iJET EXPLORE International Journal of Engineering & Technology
CENTRE OF PROFESSIONAL RESEARCH PUBLICATIONS
ISSN 2049-3444

International Journal of Engineering and Technology Volume 2 No. 7, July, 2012

Investigating the Effects of Threshold in Credit Card Fraud Detection System

Alese B. K[1]., Adewale O. S[1]., Aderounmu G. A[2]., Ismaila W.O. [3], Omidiora E. O. [3]
[1]Federal University of Technology, Akure., [2]Obafemi Awolowo University, Ile-Ife.
[3]Ladoke Akintola University of Technology, Ogbomoso

ABSTRACT

In e-commerce, credit card fraud is an evolving problem. The growing number of credit card transactions provides more opportunity for thieves to steal credit card numbers and subsequently commit fraud. Credit card fraud can be perpetrated through stolen cards, counterfeit card and stolen card details. The defensive measure issuing bank can take to overcome this liability is by introducing fraud detection systems (FDSs) in their database. Although different methods have been implemented to detect fraud but application of probability and selection of threshold value add an extra advantage for FDS to detect anomalies in on-line transactions. Therefore this paper implements another method of selecting threshold values (dynamic/adaptive) based on individual cardholder spending profile. In order to increase the confidence of the threshold values the results are verified using performance metrics. The two methods were compared and the results showed that adaptive method is suitable for detecting fraud in credit card transactions.

Keywords: *e-commerce, fraud detection system, credit card transactions, adaptive method, performance metrics*

1. INTRODUCTION

Fraud is a big business. Calls, credit card numbers, and stolen accounts can be sold on the street for substantial profit. Some of the various kinds of frauds identified are; Computer Fraud, Insurance Fraud, Money Laundering; Medical fraud, Telecommunication Fraud and Credit Card Fraud. Credit card fraud is the act of making a purchase using someone else's credit card information. In e-commerce, credit card fraud is an evolving problem. The growing number of credit card transactions provides more opportunity for thieves to steal credit card numbers and subsequently commit fraud. This can be perpetrated by individuals, merchants and also lack of security that can lead to the compromise of credit card numbers stored in online databases (computer intrusion). Despite significant efforts by merchants, card issuers and law enforcement to curb fraud, online fraud continues to plague electronic commerce web sites.

From the work of view for preventing credit card fraud, more research works were carried out with special emphasis on data mining and neural networks. For more information see Sam and Karl (2002) Kim and Kim (2002) Dipti, et al. (2010) and Qibei and Chunhua (2011). However, It has been stated as a fact by Sung et al (2009) that thresholding should be opted for two-class segmentation problems due to their simplicity. Early fraud detection algorithms often used thresholds to classify a task as legal/fraud. Threshold-based algorithms model group behavior based on a small number of control parameters (thresholds) that affect whether or not a particular task will be executed by a given swarm member based solely upon the intensity of the stimulus presented in comparison to the threshold currently assigned to the individual in question. There are two main classes of thresholds that have been applied in fraud detection viz; (i) Global/Fixed threshold, Albinav et al. (2008) developed a credit card fraud detection system using hidden Markov model and Fixed threshold to detect fraud; (ii) Dynamic/Adaptive threshold, in which the estimated thresholds are applicable to one or a group. Rupesh et al. (2007) developed a rule-based approach to detect anomalous telephone calls. This paper investigates the effect of adaptive threshold in detecting fraud in credit cards transactions.

The rest of this paper, we will discuss the motivation of this research and the analysis and performance of threshold in section 2. Section 3 will concentrate on methodology and techniques used in producing the threshold values in credit card transactions and section 4 discuss the implementation and result of the research. Finally section 5give the conclusion of this research.

1.1 Motivation

Selecting threshold value is necessary to help the fraud detection to make a good decision in identifying the anomaly. It is difficult to select the suitable threshold

value for differentiating between normal activity and abnormal activity in on-line transaction. Selecting inaccurate threshold value will cause an excessive false alarm especially if the value is too low or if it is too high, it can cause the anomaly activity being considered as normal transaction. Therefore selecting an appropriated threshold is important to detect the fraud activity.

Albinav et al. (2008) developed a credit card fraud detection system using hidden Markov model and Viterbi algorithm as predictive model. The estimated probability of old and new transactions from Viterbi algorithm were used to derive the probability of acceptance of the new transactions. And hence, various thresholds were used to test whether the new transactions are fraud or legal and the threshold that gave minimum false alarm was selected as base threshold. However, an important drawback is that this method treats cardholders identically; and more so, if threshold is set so that it finds fraud for a small business line, then a large business is likely to trip the threshold routinely.

