Global Scientific JOURNALS

GSJ: Volume 9, Issue 8, August 2021, Online: ISSN 2320-9186
www.globalscientificjournal.com

Analysis Of Machine Learning Credit Card Fraud Detection Models

Felix Uloko, Nwaukwa Johnwendy, Ismaila Abu, Bosede Osayande

ulokof@veritas.edu.ng, nwaukwaj@veritas.edu.ng, izabu.cs@buk.edu.ng, mercies66@gmail.com

Veritas University, Abuja, Bayero University, Kano

Abstract

Billions of monetary losses are caused every year by fraudulent credit card transactions. The design of efficient fraud detection algorithms is key to reducing these losses, and more and more algorithms rely on advanced machine learning techniques to assist fraud investigators. However, the design of a full-proof Fraud Detection System requires high performing machine learning algorithms that are both accurate and robust enough to handle large data. This work aims to provide solutions by examining various methods previously used for fraud detection, bringing out their strengths and weaknesses. It also examines three classification machine learning algorithms employed for fraud detection (Decision Trees, Neural Networks and the Hidden Markov Model). Finally, Random Forest classification algorithm is implemented, which improves on the weaknesses of the aforementioned algorithms and fraud detection methods, meets real world working conditions and generates accurate alerts while ensuring continuous learning. The open source and statistical programming language R is used for running the algorithm. The impressive figures of 1.000, 0.500 and 0.200 gotten from the Sensitivity, Sepecificity and False Alarm tests, as well as the accuracy of 0.999 show the power and appropriateness of the algorithm in detecting credit card fraud.

Keywords: Fraud Detection, Classification, Neural Networks, Decision Trees, Random Forest, False Positive, Hidden Markov Model

1. Main text

The popularity of online shopping is growing day by day. According to a study conducted in 2003, one-tenth of the world's population is shopping online (Bhatla et al, 2003). The growth in the e-commerce space in Nigeria has been made possible by the activities of major on-line retailing platforms such as ishopright.com, Konga.com, Jumia.com, Deal Dey, Quick Tellers, Waka Now, Ryte Deals, Checki.com, and Buga.com among others.

Fraud refers to obtaining goods/services and money by illegal way. Fraud deals with events which involve criminal motives that, mostly, are difficult to identify. Credit card fraud is a wide-ranging term for theft and fraud committed using similar payment mechanisms as a fraudulent resource of funds in a transaction. Credit card fraud has been the expanding issue in the credit card industry. Detecting credit card fraud is a difficult task when using normal process, so the development of the credit card fraud detection models has become of importance whether in the academic or business organizations currently.

Furthermore, the role of fraud has been changed suddenly during the last few decades along with advancement of technologies. Credit card fraud is one of the biggest threats to business and commercial establishments today. Machine learning systems automatically learn programs from data. This is often a very

attractive alternative to manually constructing them, and in the last decade the use of machine learning has spread rapidly throughout computer science and beyond. Machine learning is used in Web search, spam filters, recommender systems, ad placement, credit scoring, fraud detection, stock trading, drug design, and many other applications. A recent report from the McKinsey Global Institute asserts that machine learning will be the driver of the next big wave of innovation (Manyika et al, 2011).

Credit card fraud can be defined as the illegal use of any system or, criminal activity through the use of physical card or card information without the knowledge of the cardholder. The credit card is a small plastic card, which is issued to user as a system of payment. With rapid growth in the number of credit card transactions, the fraudulent activities are also increased. The credit card may be physical or virtual. In a physical-card, the cardholder presents his card physically to a merchant for making a payment. To carry out fraudulent transactions in this kind of purchase, an attacker has to steal the credit card. In the second kind of purchase, only some important information about a card such as card number, expiration date, secure code and etc, is required to make the payment. Such purchases are normally done on the Internet or over the telephone. To commit fraud in these types of purchases, a fraudster simply needs to know the card details. Most of the time, the genuine cardholder is not aware that someone else has seen or stolen his card information. In real life, fraudulent transaction are scattered with genuine transactions and simple pattern matching.

