Fraud Detection in Credit Card Industry

Vinay Nagaraj
Bellevue University
Bellevue, NE 68005, USA
vnagaraj@my365.bellevue.edu

Abstract
Credit card fraud refers to the physical loss of credit card or loss of sensitive credit card information. Credit card frauds are a growing concern in the banking industry. Due to the rise and acceleration of E-Commerce, there has been a tremendous use of credit cards for online shopping which led to high amount of fraud related to credit cards. In addition, increasing dependence on new technologies such as cloud and mobile computing in recent years has compounded the problem. Fraud detection becomes challenging due to two main reasons – first, the profiles of normal and fraudulent behaviors change frequently and secondly due to reason that credit card fraud data sets are highly skewed [2]. The most common techniques used in fraud detection methods are Naïve Bayes {NB}, Support Vector Machines {SVM}, K-Nearest Neighbor algorithms {KNN} [1]. In this paper, we will see how Data Science techniques are used to detect fraud in Credit card Industry.

Author Keywords
Fraud detection; Credit card; Support Vector Machine; Kernel function; prediction.

ACM Classification Keywords
I.5.1. Pattern recognition; Models.

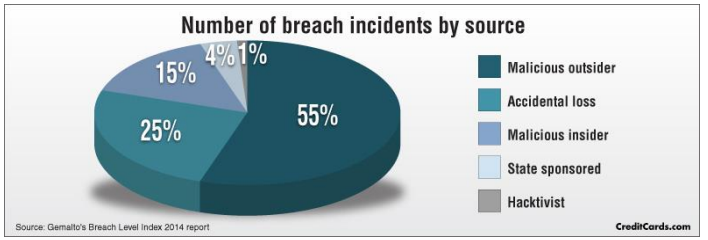
Introduction

Credit card fraud is a wide-ranging term for theft and fraud committed using or involving a payment card, such as a credit card or debit card, as a fraudulent source of funds in a transaction. Fraudsters look for sensitive credit card information to commit fraud. Credit card fraud is major issue and has considerable costs for financial institutions and card issuers. Although incidences of credit card fraud are limited to about 0.1% of all card transactions, they have resulted in huge financial losses, as the fraudulent transactions have been large value transactions. Credit card transactions had a total loss of 800 million dollars of fraud in U.S.A in 2004. In U.K, in the same year, the loss caused by the credit card fraud amounts to 425 million pounds (750 million U.S. dollars) [5]. Financial institutions like Visa and MasterCard have mandated that banks and merchants introduce EMV — Chip card technology, and biometric secured mobile payments to counter the fraud. EMV is a global standard where a chip, located in the plastic generates a unique cryptogram and sends it with the transaction. This makes it hard for criminals to replicate it & conduct fraud for card present Point of Sale transactions.

Apple, Google and Samsung – these tech giants have come up with mobile wallets with unique device account number protected by biometric security. Unique device account number (DPAN) is valid only for that particular device and will not be useful for others. Tokenization is also another highly effective data security measure designed to protect sensitive information from prying eyes. When applied to financial transactions, tokenization frees merchants from having to keep credit card data within their payment systems. This helps to reduce their PCI scope and expense. The primary advantage of tokenization is that it keeps credit card data safe — both from internal and external threats.

Common types of Credit card fraud

Credit card fraud comes in many different shapes and forms, including fraud that involves using a payment card of some description, and more.



Some of the most common types of credit card frauds are:

- Application Fraud: Application fraud generally happens in conjunction with identity theft. It happens when other people apply for credit or a new credit card in your name.
- Electronic or Manual Credit Card Imprints: This means that somebody skims information that is placed on the magnetic strip of the card. This is then used to encode a fake card or to complete fraudulent transactions.
- CNP (Card Not Present) Fraud: If somebody knows the expiry date and account number of your card, they can commit CNP fraud against you. It essentially means that somebody uses your card without actually being in physical possession of it.