1.2 Threshold Analysis and Performance

Threshold methods can be classified into five viz: (i) Basic/Fixed thresholding in which a particular threshold is selected as baseline for all the instances. When using basic threshold, a threshold value has to be selected somehow and usually manually; (ii) Band thresholding is similar to basic thresholding, but has two threshold values, which are set to maximum value and minimum value; (iii) Percentile is a method for choosing the threshold value to input to the "basic thresholding" algorithm. The threshold is chosen to be the intensity value where the cumulative sum of object intensities is closest to the percentile; (iv) Optimal thresholding selects a threshold value that is statistically optimal, based on the contents of the object; and (v) Dynamic/Adaptive threshold, in which the estimated thresholds are applicable to one or a group (the threshold adapts). See Per (2004) Artem and Roland (2003) for more information.

There have been a number of survey papers on measuring the performance of threshold like in Sung etal (2009) Mehmet and Bulent (2004) Sieracki et al (1989) and Abak et al (1997). However, in this work, four performance criteria will be used to provide evidence that shows differing performance features of fixed and adaptive thresholding methods: true positive rate, false positive rate, accuracy and precision. It is common to call true positives *hits*, false positive *false alarms*, and precision s*pecificity*. The *Specificity* indicates the degree of misclassification of non-fraudulent events. If a test shows high a false positive value, the specificity becomes poor. *True positive rate (or fraud catching rate)* is the fraction of fraudulent transactions that are correctly identified as fraudulent. False Positive rate (or *false alarm rate)* is the fraction of legitimate transactions that are incorrectly identified as fraudulent.

2. METHOD

In this work, the detection of fraud in credit card on-line transaction is used for experimentation. The process takes several steps which include; accumulation and clustering of data; mapping of data into hidden Markov model; training of data with HMM algorithms in two forms (i) non-optimized (forward-backward) and (ii) optimized (Baum-Welsh); prediction of hidden states in (i) non-optimized (Viterbi) and (ii) optimized (posterior-Viterbi); estimation of acceptance probabilities (Φ_{old}); new transactions are introduced and the processes are repeated and new acceptance probabilities are estimated (Φ_{new}); a global/fixed threshold (0.5) for all cardholders; and a model is being derived from estimated acceptance probability for each cardholder as follows:

Let the quantity $\Delta\Phi = /\Phi_{old} - \Phi_{new}/$. If $\Delta\Phi \leq 0$, it means that the new sequence is accepted (although it could be a fraud). The newly added transaction is determined to be fraudulent if the acceptance probability is above a computed threshold.

$$threshold = {(\Delta\Phi / \Phi_{new} + 0.5)} / 2$$

3. DISCUSSION OF RESULTS

In this paper, four different profiles are considered. The profiles considered are (55 35 10), (70 20 10), (95 3 2) and (34 33 33). Here, (*a*, *b*, *c*) represents a *l*s profile cardholder who has been found to carry out *a* percent of his transactions in the low, *b* percent in medium, and *c* percent in the high range. A simulated data of 16000 is used for training with HMM and the performance metrics used are true positive rate, false positive rate, accuracy and precision. The parameter settings of Abinav et al (2008) were employed. Different types of cardholder profiles were tested with four different schemes namely; optimized parameters with dynamic thresholds (Dyn_Opt_), non-optimized parameters with dynamic thresholds (Dyn_No_Opt_), optimized parameters with fixed threshold (Fix_Opt_), and non-optimized parameters with fixed threshold (Fix_No_Opt_). From figure 1, it can be seen that at (95 3 2) cardholder profile, Dyn_Opt_tp produced the highest true positive (tp) value of about 78%, followed by Dyn_No_Opt_tp with about 76%, Fix_Opt_tp produced about 59% while Fix_No_Opt_tp produced the least of about 52%. Also the same happened at (70 20 10) profile, with Dyn_Opt_tp produced the highest value, followed by Dyn_No_Opt_tp and closely by Fix_Opt_tp and Fix_No_Opt_tp produced the least value. But at (55 35 10) profile, the values

produced were low by all schemes and Dyn_Opt_tp and Dyn_No_Opt_tp produced the same values (about 42%) and so are the values produced by Fix_Opt_tp and Fix_No_Opt_tp of about 18% each.

Figure 2 depicts that the false-positive (fp) performances of the four profiles against four different schemes. 95 3 2 profile produced the relatively lowest false-positive values which are about 2.0% produced by Dyn_Opt_fp scheme, 4.1% produced by Fix_Opt_fp, 4.2% produced by Dyn_No_Opt_fp and about 4.3% produced by Fix_No_Opt_fp. The worst and highest false-positive values were produced at 34 33 33 profiles with about 18% produced by Fix_No_Opt_fp, about 11.6% produced by Fix_Opt_fp and Dyn_No_Opt_fp, and Dyn_Opt_fp produced about 10%.