Credit card fraud detection is one of the most explored domains of fraud detection (Bolton et al, 2001) and relies on the automatic analysis of recorded transactions to detect fraudulent behavior. Every time a credit card is used, transaction data, composed of a number of attributes (e.g. credit card identifier, transaction date, recipient, amount of the transaction), are stored in the databases of the service provider. However a single transaction information is typically not sufficient to detect a fraud occurrence and the analysis has to consider aggregate measures like total spent per day, transaction number per week or average amount of a transaction.

The traditional approach for fraud detection is based on developing heuristics around fraud indicators. Based on these heuristics, a decision on fraud would be made in one of two ways. In certain scenarios, rules would be framed that would determine if the case needs to be sent for investigation. In other cases, a checklist would be prepared with scores for the various indicators of fraud. An aggregation of these scores along with the value of the claim would determine if the case needs to be sent for investigation. The criteria for determining indicators and the thresholds will be tested statistically and periodically recalibrated. The challenge with the above approaches is that they rely very heavily on manual intervention which will lead to the following limitations:

(i) Constrained to operate with a limited set of known parameters based on heuristic knowledge – while being aware that some of the other attributes could also influence decisions

(ii) Inability to understand context-specific relationships between parameters (geography, customer segment, insurance sales process) that might not reflect the typical picture.

(iii) Recalibration of model is a manual exercise that has to be conducted periodically to reflect changing behavior and to ensure that the model adapts to feedback from investigations. The ability to conduct this calibration is challenging.

Incidence of fraud (as a percentage of the overall claims) is low typically less than 1% of the claims are classified. Additionally new modus operandi for fraud needs to be uncovered on a proactive basis

2. Literature Study

2.1 Anatomy of a Credit Card Transaction

A credit card transaction involves four entities. The first entity is the consumer; that is the person who owns the card and who carries out the legitimate transactions. The second entity is the credit card issuer; that is usually the consumer's bank – also known as issuing bank – which provides the credit services to consumer. The credit card issuer sends the bill to the consumer in order to request a payment for their credit card transactions. The third entity is the merchant who sells goods or services to the consumer by charging consumer's credit card. This charge is achieved through merchant's bank – the fourth entity – which sends the request for the transaction to the issuing bank. The issuing bank will check whether the amount of the transaction does not reach the credit card's limit before authorizing that transaction. If the transaction is valid, the issuing bank will block the requested amount from consumer's credit card account and send an authorization response to merchant bank. As soon as the authorization response is received by the merchant's bank, the merchant is notified; the transaction is marked as completed and the consumer can take the goods. The blocked amount on consumer's credit card account will be transferred into merchant's bank account in the following days.

2.2 Machine Learning Algorithms

There are several types of machine learning algorithms available to handle different applications. However, each algorithm is generally a combination of three components (Ashpak et al, 2013):

Representation: A classifier must be represented in some formal language that the computer can handle. Conversely, choosing a representation for a learner is tantamount to choosing the set of classifiers that it can possibly learn. This set is called the hypothesis space of the learner.

Evaluation: An evaluation function (also called objective function or scoring function*)* is needed to distinguish good classifiers from bad ones. The evaluation function used internally by the algorithm may differ from the external one that the classifier optimizes.

Optimization: A method is needed to search among the classifiers in the language for the highest-scoring one. The choice of optimization technique is key to the efficiency of the learner, and also helps determine the classifier produced if the evaluation function has more than one optimum.

2.3 Data Processing n Credit Card

This section identifies and discusses the different issues that are relevant to the processing of credit card information in order to detect fraud. These issues includes factors such as the nature of the input data, the availability (or unavailability) of labels, the output reported by the detection systems.

