Transition from Observation To Knowledge To Intelligence (TOKI)

Editors
Dr. Victor ODUMUYIWA, Dr. Olufade ONIFADE,
Prof. Amos DAVID & Prof. Charles UWADIA

Victor ODUMUYIWA
Department of Computer Sciences,
University of Lagos
Nigeria

ISBN: 978-978-976-000-8

Transition from Observation to Knowledge to Intelligence

3rd Biennial International Conference on Transition from Observation to Knowledge to Intelligence (TOKI)
15-16 August 2019
University of Lagos, Nigeria

Editors

Dr. Victor ODUMUYIWA
Dr. Olufade ONIFADE
Prof. Amos DAVID
Prof. Charles UWADIA

Credit Card Fraud Detection using k-star Machine Learning Algorithm

DADA Emmanuel Gbenga
Department of Computer Engineering
University of Maiduguri, Maiduguri, Nigeria

MAPAYI Temitope, OLAIFA Olowasogo Moses, OWOLAWI Pius Adewale
Department of Computer Systems Engineering, Faculty of ICT,
Tshwane University of Technology, Pretoria, South Africa

Abstract: As the number of users opting for credit card payment is increasing daily worldwide, the threats posed by internet fraudsters on this type of payment are also on the increase. Banks, merchants and consumers globally have lost billions of dollars as a result of this type of fraud. The shortcomings of many of the existing credit card fraud detection techniques include their inability to effectively detect fraudulent transactions, the high false alarm rate, and high computational cost. These necessitated the development of more efficient credit card fraud prevention measures. Many models have been developed in the literature; however, the accuracy of the model is critical. In this paper, fraud detection model using a K-Star machine learning algorithm is presented and the performance is evaluated using German Credit and Australian Credit datasets. The algorithm proposed in this paper proved to be highly effective and efficient with a resultant classification accuracy of 100%, very low false positive rate (0.00) and very high true positive rate of 1.00. All experiments are conducted on WEKA data mining and machine learning simulation environment.

Keywords: k-star; classification; credit card; fraud detection; machine learning

1. Introduction

Explosion in the growth of online shopping and e-businesses has mostly been ascribed to the increasing level of convictions and belief on information privacy provided by e-commerce sites (Andrea, 2015). Nevertheless, considering the evolving nature of fraud and theft perpetrated by fraudsters on e-commerce sites, one cannot but be deeply disturbed about the safety and privacy of credit card information (Akinyede, 2005). Credit card fraud is gradually becoming a very dangerous global problem in e-commerce as it has resulted into loss of several millions of dollars annually (Internet, 2011). Financial losses due to fraud often have serious negative impacts on merchants, banks and individual customers. Credit card fraud can also affect the reputation of the merchants, thereby leading to the customers' loss of trust in them and drastic reduction in the number of customers patronizing the merchants. Billions of dollars have been lost in recent years due to the nefarious activities of credit card fraudsters. A credit card fraud is perpetrated whenever any person intentionally and unsympathetically used the information on the card for dishonest purpose, impersonation and other egocentric and dubious intentions. Such act can be perpetrated using any of the following: Cardholder-Not-Present (CNP), misplaced/ thieved card, magnetic stripe obliteration, hijacked account, or card cloning and scanning (Andrea, 2015; Li and Zhang, 2005. Some of the popular methods used by fraudster to perpetrate internet credit card fraud include: site duplication, deceptive trading sites and manufacturing of illegal credit card. Credit card frauds connected to trading can be done through conspiracy. In this case, the traders and/or workers connived to do fraud by illegally gathering sensitive information about customers such as accounts details, Bank Verification Number (BVN), password and username. Moreover, fraud can also take the form of triangulation. Here, the swindlers unlawfully gain access to credit card details of the customer and use it to pay for goods bought from a reputable e-commerce site. This poses a serious challenge both to the card-holders and the vendors (Bhatla, 2003). Below in figure 1 is the credit card fraud

and identity theft statistics of two types of fraud in the United States between 2011 and 2018.

