# Credit Card Fraud Detection Techniques

**Greeshma N Pai[1], Kirana R[2], Likhitha[3], Madhushree N[4]**

[1,2,3,4]*UG Students, Dept. of Computer Science and Engineering, BNM Institute of Technology, Bangalore, India*

---

**Abstract**— *Credit card frauds are easy and friendly targets. E-commerce and many other online sites have increased the online payment modes, increasing the risk for online frauds. Increase in fraud rates, researchers started using different machine learning methods to detect and analyse frauds in online transactions. Frauds are known to be dynamic and have no patterns, hence they are not easy to identify. Fraudsters use recent technological advancements to their advantage. They somehow bypass security checks, leading to the loss of millions of dollars. Analyzing and detecting unusual activities using data mining techniques is one way of tracing fraudulent transactions. transactions. This paper gives a survey of multiple machine learning methods such as k-nearest neighbor (KNN), random forest, naive bayes, logistic regression and support vector machines (SVM) as well as the deep learning methods such as autoencoders, convolutional neural networks (CNN), restricted boltzmann machine (RBM) and deep belief networks (DBN).*

***Keywords***—credit card, fraud detection, machine learning, deep learning, random forest, k nearest neighbor, support vector machine, autoencoder, restricted boltzmann machine, deep belief networks, convolutional neural networks

## 1. INTRODUCTION

'Fraud' in credit card transactions is unauthorized and is the unwanted usage of an account by someone other than the owner of that account. Credit Card Fraud can be defined as a case where a person uses someone else's credit card for personal reasons while the owner and the card issuing authorities are unaware of the fact that the card is being used. This is a very relevant problem that demands the attention of communities such as machine learning and data science where the solution to this problem can be automated. This problem is particularly challenging from the perspective of learning, as it is characterized by various factors such as class imbalance. The number of valid transactions far outnumber fraudulent ones. Also, the transaction patterns often change their statistical properties over the course of time. These are not the only challenges in the implementation of a real-world fraud detection system, however. In real world examples, the massive stream of payment requests is quickly scanned by automatic tools that determine which transactions to authorize.

Credit card is the most popular mode of payment. As the number of credit card users is rising world-wide, the identity theft is increased, and frauds are also increasing. In the virtual card purchase, only the card information is required such as card number, expiration date, secure code, etc. Such purchases are normally done on the Internet or over telephone. To commit fraud in these types of purchases, a person simply needs to know the card details. The details of credit card should be kept private. Different ways to steal credit card details are phishing websites, steal/lost credit cards, counterfeit credit cards, theft of card details, intercepted cards etc. Necessary prevention measures can be taken to stop this abuse and the behaviour of such fraudulent practices can be studied to minimize it and protect against similar occurrences in the future.

Fraud detection methods are continuously developed to defend criminals in adapting to their fraudulent strategies. These frauds are classified as:

- Credit Card Frauds: Online and Offline
- Card Theft • Account Bankruptcy
- Device Intrusion
- Application Fraud
- Counterfeit Card
- Telecommunication Fraud

In this paper, three datasets are considered. They are the European dataset, the Australian dataset and the German dataset. In this work, the different Machine Learning and Deep Learning techniques are benchmarked. An ensemble of the best three performing models is also applied all three datasets.

Machine learning is one of the hottest topics of this decade and a subset of Artificial Intelligence. Machine learning is a combination of various computer algorithms and statistical modelling to allow the computer to perform tasks without hard coding. The acquired model would be learning from the "training data". Predictions can be made, or actions can be performed from stored experiential knowledge. Deep learning models are a part of machine learning techniques which involves Artificial Neural Networks. Convolutional neural networks, Deep Belief Network, Auto-encoders, Recurrent Neural Network, and Restricted Boltzmann Machine are all various methods. A properly trained NN would have the capability to capture unique relationships over the whole dataset.

Some of the currently used approaches to detection of such fraud are:

- Artificial Neural Network
- Fuzzy Logic
- Genetic Algorithm

- Logistic Regression
- Decision tree
- Support Vector Machines
- Bayesian Networks
- Hidden Markov Model
- K-Nearest Neighbour

## 2. LITERATURE SURVEY

Unconventional techniques such as hybrid data mining/complex network classification algorithm is able to perceive illegal instances in an actual card transaction data set, based on network reconstruction algorithm that allows creating representations of the deviation of one instance from a reference group have proved efficient typically on medium sized online transaction. There have also been efforts to progress from a completely new aspect. Attempts have been made to improve the alert feedback interaction in case of fraudulent transaction. In case of fraudulent transaction, the authorised system would be alerted and a feedback would be sent to deny the ongoing transaction. Artificial Genetic Algorithm, one of the approaches that shed new light in this domain, countered fraud from a different direction. It proved accurate in finding out the fraudulent transactions and minimizing the number of false alerts. Even though, it was accompanied by classification problem with variable misclassification costs[1].

