Credit Card Fraud Detection Using Machine Learning

**ABSTRACT:**

**This is a complete report on a fraud detection system that has been built using machine learning algorithms which will help detect fraudulent transactions before they occur. The world is clearly going the digital way and thus most of the things we do will be using our mobile devices and laptops. This increased reliance on digital devices requires that better security measures be put in place to safeguard our privacy and most importantly to ensure authenticity. The system was developed to ensure that acts of fraud in where transactions are involved are dealt with accordingly before it is too late. A program for machine learning that can confirm the legitimacy of transactions in by decreasing the time required to authenticate a single transaction in traditional systems, real-time (at the point of sale or transaction) would significantly help to reduce fraud. An application that can validate transactions in real-time before they are transferred to the blockchain, beyond which it is typically hard to reverse transactions, would be very helpful for the adoption of new-age technologies like blockchain and bitcoin. A machine learning algorithm fitting component is also a part of the program; it trains and tests a machine learning algorithm by fitting it to the known data. The algorithm's model evaluation component, which evaluates the model's performance using the supplied data, is its final part. This score determines whether a flag message indicating whether a transaction is false or real is returned. A logistic regression machine learning algorithm is used in the development of the application. A machine learning approach for classification called logistic regression gives a binary score based on the values of the classes. Regression in logistics is frequently used to solve categorization and forecasting issues. The probability of an event occurring, such as yes or no, male or female, ` or negative, and so on, is predicted using this method.**

**Keywords – Fraud, machine-learning, transactions, regression, algorithm, data.**

# Introduction:

When someone uses other user's credit card without their consent, a fraudulent credit card transaction occurs. By evaluating and analyzing these fraudulent transactions, security measures against such fraudulent acts should be put into place with the aim of preventing similar occurrences in the future. In conclusion, a credit card transaction is any instance a credit card is used to pay for something. When a fraudster uses other user's credit card without the owner's knowledge or authorization for personal expenses, the credit card issuing authorities or institutions may not be aware of the fraud.

User activity must be monitored in order to identify fraud and prevent unexpected activity like intrusion, fraud, and defaults. This is a key issue that requires the application of disciplines like machine learning and data science with the aim of automating the solution. From an educational perspective, this issue is particularly challenging to address because it has multiple characteristics, like class imbalance. The number of legitimate transactions greatly exceeds the number of fraudulent ones.

The technology we use today to do everyday activities like shopping, business, banking, and many of our hobbies is advancing quickly and for our benefit. In addition to numerous organizations, individuals concentrate on hobbies and business ventures that are compatible with digital technology as we move toward a world where all problems are solved digitally. In addition, scammers now have more chances because to this digital change.

Traditional fraud techniques are being replaced by more modern digital fraud techniques that make use of new technology currently where data held online has become so vital.

Technologies created to combat fraudsters trying to exploit holes in technical infrastructures utilized by businesses or individuals are also being developed at a rapid rate every day build a defense, shielding people and institutions.

What exactly is this idea of digital fraud, then? It is helpful to thoroughly understand this risk prior to making any necessary plans for precautions. This article has been written to help you comprehend the idea of fraud and fraud detection, familiarize yourself with the risks, and make plans for precautions.

The complete procedure used by institutions to spot fraudulent activity is referred to as fraud detection. These operations can take financial or other forms, such as hacking, data theft, or fraudulent credit card transactions. Fraud detection is typically carried out using techniques to forecast aberrant behavior while considering established rule flows.

Methods for detecting fraud can also be varied. In order to deal with the rising number of fraud cases brought on by increased digitization, fraud detection products that can be tailored in terms of the technology utilized, the processes established, and the industry in which they are employed, are also evolving quickly.

It is crucial that the techniques created for detecting fraud keep up with technological advancements, identify weaknesses before fraudsters do, and close any gaps that may exist.

doors open to scammers. Numerous con artists examine established patterns and take advantage of weaknesses. The possibilities offered by the always evolving technology are both the best friend of fraud detection and the best buddy of fraudsters.