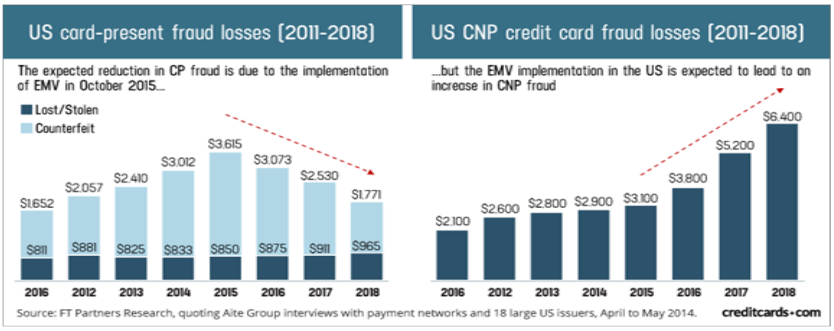

Figure 1: Credit card fraud and ID theft statistics in US 2011-2018 (Source: Steele, 2017)

2. Literature Review

2.1. Fraud Detection Process

Credit card fraud detection is the process of knowing whether or not a set of credit card transactions is in the category of fraudulent or legitimate instances of buying or selling something (Maes *et al.*, 2002). Some desirable characteristics of a Fraud Detection System (FDS) include efficient detection of fraud, and high effectiveness or productivity in relation to its cost in transaction checking (Quah and Sriganesh, 2008). It has been confirmed that vetting just 2% of transactions have the potential of decreasing the fraud cases responsible for 1% of the overall transactions value (Bhatla, 2003). Conversely, the inspection of 30% of transactions has the ability to significantly lower the financial losses to 0.06%, then astronomically raise the overhead. It is very important to employ the use of machine learning techniques to do initial checking whether the transaction is a fraud or not, so as to reduce the overhead incurred during the detection process. After this, the detectives can then analyse the instances with great risk. Figure 2 below depicts the processes involved in credit card fraud detection.

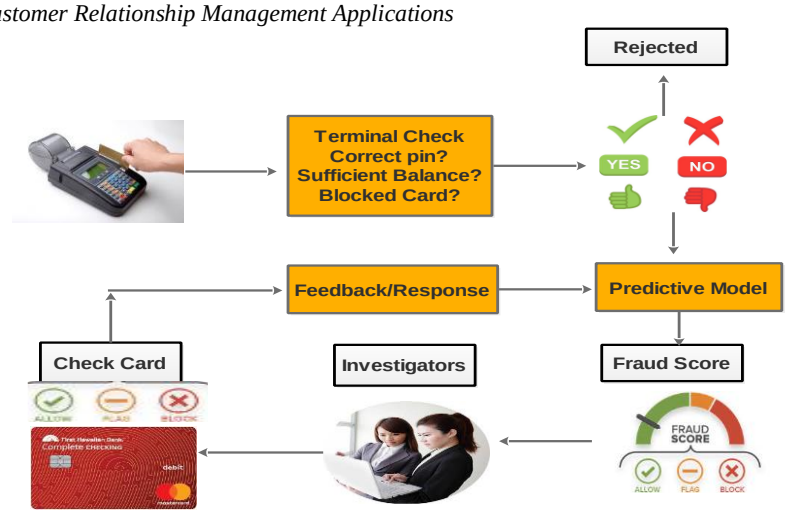

Figure 2: Credit card fraud detection process (Source: Andrea, 2015)

This is an indication that designing and implementing efficient credit card fraud detection algorithms is crucial for lowering these losses. Increasingly, fraud investigators are depending on innovative machine learning methods to aid their investigations. The non-stationary distribution of data, the substantially one-sided classes divisions and the inaccessibility of many transactions labeled by fraud investigators have made the task of developing effective fraud detection algorithms a very demanding one. Also contributing to the difficulty is the fact that public data are barely available due to privacy concerns, thereby making it difficult to know the most efficient approach to adopt in curbing this menace.