Multiple Supervised and Semi-Supervised machine learning techniques are used for fraud detection, but the aim is to overcome three main challenges with card frauds related dataset i.e., strong class imbalance, the inclusion of labelled and unlabelled samples and to increase the ability to process a large number of transactions. Different supervised machine learning algorithms like Decision Trees, Naive Bayes Classification, Least Squares Regression, Logistic Regression and Support Vector Machines are used to detect fraudulent transactions in real-time datasets. Two methods under random forests are used to train the behavioural features of normal and abnormal transactions. They are Random-tree-based random forest and CART-based. Even though random forest obtains good results on small set data, there are still some problems in case of imbalanced data. The algorithm of the random forest itself should be improved. Performance of Logistic Regression, K-Nearest Neighbour, and Naïve Bayes are analysed on highly skewed credit card fraud data where research is carried out on examining meta-classifiers and meta-learning approaches in handling highly imbalanced credit card fraud data. Though supervised learning methods can be used, there may fail at certain cases of detecting the fraud cases. A model of deep Auto-encoder and restricted Boltzmann machine (RBM) is used to construct normal transactions to find anomalies from normal patterns. Not only that, a hybrid method is developed with a combination of Adaboost and Majority Voting methods[2][3].

In [4], a empirical comparison is made of various machine learning and deep learning models. The performance of various models is compared using data sets with different sizes, complexities and characteristics with the goal to come up with recommendations on best practices of picking the most suitable model for a fraud detection application given the data of particular description. In particular, the performance of Support Vector Machine, KNN and Random forest to Deep Learning methods such as Autoencoder's, RBM, DBN and CNN are compared.

A meta-classification strategy is applied in improving credit card fraud detection. The approach consists of three base classifiers constructed using the decision tree, naïve Bayesian, and k-nearest neighbour algorithms. Using the naïve Bayesian algorithm as the meta-level algorithm to combine the base classifier predictions, the result shows 28% improvement in performance[5]. Most of the algorithms deal with unbalanced data sets where the amount of fraud is very low. The main evaluation metrics for fraud detection are True Positive Rate, False Negative Rate and Matthews Correlation Coefficient. Some studies recommend using Neural Networks as a solution for unbalanced datasets. In Tom Sweers' thesis[6], his methodology of introducing Autoencoders to normal data and detecting fraud based on reconstruction error is unique. It can also been seen how deep learning fails when there is less instances in a dataset. Working with smaller dataset failed to achieve good prediction scores. This shows that not always deep learning would able to solve problems for smaller dataset. While Chouiekha et al. [7] report that DCNN and outperforms SVMs, Random Forest and Gradient Boosted Classifier, Tuyls et al. [8], confirm that Artificial Neural Networks have a much faster fraud catching process compared to Bayesian Belief Networks.

A comprehensive survey conducted by Clifton Phua and his associates have revealed that techniques employed in this domain include data mining applications, automated fraud detection, adversarial detection. In another paper, Suman, Research Scholar, GJUS&T at Hisar HCE presented techniques like Supervised and Unsupervised Learning for credit card fraud detection. Even though these methods and algorithms fetched an unexpected success in some areas, they failed to provide a permanent and consistent solution to fraud detection.

A study of the issues and results associated with credit card fraud detection using meta-learning is geared towards investigating distribution of frauds and non-frauds that will lead to better performance, best learning algorithms between meta-learning strategy. The results show that given a skewed distribution in the original data, artificially more balanced training data leads to better classifiers. It demonstrate how meta-learning can be used to combine different classifiers and maintain, and in some cases, improve the performance of the best classifier. Multiple algorithms for fraud detection are investigated in and results indicate that an adaptive solution can provide

fraud filtering and case ordering functions for reducing the number of final-line fraud investigations necessary [9].

A comparison of logistic regression and naive bayes shows that even though the discriminative logistic regression algorithm has a lower asymptotic error, the generative naive Bayes classifier may also converge more quickly to its (higher) asymptotic error. There are a few cases reported in which logistic regression's performance underperformed that of naive Bayes, but this is observed primarily in particularly small datasets. Another comparative study on credit card fraud detection using Bayesian and neural networks shows that Bayesian network performs better than neural network in detecting credit card fraud.

Back-propagation (BP), together with naive Bayesian (NB) and C4.5 algorithms are applied to skewed data partitions derived from minority oversampling with replacement. The study shows that innovative use of naive Bayesian (NB), C4.5, and back-propagation (BP) classifiers to process the same partitioned numerical data has the potential of getting better cost savings. An adaptive and robust model learning method that is highly adaptive to concept changes and is robust to noise. Three different classification methods, decision tree, neural networks and logistic regression are tested for their applicability in fraud detections. The results show that the proposed classifier of neural networks and logistic regression approaches outperform decision tree in solving the problem under investigation.