**Motivation:**

There is increased adoption of mobile and digital baking. The use of these methods has eased the way of life for many people across the world. In addition, new emerging technologies such as e-commerce, remote assistance, digital learning, and so on, have pushed many individuals, businesses, and corporates into adopting digital methods of payment.

The adoption is digital methods of payment does, however, present multiple challenges, that many individuals and corporate entities long for solutions to. Credit card fraud has emerged as a key challenge to digital money transfer, and banking, with daily increasing cases of fraud across the globe. This raises a high need for a lasting digital solution that can be able to curtail this problem in real-time preventing loss of money, and also saving individuals and businesses long periods of verifying authentic and fake transactions.

Therefore, we have decided to implement a solution such as follows:

A credit card fraud machine learning application is an urgently needed solution to the problem of credit card fraud, both in money transfer, and service acquisition.

A machine learning application that can verify the authenticity of transactions in

real-time (at the point of sale or transaction), will greatly help alleviate fraud by reducing the time needed to verify a single transaction in traditional systems.

The adoption of new-age technologies such as blockchain, and cryptocurrency could greatly benefit from an application that can verify the transaction in real-time before they are sent to the blockchain, beyond which, it is, in most cases, impossible to reverse transactions.

**Objectives:**

* To build an application that deploys supervised machine learning techniques and algorithms in the verification of transactions.
* To build a machine learning pipeline that can score high accuracy even on new data.
* To build a machine learning application that has a perfect tradeoff between training time, and performance.
* To build a credit fraud detection machine learning that is not biased by imbalanced data.
* To build an application that can be deployed in any platform that uses transactions in its day-to-day operations.

**Related Work:**

**1 Sift**

* **Sift** - Sift provides global coverage and protection for leading payment methods. Watch the demo. Proactively stop digital **fraud**, chargebacks & easily **detect fraud** trends on your site. Prevent Content Spam. **Detect** Payment **Fraud**. Chargeback Prevention. Block Fake Accounts.
* Sift's end-to-end solution eliminates the need for disjointed tools, specialized software, and insufficient insights that deplete operational resources.
* When it comes to risk operations, the Sift Digital Trust & Safety Platform adds connected data, adaptability, and intelligent automation where other fraud technologies fall short.

Graphical user interface, application, website

Description automatically generated

**2** **seon**

* **Seon** - Built with advanced tools and real-time detection, SEON gives your online business the next wave of anti-fraud solutions. Services offered are like Day one protection, Real-time data enrichment, Flexible integration, Boost revenue opportunities.
* Stop fraud before it occurs with unrivaled speed, scale, depth, and breadth. Improve your risk assessments by using real-time data from digital, social, phone, email, IP, and devices.
* A review from a customer

" Over the course of a few months, I put a few new rules to the test and was able to increase SEON's auto approval accuracy from 95% to 99.5%. Updating your SEON rules is a time investment that yields excellent returns. Best of all, we can accomplish it all without using any software. It is very time and resource efficient from a technical standpoint, which enables us to respond considerably faster." Phillipp Keller Manager of Senior Products

Graphical user interface, website

Description automatically generated

**Proposed Framework:**

## Implementation

The application is built using a logistic regression machine learning algorithm. Logistic regression is a classification machine learning algorithm, that returns a binary score on class values.

Logistics regression is widely deployed for use in classification ad predictive analysis problems. This algorithm predicts the chance of an event occurring, such as yes or no, male or female, positive or negative, and so on. Since the outcome is a probability, the range of the dependent variable is 0 to 1. In logistic regression, a logit transformation is applied to the odds - the chance of success is divided by the probability of failure. This is what is referred to as the log odds - the natural logarithm of odds, as illustrated here:

Logit(pi) = 1/(1+ exp(-pi))

ln(pi/(1-pi)) = Beta\_0 + Beta\_1\*X\_1 + … + B\_k\*K\_k

Text

Description automatically generated

To assess model performance, the application uses the classification report and confusion matrix model evaluation methods to assess the model’s performance.