It is a normal procedure to initially filter transactions by vetting a number of critical requirements such as enough balance, and afterward use a predictive model to score the credit card as shown in figure 2. Each transaction is graded by the predictive model as either high or low risk of fraud, and those with high risk produce warning notifications. The investigators examine these warning notifications and give a response for each warning notifications which can be either true positive (fraud) or false positive (authentic). The responses are then subsequently used to enhance the fraud detecting capacity of the model. According to Bishop (2006), there are two principal ways of building a

predictive model. The first is known as expert system. This approach encodes knowledge from fraud experts into rules, however, manual adjustment of control parameters and human supervision is needed to make it work effectively. The second is using Machine Learning (ML) methods. ML algorithms make it easy to efficiently and economically detect criminal patterns in transactions, and predict the ones that are probably fraudulent. ML techniques for fraud detection are gaining more attention because they have the ability to detect patterns in high dimensional data streams (network traffic, phone conversations, web searches etc.), and every transaction is characterized by several varying features. ML prediction model is built by using an array of examples. In majority of the cases, the model is a parametric function that allows predicting the probability of a transaction to be a scam, provided there is a group of features explaining the transaction. Moreover, illegal transactions are usually compared after some period of time interval and location. Also, ML methods can assist in detecting and modelling existing approaches adopted by criminals in addition to recognising new methods related to anomaly behaviour of the cardholders. The ability of ML methods to spontaneously incorporate the responses of investigators to increase detection accuracy of the system is an added advantage. As for expert system, integrating investigators responses entails updating the rules which in most cases is cumbersome and time consuming (Andrea, 2015).

2.2. Related Work

Many techniques have been proposed in literature for detecting credit card fraud. Zareapoor and Shamsolmoali (2015) applied Bagging ensemble classifier for detection of credit card fraud. The authors compared the performance of their proposed system with NB, SVM and KNN classifiers on real life credit card transactions datasets. The Bagging algorithm proved to have a superior performance over the other algorithms compared. The proposed method was evaluated using Fraud Catching Rate, False Alarm Rate, Balance Classification Rate and Matthew Correlation Coefficient. The performance of their proposed technique is relatively low.

Dorronsoro *et al.* [1997] developed an online fraud detection system using neural classifier. The drawback of their approach is that data must be clustered by class of account making it to be time consuming. Maes *et al*. (2002), used Bayesian networks classifier to detect fraud. Their approach produced excellent results. Time constraint is the major shortcoming of their method. Leonard (1995) used rule-based expert systems for credit card fraud. Bentley *et al.* (2000) applied genetic programming to create logic rules that have the ability to classify credit card transactions into different classes such as suspicious and non-suspicious classes. Their approach produced good results when tested using real home insurance data and may possibly be an effective approach to credit card fraud detection in the future.

Halvaiee and Akbari (2014) used Artificial Immune Recognition System (AIRS) for credit card fraud detection. Their approach is an enhancement of the conventional AIS model. They used negative selection to realize enhanced accuracy, better precision and lower system response time. Mahmoudi and Duman (2015) developed a modified Fisher Discriminant function for credit card fraud detection. The adjustment made the conventional functions to become more sensitive to principal instances. A weighted average was used to compute variances, which permitted learning of beneficial transactions.

Olszewski (2014) proposed a fraud detection approach that uses user accounts visualization and threshold-type detection. The Self-Organizing Map (SOM) was applied as an imagining method. The performance of the system was evaluated using real-world data sets linked to telecommunications fraud, computer network intrusion, and credit card fraud. The proposed model proved to be efficient and economical. Randhawa *et al.,* (2017) used AdaBoost and majority voting to detect credit card fraud. The performance of the proposed system was compared with other standard models using publicly available credit card data set. Afterward, a real-world credit card data set obtained from a financial institution is used to further evaluate the models. The authors also inserted noise to the data set in order to further evaluate the robustness of the classifiers. The results showed that the majority voting approach produced better performance compared to

other models. Apapan and Liu (2018) applied deep learning Auto-encoder (AE) and restricted Boltzmann machine (RBM) to create model for detecting fraud in transactions based on previous history. The auto-encoder (AE) is an unsupervised learning algorithm that uses backpropagation to set the inputs so that they are equal to the outputs (Pumsirirat and Yan, 2018). The RBM is made up of two layers: the input layer (visible) and hidden layer. The authors used TensorFlow library from Google to implement AE, RBM, and H2O. The performance of the proposed models were evaluated using European, Australian and German Datasets. The results showed that their methods can accurately predict credit card detection with a large dataset.

