iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 8 **Issue:** VII **Month of publication:** July 2020

**DOI:** https://doi.org/10.22214/ijraset.2020.30614

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429*
*Volume 8 Issue VII July 2020- Available at www.ijraset.com*

# Survey of Various Techniques used for Credit Card Fraud Detection

Aayushi Agarwal[1], Md Iqbal[2], Baldivya Mitra[3]
[1, 2, 3]*Department of Computer Science & Engineering, MIET, Meerut, U.P, India*

***Abstract:** In today's era , technology is changing rapidly and with the increase in new innovations and advancements our way of life has changed . Government is making attempt to make India a digital country, So using an ATM or credit card is a convenient way of fulfilling the government's aim. Banks and its customers are suffering huge losses due to fraudulent activities. So, researchers are trying to find the solution by applying algorithms like Data Mining, Machine Learning and Deep Learning, to prevent the fraudulent transactions by building efficient system. This paper is prepared to disclose the survey of existing techniques.*

***Keywords:** credit card fraud detection, machine learning, deep learning*

## I. INTRODUCTION

**C**redit card fraud is the largest threat in the world and every company is inside the trap of facing huge losses due to this. It is done by stealing the confidential information of a credit card user and using it for illegal purposes[1]. According to the report of Federal Trade Commission, the credit card fraud asserts in 2017 was 40% greater than the previous years.Also,13,000 and 8,000 cases of credit card fraud were found in states like California and Florida which have the highest rates of such type of fraud. In 2018,loss of $24.26 billion was noticed due to fraud and has incremented by 18.4% in the same year. Moreover , it is estimated that it will surpass roughly $30 billion by 2020[2].

Credit card fraud is typically the cause of card owner's carelessness such as revealing the card number to the unauthorized calls, when a card gets lost or stolen, fraudsters building counterfeit cards to commit frauds or by being the victim of using non-secure websites. So , after seeing the consequences of using credit card , it is necessary to detect the fraudulent transactions in time so no one can suffer the losses.

To correctly identify the fraud , many researchers and banking institutions are trying to curb this situation but it is a very challenging task, many machine learning algorithms have been also applied. But now a days, fraudsters or scammers are so smart that they always try to steal the data through new techniques.

### *A. Types of Fraud*

1) *Application Fraud:* This happen when the users by mistake fill wrong application at the time he is applying for credit card. It could be done by two ways:

*a)* Whenever the attacker illegally acquires the personal information of the card holder then he can open his or her account by his own name.

*b)* When the user gives his wrong information about his financial records, then it will give rise to financial fraud.

2) *Lost/ Stolen Cards:* This type of fraud happens when the card is lost by the user or it has been stolen by someone. The fraudster make purchases from the details of the card and the card's owner will only get to know about the purchases from his/her monthly statement. It is a very dangerous and oldest fraud where people can be easily scammed.

3) *Account Takeover:* This fraud is the most common fraud amongst all the frauds taking place. In this , the fraudster access all the details of the user and contacts the credit card company as a valid user to change the address information , then the fraudster receives a new card but with the identity of a valid user and enjoy the benefits.

4) *Skimming:* This is a type of credit card fraud where skimmer uses a small camera which is fixed in the swipe device at shops. When a user swipes the card , the device records all the details stored in the card's magnetic stripe. And fraudster can generate a new card with the help of these details and finally is able to make further illegal charges with a clone card.

©IJRASET: All Rights are Reserved

*B. Prevention Techniques*

*1) Keep all of your cards and financial details safe*:

*a)* One should look only once at the time of transaction, if he is making payment publically. The card holder tries to memorize all the details.

*b)* One should regularly and properly checks and verifies the card details. Always free to contact the credit card company if you face any unusual activity in our account.

*c)* The cards should not be carried along with the cash. One should keep his cards in pockets. As, if someone steals your purse then your card will be saved from being used illegally. Carry your card only when you needed it the most.

*2) Secure your PIN*

*a)* The user should memorize his PIN and destroy all the evidences in which he has mentioned his card details.

*b)* One should not share his card details with anymore. The PIN code should change after every regular interval. One should never write/ record your details. Banks or any credit card companies will never call you and ask you anything about your PIN code.