Nature of Input Data: A key aspect of any anomaly detection technique is the nature of the input data. Input is generally a collection of data instances (also referred as object, record, point, vector, pattern, event, case, sample, observation, entity) (Anderson, 2007). Each data instance can be described using a set of attributes (also referred to as variable, characteristic, feature, field, and dimension). The attributes can be of different types such as binary, categorical (nominal or ordinal scales) or continuous (interval or ratio scales). Each data instance might consist of only one attribute (univariate) or multiple attributes (multivariate). In the case of multivariate data instances, all attributes might be of same type or might be a mixture of different data types. Specific attributes in credit transaction data are often not revealed but they should comprise of date/time stamps, current transaction (amount, geographical location, merchant industry code and validity code), transactional history, payment history, and other account information. (Ghosh and Reilly, 1994).

2.4 Why Use Machine Learning In Fraud Detection

A Fraud Detection System (FDS) should not only detect fraud cases efficiently, but also be cost-effective in the sense that the cost invested in transaction screening should not be higher than the loss due to frauds (Bolton and Hand, 2002). Screening only 2% of transactions can result in reducing fraud losses accounting for 1% of the total value of transactions. However, a review of 30% of transactions could reduce the fraud losses drastically to 0.06%, but increase the costs exorbitantly. In order to minimize costs of detection it is important to use expert rules and statistical based models (e.g. Machine Learning) to make a first screen between genuine and potential fraud and ask the investigators to review only the cases with high risk.

Using Machine Learning (ML) techniques we can efficiently discover fraudulent patterns and predict

transactions that are most likely to be fraudulent. ML techniques consist in inferring a prediction model on the basis of a set of examples. The model is in most cases a parametric function, which allows predicting the likelihood of a transaction to be fraud, given a set of features describing the transaction. In the domain of fraud detection, the use of learning techniques is attractive for a number of reasons. First, they allow to discovery patterns in high dimensional data streams, i.e. transactions arrive as a continuous stream and each transaction is defined by many variables. Second, fraudulent transactions are often correlated both over time and space (Bishop, 2006). For example, fraudsters typically try to commit frauds in the same shop with different cards within a short time period. Third, learning techniques can be used to detect and model existing fraudulent strategies as well as identify new strategies associated to unusual behavior of the cardholders.

3. Analysis of Proposed System

The proposed system utilizes the strength of the Random Forest Algorithm. Its strengths include the following:

1. It is unexcelled in accuracy among current algorithms.
2. It runs efficiently on large data bases.
3. It can handle thousands of input variables without variable deletion.
4. It has an effective method for estimating missing data and maintains accuracy when a large proportion of the data are missing.
5. It has methods for balancing error in class population unbalanced data sets.

Random Forest is an algorithm for classification and regression. It is an ensemble of decision tree classifiers. The output of the Random Forest classifier is the majority vote amongst the set of tree classifiers. To train each tree, a subset of the full training set is sampled randomly. Then, a decision tree is built in the normal way, except that no pruning is done and each node splits of the full feature set. Training is fast, even for large data sets with many features and data instances, because each tree is trained independently of the others. The Random Forest algorithm has been found to be resistant to overfitting and provides error (without having to do cross-validation) through the “out-of-bag” error rate that it returns.

3.1 The Algorithm

The random forests algorithm (for both classification and regression) is as follows:

a. Draw ntree bootstrap samples from the original data.
b. For each of the bootstrap samples, grow an unpruned classification or regression tree, with the following modification: at each node, rather than choosing the best split among all predictors, randomly sample mtry of the predictors and choose the best split from among those variables. (Bagging can be thought of as the special case of random forests obtained when mtry = p, the number of predictors.)
c. Predict new data by aggregating the predictions of the ntree trees (i.e., majority votes for classification, average for regression).

An estimate of the error rate can be obtained, based on the training data, by the following:

a. At each bootstrap iteration, predict the data not in the bootstrap sample ("out-of-bag", or OOB, data) using the tree grown with the bootstrap sample.
b. Aggregate the OOB predictions. Calculate the error rate, and call it the OOB estimate of error rate.

