A Comparative Analysis of Various Credit Card Fraud Detection Techniques

Yashvi Jain, NamrataTiwari, ShripriyaDubey,Sarika Jain

Abstract: ***Fraud is any malicious activity that aims to cause financial loss to the other party. As the use of digital money or plastic money even in developing countries is on the rise so is the fraud associated with them. Frauds caused by Credit Cards have costs consumers and banks billions of dollars globally. Even after numerous mechanisms to stop fraud, fraudsters are continuously trying to find new ways and tricks to commit fraud. Thus, in order to stop these frauds we need a powerful fraud detection system which not only detects the fraud but also detects it before it takes place and in an accurate manner. We need to also make our systems learn from the past committed frauds and make them capable of adapting to future new methods of frauds.***

In this paper we have introduced the concept of frauds related to credit cards and their various types. We have explained various techniques available for a fraud detection system such as Support Vector Machine (SVM), Artificial Neural Networks (ANN), Bayesian Network, K- Nearest Neighbour (KNN), Hidden Markov Model, Fuzzy Logic Based System and Decision Trees. An extensive review is done on the existing and proposed models for credit card fraud detection and has done a comparative study on these techniques on the basis of quantitative measurements such as accuracy, detection rate and false alarm rate. The conclusion of our study explains the drawbacks of existing models and provides a better solution in order to overcome them.

Keywords: Neural Network, Genetic Algorithm, Support Vector Machine, Bayesian Network, K- Nearest Neighbour, Hidden Markov Model, Fuzzy Logic Based System, Decision Trees.

I. INTRODUCTION

Today use of Credit Card even in developing countries has become a common scenario. People use it to shop, pay bills and for online transactions. But with increase in number of Credit Card users, the cases of fraud in Credit Card have also been on rise. Credit Card related frauds cause globally a loss of billions of dollars. Fraud can be classified as any activity with the intent of deception to obtain financial gain by any manner without the knowledge of the cardholder and the issuer bank. Credit Card fraud can be done in numerous ways. By lost or stolen cards, by producing fake or counterfeit cards, by cloning the original site, by erasing or modifying the magnetic strip present at the card which contains the user's information, by phishing, by skimming or by stealing data from a merchant's side. Fraud detection deals with finding a fraud activity amongst thousands of genuine ones, which in fact puts forward a challenge. With continued advancement in fraudulent strategies it is important to develop effective models to combat these frauds in their initial stage only, before they can take to completion. But the major challenge in developing such a model is that the number of fraudulent transactions among the total number of transaction is a very small number and hence the work of finding a fraudulent transaction in an effective and efficient way is quite bothersome.

Credit card frauds can be of following types:

1. Application Frauds: When the fraudster gains control of the application system by accessing sensitive user details like password and username and open a fake account. It generally happens in relation to the identity theft. When the fraudster applies for credit or a new credit card altogether in the name of the card holder. The fraudster steals the supporting documents in order to support or substantiate their fraudulent application.

2. Electronic or Manual Credit Card Imprints: When the fraudster skims information that is placed on the magnetic strip of the card. This information is very confidential and by accessing it the fraudster may use it for fraudulent transactions in future.

3. CNP (Card Not Present): When the fraudster knows the expiry date and account number of the card, the card can be used without its actual physical possession.

4. Counterfeit Card Fraud: It is generally attempted through the process of skimming. A fake magnetic swipe card is made and it holds all the details of the original card. The fake card is fully functional and can be used to commit transactions in future.

5. Lost and Stolen Card Fraud: In cases when the original card holder misplaces their card, it can get to the hands of fraudsters and they can then use it to make payments. It is hard to do this through machine as a pin number is required however; online transactions are easy enough for the fraudster.

6. Card ID Theft: This fraud is similar to application frauds. In ID theft the fraudster acquires the details of the original card to make use of a card or to open a new account. This type of fraud is the most difficult to identify.

7. Mail Non-Receipt Card Fraud: When a customer applies for a card, it takes some time for all the procedural formalities. If fraudster intercepts in the middle of the delivery, they may register the card in their name and may use it to make purchases. This fraud is also known as never received issue fraud.

8. Account Takeover: It is one of the most common forms of frauds. The fraudster may access the account details of

Revised Manuscript Received on Janurary 25, 2019.