*c)* At the time of transaction, you need to hide your PIN code while making any transaction with your hand. If you have doubt that someone has seen your code than you should immediately change your code at cash machine (ATM) or by contacting the desired bank.

*3) Take Care once using Cash Machines*

*a)* You need to ensure your personal safety measures first. If you are not feeling comfortable inside the ATM then cancel the transaction and use some other ATM.

*b)* If there is any unusual activity in the ATM or if there is any chances of damaged ATM then it's better to not use that machine. Report to the respective bank.

*c)* If you think that someone is staring at you at the time of transaction then delete all the details you have entered and use another machine. Do not let anybody to help you in order to make transaction and have complete focus on the screen.

*4) Contact your Bank as Soon as Possible If Your Card Or Personal Info Has Been Compromised*

*a)* One should never sign on the blank paper, as your signature can be forged and use for illegal purpose.

*b)* All the receipts should be properly maintained and all the transaction statements should properly matched with the receipts.

***c)*** All the bills should carefully maintain and verify the purchases regularly.

*C. Fraud Detection Techniques*

The two significant categorizations for the Credit Card Fraud Detection techniques are: First, Supervised Learning Approach, a database with labeled transactions is utilized. These transactions are classified as fraudulent or normal depending upon the existing historical data. The Classification models based on algorithms used to distinguish between the fraudulent or normal transactions. Every new transaction that comes in is classified on the basis of classification model. This model has two major drawbacks. Firstly, the data with labeled transactions is often unavailable, in case the labeled data is available; its accuracy is not guaranteed. Due to this, undetected fraud can be labeled as legitimate action. Secondly, the algorithms used to create these classification models are very complex and time consuming. In Unsupervised Leaning Approach, the labels are not assigned to data set. A model is created on the basis of normal behavior, as it is assumed that fraudulent events are less. New transactions are compared against legitimate user behavior model, if differences in transactions are large enough; it is recognized as fraudulent activity. The activity information pertaining to account like time and location of transaction amount are included. The main advantage of this approach is, it can handle large amount of data without prior knowledge of historical data.

*D. Classification Techniques*

Different classification techniques have been applied for detecting the frauds that occur in credit card transactions.

*1) Artificial neural network (ANN):* It is known as a classifier that works on the concept of functioning of human brains [10]. The nodes are interlinked with each other in its architecture. The nodes that are present near to them are assigned with the weighted links of each other. It collects all the information sensed by the connecting nodes. Further, each node calculates the output values with the help of weights used with a simple function. A complex system that includes specialized tissues, cells, chemical molecules as well as organs generating an intricate network is known as the natural immune system [11]. The antibodies which have the capacity to identify and eliminate the harmful and risky antigens are known as the detectors of the immune system.

©IJRASET: All Rights are Reserved

2) *Artificial Immune System (AIS):* On the basis of the biological metaphor of the immune system, a recent sub-field developed is the Artificial Immune System (AIS). Inspiring from the natural evolution, generating algorithms are designed lately [8]. The binary strings which denote the populations of candidate solutions are called the chromosomes. The chromosomes that have higher quality or the fitness value have higher chances of survival as per the concept of this classifier.
3) *Hidden Markov model:* It is known as a mechanism that generates a highly complex stochastic process with the help of a double embedded stochastic method. In the underlying system, the unobserved states are observed here [12].
4) *k-NN:* A non-parametric algorithm through which regression and classification are performed with high efficiency is known as k-NN. The k-nearest training samples available in the feature space are given as input for this classifier. Further, based on the classification or regression categories, the output is generated.

### *E. Challenges in Credit Card Fraud Detection*

There are numerous challenges faced by the fraud detection techniques developed by different researchers. For providing highly efficient results, it is important to ensure that any fraud detection technique has the capability to handle the following difficulties.

1) Imbalanced data: It is imbalanced in nature. This means there is very few chances of credit card fraud. This will create difficulty to detect the false transaction and very difficult to imprecise it.
2) During detection process, every misclassification errors have different significance. Misclassifications of the normal transaction will not create much problem as compared to considering the fraud transaction as the normal transaction. Because the problem of misclassification can be removed or sorted in another step.
3) Overlapping data: Sometimes many legitimate or genuine transactions are considered as the false or negative transaction and vice versa. This will create problem to identify the actual and original transaction. It is the biggest challenge being faced by every credit card company.