4. Implementation and Results

The Random Forest algorithm was run on datasets gotten from the UCI Machine Learning Repository (https://archive.ics.uci.edu and https://data.world/), a collection of databases, domain theories, and data generators that are used by the machine learning community for the empirical analysis of machine learning algorithms. The dataset contains over 5000 instances and 31 attributes. The programming language used for the implementation is the R language. R is a language and environment for statistical computing and graphics.

The performance of the proposed system is evaluated in terms of 3 classification metrics (Damien Francis, 2011) relevant to credit card fraud detection—fraud detection rate, false alarm rate, and Matthews correlation coefficient.. Here, fraud is considered as positive class and legal as negative class and hence the meaning of the terms P, N, TP, TN, FP, and FN are defined as follows:

POSITIVES (P): number of fraud transaction;
NEGATIVES (N): number of negative transactions;
TRUE POSITIVES (TP): number of fraud transactions predicted as fraud;
TRUE NEGATIVES (TN): number of legal transactions predicted as legal;
FALSE POSITIVES (FP): number of legal transactions predicted as fraud;
FALSE NEGATIVES (FN): number of fraud transactions predicted as legal;

4.1 Sensitivity / Fraud Catching Rate

Sensitivity represents the portion of actual positives which are predicted positives. In credit card fraud detection, sensitivity denotes the fraud detection rate and it is defined as:

Sensitivity=TP / P

The results for the Sensitivity test carried out on the algorithms are as shown in Figure 1.

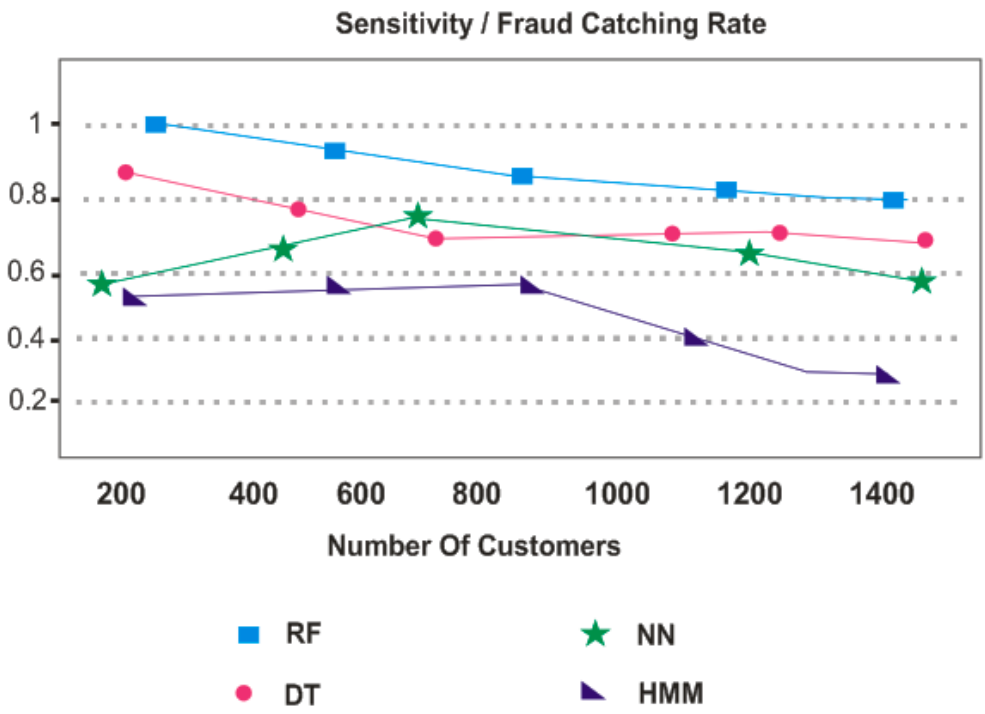

Figure 1: Sensitivity result of Random Forest, Decision Trees, Neural Network and Hidden Markov Model

It can be seen that Random Forest performs better when compared with the other 3 machine learning algorithms. With an average position of almost 1, it ensures that the fraud detection rate is steady and consistent, without dropping lower than 0.8 at any point.