Yashvi Jain, Department of Computer Applications, National Institute of Technology, Haryana, India (yashvijain.0296@gmail.com)

NamrataTiwari, Department of Computer Applications, National Institute of Technology, Haryana, India (namrata.tiwari929@gmail.com)

ShripriyaDubey, Department of Computer Applications, National Institute of Technology, Haryana, India (shriya2021@gmail.com)

Sarika Jain, Department of Computer Applications, National Institute of Technology, Haryana, India (jasarika@gmail.com)

the original card holder and several relevant documents. They then can contact the credit card company and pretend to be the original card holder and may even ask them to change the address. As they have all the details as proof, hacked through or otherwise obtained, they can provide them as proof. The duplicate card will then be sent to the new or fake address and the criminal will be able to make use of that.

9. False Merchant Sites: This is similar to the phishing attack where the customer gets trapped in a fake webpage, created by the fraudster, which looks very similar to a known and genuine website. This webpage may offer several discounts in order to entice the customer to buy the products. Once the transaction is made, all the transaction related information is gathered and the fraudster uses it further perform fraudulent exchanges.

10. Merchant Collusion: When the merchant deliberately passes on the relevant information related to the card holder without the card holder knowing.

Detecting a fraud is a complicated computational task. The number of parameters to choose, cluster and classify are huge and classification of parameters will decide the success of any fraud detection technique. Moreover a transaction cannot be purely classified as a fraud or a genuine one by the existing systems; they just find the likelihood of a transaction being fraud based upon the extensive study of customer's behaviour, their spending habits and also analysing the previously committed frauds and observing their patterns. Hence two major challenges faced by any credit card fraud detection system are that, firstly they have a very limited time period in which they have to make a decision to term the transaction as a fraud or genuine and Secondly, they have to process a huge amount of parameters while training and while making a decision.

The properties of any good fraud detection system should be:

a) It should be able to identify the frauds accurately that means the number of wrong classifications should be minimum.

b) It should be able to detect the fraud while it is in transit.

c) It should not term any genuine transaction as fraudulent.

In our paper we have tried to study all the techniques that can be used in a fraud detection system and have tried to do a comparative study to show which technique performs better under what scenarios. Contributions of this review paper are:

1. Summary and categorization of all the existing techniques in fraud detection.
2. Literature review of all the work done on fraud detection systems.
3. Parametric comparison of all the existing techniques and proposed model.

Rest of the paper has following sections. Sections II explains and summarize all the existing techniques that can be used in a fraud detection system. Section III discusses the work done and models proposed till date on the fraud detection systems for credit cards. Section IV is a parametric comparison of the various such techniques on the basis of some evaluation parametrics such as precision, recall, hit rate accuracy. Finally Section V is the conclusion and the future scope in credit card fraud detection techniques.

II. VARIOUS TECHNIQUES OF CREDIT CARD FRAUD DETECTION

We know that all fraudulent transaction follow a similar pattern and by using any pattern recognition system such as Support Vector Machine (SVM), Artificial Neural Networks, Naïve Bayesian Network, K- Nearest Neighbour (KNN), Hidden Markov Model, Fuzzy Logic Based System or Decision Trees we can classify transactions as fraudulent whose working is explained below.

1. Artificial Neural Network

It combines the thinking power of human brain with computational power of machine. It makes use of neurons as the deciding sites and the edges between neurons to calculate the contribution of each neuron in the previous layer in the decision and result at the current neuron. It is based on pattern recognition. Previous year's data is fed into the network and then based upon that data it recognises a new incoming transaction to be a fraud or genuine one. Its training can either be supervised i.e. the outcome is already known for a given transaction and the expected output is compared with actual to train the system or it can be unsupervised where we have no actual results to compare it with and thus are not sure about the results. [1]

2. Decision Tree

It is a computational tool for classification and prediction. A tree comprises of internal nodes which denote a test on an attribute, each branch denotes an outcome of that test and each leaf node (terminal node) holds a class label. It recursively partitions a dataset using either depth first greedy approach or breadth first greedy approach and stops when all the elements have been assigned a particular class. For the partition rule to be efficient it must separate the data into groups where a single class predominates in each group. In other words, the best partition will be the one in which the subsets do not overlap i.e. they are clearly disjoint to a maximum amount. [2]