Detection of credit card fraud using decision trees and support vector machines is investigated and the results show that the proposed classifiers of decision tree approaches outperform Support Vector Machine approaches in solving the problem under investigation. In another study, classification models based on Artificial Neural Networks (ANN) and Logistic Regression (LR) are developed and applied on credit card fraud detection problem using a highly skewed data. The results show that the proposed ANN classifiers outperform LR classifiers in solving the problem under investigation. The logistic regression classifiers tend to over fit the training data as it increases. This is due to lack of adequate sampling in the work.

Fig 2.1 refers to the flowchart for Credit Card Fraud Detection. Machine Learning algorithms are employed to analyse all the authorized transactions and report the suspicious ones. These reports are investigated by professionals who contact the cardholders to confirm if the transaction was genuine or fraudulent

The investigators provide a feedback to the automated system which is used to train and update the algorithm eventually improve the fraud-detection performance over time.

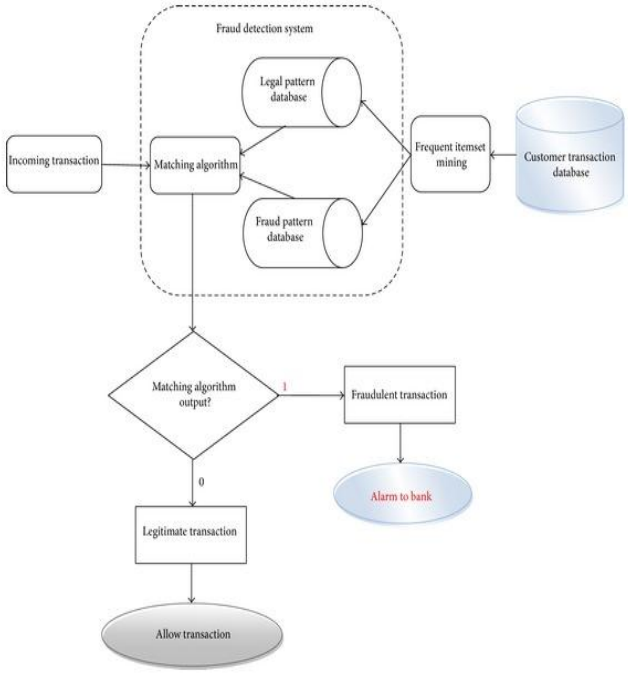


Fig 2.1: Flowchart for Credit Card Fraud Detection

### Algorithm steps for finding the Best algorithm:

Step 1: Import the dataset
Step 2: Convert the data into data frames format
Step 3: Do random sampling
Step 4: Decide the amount of data for training and testing
Step 5: Assign train dataset to the models
Step 6: Apply different machine learning and Deep learning
Algorithms and create the model
Step 7: Make predictions for test dataset for each Algorithm.
Step 8: Calculate the accuracy of each by using Confusion matrix

**Test data:** After training is done on the dataset then testing process take place.

**Outcome for test data**: The respective results for each algorithm and performance is displayed in graphs.

**Accuracy results:** Finally results of each algorithm are shown with accuracy and the best algorithm is identified.

**Evaluation:** There are a variety of measures for various algorithms and these measures have been developed to evaluate very different things. So it should be criteria for evaluation of various proposed method. False Positive (FP), False Negative(FN), True Positive(TP), True Negative(TN) and the relation between them are quantities which usually adopted by credit card fraud detection researchers to compare the accuracy of different approaches. The definitions of mentioned parameters are presented below:

**True Positive(TP):** The true positive rate represents the portion of the fraudulent transactions correctly being classified as fraudulent transactions.True positive=TP/TP+FN.

**True Negative(TN):** The true negative rate represents the portion of the normal transactions correctly being classified as normal transactions. True negative=TN/TN+FP.

**False Positive (FP):** The false positive rate indicates the portion of the non-fraudulent transactions wrongly being classified as fraudulent transactions. False positive=FP/FP+TN.

**False Negative (FN):** The false negative rate indicates the portion of the non-fraudulent transactions wrongly being classified as normal transactions. False negative=FN/FN+TP

**Confusion matrix:** Fig 2.2 refers to the Confusion Matrix. The confusion matrix provides more insight into not only the performance of a predictive model, but also which classes are being predicted correctly, which incorrectly, and what type of errors are being made.

| Predicted | Positive | Negative |
|---|---|---|
| Positive | TP | FN |
| Negative | FP | TN |

Fig 2.2: Confusion Matrix

**Accuracy:** Accuracy is the percentage of correctly classified instances. It is one of the most widely used classification performance metrics.
Accuracy=Number of correct predictions / Total Number of predictions
Or for binary classification models, the accuracy can be defined as:
Accuracy= TP+TN / (TP+TN+FP+FN)

**Precision and recall:** Precision is the number of classified Positive or fraudulent instances that actually are positive instances.
Precision = TP/(TP+FP).
Recall is a metric that quantifies the number of correct positive predictions made out of all positive predictions that could have been made. Unlike precision that only comments on the correct positive predictions out of all positive predictions, recall provides an indication of missed positive predictions. Recall is calculated as the number of true positives divided by the total number of true positives and false negatives.
Recall = TP / (TP + FN).