4.2 False Alarm Rate

False alarm rate represents portion of actual negatives which are predicted as positives and it is defined as:

False Alarm Rate = FP / N

The results for the Sensitivity test carried out on the algorithms are as shown in Figure 4.2.

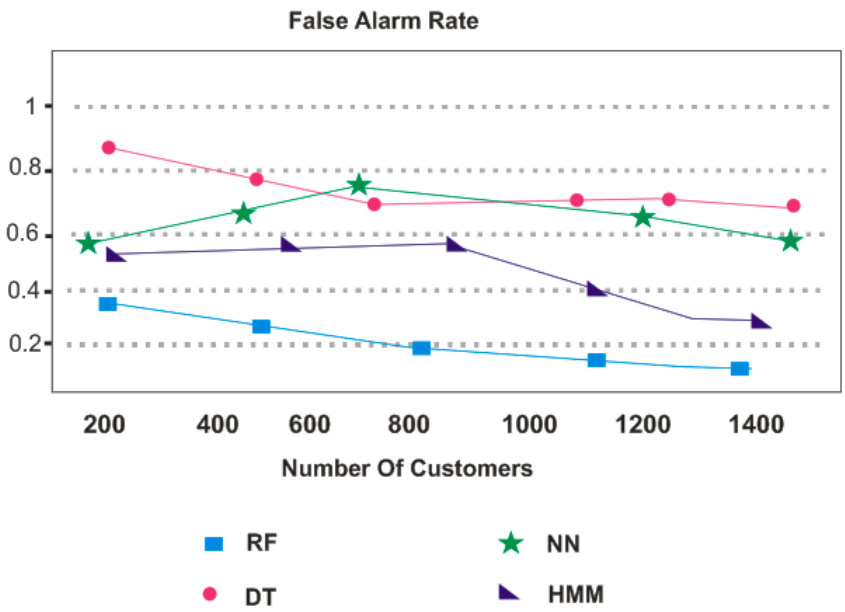

Figure 2: False Alarm result of Random Forest, Decision Trees, Neural Network and Hidden Markov Model

Figure 2 shows the performance of Random Forest on false alarm rate in comparison with other algorithms. This metric should typically be low since false alarm leads to customer dissatisfaction. With a maximum value of about 0.3 and a minimum value approaching 0.1, the Random Forest Algorithm certainly ticks this box.

4.3.3 Specificity

This is the proportion of actual negative which are predicted negative.

It is expressed as TN / (TN + FP)