3. Fuzzy Logic

It is used in the cases when we do not have discrete truth values i.e., they are continuous. It is a multivalued logic. There are certain set of rules based on which a transaction is classified as a genuine or fraud one. There are three important components in fuzzy logic that need to be executed in the stated order: [3]

- Fuzzification
- Rule Based
- Defuzzification

In fuzzification we classify an incoming transaction in the categories of high, low or medium based upon the monetary value associated with the transaction. Rule based deals with drafting the rules based on the customer behaviour. The transaction is allowed to occur if it satisfies given set of rules. In Defuzzification, if a transaction does not comply with the predefined set of rules it isn't allowed to occur. It is immediately stopped and then cross checked with the customer that whether it should be granted the permission to continue or be aborted.

4. Support Vector Machines

It is a supervised learning algorithm in which given a dataset it separates them into different classes using a hyperplane. The goal of SVM is to find this hyperplane. There could be many hyperplanes but we are determined to find an optimal hyperplane. The points closest to the hyperplane in the different classes are known as support vectors and these support vectors are used to predict the classes of new data points. A new incoming point is put on the equation of the hyperplane and then is classified as to which class it belongs on the basis of which side of hyperplane it falls on the vector space. To train our machine we feed supervised data i.e. data with results already known. It learns the behaviour of fraud and genuine transactions and then it can classify new transaction as to which class it belongs. [4]

5. Bayesian Network

It is based upon the Bayes Theorem of conditional probability; hence it is a probabilistic model that is used for automated detection of various events. It consists of nodes and edges, wherein the nodes represent the random variables and the edges between the nodes represent the relationships between these random variables and their probabilistic distribution. We calculate predefined minimum and maximum value of probabilities of a transaction being fraud or legal. Then for a new incoming transaction we see that whether it's probability of being legal is less than the minimum defined value for legal transaction and is greater than the maximum defined value for a fraud transaction. If true then the transaction is classified as a fraud. [5]

6. K- Nearest Neighbour

It is one of the most used algorithms for both classification and regression predictive problems. Its performance depends on three factors: the distance metrics, the distance rule and the value of K. Distance metrics gives the measure to locate nearest neighbours of any incoming data point. Distance rule helps us to classify the new data point into a class by comparing its features with that of data points in its neighbourhood. And the value of K decides the number of neighbours with whom to compare. The important question is how do we choose the factor K? In order to obtain the optimal value of K, the training and validation is segregated from the initial dataset. Now a graph based on the validation error curve is plotted to achieve the value of K. This value of K should be used for all predictions. We calculate the dominant class in the vicinity of any new transaction and classify the transaction to belong to that dominant class. [6]

7. Hidden Markov Model

There is a change of state with time hence the name markov. The states are hidden hence cannot be observed directly. But something correlated to them can be observed and based on that sequence of observations we predict the order of state changes. We first train our model based upon given set of parameters like spending habit of cardholder. Initial set of probabilities are chosen based on this profile. Then any new incoming transaction is analysed by our model and classified as fraudulent if it varies from the general profile and behaviour of a cardholder by more than a threshold value and hence it cannot be accepted by the states in hidden markov model. [7]

8. Logistic Regression

To combat the anomalies of linear regression where it gave values greater than 1 and less than 0, logistic regression comes into play. Despite the name being regression, LR is used for classification problems for predicting binomial and multinomial outcomes, having the goal of estimating the values of parameter's coefficients using the sigmoid function. Logistic regression is used for clustering and when a transaction is ongoing it examines the values of its attributes and tells whether the transaction should proceed or not. [8]

