Journal of Engineering Sciences
Vol 10, Issue 9, Sept /2019
ISSN NO:0377-9254

AN ANOMALY BASED FINANCIAL FRAUD AND FEATURE DETECTION

Manohar Gosul[1], L. Prasanna Laxmi[2]

[1]Assistant Professor, Department of CSE, Bharat Institute of Engineering and Technology, Hyderabad, Telangana, India, manohargosul5@gmail.com

[2]M.TECH Student, Department of CSE, Bharat Institute of Engineering and Technology, Hyderabad, Telangana, India likkiprasanna253@gmail.com

ABSTRACT: Monetary scams, such as money laundering, is understood to be a major procedure of crime that makes illegitimately gotten funds most likely to terrorism or various other criminal task. This kind of unlawful activities include complicated networks of trade and also financial transactions, that make it hard to identify the scams entities and also uncover the functions of scams. Luckily, trading/transaction network as well as attributes of entities in the network can be built from the complex networks of profession as well as financial purchases. Trading/transaction network discloses the communication between entities and therefore anomaly discovery on trading networks can reveal the entities involved in the scams activity; while attributes of entities are the summary of entities as well as anomaly discovery on functions can reflect information of the scams tasks. Thus, network and also attributes provide corresponding details for fraud discovery, which has possible to improve fraud detection efficiency. Nevertheless, the majority of existing approaches concentrate on networks or features information separately, which doesn't make use of both info. In this paper, we propose an unique fraud detection structure, CoDetect, which can leverage both network information and also function details for monetary fraud detection. On top of that, CoDetect can all at once detecting monetary scams tasks as well as the feature patterns related to the scams activities. Comprehensive experiments on both synthetic data as well as real life information show the performance as well as the efficiency of the suggested framework in combating economic scams, specifically for loan laundering.

Key words: - Anomaly feature detection, Co Detect, financial fraud.

I. INTRODUCTION

Nowadays the modes of payment methods are changed into online transactions. Banking system provides different type of payments like e-cash, card payments, internet banking, and e-services for improving online transaction. Credit card is one of the most custom ways of the online transaction. Credit cards are used for purchasing goods and services using online transaction and physical card for the offline transaction. In credit card based purchase, the cardholder presents his card to a merchant for making payment. To make fraud in this kind of acquisitions, the person doing fraud has to steal the credit card. If the legitimate user does not understand the loss of card, it can lead to important financial loss to the credit card company and also to the user. Credit card is a medium of selling goods or services without having cash in hand. With more

number of such money less transaction, a number of fraudulent transactions also increasing? During the online transaction, we do not need any physical card; we need only card number, cvv number, and expiry date so there are more chances of fraud will be happen. In this method of fraud detection, we generate fraud behavior on the basis of cardholder's transaction habits. Most of the credit card fraud detection methods based on anomaly detection try to extract the historical behavior patterns as rules and compute the similarity between an incoming transaction and these behavior patterns. The main idea of this kind of approach is that people may have personalized transaction habits that depend on their different accounts, different income sources, and different motivations and so on. Banking system provides different type of payments like e-cash, card payments, internet banking, and eservices for improving online transaction. Credit card is one of the most custom ways of online transaction. Credit card is medium of selling goods or services without having cash in hand. With increased number of such cashless transaction, number of fraudulent transactions also increasing. During the online transaction we do not need any physical card, we need only card number, cvv, and expiry date so there is more chances of fraud should be happen. In this method of fraud detection we generate behavior certificate on the basis of cardholder's transaction habits. Most of the credit card fraud detection methods based on anomaly detection try to extract the historical behavior patterns as rules and compute the similarity between an incoming transaction and these behavior patterns. The main idea of this kind of approach is that people may have personalized transaction habits that depend on their different accounts, different income sources, and different motivations and so on.