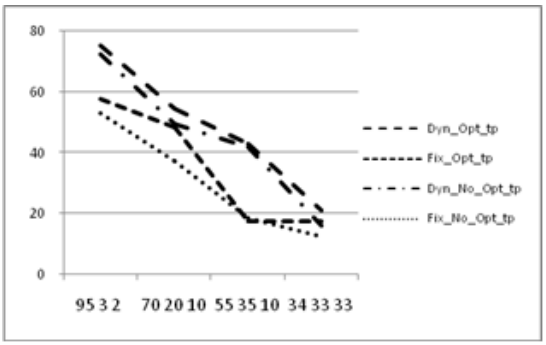

Figure 1: Graph of True-Positive averaged over all the 15 sequence lengths for different cardholder profiles when parameters are optimized and non-optimized with dynamic and fixed Thresholds

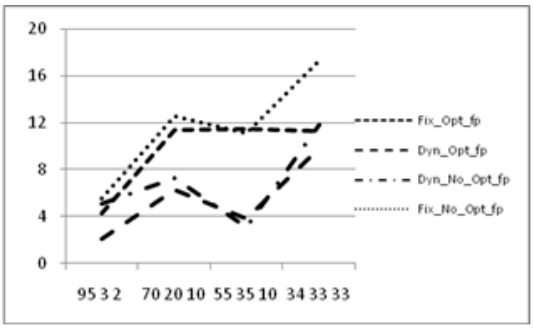

Figure 2: Graph of False-Positive averaged over all the 15 sequence lengths for different cardholder profiles when parameters are optimized and non-optimized with dynamic and fixed Thresholds

In figure 3, 95 3 2 profile produced the highest precision (pre) values across all the schemes with Dyn_Opt_pre producing about 97%, Dyn_No_Opt_pre and Fix_No_Opt_pre producing about 94%, while Fix_Opt_pre producing about 91%. At 70 20 10 profile, Dyn_Opt_pre produced about 93%, Dyn_No_Opt_pre produced about 90% , while Fix_Opt_pre scheme produced (about 84%) a higher precision than Fix_No_Opt_pre (about 78%). However, at 55 35 10 profile, Dyn_Opt_pre produced about 94%, Dyn_No_Opt_pre produced about 86%, while Fix_No_Opt_pre scheme produced (about 64%) a higher precision than Fix_Opt_pre (about 62%). But at 34 33 33 profile, Dyn_Opt_pre produced about 70%, Dyn_No_Opt_pre produced about 58% , while Fix_Opt_pre scheme produced (about 62%) a higher precision than Fix_No_Opt_pre (about 43%).

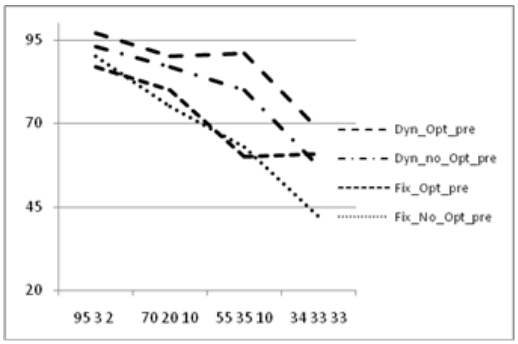

Figure 3: Graph of Precision averaged over all the 15 sequence lengths for different cardholder profiles when parameters are optimized and non-optimized with dynamic and fixed Thresholds

Also figure 4 shows the graphs of accuracy (acc) of the four profiles. At 95 3 2 profile, Dyn_Opt_acc produced about 88%, Dyn_No_Opt_acc produced about 83%, Fix_Opt_acc producing about 82%, while Fix_No_Opt_acc producing about 78%. At 70 20 10 profile, Dyn_Opt_acc produced about 82%, Dyn_No_Opt_acc produced about 74%, Fix_Opt_acc scheme produced about 84% (higher precision than Dyn_Opt_acc), and Fix_No_Opt_acc produced about 68%). However, at 55 35 10 profile, Dyn_Opt_acc produced about 84%, Dyn_No_Opt_acc produced about 72%, while Fix_No_Opt_acc and Fix_Opt_acc produced about 80% respectively. At 34 33 33 profile, Dyn_Opt_acc produced about 86%, Dyn_No_Opt_acc produced about 78% , while Fix_Opt_acc scheme produced about 80% and Fix_No_Opt_acc produced about 70%.

