lead to loss of cardholder's data. The more quantity of datasets and the dimensionality may be very high. It is not a clean procedure to deal with the massive quantity of data efficiently. The scalable device gaining knowledge of gadget is wanted to process the massive quantity of facts. The actual facts isn't always shared for the wide variety of motives which include to preserve the privacy of the consumer. Generally the misclassification data is high for these detection. Efficient measure has to take to reduce the misclassification value.

CONCLUSION

In recent years, credit card usage has extended considerably. Fraudulent operations and misuse of the credit card is quite frequent in many countries. Many techniques have been reported in the literature to detect fraudulent transactions that are performed after credit card theft. Finding the most efficient technique to detect the fraud from credit card is quite challenging. But, it is possible to curb the number of frauds through accurate analysis of the data collected from several credit card transactions. Therefore, in this paper, we presented a brief survey of applications of basic machine learning algorithms towards fraud detection. The key criteria of survey was to select the three machine learning algorithms; SVM, RF and ANN; and find their ability in performing classification of unseen observation to a class, by having the classifiers trained with the history of transactions. The study is intended to continue with the empirical analysis of all leading machine learning algorithms on a big data platform using distributed computing frame works.

REFERENCES

[1] Chavan, J., 2013. Internet banking-benefits and challenges in an emerging economy. *International Journal of Research in Business Management*, *1*(1), pp.19-26.

[2] Al Hasib, A., 2009. Threats of online social networks. *IJCSNS International Journal of Computer Science and Network Security*, *9*(11), pp.288-93.

[3] Resnick, P. and Zeckhauser, R., 2002. Trust among strangers in Internet transactions: Empirical analysis of eBay's reputation system. In *The Economics of the Internet and E-commerce* (pp. 127-157). Emerald Group Publishing Limited.

[4] Franklin, J., Perrig, A., Paxson, V. and Savage, S., 2007, October. An inquiry into the nature and causes of the wealth of internet miscreants. In *ACM conference on Computer and communications security* (pp. 375-388).

[5] Özkan, S., Bindusara, G. and Hackney, R., 2010. Facilitating the adoption of e-payment systems: theoretical constructs and empirical analysis. *Journal of enterprise information management*, *23*(3), pp.305-325

[6] Minelli, M., Chambers, M. and Dhiraj, A., 2012. *Big data, big analytics: emerging business intelligence and analytic trends for today's businesses*. John Wiley & Sons.

[7] Davenport, T. and Harris, J., 2017. *Competing on Analytics: Updated, with a New Introduction: The New Science of Winning*. Harvard Business Press.

[8] Bhattacharyya, S., Jha, S., Tharakunnel, K., and Westland, J. C. (2011). Data burrowing for Mastercard deception: A close report. Decision Support Systems, 50(3), 602613. Elsevier B.V.

[9] Rahul Johari and shalini gupta" A New Framework for Credit Card Transactions including Mutual Authentication among Cardholder and Merchan 978-0-7695-4437-3/11 $26.00 © 2011 IEEE DOI 10.1109/CSNT.2011.12

[10] Mahmoud Reza Hashemi and Leila Seyedhossein" Mining Information from Credit Card Time Series for Timelier Fraud Detection" 978-1-4244-8185-9/10/$26.00 ©2010 IEEE

[11] M.Kavitha and Dr.M.Suriakala 'Constant Credit Card Fraud Detection on Huge Imbalanced Data utilizing Meta-Classifiers'978-1-5386-4031-9/17/$31.00 ©2017 IEEE

[12] M.Kavitha and Dr.M.Suriakala 'Constant Credit Card Fraud Detection on Huge Imbalanced Data utilizing Meta-Classifiers'978-1-5386-4031-9/17/$31.00 ©2017 IEEE

[13] Mohammed Ibrahim Alowais and lay-ki-soon' Credit Card Fraud Detection: Personalized or Aggregated Model' 978-0-7695-4727-5/12 $26.00 © 2012 IEEE DOI 10.1109/MUSIC.2012.27

[14] Chaitanya Ghorpade and ankit Mishra 'Charge card Fraud Detection on the Skewed Data Using Various Classification and Ensemble Techniques' 978-1-5386-2663-4/18$31.00 c 2018 IEEE

[15] Mrs.Vimala Devi. J , Dr.Kavitha,K.S "Misrepresentation Detection in Credit Card Transactions by utilizing Classification Algorithms" 978-1-5386-3243-7/17/$31.00 ©2017 IEEE

[16] References: Shukur, H.A. and Kurnaz, S., 2019. Credit Card Fraud Detection using Machine Learning Methodology.

[17] An Evaluation of Computational Intelligence in Credit Card Fraud Detection Mohammad Sultan Mahmud Department of Computer Science and Engineering World University of Bangladesh Dhaka-1205, Bangladesh 978-1-4673-8139-0/16/$31.00 ©2016 IEEE

[18] Djeffal Abdelhamid1 , Soltani Khaoula1 , Ouassaf Atika2 Automatic Bank Fraud Detection Using Support Vector Machines Proceedings of the International conference on Computing Technology and Information Management, Dubai, UAE, 2014

[19] References: A Comparison of Machine Learning Techniques for Credit Card Fraud Detection Lusis April 20, 2017

[20] Mrs.Vimala Devi. J , Dr.Kavitha,K.S Cambridge Institute of Technology, Global Academy of Technology, Bangalore-98 Fraud Detection in Credit Card Transactions by using Classification Algorithms 978-1-5386-3243-7/17/$31.00 ©2017 IEEE

[21] International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 24 (2018) pp. 16819-16824 © Research India Publications. http://www.ripublication.com 16819 Machine Learning For Credit Card Fraud Detection System Lakshmi S V S S1 Selvani Deepthi Kavila2

[22] Credit Card Fraud Detection on the Skewed Data Using Various Classification and Ensemble Techniques Ankit Mishra MANIT Bhopal, Bhopal, Madhya Pradesh , 2018 IEEE International Students' Conference on Electrical, Electronics and Computer Science

[23] Cost Sensitive Modeling of Credit Card Fraud Using Neural Network Strategy Fahimeh Ghobadi Computer Engineering Department Islamic Azad University South Tehran Branch Tehran, Iran Ghobadi.Fahimeh@Gmail.com 978-1-5090-5820-4/16/$31.00 ©2016 IEEE

[24] Cluster Analysis and Artificial Neural Networks A Case Study in Credit Card Fraud Detection Emanuel Mineda Carneiro, Luiz Alberto Vieira Dias; Adilson Marques da Cunha 978-1-4799-8828-0/15 $31.00 © 2015 IEEE DOI 10.1109/ITNG.2015.25

[25] Analysis on Credit Card Fraud Detection Methods 1 S. Benson Edwin Raj, 2A. Annie Portia 978-1-4244-9394-4/11/$26.00 ©2011 IEEE

[26] Proceedings of the Seventh International Conference on Machine Learning and Cybernetics, Kunming, 12-15 July 2008 978-1-4244-2096-4/08/$25.00 ©2018 IEEE 3630 NEURAL DATA MINING FOR CREDIT CARD FRAUD DETECTION TAO GUO, GUI-YANG LI

[27] Improved Fraud Detection in e-Commerce Transactions Jisha Shaji PG Scholar Department of Computer Engineering St. Francis Institute of Technology, Mumbai, India 978-1-5090-4381-1/17/$31.00 © 2017 IEEE

[28] Wells, A.J., 2019. Cyber-Security Incidents and Organizational Policies in Healthcare (Doctoral dissertation, Northcentral University).