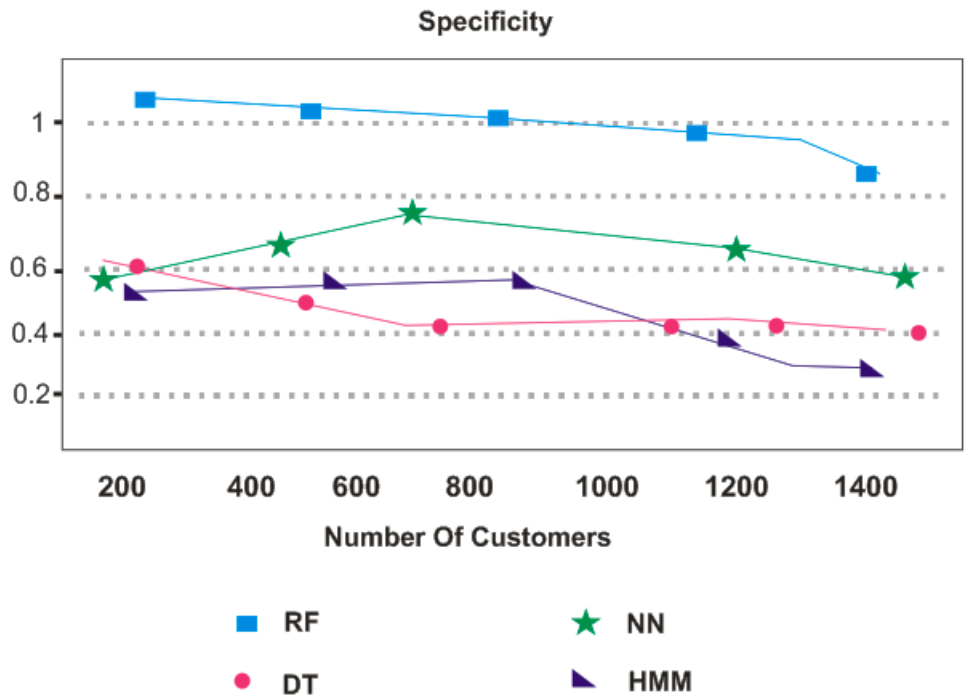

Figure 3 : Specificity result of Random Forest, Decision Trees, Neural Network and Hidden Markov Model

Random Forest equally performs best in figure 3, with a sure chance of predicting actual negatives that are negatives. Its high point of over 1 confirms this.

This study has revealed the strength of the Random Forest algorithm in handling Fraud Detection. The impressive figures of 1.000, 0.500 and 0.200 gotten from the Sensitivity, Specificity and False Alarm tests, as well as the accuracy of 0.999 show the power and appropriateness of the algorithm.

Conclusion

The impact of machine learning goes beyond its obvious role as a method for software development. Machine learning is also likely to help reshape our view of Computer Science more generally. By shifting the question from “how to program computers” to “how to allow them to program themselves,” machine learning emphasizes the design of self-monitoring systems that self-diagnose and self-repair, and on approaches that model their users, and the take advantage of the steady stream of data flowing through the program rather than simply processing it. Similarly, Machine Learning will help reshape the field of Statistics, by bringing a computational perspective to the fore, and raising ideas such as never-ending learning.

References

Aleskerov E., Freisleben B., and Rao B., (1997). “CARDWATCH: A Neural Network Based Database Mining System for Credit Card Fraud Detection”. Proc. IEEE/IAFE: Computational Intelligence for Financial Eng. pp.:220-226.

Ashphak P. (2013). “Credit Card Fraud Detection System through Observation Probability Using Hidden Markov Model”. International Journal of Thesis Projects and Dissertations (IJTPD). 1(1):7.

Anderson R. (2007). “The Credit Scoring Toolkit: Theory and Practice for Retail Credit Risk Management and Decision Automation”. Oxford University Press. pp. 123-125.

Bhatla T.P, Prabhu V., and Dua A. (2003). “Understanding credit card frauds”. Cards business review. 1(6). pp 45-60

Bishop M.C. (2006). “Pattern recognition and machine learning”. 6(4). pp 35-67.

Bolton R.J. and Hand. D.J (2002). “Statistical fraud detection: A review”. Statistical Science. 5(3):235-249.

Brause R., Langsdorf T., and Hepp M. (1999) “Neural Data Mining for Credit Card Fraud Detection”. Proc. IEEE Int’l Conf. Tools with Artificial Intelligence. pp:103-106

Chaudhar K., Yadav K., and Mallick B. (2012). “A review of Fraud Detection Techniques: Credit Card”. International Journal of Computer Applications. 45(1): 34-45.

Dheepa1 V. and Dhanapal R. (2009). “Analysis of Credit Card Fraud Detection Methods”. International Journal of Recent Trends in Engineering. 2(3):44-67.

Divya M., et al (2014). “Credit Card Fraud Detection Using Neural Networks”. International Journal of Students Research in Technology & Management Vol 2 (02), March-April 2014, ISSN 2321-2543, pp. 84-88.

Dorronsoro J.R., Francisco G., Carmen S., and Carlos S.C. (1997) “Neural Fraud Detection in Credit Card Operation.” IEEE Transaction on Neural Network. 8(4):827-834.

Eibe F. and Witten I. H. (2005). “Data Mining – Practical Machine Learning Tools and Techniques, Second Edition”. University of Waikato, Amsterdam. pp. 124 – 135.