III. LITERATURE REVIEW

In 2015, J. Esmaily and R. Moradinezhad[9] in their paper proposed a hybrid of artificial neural network and decision tree. In their model they used a two-phase approach. In first phase the classification results of Decision tree and Multilayer perceptron were used to generate a new dataset which in second phase is feed into Multilayer perceptron to finally classify the data. This model promises reliability by giving very low false detection rate.Siddhartha Bhattacharyya and 4 others [10] in their paper in 2011 did a detailed comparative study of Support vector machine and random forest along with logistic regression. They concluded through experiments that Random Forest technique shows most accuracy followed by Logistic Regression and Support Vector Machine.RaghavendraPatidar and Lokesh Sharma [11] in 2011 have proposed a hybrid of Artificial Neural Network and Genetic Algorithm in their paper. They used a neural network to classify the transactions and genetic algorithm to optimize the solution and to not over train the system.In 2015, [12]Tanmay Kumar and SuvasiniPanigrahi in their paper proposed a hybrid approach to credit card fraud detection using fuzzy clustering and neural network. It makes use of two phases. In phase one, they used a c-means clustering algorithm to generate a suspicious score of the transaction and in next phase if a transaction is suspicious it is feed into neural network to determine whether it was really fraudulent or not.In their paper the authors 'Wen-Fang Yu' and 'Na Wang' [13] proposed credit card fraud detection using outlier mining based on distance sum. Outlier mining is a field of data mining which is basically used in monetary and internet fields. It deals with detecting objects that are detached from the main system i.e. the transactions that aren't genuine. They have taken attributes of customer's behaviour and based on the value of those attributes they've calculated that distance between the observed value of that attribute and its predetermined value.AyushiAgrawal and others [14] proposed testing a transaction using Hidden Markov Model, Behaviour based technique and Genetic Algorithm, wherein they used the Hidden Markov Model to maintain the record of previous transactions, Behaviour based technique for grouping of datasets and lastly genetic algorithm for optimization i.e.

calculating the threshold value.

Sam Maes[15] proposed detecting frauds in credit card using two machine learning techniques namely Bayesian Netwoks and Artificial Neural Network. The paper discussed that how Bayesian networks after a short training gave good results and their speed was enhanced by the use of ANN.

ThurayaRazooqi[16] proposed a system of fraud detection using Fuzzy Logic and Neural Network. They found out that ANN was 33% more accurate than fuzzy logic. The existing data in the system was used for decision making and using fuzzy logic each data was given a membership attribute then for the validation of results ANN was used.

Y. Sahin and E. Duman [17] proposed fraud detection in credit card using a combination of Support Vector Machines and Decision Trees. Decision Trees outperformed SVMs when the size of data set was small but with increase in size of dataset SVM reached accuracy of decision trees.

Geoffrey F.Miller, Peter M.Todd and SaileshHegde [18] have elaborated the concept of designing of Neural Networks using Genetic Algorithms. They have stated the problem associated with intuitive network design by humans and proposed the idea of an automated evolutionary deign method based on genetic algorithms as a solution to it. They build a system which would have applications in biological, neurological and psychological modelling as well as the engineering and design applications using automated network design. Their paper aims to free the network design process from the constraints of human biases.

EkremDuman and M. HamdiOzcelik [19] they proposed a method that would improve the then existing credit card detection systems in banks. They devised a system to credit each transaction a certain score and based on that score the transaction was judged and for this they combined neural networks with scatter search.

Alireza Pouramirarsalani1, MajidKhalilian, AlirezaNikravanshalmani[20] proposed a new method of fraud detection which used a hybrid of feature selection and genetic algorithm. They observed the salient features of the transactions and used the same while detecting any unusual feature and flagging it to be the fraud one. The genetic algorithm was used in the optimization and search problems.

PoojaChougule and others [21] proposed simple K-means and Simple Genetic Algorithm for fraud detection. In this paper they showed that how k-means algorithm grouped the transactions based on the distinct attribute values and genetic algorithm was used for optimization since with the increase in size of the input k-means algorithm produced outliers. Basically k-means algorithm produced clusters which were then optimized by the genetic algorithm.

S.Fashoto, O.Adeleye and J.Wandera[22] have used a hybrid of K-means clustering with Multilayer Perceptron (MLP) and the Hidden Markov Model (HMM) in their paper. They have used K-means clustering in order to group together the suspected fraudulent transactions into a similar cluster. The output of this stage is used to train the HMM and the MLP which then classify the incoming transactions. They found in their results that the detection accuracy of "MLP with K-means Clustering" is higher than the "HMM with K-means clustering" but the result is reversed for 10-fold cross-validation.

M.R. HaratiNik, M. Akrami, S. Khadivi and M. Shajari[23] in their paper have proposed a fusion on Fuzzy expert system and Foggbehavioural analysis thus naming it the FUZZGY hybrid model. The Fuzzy expert system logically identifies the refutation between current activities and historical ones. The Foggbehavioural model describes the merchant behaviour in two dimensions: motivation and ability to make a fraud. The fraud tendency weight is then calculated for each merchant followed by the degree of suspicion for the incoming transactions.