Text

Description automatically generated

# Features:

The application is comprised of a data preprocessing component, that can prepare new data for prediction in real-time.

The application is also comprised of a machine learning algorithm fitting component, that fits a machine learning algorithm with the known data, trains it, and tests it. The final component of the algorithm is the model evaluation component that assesses the model’s scoring on the provided data. It is from this score that a flag message is returned on whether a transaction is fake or authentic.

**Data description:**

## Dataset

The dataset used to train the machine learning model contains 5 rows and 32 columns. Of the columns, there are; time, amount, and transaction columns.

The dataset includes a feature column that classifies the transaction as fake or authentic.

## Feature Design & Feature Engineering

The main feature design and engineering operation are handling the imbalanced target feature that only has a few entities classified as fraud and most of the other transactions classified as authentic. As it is, the data could result in the model overfitting and overconfidence, hence a need to fix the data.

Chart, scatter chart

Description automatically generated

A visualization of the imbalance in the target column.

Graphical user interface, text

Description automatically generated

A code snippet of a sampling technique, that samples target values from the target columns for the class that has the least values. The result is a target column that contains fairly sampled entities from both classes, authentic and fake transactions.

**Results/Experimentation:**

## Analysis

An initial analysis is performed to check the class distribution of the target column.

Icon

Description automatically generated

The number of normal (authentic) transactions surpasses the number of fraudulent transactions by a huge margin. If fitted on the model, the model is more likely to vote on normal transactions than it would on fake transactions. Hence the need for deploying a sampling technique to randomly select a fair number of entities from both classes.

## Preliminary Results

The model scores a general accuracy of 90.35%.

The confusion matrix score indicates 94% correctly classified True Positives (TP), and 84% correctly classified True Negatives (TN). There are 5% of values classified as fraud that is not fraud and 14% of cases classified as authentic despite them being a fraudulent transaction.

This misclassification penalty is evidenced by the 87% Recall score.

Text

Description automatically generated

## Project Management

Credit card fraud is a sensitive problem that requires models that are extremely accurate in detecting fraudulent transactions. The applications despite scoring accuracy of 90%, still require improvement to ensure that there are very few or no cases of misclassified transactions.

The deployment of alternative fast-performing machine learning algorithms can be a good step towards improving the scoring power of the application. Alternative algorithms that have greatly minimized the MCC (Mathews Correlation Coefficient) score are Naïve Bayesian classifiers, Decision Trees, Random Forests, Gradient Boosted Trees (GBT), Decision Stump, Random Trees, Deep Learning Neural Networks (DLNN), and multilayer perceptron.

The sampling index for the application has been set based on the data used to build the application, however, in production, this number should be varied depending on the volume of data the application processes at a particular instance. Also, the application can be improved to return a classification score for a single instance transaction without the need for retraining the entire model.

**References:**

[1] [Dropout: a simple way to prevent neural networks from overfitting](http://jmlr.org/papers/volume15/srivastava14a/srivastava14a.pdf), by Hinton, G.E., Krizhevsky, A., Srivastava, N., Sutskever, I., & Salakhutdinov, R. (2014).

[2] [Learning deep features for scene recognition using places database](http://places.csail.mit.edu/places_NIPS14.pdf), by Lapedriza, À., Oliva, A., Torralba, A., Xiao, J., & Zhou, B. (2014). NIPS

[3] [Generative adversarial nets](http://datascienceassn.org/sites/default/files/Generative%20Adversarial%20Nets.pdf), by Bengio, Y., Courville, A.C., Goodfellow, I.J., Mirza, M., Ozair, S., Pouget-Abadie, J., Warde-Farley, D., & Xu, B.

[4] [High-Speed Tracking with Kernelized Correlation Filters](https://arxiv.org/pdf/1404.7584), by Batista, J., Caseiro, R., Henriques, J.F., & Martins, P. (2015). CoRR, abs/1404.7584.