II. RELATED WORK

Financial fraud detection concerns about the detection of fraud in insurance, credit card, telecommunications and other financial crime activities such as money laundering. Statistical models have been used for detection of financial fraud. Bahnsen et al. improve the detection performance by calibrating probabilities before establishing Bayes model. HMM model is used to model the customers' credit card shopping patterns for detection of credit card fraud. The shopping items indicate the hidden state and the corresponding prices from certain ranges are the observation. LR(Logistic Regression), Support Vector Machines(SVMs) and Random Forest(RF) are evaluated for credit card detection. The detection models are built on primary features and derived features from transaction. Whit row et al. proposed a new pre-processing strategy for better fraud detection with SVMs and KNN classification. Transactions aggregated in term of time window, and then data with new features is used to model the pattern. Wei et al. addressed the problem of unbalanced financial data and employed cost sensitive neural network to punish the misclassification of fraud transaction.

John Richard D. Kho , Larry A. Vea this paper is suggesting that a detection model must be available to capture the possible anomalous transactions – a fallback in case the technology will fail. Several classifiers were evaluated during the model creation however only the Random Tree and J48 yielded the highest accuracy value. Dhiya Al-Jumeily, Abir Hussain states the types of fraud and current techniques which are being used to avoid fraudulent activities.This techniques supports the development

of Fraud Detection System. Balasupramanian.N, Imad Salim Al-Barwani suggests the big data analytics techniques to detect and prevent online fraudulent cases.This paper proposes a system in which data is collected cleaned & features are extracted.Using these pattern it can prevent the online fraud before it happens. Kadek Dwi Febriyanti, Riyanarto Sarno, Yutika Amelia Effend belives some fraud occured due to variations in buisness processes.So this can be detected by applying association rule learning approach.This proposes an idea to present solution for detection of fradulent activity by learning the historical data. Dongxu Huang, Dejun Mu, Libin Yang proposes a fraud detection system names as CoDetect which can uses both network and feature information for financial fraud detection. It can detect financial fraud activities and feature patterns associated with it.

III. PROPOSED MODEL

Random Tree is the supervised classifier Random Tree is use to construct the random set of data for constructing decision tree. Random Tree algorithm deals with classification and regression problems. Random Tree is the group of tree predicators that called as forest. In Random Tree, classifier get input feature vector and classify it with every tree in forest and output of class label received majority votes. In regression, the classifier reply average of responses over tree in forest. Random Tree is the combination of two algorithms from machine learning. Single Model Tree combines with Random Tree to improve the functioning of Random Tree. Single Model Tree is the decision tree in which leaf node hold linear model. Random Tree improves the performance of decision tree. Random Tree is reasonably balance tree. In this Random Tree one global setting works across the all leaves and thus simplifying optimization procedure. This feature of Random Tree reduces the time and efforts. Random Tree produces slightly better classification accuracy than Random Forest. Random Tree yielded the highest accuracy value of 94.32%.

Fig.3.1. Home page.

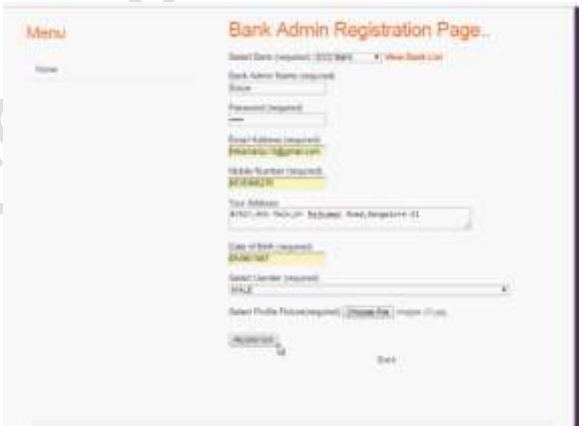

Fig.3.2. Bank representation.