Krishna K. Tripathi and Mahesh A. Pavaskar [24] have done a comparative study of different techniques in their paper and one of the techniques they have worked upon is a fusion of Dempster-Shafer theory and Bayesian learning which combines the evidences or datasets from past as well as the current behaviour. The rule-based filter, Dempster-Shafer adder, transaction history and Bayesian learner are the 4 stages of this system via which we decide the suspicious and unsuspicious transactions altogether. In the first component the extent to which the incoming transaction has deviated is determined so as to get the suspicion level. The second component combines multiple such patterns to get an initial belief which are again combined to obtain an overall belief. The transaction is then classified as suspicious or unsuspicious depending on its belief. Once found suspicious, the belief may be further given more strength or may be weakened as per its comparative similarity between with fraudulent or genuine transactional history using the Bayesian learning.

IV. COMPARATIVE ANALYSIS

In order to compare various techniques we calculate the true positive, true negative, false positive and false negative generated by a system or an algorithm and use these in quantitative measurements to evaluate and compare performance of different systems.

True Positive (TP) is number of transactions that were fraudulent and were also classified as fraudulent by the system. True Negative (TN) is number of transactions that were legitimate and were also classified as legitimate. False Positive (FP) is number of transactions that were legitimate but were wrongly classified as fraudulent transactions. False Negative (FN) is number of transactions that were fraudulent but were wrongly classified as legitimate transactions by the system. The various metrics for evaluation are:

1. Accuracy is the fraction of transactions that were correctly classified. It is one of the most powerful and commonly used evaluation metrics.
   Accuracy (ACC)/Detection rate = (TN + TP) / (TP + FP + FN + TN)
2. Precision also known as detection rate is the number of transactions either genuine or fraudulent that were correctly classified.
   Precision/Detection rate/Hit rate = TP / TP + FP

3. Sensitivity measures the fraction of abnormal records (the records that have maximum chances of being fraudulent) correctly classified by the system.
   True positive rate/Sensitivity = TP / TP + FN
4. Specificity measures the fraction of normal records (the records that have minimum chances of being fraudulent) correctly classified by the system.
   True negative rate /Specificity = TN / TN + FP
5. False Alarm rate measure out of total instances classified as fraudulent how many were wrongly classified.
   False Alarm Rate = FP/FP+TN
6. Cost tells the effective cost of our system.
   Cost = 100 * FN + 10 * (FP +TP)

We have compiled a comparison done on the KDD dataset from the standard KDD CUP 99 Intrusion Dataset on all of the techniques mentioned in previous section using four measurement metrics: Accuracy, Precision, False Alarm Rate and Cost [25][26].

Techniques	Accuracy	Detection Rate (Precision)	False Alarm Rate
Support Vector Machine (SVM)	94.65%	85.45%	5.2%
Artificial Neural Networks (ANN)	99.71%	99.68%	0.12%
Bayesian Network	97.52%	97.04%	2.50%
K- Nearest Neighbour (KNN)	97.15%	96.84%	2.88%
Fuzzy Logic Based System	95.2%	86.84%	1.15%
Decision Trees	97.93%	98.52%	2.19%
Logistic Regression	94.7%	77.8%	2.9%

From the above table it is clear that the neural network and naive bayesian network gives the highest accuracy. K-nearest neighbour, support vector machine and decision tree offers medium level of accuracy whereas fuzzy logic system and logistic regression gives low accuracy as compared to others. High detection rate is offered by neural network, naïve bayesian, fuzzy systems and KNN. On the other hand logistic regression, SVM and decision tree provides low detection rate. Low false rate is given by neural network only and SVM gives high false rate. Other techniques KNN, Logistic regression, Bayesian network, Fuzzy system and Decision trees all offers medium false detection rate.

But it is also notable that even though artificial neural networks and naive bayesian networks perform better at all parameters, they are expensive to train whereas logistic regression is not at all expensive to train. Other system such as KNN, SVM, Fuzzy systems and decision tree are somewhat expensive to train.

The major gaps in the current models and methods for fraud detection techniques are:

1. Unavailability of complete data for credit cards as they are a private property and neither banks nor customers which to disclose their information thus leading to improperly and undertrained systems.
2. Unavailability of a single powerful algorithm that can perform consistently in all environments and can outperform all other algorithms.
3. We have a lack of good and efficient evaluation parameters that can not only describe the accuracy of the system but can give a better comparative result among different approaches.
4. Inability of a system to adapt itself effectively to changing environment, new fraudulent techniques and genuine changes made in purchase habits of a user.