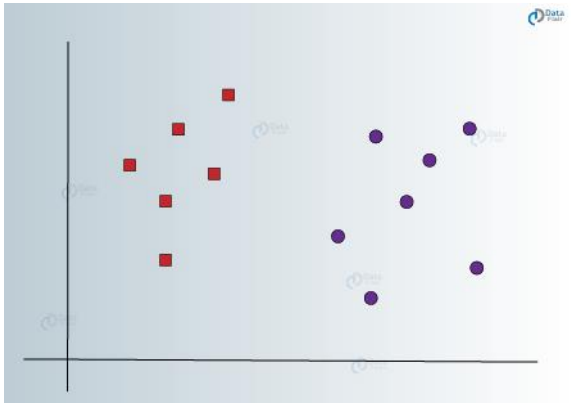
- Counterfeit Card Fraud: Counterfeit card fraud is usually committed through skimming. This means that a fake magnetic swipe card holds all your card details. This fake strip is then used to create a fraudulent card that is fully functional.
- Lost and Stolen Card Fraud: Here, your card will be taken from your possession, either through theft or because you lost it. The criminals who get their hands on it will then use it to make payments.
- Mail Non-Receipt Card Fraud: This type of fraud is also known as never received issue or intercept fraud. In this case, you were expecting a new card or replacement one and a criminal is able to intercept these. The criminal will then register the card and they will use it to make purchases and more.
- Account Takeover: Account takeover is actually one of the most common forms of credit card fraud. Basically, a criminal will somehow manage to get hold of all of your information and relevant documents. This is usually done online.

Models, Methods and Algorithms

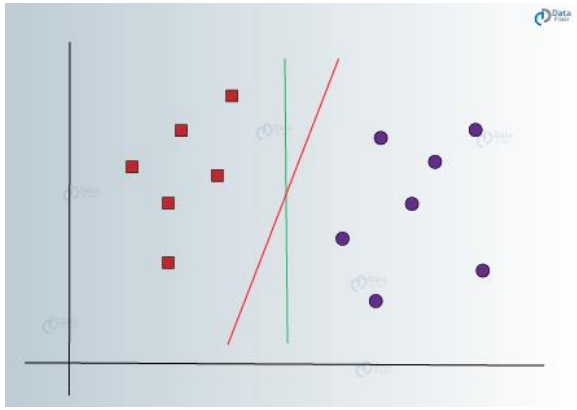
We have many models and methods to detect fraud in the credit card industry. In this paper, we will discuss one of the commonly used fraud detection techniques/method that is Support Vector Machines (SVM).

Support Vector Machine (SVM) is a statistical learning technique that is suitable for binary classification technique such as credit card fraud detection which only two classes are needed – The legitimate class and the fraudulent class. The theory of SVM is minimizing the expected error of learning machine, which reduce the over-fitting problem. It is a discriminative classifier formally defined by a separating hyperplane. In other words, given labeled training data (supervised learning), the algorithm outputs an optimal hyperplane which categorizes new examples. In two-dimensional space this hyperplane is a line dividing a plane in two parts where in each class lay in either side. The goal of SVM method is to construct a 'hyperplane' which separate the data instances into two classes: Positive & Negative.

The basic principle behind the working of Support vector machines is simple – Create a hyperplane that separates the dataset into classes [14]. In the graph provided below, you have to classify red triangles from blue circles. Your goal is to create a line that classifies the data into two classes, creating a distinction between red triangles and blue circles.

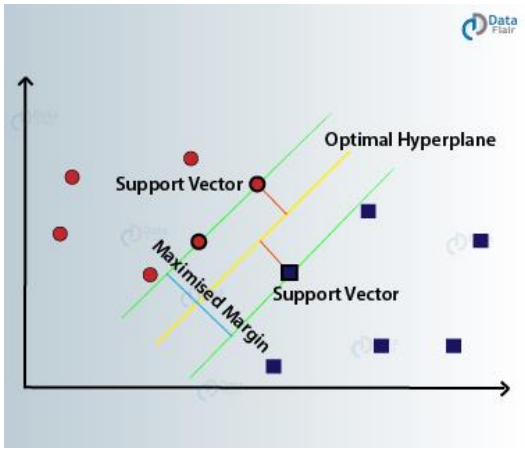


We might come up with something like below to separate the two classes. Any point that is left of line falls into red square class and on right falls into blue circle class. *Separation of classes*. That is what SVM does. It finds out a line/ hyper-plane. More than one line can be drawn that can separate the two classes or perform our task.