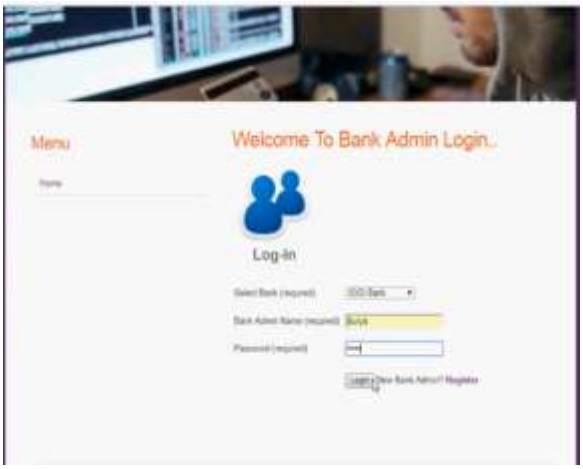

Fig.3.3. Admin menu.

Fig.3.4. Output page.

Here the new proposed scheme called Financial Fraud Detection with Anomaly Feature Detection on credit card is introduced. In this paper, we would like to develop a novel framework for fraud detection by considering the special detecting and tracing demanding of fraud entities and behaviors. Specifically, we investigate: (1) how to utilize both graph matrix and feature matrix for fraud detection and fraud tracing; (2) how to mathematically model both graph matrix and feature matrix so as to simultaneously achieve the tasks of fraud detection and tracing. In an attempt to solve these challenges, we proposed a novel detection framework Co Detect, as Fig. 1 shown, for financial data, especially for money laundering data. We incorporate fraud entities detection and anomaly feature detection in the same framework to find fraud patterns and corresponding features simultaneously.

IV CONCLUSION

We propose a new framework, Co Detect, which can perform fraud detection on graph-based similarity matrix and feature matrix simultaneously. It introduces a new way to reveal the nature of financial activities from fraud patterns to suspicious property. Furthermore, the framework provides a more interpretable way to identify the fraud on sparse matrix. Experimental results on synthetic and real world data sets show that the proposed framework (Co Detect) can effectively detect the fraud patterns as well as suspicious features. With this codetection framework, executives in financial supervision can not only detect the fraud patterns but also trace the original of fraud with suspicious feature.

V. REFERENCES

[1] C. Sullivan and E. Smith. ‘‘Trade-Based Money Laundering: Risks and Regulatory Responses,’’ Social Sci. Electron. Publishing, 2012, p. 6.

[2] United Press International. (May 2009). Trade-Based Money Laundering Flourishing. [Online]. Available: lourishing/UPI17331242061466.

[3] L. Akoglu, M. McGlohon, and C. Faloutsos, ‘‘OddBall: Spotting anomalies in weighted graphs,’’ in Proc. Pacific-Asia Conf. Knowl. Discovery Data Mining, 2010, pp. 410–421.

[4] V. Chandola, A. Banerjee, and V. Kumar, ‘‘Anomaly detection: A survey,’’ ACM Comput. Surv., vol. 41, no. 3, 2009, Art. no. 15.

[5] W. Eberle and L. Holder, ‘‘Mining for structural anomalies in graph-based data,’’ in Proc. DMin, 2007, pp. 376–389.

[6] C. C. Noble and D. J. Cook, ‘‘Graph-based anomaly detection,’’ in Proc. 9th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, 2003, pp. 631–636.

[7] H. Tong and C.-Y. Lin, ‘‘Non-negative residual matrix factorization with application to graph anomaly detection,’’ in Proc. SIAM Int. Conf. Data Mining, 2011, pp. 1–11.

[8] S. Wang, J. Tang, and H. Liu, ‘‘Embedded unsupervised feature selection,’’ in Proc. 29th AAAI Conf. Artif. Intell., 2015, pp. 470–476.

[9] Z. Lin, M. Chen, and Y. Ma. (2010). ‘‘The Augmented lagrange multiplier method for exact recovery of corrupted low-rank matrices.’’ [Online]. Available: https://arxiv.org/abs/1009.5055.

[10] J. Sun, H. Qu, D. Chakrabarti, and C. Faloutsos, ‘‘Neighborhood formation and anomaly detection in bipartite graphs,’’ in Proc. 15th IEEE Int. Conf. Data Mining, Nov. 2005, p. 8.