3. Materials and Methods

3.1. Datasets

The datasets used for this study are the German credit dataset and the Australian credit dataset obtained from the credit data analysis from UCI Data Repository (UCI, 2018). The German credit dataset is made up of 21 attributes and 1000 instances. It contains two classes, referred to as good and bad. The final determination of the class is based on the values of all the 21 attributes. While the Australian credit dataset comprises of 15 attributes and 690 instances. This dataset also have two classes: good (1) and bad (0). This attributes that make up this dataset is a combination of continuous, nominal (alongside few numbers of values), and nominal (having greater numbers of values). It also has a small number of missing values (Quinlan, 1987). The readers can find the detailed descriptions of these datasets in (UCI, 2018).

a. K-Start (K*) Instance-Based Learner

Instance-based (IB) learners, also known as memory-based learners, are classical example of lazy algorithms which store the training examples in an array of data to map input values to output values (Alpaydin, 2010). One of the strength of IB learners is its ability to learn fast from a small dataset unlike the rule induction approach that needs a sufficient depiction of every rule prior to their production. Only one instance per group is sufficient for an instance-based learner to start

making valuable predictions. It has high classification accuracy rate. Moreover, it is worth noting that since they keep each example as a distinct model, they therefore, have the capacity to employ discrete valued features and predict numeric valued misses (Martin, 1995). K* instance based learner was proposed by John Cleary and Leonard Trigg in (Cleary and Trigg, 1995). The algorithm produced high performance in term of classification accuracy, effectively handle missing values, cope with diversified values and satisfactorily solve smoothness problems (Hernández, 2015).

The working principle of the K* is described in this section. The classifier employs a measure of the disorder or randomness (known as entropy) built on the likelihood of converting an example into another form by arbitrarily selecting among all likely conversions. The use of entropy as a measure for sample distance is highly advantageous. Moreover, the mathematical study of the coding of information aids in calculating the distance among the samples. The distance between one sample and another is referred to as the complexity of converting a sample from one form to another. The following steps are used to accomplish this: Initially specify a limited number of conversions that will connect one sample to another one. Subsequently convert one sample (x) to (y) through the aid of the program in a limited string of conversions beginning at (x) and stopping at (y). Assuming there is an array of unbounded points and a series of limited conversions C, let c be a value of the series C as shown in equation 1. Then c will connect c: J→J. To connect examples with itself δ is used in T (δ (x) =x). δ stops Q, the series of all affix codes from C*. Associates of C* and Q individually specify a conversion on J.

$$\bar{C}(\delta) = C_n(C_{n-1}(\ldots C_1(\delta)\ldots)) \quad (1)$$

where $C = C_1 \ldots C_n$

Q is probability function on C*. It fulfills the following properties expressed in equations 2 to 4:

$$0 \leq \frac{q(\bar{c}u)}{q(\bar{c})} \leq 1 \quad (2)$$

$$\sum_u q(\bar{c}u) = q(\bar{c}) \quad (3)$$

$$C(\wedge) = 1 \quad (4)$$

As a result it fulfills the following shown in equation 5:

$$\sum_{C \in Q} q(\bar{c}) = 1 \quad (5)$$

The probability function Q* is expressed as the chance of every route from sample *x* to sample *y* is expressed in equation 6:

$$Q * (y|x) = \sum_{\bar{c} \in Q : \bar{c}(x) = y} q(\bar{c}) \quad (6)$$

The K* function is then expressed as below in equation 7:

$$k * \left(\frac{y}{x}\right) = -log_2 * \left(\frac{y}{x}\right) \quad (7)$$

The figure 3 shows the flowchart of the proposed system. The diagrammatical representation of our proposed system is depicted in figure 3 below. The customer initiates a transaction by placing order for the commodity through the internet by making use of the credit card. Subsequently, the originating bank directs the transaction to the procuring bank by transferring the money, date and time of payment, internet usage location, and other relevant information. The credit card fraud detection system is then used to authenticate the attributes of the credit card. It achieve this by requesting the customer's data profile from the database to input their attributes into the K-Star machine learning model. The procuring bank sends the input which is all relevant information about the transaction. Afterward, K-Star algorithm uses past behaviours to train the model, after which it uses the new incoming transaction as an evaluation test for the customer transaction. The credit card is scored after some computations are carried out by the K-Star algorithm. Based on the score of the credit card, if K-Star predictive model classify the transaction as a fraud, the proposed system will register the transaction in the database as a fraud, and will immediately decline it. Consequently, the procuring bank will send a SMS alert to the authentic owner of the credit card that the transaction has been declined, since the transaction was classified as fraudulent by the system.

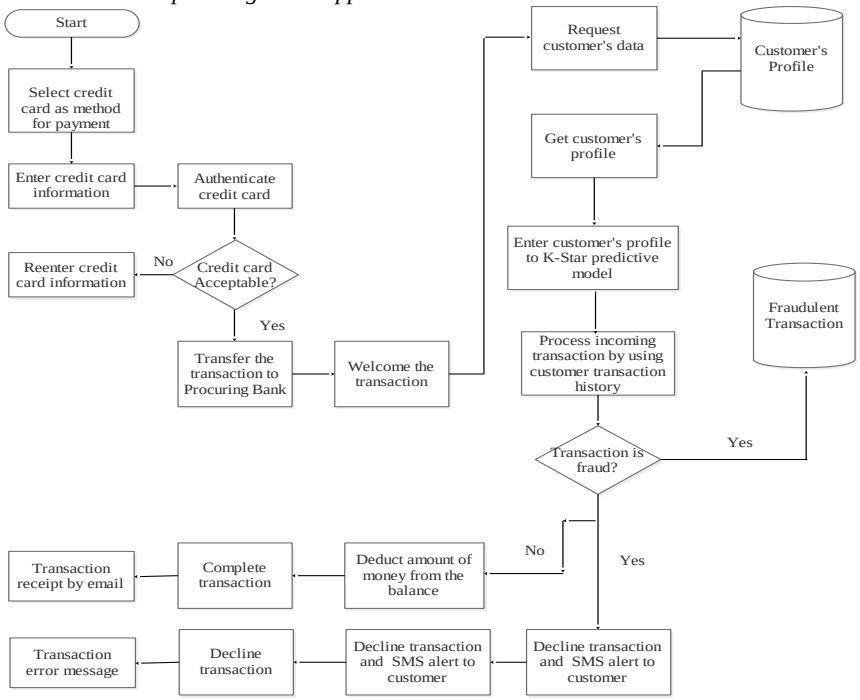

Figure 3: Credit card fraud detection based on K-Star algorithm

4. Experimental Results and Discussion

This section presents the experimental setup, results of the experiments performed and discussion of the results. K* machine learning algorithm was simulated using WEKA (Wang, 2005). All experiments were conducted on a machine with an AMD A 10-7300 Radeon R6, 10 Compute Cores 4C+6G, 1.90 GHz, 8.00GB of RAM.

The K* algorithm was applied to classify and evaluate the German credit and Australian credit datasets. The credit card transaction data is classified as either good or bad using the K* classifier. We used the training dataset and 10-fold cross validation test which is an approach employed in appraising predictive models that divide the original set into a training sample to train the model, and a test set for its evaluation. Firstly, the training of the datasets was performed with the feature vectors extracted by analyzing the dataset for attributes. The performance of the trained models is evaluated using 10-fold cross validation for its classification accuracy. Classification accuracy rate is

one of the performance metrics used in this study. It is measured as the ratio of number of correctly classified instances in the test dataset and the total number of test cases.