## II. LITERATURE SURVEY

Literature survey includes all the research done by various researchers on the respective topic. It inculcates all the published and unpublished works from all the secondary materials to the researcher's point of view. Its main objective is to increase the knowledge on this area. it formulates the techniques and methods used in this research.

Saurabh C. Dubey et al.[3] created a model using ANN and Back-propogation to avert credit card frauds which causes a significant loss in every sector. ANN is a neural network which functions similar to our brains and when compared with different algorithms it yields exact results. To implement this model, the data of the customer is gathered with different number of attributes which helps the model to identify in which situation the transaction is fraud or non-fraud. They splitted the dataset in the ratio where eighty percent is training data and rest of the data is testing and validation data. This model gives good results and will be beneficial for real time detection.

Ruttala Sailusha et al. [4]implemented two machine learning algorithms to detect the counterfeit transactions. First one is Random Forest and the another one is Adaboost. The outcomes are generated using evaluation metrics namely Accuracy , Precision , recall and F1 score. Both the algorithms are compared on the basis of these evaluation metrics and also ROC curve is plotted for better visualization of good algorithm.

Samidha Khatri et al.[5] presented an analogy between different supervised learning algorithms for the detection of real or counterfeit transactions. The models used in the paper are as follows: Decision Tree, KNN, Random Forest, Naive Bayes and Logistic regression on the imbalanced dataset from the Kaggle where transactions are done by European cardholders. The Precision , Time and sensitivity are used to predict the best model in detecting the fraud transactions.

S. Dhankhad et al.[6] has applied Supervised ML techniques to recognize the fraudulent transactions. In addition , they implemented a super classifier by using various ensemble learning methods. They also recognize the most significant variables that prompt for good accuracy in fraud detection. Furthermore, the comparison of various algorithms and super classifier executed in this paper is done.

S. M. S. Askari et al.[7] has proposed an algorithm named Fuzzy-ID3 as due to exponential development of the Credit Card clients the fraud has expanded drastically. Due to the similarity in the transactions it has become very difficult to identify which transaction is fraud or normal. So, in this paper, Intermediary nodes were split utilizing variables having largest Information Gain. Then, the leaf nodes categorize the transactions as suspicious, counterfeit or real. Trial result shows that the procedure is productive one in distinguishing fakes.

©IJRASET: All Rights are Reserved

Zahra Kazemi et al.[8] presented a deep learning technique which is a part of machine learning and showing great results in detecting credit card fraud. So, here the deep autoencoder is used to derive important features which would be helpful in determining which transaction is fraud or not. After that , a softmax layer is added at the end to determine the labels whether 0 or 1. This method is really beneficial for huge datasets and also gives good accuracy as compared to others techniques.

M. F. Zeager et al.[9] used Adversarial learning method to display the scammer's optimum procedure and proactively adjusts the system to sort the transactions into real or fraud. Applying logistic regression as the detection classifier , they recognize the optimum approach for the adversary on the basis of number of fraudulent transactions which go unidentified and conclude that adversary utilizes this procedure for upcoming transactions to enhance the result of the classifier. Previous research shows the use of Game Theoretic models for adversarial learning in the fields of credit card , email spam etc, but this paper extends this idea into experiment using real-life example. Test outcomes shows the above framework constructs an expanding AUC scores on validation data.

Sangeeta Mittal et al.[10] presented Supervised and Unsupervised algorithms to identify frauds in an imbalanced dataset. In this paper , it is concluded that unsupervised machine learning models operate the distortion in the dataset and provide best results. Different criteria of evaluation are used for assessing the performance of each model and the graph is plotted representing the accuracy of each model. For future work , they focus on resampling techniques to minimize the skewness of the dataset.

S. Xuan et al.[11] used two types of Random Forest classifier for training the behavorial characteristics of credit card transactions. The types are: Random tree based random forest and CART based random forest. The comparison is drawn to examine the performance of the classifiers on the dataset. Furthermore, performance measures are calculated to measure the model's effectiveness.