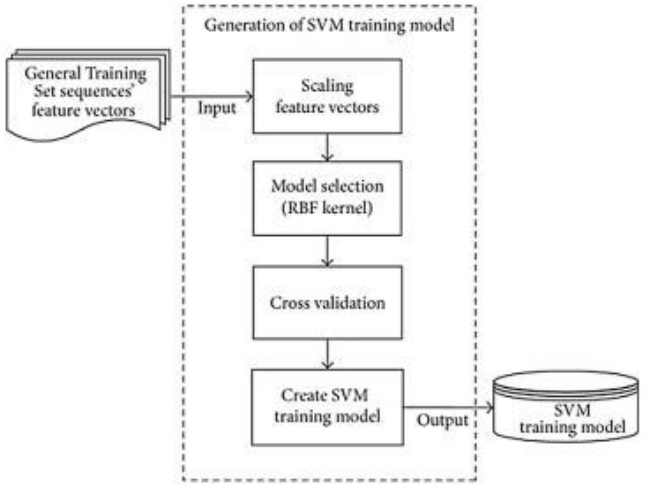


In the above figure, we have a green line and a red line. The red line is the ideal line as that partitions the two classes properly whereas ehe green line lies too close to the red class. Therefore, it does not provide a proper generalization which is our end goal.

According to SVM, we have to find the points that lie closest to both the classes. These points are known as support vectors. In the next step, we find the proximity between our dividing plane and the support vectors. The distance between the points and the dividing line is known as margin. The aim of an SVM algorithm is to maximize this very margin. When the margin reaches its maximum, the hyperplane becomes the optimal one.



Below figure shows the steps of a generation of SVM training model which is mostly used for any study.



In order to generate a training model [8], a "General Training Set" has to be prepared. All sequences in the

General Training Set will be formed by the training sequences that cannot be predicted by the sequence alignment method. This training set consists of an equal number of positive training and negative training sequences scaling the feature vectors before applying SVM for both test and training sequences is very important as it can improve the accuracy of the prediction. This is because the scaling process can help to avoid attributes in greater numeric ranges dominating those in smaller ranges. In addition, scaling can also avoid the numerical difficulties during calculation as kernel values usually depend on the inner products of feature vectors. The radial basis function (RBF) kernel is best suitable to train the SVM model.

Recently, the application of SVM to time-series forecasting, called Support Vector Regression (SVR), has also shown many breakthroughs and plausible performance, such as forecasting of financial market [9], forecasting of electricity price [10], estimation of power consumption [11], and reconstruction of chaotic systems [12]. Traffic-flow prediction is a notable exception [13].

Kernel Functions in SVM

The strength of SVM is the two main properties: Kernel representation and margin optimization. In machine learning, a 'Kernel' refers to the kernel trick, a method using a linear classifier to solve a non-linear problem. It entails transforming linearly inseparable data to linearly separable data. Complex regions are learnt by the use of Kernels, such as radial basis function (RBF).

A kernel function represents the dot product of projections of two data instance in a high dimensional feature space. The basic technique finds the smallest 'hypersphere' in the kernel space that contains all training instances and determines on which side of 'hypersphere' a test instance lies. This classifier finds the maximum margin hyper plane, and it classifies all training instances correctly by separating them into correct classes through hyper plane. The maximum margin hyper plane is the one that gives the greatest separation between classes. The instances that are nearest to the maximum margin hyper plane are called support vectors.

In credit card fraud detection, if a test instance lies within the learned region it is stated as normal, else it is declared anomalous. SVM methods require large training dataset sizes in order to achieve maximum prediction accuracy. However, regular SVM method is invalid to the imbalanced data sets as the learned boundary is close to the minority instances. SVM is should be biased in a way that will push the boundary away from the positive samples [15].

Conclusion

Credit card fraud detection is one of the most explored domains of fraud detection and relies on the automatic analysis of recorded transactions to detect fraudulent behavior.