Fraud is considered as a positive class and legal as negative class and hence the meaning of the terms TP, TN, FP and FN are defined as follows:

True Positive (TP) = Number of fraud transactions predicted as fraud

True Negative (TN) = Number of legal transactions predicted as legal

False Positive (FP) = Number of legal transactions predicted as fraud

False Negative (FN) = Number of fraud transactions predicted as legal

It is not enough to describe the true and false positives and negatives using a single metric, the most ideal metric is the Matthews Correlation Coefficient (MCC) (Powers, 2011). The formula below can be used to compute the value for MCC:

$$MCC = \frac{(TPxTN)-(FNxFN)}{\sqrt{(TP+FP)(TP+FN)}(TN+FP)(TN+FN)} \qquad (1)$$

When the outcome is +1 it signifies the best prediction, while −1 denotes a complete disparity.

We compared the performance of K* classifier on WEKA using both datasets with some state of the art machine learning techniques. Tables 1 and 2 below depicts our comparison.

Table 1: Performance comparison of K* with some other algorithms for German Credit dataset

Model	Time (Sec.)	Classification Accuracy (%)	Fraud (%)	Non-fraud (%)	MCC	Mean Absolute Error	Correctly Classified Instance
LWL	8.05	70	63.491	70.99	0.259	0.3690	700
SVM	0.25	78.4	89.946	78.53	0.798	0.2160	784
MLP	0.30	99.3	80.897	99.97	0.798	0.0120	993
Simple Logistic	0.23	77.4	87.899	77.58	0.715	0.2987	774
Naïve Bayes	0.14	77.2	67.587	77.45	0.289	0.2821	772
HMM	0.02	70	62.294	70.98	0.228	0.5000	700
J48	0.01	85.5	45.907	85.57	0.697	0.5000	855
K-Star	21.93	100	100	100	1.000	0.0000	1000

Table 1 represents the experimental results from different models for German credit dataset. It is very clear that the accuracy rates are relatively low except for MLP and K-Star. The result that matters most can be seen from the rate of fraud detection which changes from 45.907% for J48 up to 100% for K-Star. The rate of non-fraud detection is related to the accuracy rates. K-Star generates the highest MCC score of 1.000, while the lowest is from HMM with an MCC score of 0.228. The result for the Australian Credit dataset is represented in table 8 below. The classification accuracy is also not too high except for MLP and K-Star. The rate of fraud detection which changes from 64.89% for SVM up to 100% for K-Star. K-Star generates the highest MCC score of 1.000, while the lowest is from HMM with an MCC score of 0.245.

Table 2: Performance comparison of K* with some other algorithms
Australian Credit dataset

Model	**Time (Sec.)**	**Classification Accuracy (%)**	**Fraud (%)**	**Non-fraud (%)**	**MCC**	**Mean Absolute Error**	**Correctly Classified Instance**
LWL	4.34	85.50	74.58	85.59	0.720	0.2266	590
SVM	0.08	85.94	64.89	85.99	0.733	0.1406	593
MLP	0.08	97.24	87.69	98.95	0.944	0.0437	671
Simple Logistic	0.03	88.41	77.89	88.96	0.770	0.1815	610
Naïve Bayes	0.06	77.68	66.79	77.99	0.558	0.2218	536
HMM	0.02	49.49	69.92	44.49	0.245	0.5000	307
J48	0.08	91.0	70.58	91.99	0.818	0.1493	628
K-Star	11.44	100	100	100	1.000	0.0001	690

5. Conclusion

This paper presents a study on credit card fraud detection using K-Star machine leaning algorithm. Some other state-of-the-art models such as LWL, SVM, MLP, SimpleLogistic, NB, HMM and J48 were also used in the study and their statistical assessments presented. Two publicly available credit card data sets: German credit card data set and Australian credit card data set were used for evaluating the performances of the systems. Performance metrics such as accuracy, TPR, FPR, precision, F-measure, ROC curve, and MCC were adopted. The best MCC score is 1.000, attained by K-Star on both data sets. The results of our experiments show that K-Star is a promising algorithm

that can be used to build effective predictive model for accurate detection of credit card transactions.

List of References

Andrea, D. P. (2015) Adaptive Machine Learning for Credit Card Fraud Detection. PhD Thesis, Department of Computer Science, Université Libre de Bruxelles.

Akinyede, R. O. (2005) Development of a Payment System for e-Commerce and banking industry in Nigeria". A Thesis Submitted for Fulfillment of the Requirements for the Degree of Masters of Technology, Computer Science, The Federal University of Technology, Akure, Nigeria.