## III. COMPARISON OF VARIOUS FRAUD DETECTION TECHNIQUES

| Author's Name | Technique | Advantages/ Features | Disadvantages/ Improvements |
|---|---|---|---|
| Saurabh C. Dubey et al. | Artificial Neural Network(ANN) | Proposed deep learning algorithm, produces better results. | This algorithm is difficult to handle as sometimes it produces same results with incomplete information too. |
| Ruttala Sailusha et al. | Random Forest and Adaboost algorithm | Both the algorithms are considered as the best algorithm. | New machine learning algorithms can be used in future for better prediction. |
| Samidha Khatri et al. | Various Machine Learning Algorithms are used. | Out of all the techniques , Decision tree is selected as preferred model. | Future enhancement will be to apply re-sampling techniques for better results. |
| Shiyang Xuan et al. | Random Forest and CART | These algorithms works good in small datasets. | Future work will focus on the problems of imbalanced data. |
| M. Kavitha et al. | Meta-Classifiers | On two processing layers, an effective meta-classifier model is proposed. | Future work will aim to make better prediction rates. |
| Zahra Kazemi et al. | Deep auto-encoder | Using Deep networks improves the detection rate. | In future work, CNN and RCNN can be used. |
| S Md. S Askari et al. | Fuzzy ID3 | Authors have applied fuzzy logic technique to propose ID3 decision tree approach. | Further work would involve Fuzzy concept to predict the fraud accurately. |
| Mary Frances Zeager et.al | Adversarial Learning | Adversarial framework outperforms other static models. | Future improvements includes addition of velocity variables. |

Table i: Comparison of Techniques

©IJRASET: All Rights are Reserved

## IV. CONCLUSIONS

Credit card has become a need of every individual nowadays and due to this , frauds are also taking place rapidly. The best plan for fraud detection is by considering their history of transactions to know which is fraudulent or genuine. This paper includes several techniques that are proposed to minimize or avoid the credit card fraud. Furthermore, the advantages and disadvantages of methods were cited and compared. But there is a need to improve in the techniques for better results to avoid fraudulent activities in the future.

## REFERENCES

[1] K. Modi and R. Dayma, "Review on fraud detection methods in credit card transactions," 2017 International Conference on Intelligent Computing and Control (I2C2), Coimbatore, 2017, pp. 1-5.

[2] https://spd.group/machine-learning/credit-card-fraud-detection/[Accessed on 5 july, 2020]

[3] S. C. Dubey, K. S. Mundhe and A. A. Kadam, "Credit Card Fraud Detection using Artificial Neural Network and BackPropagation," 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2020, pp. 268-273.

[4] R. Sailusha, V. Gnaneswar, R. Ramesh and G. R. Rao, "Credit Card Fraud Detection Using Machine Learning," 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2020, pp. 1264-1270.

[5] S. Khatri, A. Arora and A. P. Agrawal, "Supervised Machine Learning Algorithms for Credit Card Fraud Detection: A Comparison," 2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 2020, pp. 680-683.

[6] S. Dhankhad, E. Mohammed and B. Far, "Supervised Machine Learning Algorithms for Credit Card Fraudulent Transaction Detection: A Comparative Study," 2018 IEEE International Conference on Information Reuse and Integration (IRI), Salt Lake City, UT, 2018, pp. 122-125.M. Wegmuller, J. P. von der Weid, P. Oberson, and N. Gisin, "High resolution fiber distributed measurements with coherent OFDR," in *Proc. ECOC'00*, 2000, paper 11.3.4, p. 109.

[7] S. M. S. Askari and M. A. Hussain, "Credit card fraud detection using fuzzy ID3," 2017 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, 2017, pp. 446-452. (2002) The IEEE website. [Online]. Available: http://www.ieee.org/

[8] Z. Kazemi and H. Zarrabi, "Using deep networks for fraud detection in the credit card transactions," 2017 IEEE 4th International Conference on Knowledge-Based Engineering and Innovation (KBEI), Tehran, 2017, pp. 0630-0633.