V. CONCLUSION

Although there are several fraud detection techniques available today but none is able to detect all frauds completely when they are actually happening, they usually detect it after the fraud has been committed. This happens because a very minuscule number of transactions from the total transactions are actually fraudulent in nature. So we need a technology that can detect the fraudulent transaction when it is taking place so that it can be stopped then and there and that too in a minimum cost. So the major task of today is to build an accurate, precise and fast detecting fraud detection system for credit card frauds that can detect not only frauds happening over the internet like phishing and site cloning but also tampering with the credit card itself i.e. it signals an alarm when the tampered credit card is being used.

The major drawback of all the techniques is that they are not guaranteed to give the same results in all environments. They give better results with a particular type of dataset and poor or unsatisfactory results with other type. [27] Some techniques like Artificial Neural Network and Naive Bayesian Network though have high detection rates and gives high accuracy they are very expensive to train. Some like KNN and SVM gives excellent results with small data sets but are not scalable to large datasets. Some techniques like decision tree and support vector gives better results on sampled and pre-processed data whereas some techniques like logistic regression and fuzzy systems give better accuracies with raw unsampled data.

A solution to these gaps by creating a hybrid of various techniques that are already used in fraud detection to cancel out their limitations and get enhanced performance. J. Esmaily and R. Moradinezhad have proposed a hybrid of Decision Tree and Neural Network; R. Patidar and L. Sharma have proposed a hybrid of Neural Network and Genetic Algorithm [11]; T. Kumar and S. Panigrahi [12] have proposed a hybrid of Fuzzy Clustering and Neural Network; A. Agrawal and others proposed a hybrid of

Hidden Markov Model, Behaviour based technique and Genetic Algorithm; Sam Maes have proposed a hybrid Bayesian Network and Artificial Neural Network; Y. Sahin and E.

Duman have proposed a hybrid of Support Vector Machines and Decision Trees; M. R. HaratiNik and others have proposed a hybrid of Fuzzy expert system and Foggbehavioural analysis.

The key to develop a good hybrid model is to pair an expensive technique which takes long to train but gives highly accurate and precise results with an optimization technique to lower the cost of the system and make the system train quickly. The choice of techniques for a hybrid will depend on the applications and environment of the fraud detection system.

VI. FUTURE SCOPE

From the above comparative analysis of the various credit card fraud detection techniques it is clear that Artificial Neural Networks performs best in this scenario. But the drawbacks of Artificial Neural Networks is that they are very expensive to train and can be easily over trained. In order to minimize their expense we need to create a hybrid of neural network with some optimisation technique. Optimisation techniques that could be successfully paired with Neural Network are Genetic Algorithm, Artificial Immune System, Case Based Reasoning and any other similar optimisation technique. Genetic Algorithm [11] helps by selecting the optimised weight of the edges in neural network. Artificial Immune System [28] reduces the cost by eliminating the weights that cause the maximum error and Case Based Reasoning [29] first tries to predict the outcome on the basis of a direct match with the user's profile.