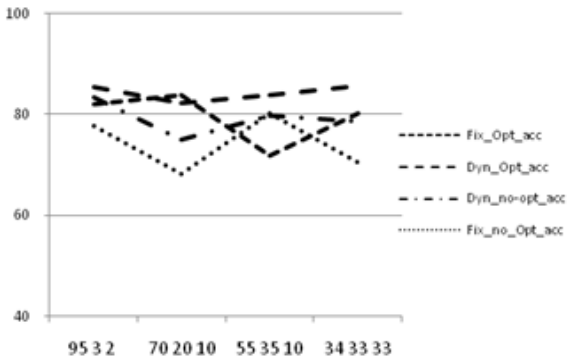

Figure 4: Graph of Accuracy averaged over all the 15 sequence lengths for different cardholder profiles when

parameters are optimized and non-optimized with dynamic and fixed Thresholds

4. CONCLUSION

In this paper, we introduced a new approach in detecting fraud in credit card transactions using adaptive threshold value. The threshold value is obtained using the average of initial threshold (0.5) and ratio of acceptance probabilities of old and new transactions estimated from HMM algorithms. The performance of the system was tested with different cardholder profiles cum non-optimization and optimization of HMM parameters using some selected performance metrics. Thus the adaptive thresholds gave a better performance than fixed threshold.

REFERENCES

[1] Abak, T., Baris¸ U., and Sankur, B. (1997). ‘‘The performance of thresholding algorithms for optical character recognition,’’ Intl. Conf. Document Anal. Recog. ICDAR’97, pp. 697–700.

[2] Abhinav S., Amlan K., Shamik S. and Arun K. (2008). Credit Card Fraud Detection Using Hidden Markov Model, IEEE Transactions on Dependable and Secure Computing, vol. 5, no.1, 37-48.

[3] Artem L. Ponomarev and Ronald L. Davis (2003): An adjustable-threshold algorithm for the identification of objects in three-dimensional images, Bioinformatics 19(11) Oxford University. Vol. 19 no. 11 2003, pages 1431–1435.

[4] **Bec**ker R**.** A., Volinsky C, and Wilks A. (2010). Fraud Detection in Telecommunications: History and Lessons Learned, TECHNOMETRICS, Vol. 52, no. 1.

[5] Dipti D.P., Sunita M.K., Vijay M.W., Gokhale J. A., Prasad S. H. (2010), Efficient Scalable Multi-Level Classification Scheme for Credit Card Fraud Detection, International Journal of Computer Science and Network Security, Vol.10, No.8.

[6] Faizal M. A., Mohd Zaki M., Shahrin S., Robiah Y, Siti Rahayu S., Nazrulazhar B. (2009) Threshold Verification Technique for Network Intrusion Detection System *International Journal of Computer Science and Information Security, Vol. 2, No.1.*

[7] Kim M.J. and Kim T.S., (2002)“A Neural Classifier with Fraud Density Map for Effective Credit Card Fraud Detection,” Proc. International Conference on Intelligent Data Engineering and Automated Learning, Lecture Notes in Computer Science, Springer Verlag, no. 2412, pp. 378383.

[8] Moysan J., Corneloup G., and Sollier T., (1999). ‘‘Adapting an ultrasonic image threshold method to eddy current images and defining a validation domain of the thresholding method,’’ NDT & E Intl. 32, 79–84.

[9] Mehmet Sezgin, Bulent Sankur (2004): Survey over image thresholding techniques and quantitative performance evaluation Journal of Electronic Imaging. Vol. 13(1), 165

[10] Per C. H. (2004): Exercise in Computer Vision: A Comparison of Thresholding Methods. http://www.ifi.uio.no/forskning/grupper/dsb/Programvare/Xite/

[11] Rupesh K. G., and Saroj K. M. (2007). A Rule-based Approach for Anomaly Detection in Subscriber Usage Pattern,World Academy of Science, Engineering and Technology 34.

[12] Qibei Lu, and Chunhua Ju (2011). Research on Credit Card Fraud Detection Model Based on Class Weighted Support Vector Machine Journal of Convergence Information Technology, Vol.6, Number 1. pp. 62-68.

[13] Sokbae Lee, Myung Hwan Seo, and Youngki Shin. Testing for Threshold Effects in Regression Models. The Institute for Fiscal Studies Department of Economics, UCL cemmap working paper CWP36/10

[14] Sung S., Mohamed-Slim A., Hong-Chuan Y., Seniand K., (2009): Performance Evaluation of Threshold-Based Power Allocation Algorithms for Down-Link Switched-based Parallel Scheduling, IEEE Transactions on Wireless Communications, Vol. 8, No. 4.

[15] Sam M., Karl T., Bram V., Bernard M.. (2002) Credit Card Fraud Detection Using Bayesian and Neural Networks First International NAISO Congress on Neuro Fuzzy Technologies, Havana..

[16] Sieracki, M. E., Reichenbach S. E. and Webb K. L. (1989). ‘‘Evaluation of automated threshold selection methods for accurately sizing microscopic fluorescent cells by image analysis,’’ Appl. Environ. Microbiol. 55, 2762–2772.

[17] Venkatesh S. and Rosin P. L., (1995). ‘‘Dynamic threshold determination by local and global edge evaluation,’’ CVGIP: Graph. Models Image Process. 57, 146–160.