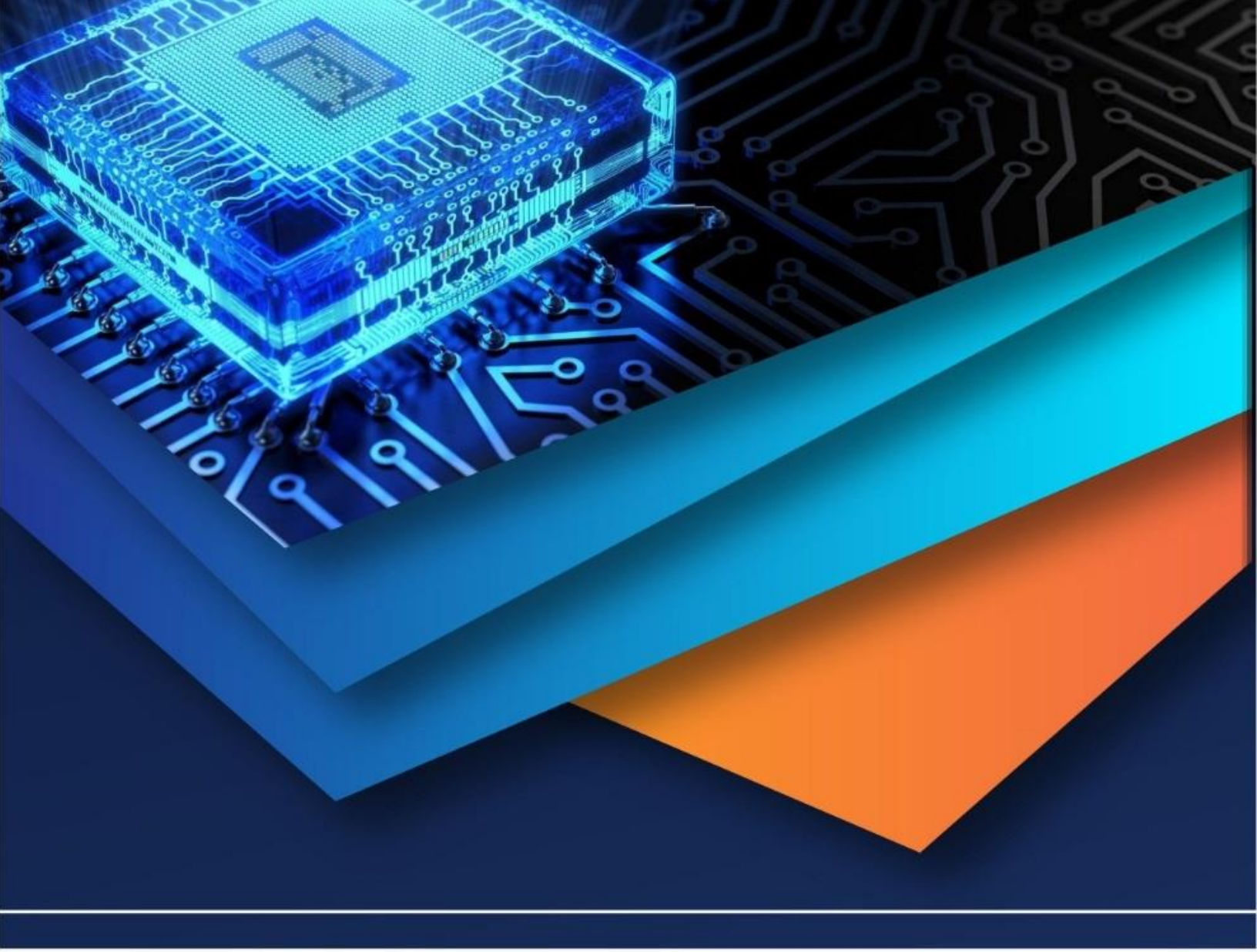
[9] M. F. Zeager, A. Sridhar, N. Fogal, S. Adams, D. E. Brown and P. A. Beling, "Adversarial learning in credit card fraud detection," 2017 Systems and Information Engineering Design Symposium (SIEDS), Charlottesville, VA, 2017, pp. 112-116.

[10] S. Mittal and S. Tyagi, "Performance Evaluation of Machine Learning Algorithms for Credit Card Fraud Detection," 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 2019, pp. 320-324.

[11] S. Xuan, G. Liu, Z. Li, L. Zheng, S. Wang and C. Jiang, "Random forest for credit card fraud detection," 2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC), Zhuhai, 2018, pp. 1-6.

[12] M. Kavitha, Dr. M. Suriakala, "Real Time Credit Card Fraud Detection on Huge Imbalanced Data using Meta-Classifiers", *Proceedings of the International Conference on Inventive Computing and Informatics (ICICI 2017)*, Vol. 45, SU-76, pp. 34-40, April 2017

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)