REFERENCES

1. d. l. g. s. chandrahas mishra, "credit card fraud detection using neural networks," *international journal of comoputer science*, vol. 4, no. 7, July 2017.
2. h. s.,. j. g. d.,. b. snehal patil, "credit card fraud detection using decision tree induction algorithm," *international journal of computer science and mobile computing*, vol. 4, no. 4, pp. 92-95.
3. a. a. pansy khurana, "credit card fraud detection using fuzzy logic and neural network," *SpringSim*, 2016.
4. a. a. nancy demla, "credit card fraud detection using svm and reduction of false alarms," *inyternation journal of innovations in engineering and technology*, vol. 7, no. 2, 2016.
5. D. S. G. S.Saranya, "fraud detection in credit card transaction using bayesian network," *international research journal of engineering and technology*, vol. 4, no. 4, April 2017.
6. T. R. C.Sudha, "credit card fraud detection in internet using k nearest neighbour algorithm," *IPASJ international journal of computer science*, vol. 5, no. 11, 2017.
7. a. k. s.,. m. abhinav srivastava, "credit card fraud detection using hidden markov model," *IEEE*, vol. 5, no. 1, 2008.
8. E. D. Yusuf Sahin, "detecting credit card fraud by ann and logistic regression," 2011.
9. R. M. jamail esmaily, "Intrusion detection system based on multilayer perceptron neural networks and decision tree," in *International conference on Information and Knowledge Technology*, 2015.
10. S. J. K. T. J. C. W. Siddhatha Bhattacharya, "Data Mining for credit card fraud: A comparative study," *Elsevire*, vol. 50, no. 3, pp. 602-613, 2011.
11. "Raghavendra Patidar and Lokesh Sharma," *International Journal of soft computing and engineering*, vol. 1, no. NCAI2011, 2011.
12. s. p. tanmay kumar behera, "credit card fraud detection: a hybrid approach using fuzzy clustering and neural network," in *international conference on advances in computing and communication Engineering*, 2015.
13. N. W. Wen -Fang Yu, "Research on credit card fraud detection model based on distance sum," in *International joint conference on artificial intelligence*, Hainan Island,China, 2009.
14. S. k. A. K. M. Ayushi agarwal, "Credit card fraud detection: A case study," in *IEEE*, New Delhi, India, 2015.
15. K. T. B. V. Sam Maes, "Credit cards fraud detection using bayesian and neural networks," p. 7, August 2002.
16. P. K. D. K. R. D. A. A. Thuraya Razoogi, *Credit card fraud detection using fuzzy logic and neural networks*, Society for modelling and simulation International(SCS), 2016.
17. E. D. Y. Sahin, "Detecting credit card fraud by decision trees," in *Proceedings of the international multiconference of engineers and computer science*, Hong Kong, 2011.
18. P. M.,. S. H. Geoffrey F.Miller, "Designing Neural networks using genetic algorithms," [Online]. Available: https://static1.squarespace.com/static/58e2a71bf7e0ab3ba886cea3/t/5909113c1b631b40f8137956/1493766462349/1989+neural+networks.pdf.
19. M. H. O. Ekrem duman, "Detecting credit card fraud by genetic algorithm and scatter search," *Expert Systems with applications: An International Journal*, vol. 38, no. 10, pp. 13057-13063, 2011.
20. M. K. A. N. Alireza Pouramirarsalani1, "Fraud detection in E-Banking by using the hybrid feature selection and evolutionary algorithms," *International Journal Of Computer Science and Network Security*, vol. 17, no. 8.
21. A. T. P. K. M. G. P. N. Priya Chougle, "Genetic K- Means Algorithm for credit card fraud detection," *International journal of computer science and information technologies*, vol. 6, pp. 1724-1727, 2015.
22. O. O. O. A.,. W. Stephen Fashoto, "Hybrid Methods for credit card fraud detection," Kampala International University, Kampala, Uganda, University of Abuja, Nigeria, Redeemer's University, Ede, Osun State, Nigeria, [Online]. Available: http://www.journalrepository.org/media/journals/BJAST_5/2015/Dec/Fashoto1352015BJAST21603.pdf.
23. M. A. S. K. M. S. MR HaratiNik, "FUZZGY model," [Online]. Available: https://ieeexplore.ieee.org/document/6483148.
24. M. A. P. Krishna K. Tripathi, "Survey on credit card fraud detection methods," 1Computer Engg., M.E Computer, TERNA Engg College NERUL, Mumbai University, Mumbai, Maharashtra, India., [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.414.3256&rep=rep1&type=pdf.
25. A. O. A. S. A. O. John o. Awoyemi, "credit cars fraud detection using machine learning techniques: A comparative analysis," in *International conference on computing networking and infomatics*.
26. E. Aji M. Mubarek, "Multilayer perceptron neural network technique for fraud detection," in *International Conference on Computer Science and Engineering(UBMK)*, 2017.
27. S. K. M. A. Masoumeh Zareapoor, "analysis of credit card fraud detection techniques: based on design criteria," in *international journal of computer applications*, 2012.
28. J. I. T. L. N. de Castro, "Artificial immune systems as a novel soft computing paradigm," *Journal of Soft Computing*, vol. 7, p. 526–544, 2003.
29. A. S. Wheeler R, " Multiple algorithms for fraud detection. Knowledge-Based Systems," no. S0950-7051(00)00050-2, 2000.