The performance of SVM methods in fraud detection are generally very effective. SVM predicts 94.3% customers correctly; only 6.7% true bad customers are predicted as good customers; and 13.3% true good customers are predicted as bad ones. [4]

In future, the cost based support vector machine with effective kernel function will be used to find the fraud detection with lower error rates.

Acknowledgement

I would like to thank all the researchers & scientists who have contributed to the research on fraud detection techniques using Data Science or Machine Learning algorithms.

References

1. Zareapoor, M., & Shamsolmoali, P. (2015). Application of credit card fraud detection: Based on bagging ensemble classifier. Procedia computer science, 48(2015), 679-685.
2. Campus, K. (2018). Credit Card Fraud Detection Using Machine Learning Models and Collating Machine Learning Models. International Journal of Pure and Applied Mathematics, 118(20), 825-838.
3. Dheepa, V., & Dhanapal, R. (2012). Behavior based credit card fraud detection using support vector machines. ICTACT Journal on Soft computing, 6956, 391-397.
4. Kamboj, M., & Shankey, G. (2016). Credit card fraud detection and false alarms reduction using support vector machines. International Journal of Advance Research, Ideas and Innovations in Technology, 2(4), 1-10.
5. Shen, A., Tong, R., & Deng, Y. (2007, June). Application of classification models on credit card fraud detection. In 2007 International conference on service systems and service management (pp. 1-4). IEEE.
6. Nipane, V. B., Kalinge, P. S., Vidhate, D., War, K., & Deshpande, B. P. (2016). Fraudulent Detection in Credit Card System Using SVM & Decision Tree. *International Journal of Scientific Development and Research (IDSDR)*, *1*(5), 590-594.
7. Demla, N., & Aggarwal, A. (2016). Credit Card Fraud Detection using SVM and Reduction of False Alarms. *International Journal of Innovations in Engineering and Technology (IJIET)*, *7*(2), 176-182.
8. Ng, X. Y., Rosdi, B. A., & Shahrudin, S. (2015). Prediction of antimicrobial peptides based on sequence alignment and support vector machine-pairwise algorithm utilizing LZ-complexity. *BioMed research international*, *2015*.
9. Yang H, Chan L, King I. Support vector machine regression for volatile stock market prediction. In: International Conference on Intelligent Data Engineering and Automated Learning; 2002. p. 391–96.
10. D.C. Sansom, T. Downs, T.K. Saha Evaluation of support vector machine based forecasting tool in electricity price forecasting for Australian national electricity market participants J Electric Electron Eng, Australia, 22 (2003), p. 227
11. B.-J. Chen, M.-W. Chang Load forecasting using support vector machines: A study on EUNITE competition 2001 IEEE Trans Power Syst, 19 (2004), pp. 1821-1830
12. Mattera D, Haykin S. Support vector machines for dynamic reconstruction of a

chaotic system. In: Advances in kernel methods; 1999. p. 211–41.
13. Ding A, Zhao X, Jiao L. Traffic flow time series prediction based on statistics learning theory. In: Intelligent Transportation Systems, 2002. Proceedings. The IEEE 5th International Conference on; 2002. p. 727–30.
14. Team, D. F. (2019, August 29). Support Vector Machines Tutorial - Learn to implement SVM in Python.
15. Zareapoor, M., Seeja, K. R., & Alam, M. A. (2012). Analysis on credit card fraud detection techniques: based on certain design criteria. *International journal of computer applications*, *52*(3).
16. Naik, H., & Kanikar, P. Credit card Fraud Detection based on Machine Learning Algorithms. International Journal of Computer Applications, 975, 8887.
17. Ogwueleka, F. N. (2011). Data mining application in credit card fraud detection system. Journal of Engineering Science and Technology, 6(3), 311-322.
18. Bhatla, T. P., Prabhu, V., & Dua, A. (2003). Understanding credit card frauds. Cards business review, 1(6).
19. Pawar, A. D., Kalavadekar, P. N., & Tambe, S. N. (2014). A survey on outlier detection techniques for credit card fraud detection. IOSR Journal of Computer Engineering, 16(2), 44-48.
20. Singh, K., & Upadhyaya, S. (2012). Outlier detection: applications and techniques. International Journal of Computer Science Issues (IJCSI), 9(1), 307.