Internet Fraud Statistics Reports (2011), http://www.fraud.org/internet/intstat.htm.

Li Y. and Zhang, W. (2005) Securing credit card transactions with one-time payment scheme. Electronic Commerce Research and Applications, Volume 4, Issue 4, Pages 413-426. https://doi.org/10.1016/j.elerap.2005.06.002

Bhatla, R. O. (2003) Understanding Credit Card Fraud, Card Business Review retrieved from http://www.tcs.com/0_whitepapers/htdocs/ credit_card_fraud_ white_paper_V_1.0.pdf

Steele, J (2017) Credit card fraud and ID theft statistics. Available at https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php

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

Bishop, C. M. (2006) Pattern recognition and machine learning", volume 4, springer New York.

Alpaydin, E. (2010) Introduction to Machine Learning, T. Dietterich, Editor: London, England.

Martin, B (1995) Instance-Based Learning: Nearest Neighbour with Generalisation, in Department of Computer Science, University of Waikato: Hamilton, New Zealand. p. 83.

Cleary, J and Trigg, L. (1995) K*: An Instance-based Learner Using an Entropic Distance Measure", in 12th International Conference on Machine Learning, p. 108-114.

Hernández, C. D. T. (2015) An Experimental Study of K* Algorithm. I.J. Information Engineering and Electronic Business, 2, 14-19.DOI: 10.5815/ijieeb.2015.02.03.

UCI Machine Learning Data Repository – http://archive.ics.uci.edu/ml/datasets.

Wang, X. (2005) Learning to classify email: A survey. Proceedings of 2005 International Conference on Machine Learning and Cybernetics, 2005.

Quinlan, (1987) Simplifying decision trees", Int J Man-Machine Studies, pp. 221-234, 27 Dec 1987.

Zareapoor, M and Shamsolmoali, P (2015) Application of credit card fraud detection: Based on Bagging Ensemble Classifier. International conference on intelligent computing, communication and convergence (ICCC-2015). Procedia computer science 48(2015): 679-685.

Dorronsoro, J.R., Ginel, F., Sgnchez, C. and Cruz, C.S., (1997) Neural fraud detection in credit card operations. IEEE transactions on neural networks, 8(4), pp.827-834.

Maes, S., Tuyls, K., Vanschoenwinkel, B. and B Manderick. (2002). Credit Card Fraud Detection using Bayesian and Neural Networks, Proc. of the 1st International NAISO Congress on Neuro Fuzzy Technologies.

Leonard, K. (1995) The development of a rule based expert system model for fraud alert in consumer credit. European Journal of Operational Research, 80; 350-356

Bentley, P., Kim, J., Jung. G. and J Choi. (2000). Fuzzy Darwinian Detection of Credit Card Fraud, Proc. of 14th Annual Fall Symposium of the Korean Information Processing Society.

Halvaiee, N. S. and Akbari, M. K. (2014) A novel model for credit card fraud detection using Artificial Immune Systems. Applied Soft Computing, vol. 24, pp. 40–49.

Mahmoudi, N and Duman, E. (2015) Detecting credit card fraud by modified Fisher discriminant analysis, Expert Systems with Applications, vol. 42, no. 5, pp. 2510–2516.

Olszewski, D. (2014) Fraud detection using self-organizing map visualizing the user profiles. Knowledge-Based Systems, vol. 70, pp. 324–334.

Powers, M. W. (2011) Evaluation: From Precision, Recall and F-Measure to ROC, Informedness, Markedness & Correlation, Journal of Machine Learning Technologies, vol. 2, no. 1, pp. 37–63.

Randhawa, K., Loo, C. K., Seera, M., Lim, C. P and Nandi, A. K. (2017). Credit card fraud detection using AdaBoost and majority voting. IEEE Access. DOI 10.1109/ACCESS.2018.2806420,IEEE.

Pumsirirat, A and Yan, L. (2018). Credit Card Fraud Detection using Deep Learning based on Auto-Encoder and Restricted Boltzmann Machine. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 9, No. 1, pp. 18-25.