Ehramikar S. (2000). "The Enhancement of Credit Card Fraud Detection Systems using Machine Learning Methodology", MASc Thesis, Department of Chemical Engineering, University of Toronto. pp. 35 – 60.

Eromosele A. (2015). “ Worth of Nigeria’s E-commerce sector by 2018”. Allafrica.com/stories/201506100547 (Accessed: 12-11-2016).

Falaki S. O. and Alese B. K. (2010). “An Update Research On Credit Card On-Line Transactions”. International Journal of Economic Development Research and Investment, Vol. 1 Nos. 2 & 3. pp. 34-35 .

Ghosh S., and Reilly D.L. (1994). “Credit Card Fraud Detection with a Neural- Network”. Proceedings of the International Conference on System Science. pp. 621-630.

Gottlieb O. (2006). “Detecting Corporate Fraud: An Application of Machine Learning”. A publication of the American Institute of Computing. pp. 100-215.

Hand D.J, G. Blunt, and N.M. Adams (2000). “Data Mining for Fun and Profit,” Statistical Science, 15(2):111-131.

https://archive.ics.uci.edu/ml/datasets/Credit+Approval (Accessed: 15-12-2016)

https://data.world/raghu543/credit-card-fraud-data (Accessed: 15-12-2016)

Hetvi M. et al (2013). "Fraud Detection in Credit Card System Using Web Mining". International Journal of Innovative Research in Computer and Communication Engineering. 1(2):56-66.

Hodge, V.J. and Austin, J. (2004). "A survey of outlier detection methodologies". Artificial Intelligence Review. pp. 124 – 345.

Kokkinaki, A.(1997). "On Atypical Database Transactions: Identification of Probable Frauds using Machine Learning for User Profiling." Knowledge and Data Engineering Exchange Workshop. IEEE. pp:107-113.

Manyika J. et al (2011). "Big data: The next frontier for innovation, competition, and productivity". Technical report, McKinsey Global Institute. pp. 23 – 26.

Nils J.N. (1998). "Introduction To Machine Learning - An Early Draft Of A Proposed Textbook". Robotics Laboratory - Department of Computer Science Stanford University. pp. 56 – 78.

Oxford Concise English Dictionary, 11th Edition (2009). Oxford University Press.

Phua C., Lee. V., Smith K. & Gayler, R. (2005). "A comprehensive survey of data mining-based fraud detection research". Artificial Intelligence Review. 6(6):1–14.

Quah T.S. and Sriganesh M. (2008). "Real-time credit card fraud detection using computational Intelligence". Expert Systems with Applications, 35(4):1721–1732.

Sahin Y. and Duman E. (2011). "Detecting Credit Card Fraud by Decision Trees and Support Vector Machines". International Multiple Conference. pp. 45 – 78.

Salvatore J. S. (2009). "Machine Learning and it Applications". Department of Computer Science, Columbia University. pp 48 – 80.

Statistics for General and On-Line Card Fraud (2007). Available at "http://www.epaynews.com/statistics/fraud.html". (Accessed 10-11-2016)

Stolfo S.J., Fan D.W., Lee W., Prodromidis A.L., and Chan P.K. (1997) "Credit Card Fraud Detection Using Meta-Learning: Issues and Initial Results". Proc. AAAI Workshop AI Methods in Fraud and Risk Management. pp:83-90.

Sharma A. and Kumar P.P. (2012). "A Review of Financial Accounting Fraud Detection based on Data Mining Techniques". International Journal of Computer Applications. 39(1): 55-67.

Shai S.S and Shai B.D. (2014). "Understanding Machine Learning: From Theory to Algorithms". Published 2014 by Cambridge University Press. pp. 35 – 46.

Wang J., Liao, Y., Tsai T. & Hung G. (2006). “Technology-based financial frauds in Taiwan: Issue and Approaches”. IEEE Conference on: Systems, Man and Cyberspace.4(3):1120–1124.