[5] [A Review on Multi-Label Learning Algorithms](http://doi.ieeecomputersociety.org/10.1109/TKDE.2013.39), by  Zhang, M., & Zhou, Z. (2014). IEEE TKDE

[6] [How transferable are features in deep neural networks](http://papers.nips.cc/paper/5347-how-transferable-are-features-in-deep-neural-networks.pdf), by Bengio, Y., Clune, J., Lipson, H., & Yosinski, J. (2014) CoRR, abs/1411.1792.

[7] [Do we need hundreds of classifiers to solve real world classification problems](http://jmlr.org/papers/volume15/delgado14a/delgado14a.pdf), by Amorim, D.G., Barro, S., Cernadas, E., & Delgado, M.F. (2014).

[8] [Knowledge vault: a web-scale approach to probabilistic knowledge fusion](https://www.cs.cmu.edu/~nlao/publication/2014.kdd.pdf), by Dong, X., Gabrilovich, E., Heitz, G., Horn, W., Lao, N., Murphy, K., ... & Zhang

[9] [Scalable Nearest Neighbor Algorithms for High Dimensional Data](http://ieeexplore.ieee.org/document/6809191/), by Lowe, D.G., & Muja, M. (2014). IEEE Trans. Pattern Anal. Mach. Intell.,

[10] [Trends in extreme learning machines: a review](http://www.ntu.edu.sg/home/egbhuang/pdf/ELM-Suvey-Huang-Gao.pdf), by Huang, G., Huang, G., Song, S., & You, K. (2015).

[11] [A survey on concept drift adaptation](http://www.win.tue.nl/~mpechen/publications/pubs/Gama_ACMCS_AdaptationCD_accepted.pdf), by Bifet, A., Bouchachia, A., Gama, J., Pechenizkiy, M., & Zliobaite, I.  ACM Comput. Surv., 2014

[12] [Multi-scale Orderless Pooling of Deep Convolutional Activation Features](http://slazebni.cs.illinois.edu/publications/yunchao_eccv14_mopcnn.pdf), by Gong, Y., Guo, R., Lazebnik, S., & Wang, L. (2014).

[13] [Simultaneous Detection and Segmentation](https://arxiv.org/pdf/1407.1808), by Arbeláez, P.A., Girshick, R.B., Hariharan, B., & Malik, J. (2014) ECCV ,

[14] Adichie, J. N. [1967], “Estimates of regression parameters based on rank tests,” Ann. Math. Stat., 38, 894–904.

[15] Allen, D. M. [1971], “Mean square error of prediction as a criterion for selecting variables,” Technometrics, 13, 469–475.

[16] Allen, D. M. [1974], “The relationship between variable selection and data augmentation and a method for prediction,” Technometrics, 16, 125–127.

[17] Andrews, D. F. [1974], “A robust method for multiple linear regression,” Technometrics, 16, 523–531.

[18] [Microsoft COCO: Common Objects in Context](https://arxiv.org/pdf/1405.0312.pdf), by Belongie, S.J., Dollár, P., Hays, J., Lin, T., Maire, M., Perona, P., Ramanan, D., & Zitnick, C.L. (2014). ECCV.

[19] [Deep Residual Learning for Image Recognition](http://www.cv-foundation.org/openaccess/content_cvpr_2016/papers/He_Deep_Residual_Learning_CVPR_2016_paper.pdf), by He, K., Ren, S., Sun, J., & Zhang, X. (2016).

[20] [Batch Normalization: Accelerating Deep Network Training by Reducing Internal Covariate Shift](http://jmlr.org/proceedings/papers/v37/ioffe15.pdf), by Sergey Ioffe, Christian Szegedy (2015) ICML

[21] [Large-Scale Video Classification with Convolutional Neural Networks](http://www.cv-foundation.org/openaccess/content_cvpr_2014/papers/Karpathy_Large-scale_Video_Classification_2014_CVPR_paper.pdf), by Fei-Fei, L., Karpathy, A., Leung, T., Shetty, S., Sukthankar, R., & Toderici, G. (2014).