**F1 score:** F1 Score is the weighted average of Precision and Recall. Therefore, this score takes both false positives and false negatives into account.

F1 Score = 2*(Recall * Precision) / (Recall + Precision).

**Support:** The support is the number of samples of the true response that lie in that class. Support is the number of actual occurrences of the class in the specified dataset. Imbalanced support in the training data may indicate structural weaknesses in the reported scores of the classifier and could indicate the need for stratified sampling or rebalancing. Support doesn't change between models but instead diagnoses the evaluation process.

## 3. CONCLUSIONS

Research related to Fraud Detection has been around for over 20 years now and has used various methods from manual checking to customer end authentication. Machine learning models have also had wide successes in this area. Deep learning models have been recently adopted in many applications enabled by the rise in higher computation power and cheap computing cost.

This paper provides an empirical investigation comparing various machine learning and deep learning models on different data sets for the detection of fraudulent transaction. The main aim of this study is to find insights of which methods would be best suitable for which type of datasets. As nowadays, many companies are investing in new techniques to improve their business this paper could potentially help practitioners and companies to better understand how different methods work on certain types of datasets.

A limitation of this study is however that it only deals with detecting fraud in a supervised learning context. Although supervised learning KNN, Random Forest seem attractive and produce good results, they do not work well for dynamic environments. Fraud patterns typically change over time and would be hard to catch. New data sets would need to be collected and machine learning models need to be retained.

In this paper, we studied applications of machine learning like Naïve Bayes, Logistic regression, Random forest with boosting and shows that it proves accurate in deducting fraudulent transaction and minimizing the number of false alerts. Supervised learning algorithms are novel one in this literature in terms of application domain. If these algorithms are applied into bank credit card fraud detection system, the probability of fraud transactions can be predicted soon after credit card transactions. And a series of anti-fraud strategies can be adopted to prevent banks from great losses and reduce risks.

Our study reveals that to detect fraud, the best methods with larger datasets would be using SVMs, potentially combined with CNNs to get a more reliable performance.
For the smaller datasets, ensemble approaches of SVM, Random Forest and KNNs can provide good enhancements. Convolutional Neural Networks (CNN) usually, outperforms other deep learning methods such as Auto encoders, RBM and DBN methods such as CNN,

## REFERENCES

[1] Credit Card Fraud Detection using Machine Learning and Data Science by S P Maniraj , Aditya Saini, Swarna Deep Sarkar and Shadab Ahmed, International Journal of Engineering Research & Technology (IJERT), Vol. 8 Issue 09, September-2019. Available: www.ijert.org

[2] Credit card fraud detection using Machine learning algorithms by AndhavarapuBhanusri, K.RatnaSree Valli , P.Jyothi , G.Varun Sai , R.Rohith Sai Subash, Journal of Research in Humanities and Social Science Volume 8 ~ Issue 2 (2020). Available:www.questjournals.org

[3] Credit Card Fraud Detection using Machine Learning Algorithms by Vaishnavi Nath Dornadulaa and Geetha S, international conference on recent trends in advanced computing 2019, icrtac 2019. Available: www.sciencedirect.com

[4] Fraud Detection using Machine Learning and Deep Learning by Pradheepan Raghavan and Neamat El Gayar, 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE) December 11–12, 2019, Amity University Dubai,UAE. Available: ieeexplore.ieee.org

[5] Credit card fraud detection using Machine Learning Techniques by John O. Awoyemi, Adebayo O. Adetunmbi and Samuel A. Oluwadare

[6] Tom Sweers. "Auto encoding Credit Card Fraud". Bachelor Thesis, Radboud University, June 2018.

[7] Alae Chouiekha, EL Hassane Ibn EL Haj. "ConvNets for Fraud Detection analysis". Procedia Computer Science 127, pp.133–138. 2018.

[8] S. Maes, K. Tuyls, B. Vanschoenwinkel, B. Manderick. "Credit Card Fraud Detection Using Bayesian and Neural Networks". 2002. [Online]. Available: https://www.researchgate.net/publication/2524707_Credit_Card_Fraud_Detection_Using_Bayesian_and_Neural_Networks.

[9] Stolfo, S., Fan, D. W., Lee, W., Prodromidis, A., & Chan, P. (1997). Credit card fraud detection using meta-learning: Issues and initial results. In AAAI-97 Workshop on Fraud Detection and Risk Management